Data Security Manager Help
Websense® TRITON® AP-DATA Gateway and Discover

v8.0.x
# Contents

## Part 1: Getting Started

### Chapter 1  
Overview .................................................. 1
- TRITON AP-DATA basics  .................................. 2
- TRITON AP-DATA protector  .............................. 2
- TRITON AP-DATA databases  ............................. 3
- What can I protect? ....................................... 3
- Data classification ....................................... 5
- Managing TRITON AP-DATA  .............................. 6
- TRITON AP-WEB mode  .................................... 6
- TRITON AP-EMAIL mode  .................................. 7

### Chapter 2  
Navigating the System ..................................... 9
- TRITON AP-DATA’s navigation and content panes ....... 9
  - Main tab .................................................. 11
  - Settings tab .............................................. 12
- Today page ............................................... 13
- Deploy button ............................................. 13
- Icons ....................................................... 15
- Breadcrumbs ............................................... 19
- Check boxes ............................................... 20
- Pagination .................................................. 20

### Chapter 3  
Initial Setup .................................................. 23
- Entering your subscription key  ......................... 24
- Defining general system settings  ...................... 25
  - Configuring user directory server settings  ......... 25
  - Setting up alerts ....................................... 27
- Setting up notifications .................................. 28
- Configuring system modules  ......................... 30
  - Configuring the protector ................................ 31
- Deploying your settings ................................ 34
## Part 2: Securing Your Company’s Data

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Policies Overview</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 4</td>
<td>Policies Overview</td>
<td>37</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Configuring the Email Data Loss Prevention Policy</td>
<td>53</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Configuring the Web Data Loss Prevention Policy</td>
<td>61</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Configuring the Mobile Data Loss Prevention Policy</td>
<td>69</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Using Predefined Policies</td>
<td>75</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Creating Custom DLP Policies</td>
<td>79</td>
</tr>
</tbody>
</table>

### Chapter 4
- What’s in a policy? 39
- Viewing policies 40
- Editing a policy 43
- Update rules of current policy 43
- Update exceptions of current rule 44
- Update rules of multiple policies 45
- Update exceptions of multiple rules 46
- Delete policies 47
- Policy levels 47
- Selecting items to include or exclude in a policy 49

### Chapter 5
- Configuring outbound and inbound attributes 55
- Defining policy owners 59
- Identifying trusted domains 59

### Chapter 6
- Configuring Web attributes 62
- Selecting Web destinations 66
- Defining policy owners 68

### Chapter 7
- Configuring attributes 70
- Defining policy owners 73

### Chapter 8
- Adding a predefined policy 75
- Welcome 75
- Regions 76
- Industries 76
- Finish 76
- Policy list 76
- Changing the policies you selected 77
- Changing your industry or region 77

### Chapter 9
- Custom Policy Wizard - General 80
- Custom Policy Wizard - Condition 80
- Viewing or editing conditions and thresholds 83
- Custom Policy Wizard - Severity & Action 85
- Custom Policy Wizard - Source 88
- Custom Policy Wizard - Destination 88
Performing Outlook PST discovery ........................................217
Performing endpoint discovery ........................................218
Mapping FCI rules to discovery policies ............................219
Viewing discovery status ..............................................219
Viewing discovery results ............................................220
Updating discovery ......................................................220
Configuring discovery incidents .....................................220
Copying or moving discovered files .................................221
Preparing and running the remediation scripts .................222

Chapter 13  
Scheduling Discovery Tasks ........................................225
Scheduling network discovery tasks .................................229
File System tasks .......................................................230
SharePoint tasks .......................................................235
Box Cloud tasks .......................................................239
Database tasks .........................................................244
Exchange tasks .........................................................249
Outlook PST tasks .....................................................254
Domino tasks ........................................................258
Scheduling endpoint discovery tasks ..............................265
Configuring FCI tasks ................................................268
Mapping FCI rules .....................................................268

Chapter 14  
Viewing Incidents and Reports ......................................271
The report catalog .......................................................272
Editing a report ........................................................274
Scheduling tasks .......................................................297
Viewing the incident list .............................................300
Previewing incidents ................................................304
Managing incident workflow .......................................307
Remediating incidents ..............................................313
Escalating incidents ................................................315
Managing incident reports ........................................317
Tuning policies .........................................................322
Data Loss Prevention reports .....................................324
DLP dashboard ........................................................326
Top violated policies .................................................327
User risk summary (all incidents) ................................327
User risk summary (data theft risk indicators) ...............327
Violations by severity and action .................................328
Top sources and destinations ....................................328
Incident trends ........................................................329
Incident status .........................................................329
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Configuring Authorization</td>
<td>393</td>
</tr>
<tr>
<td></td>
<td>Defining administrators</td>
<td>393</td>
</tr>
<tr>
<td></td>
<td>Viewing administrators</td>
<td>395</td>
</tr>
<tr>
<td></td>
<td>Editing administrators</td>
<td>396</td>
</tr>
<tr>
<td></td>
<td>Working with roles</td>
<td>398</td>
</tr>
<tr>
<td></td>
<td>Adding a new role</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td>Configuring personal settings</td>
<td>403</td>
</tr>
<tr>
<td>18</td>
<td>Archiving Incidents</td>
<td>405</td>
</tr>
<tr>
<td></td>
<td>Remote SQL Server machines</td>
<td>407</td>
</tr>
<tr>
<td></td>
<td>Archiving a partition</td>
<td>408</td>
</tr>
<tr>
<td></td>
<td>Restoring a partition</td>
<td>409</td>
</tr>
<tr>
<td></td>
<td>Deleting a partition</td>
<td>409</td>
</tr>
<tr>
<td></td>
<td>Archive threshold</td>
<td>410</td>
</tr>
<tr>
<td>19</td>
<td>Updating Predefined Policies and Classifiers</td>
<td>411</td>
</tr>
<tr>
<td></td>
<td>Viewing your update history</td>
<td>411</td>
</tr>
<tr>
<td></td>
<td>Installing policy updates</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>Restoring policies to a previous version</td>
<td>414</td>
</tr>
<tr>
<td></td>
<td>Determining the policy version you have</td>
<td>415</td>
</tr>
<tr>
<td>20</td>
<td>Managing System Modules</td>
<td>417</td>
</tr>
<tr>
<td></td>
<td>Adding modules</td>
<td>419</td>
</tr>
<tr>
<td></td>
<td>Configuring modules</td>
<td>419</td>
</tr>
<tr>
<td></td>
<td>Configuring the management server</td>
<td>420</td>
</tr>
<tr>
<td></td>
<td>Configuring a supplemental TRITON AP-DATA Server</td>
<td>421</td>
</tr>
<tr>
<td></td>
<td>Configuring the fingerprint repository</td>
<td>422</td>
</tr>
<tr>
<td></td>
<td>Configuring the endpoint server</td>
<td>424</td>
</tr>
<tr>
<td></td>
<td>Configuring the crawler</td>
<td>425</td>
</tr>
<tr>
<td></td>
<td>Configuring the forensics repository</td>
<td>425</td>
</tr>
<tr>
<td></td>
<td>Configuring the policy engine</td>
<td>426</td>
</tr>
<tr>
<td></td>
<td>Configuring the optical character recognition (OCR) server</td>
<td>427</td>
</tr>
<tr>
<td></td>
<td>Configuring the protector</td>
<td>431</td>
</tr>
</tbody>
</table>
Contents

Configuring ICAP .................................................. 437
Configuring the Web Content Gateway module .................. 439
Configuring the TRITON AP-EMAIL module ....................... 441
Configuring the TMG agent ........................................ 442
Configuring the integration agent .................................. 443
Configuring the mobile agent ....................................... 444
Configuring the Microsoft FCI agent .............................. 448
Configuring protector services ...................................... 449
Configuring SMTP .................................................. 449
Configuring HTTP .................................................. 455
Configuring FTP .................................................... 457
Configuring chat .................................................... 459
Configuring plain text .............................................. 460
Balancing the load .................................................. 462
Defining load balancing distribution ................................. 463

Chapter 21 Configuring Endpoint Deployment .................. 465
Viewing and managing endpoint profiles ......................... 467
Configuring encryption for removable media .................... 467
Adding an endpoint profile ........................................ 468
  General tab ..................................................... 469
  Servers tab ..................................................... 470
  Properties tab .................................................. 471
  Encryption tab .................................................. 472
Rearranging endpoint profiles ...................................... 475
Deploying endpoint profiles ....................................... 475
Backing up encryption keys ........................................ 476
Restoring encryption keys .......................................... 476
Configuring endpoint settings ...................................... 477
Monitoring endpoint removable media .............................. 478
Selecting endpoint destination channels to monitor .............. 479
Bypassing endpoint clients ........................................ 482
Updating the endpoint client ....................................... 483
Using the endpoint client software .................................. 484

Chapter 22 Troubleshooting ........................................ 485
Problems and Solutions ............................................. 485
  Discovery ....................................................... 486
  Endpoint ....................................................... 486
  Fingerprinting ................................................. 488
  Incidents ....................................................... 490
  Miscellaneous ................................................... 491
  Performance ..................................................... 492
Part 4: Appendices

Appendix A  How Do I ......................................................... 499
  Archive my incident data? ............................................ 499
  Configure a DLP policy? .............................................. 500
  Define an exception? .................................................. 501
  Filter incidents? ....................................................... 501
  Fingerprint data? ..................................................... 502
  Ignore sections of my document when fingerprinting? ........ 503
  Fingerprint specific field combinations in a database table?  504
  Mitigate false positives in pattern or dictionary phrases? .... 505
  Move from monitor to protect? ...................................... 505
  Perform discovery? ................................................... 506

Appendix B  Glossary ...................................................... 509

Appendix C  Copyrights .................................................. 517
  Trademarks ........................................................... 517
  Other Acknowledgments .............................................. 517

Index ........................................................................... 553
Part I

Getting Started
Overview

Websense® TRITON® AP-DATA Gateway protects organizations from information leaks and data loss both at the perimeter and inside the organization.

It can operate alone in the network, or data loss prevention (DLP) modules can be paired with TRITON AP-WEB or TRITON AP-EMAIL to provide a well-rounded security solution for your organization.

The Web DLP module prevents data loss over Web channels such as HTTP, HTTPS, and FTP.

The Email DLP module prevents data loss through email.

You can manage all 3 Websense solutions—web, data, and email—from a central location: the TRITON Manager.

If desired, you can prevent data loss over other channels—such as mobile devices, USB drives, or LANs—or you can use TRITON AP-DATA Discover to learn the location of sensitive data inside your network.

TRITON AP-DATA can utilize a variety of agents to intercept data on TMG and other servers. Endpoint software that is installed 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.

Speak to your Websense sales representative for more information about these DLP options.
TRITON AP-DATA basics

TRITON AP-DATA protects organizations from data loss by:

- 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 TRITON AP-DATA are:

- The TRITON management server
- The TRITON AP-DATA Policy Engine

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

There is a *policy engine* on all TRITON AP-DATA servers, TRITON AP-WEB proxies, and TRITON AP-EMAIL appliances. The policy engine is responsible for parsing your data and using analytics to compare it to the rules in your policies.

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

TRITON AP-DATA protector

If you have a TRITON AP-DATA Gateway subscription, you may also make use of the TRITON AP-DATA *protector*. 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 TRITON AP-DATA 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. Content analysis is performed by the on-box policy engine, so no sensitive data leaves the protector during this process.
TRITON AP-DATA databases

TRITON AP-DATA has 2 databases for incident and forensics data:

- The *incident database* contains information about policy breaches, such as what rule was matched, how many times, what were the violation triggers, what was the date, channel, source, ID, and more. It is stored in Microsoft SQL Server along with policy configuration data.

  When the incident database gets very large, it is partitioned so you can archive it onto different physical disks. You do this by navigating to **Settings > General > Archive** and using the options on the resulting screen.

- The *forensics repository* contains information about the transaction that resulted in the incident, such as the contents of an email body: From:, To:, Cc: fields; attachments, URL category, hostname, file name, and more.

  To configure the size and location of the forensics repository, navigate to **Settings > Deployment > System Modules** and click **Forensics Repository** on the management server.

Both incident data and forensics data are displayed in the **Incidents, Last n days** report.

What can I protect?

TRITON AP-DATA Gateway 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

TRITON AP-DATA Gateway secures:

Related topics:

- *Sources and destinations*, page 173
- *Classifying Content*, page 107
- *Defining Resources*, page 171
- *Remediation*, page 188
● **Network and endpoint email*** - You can monitor or prevent sensitive information from being emailed in or outside of your domain from both network and endpoint computers.

● **Mobile email** - You can define what content can and cannot be synchronized to mobile devices—such as phones and tablets—from network email systems. This protects data in case an employee’s mobile devices is lost or stolen.

● **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 website, blog, or forum via HTTP.
  - **Endpoint HTTP/HTTPS*** - You can monitor or protect endpoint devices such as laptops from posting data over the Web.

● **Endpoint applications*** - You can monitor or prevent sensitive data from being copied and pasted from one application to another on Windows 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.

TRITON AP-DATA supports DLP analysis, encryption, and blocking for USB drives; it supports DLP analysis and blocking for native Windows CD/DVD writers. (Third-party CD/DVD authoring tools are not supported.)

● **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 IP addresses, 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 to the corporate network).

Note that Endpoint LAN control is currently applicable to Microsoft sharing only.

● **Endpoint printing*** - You can monitor or prevent sensitive data from being printed on local or network printers from endpoint client machines. Requires TRITON AP-ENDPOINT software.

*Endpoint channels require a subscription to TRITON AP-ENDPOINT DLP.

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

There are several ways to classify your data using TRITON AP-DATA:

- **Pre-defined scripts, dictionaries, file-types, regular expression patterns, and key phrases** - TRITON AP-DATA includes classifiers out-of-the box so you can start classifying your data right away. RegEx patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789. File properties classifier let you classify data by file name, type or size.

- **Custom scripts, dictionaries, file-types, regular expression patterns, and key phrases for specific (described) data** - You can create your own custom classifiers for data that you describe.

- **Fingerprinting (registered) data** - 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 (databases) and unstructured (files and folders).

- **Machine learning** - In machine learning classifiers, you provide examples of the type of data that you want to protect and that you don’t want to protect, so the system can learn and identify sensitive data in traffic. These are called positive and negative training sets because the examples educate the system. Unlike fingerprinting, the files do not need to contain parts of the analyzed files but can look similar or be on a similar topic. The system learns and recognizes complex patterns and relationships and makes decisions on them without exact include/exclude criteria that are specified in fingerprinting classifiers. Machine learning can even protect new, zero-day documents in this way.

For more information on content classification methods, including which is most and least accurate, see *Classifying Content, page 107*. 

Related topics:

- *File fingerprinting, page 127*
- *Database fingerprinting, page 144*
- *Scripts, page 125*
- *Classifying Content, page 107*
Managing TRITON AP-DATA

The interface that you use to manage TRITON AP-DATA is called the TRITON Manager. TRITON has modules for web, email, 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 all 3 modules in the same location.

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

For more information on using the TRITON interface, see the TRITON Help system. Select TRITON Settings on the TRITON toolbar, then click Help > Help Contents.

TRITON AP-WEB mode

If you have TRITON AP-WEB and the Web DLP module, only content on web channels is analyzed, and you are not required to purchase a separate TRITON AP-DATA subscription or a protector appliance.

The web channels covered by TRITON AP-WEB include HTTP, HTTPS, FTP, and FTP-over-HTTP. This allows you to prevent posts to websites, blogs, and forums as well as FTP sites.

Note

If you have TRITON AP-WEB, you won’t see all the options that are presented in this Help documentation. If you require access to other options and channels that you see here, talk to your Websense account representative about purchasing a full TRITON AP-DATA subscription.
TRITON AP-EMAIL mode

If you have TRITON AP-EMAIL and the Email DLP module, data loss is prevented over email. You are not required to purchase a separate TRITON AP-DATA subscription, agent, or a protector appliance.

Note

If you have TRITON AP-EMAIL, you won’t see all the options that are presented in this Help documentation. If you require access to other options and channels that you see here, talk to your Websense account representative about purchasing a full TRITON AP-DATA subscription.
TRITON Manager navigation is described in the TRITON Help System. Select TRITON Settings on the TRITON toolbar, then click Help > Help Contents for more information.

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

- TRITON AP-DATA's navigation and content panes
- Today page
- Deploy button
- Icons
- Breadcrumbs
- Check boxes
- Pagination

**TRITON AP-DATA's navigation and content panes**

The left pane of the TRITON Manager 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.

The navigation pane is collapsible to enable larger working space and a wider display area for all TRITON pages. In the Data Security manager, this is especially useful for the Data Loss Prevention and 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.
Navigating the System

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

- 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 TRITON AP-WEB, 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 271
- *Creating Custom DLP Policies*, page 79
- *Creating Discovery Policies*, page 207
- *Scheduling Discovery Tasks*, page 225
- *Classifying Content*, page 107
- *Defining Resources*, page 171
- *Viewing Status and Logs*, page 339

**Reporting**

- **Data Loss Prevention**: View and manage data loss prevention 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.

- **Discovery***: View information about incidents that were discovered through discovery. Using this screen, you can assign, view, and monitor discovery incidents.

  *Not included with TRITON AP-WEB or TRITON AP-EMAIL.*

**Policy Management**

- **Data Loss Prevention (DLP) Policies**: Create or manage a network or endpoint policies. You can create policies from scratch or by using predefined policies.

- **Discovery Policies***: Create or manage discovery policies. You can create policies from scratch or by using a predefined regulatory template.
Navigating the System

- **Discovery Tasks**: Schedule discovery tasks.
- **Content Classifiers**: Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, scripts, a database 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).

  *Not included with TRITON AP-WEB or TRITON AP-EMAIL.*

**Status**

- **Today**: The Today page appears first when you first view the Data Security manager. 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 13*.

- **System Health**: This enables you to monitor TRITON AP-DATA performance. See *Monitoring system health, page 342*.

- **Endpoint Status**: On this page you can view a list of data endpoints that are registered with the TRITON management server, including information regarding an endpoint’s discovery, profile and policy, and the host’s system summary. See *Viewing endpoint status, page 346*.

- **Traffic Log**: This enables you to see details of the traffic being monitored by TRITON AP-DATA. See *Traffic log, page 348*.

- **System Log**: Here you can view a list of the events sent from system components, such as the TRITON AP-DATA servers, protectors, and policy engines. See *System log, page 349*.

- **Audit Log**: This page displays a list of actions that administrators have performed in the system. See *Audit log, page 349*.  

  * Not included with TRITON AP-WEB.

**Settings tab**

Related topics:

- *Configuring System Settings, page 357*
- *Configuring Authorization, page 393*
- *Archiving Incidents, page 405*
- *Managing System Modules, page 417*
- *Configuring Endpoint Deployment, page 465*
- *Main tab, page 11*
Navigating the System

General

- **System**: Configure basic system settings for incidents and forensics, user directories, mail gateways, Websense product integration, and more.
- **Authorization**: Set up and manage TRITON AP-DATA system administrators and assign roles.
- **Archive**: Archive partitions for incident storage.
- **Policy Updates**: Install updates to Websense predefined policies.

Deployment

- **System Modules**: Manage system components such as TRITON AP-DATA servers, fingerprint repositories, policy engines, and agents.
- **Endpoint***: Configure endpoint profiles.
  
* Not included with TRITON AP-WEB or TRITON AP-EMAIL.

Today page

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

When you log onto the Data Security manager, the Today page displays. This page includes a comprehensive view of data loss prevention incidents that occurred in the last 24 hours, and the total number of 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 hostnames 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 340.*

Deploy button

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

![Deploy button]

In TRITON AP-DATA, your policy and configuration changes are saved as soon as you make them and click **OK**, but they are localized to the TRITON management server.

To deploy changes across all servers running TRITON AP-DATA components in your network, you must click the **Deploy** button on the TRITON toolbar.
The **Deploy** button deploys your policy changes across all TRITON AP-DATA 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 turns 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 Web Security manager, the **Save All** button performs a similar function.

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.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Deployment Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS Server on D3-Win2k3E...</td>
<td>Processing</td>
<td>Not Deployed</td>
</tr>
<tr>
<td>Endpoint Server D3-Win2k...</td>
<td>✔️ Success</td>
<td>All configuration settings were committed</td>
</tr>
<tr>
<td>Policy Engine D3-Win2k3...</td>
<td>✔️ Success</td>
<td>All configuration settings were committed</td>
</tr>
<tr>
<td>Forensics Repository D3...</td>
<td>✔️ Success</td>
<td>All configuration settings were committed</td>
</tr>
<tr>
<td>SMTP Agent: D3-Win2k3En-...</td>
<td>✔️ Success</td>
<td>All configuration settings were committed</td>
</tr>
<tr>
<td>PreciFingerprint Re...</td>
<td>Processing</td>
<td>Not Deployed</td>
</tr>
<tr>
<td>Crawler D3-Win2k3En-01...</td>
<td>✔️ Success</td>
<td>All configuration settings were committed</td>
</tr>
</tbody>
</table>
```

Deploying changes can take time, and if a component is down or disconnected from the network, deployment to that specific component will fail. However, once the component becomes available again, it will get all the pending updates. If TRITON AP-DATA 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 change 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 in inline mode, users lose Internet connection for approximately 5 seconds when you deploy changes to network settings.

---

**Icons**

The following icons are used throughout the Data Security manager interface:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="TRITON management server" /></td>
<td>TRITON management server</td>
</tr>
<tr>
<td><img src="image" alt="TRITON AP-DATA Server" /></td>
<td>TRITON AP-DATA Server</td>
</tr>
<tr>
<td><img src="image" alt="Protector" /></td>
<td>Protector</td>
</tr>
<tr>
<td><img src="image" alt="Content Gateway" /></td>
<td>Content Gateway</td>
</tr>
<tr>
<td><img src="image" alt="TMG agent" /></td>
<td>TMG agent</td>
</tr>
<tr>
<td><img src="image" alt="TRITON AP-EMAIL agent" /></td>
<td>TRITON AP-EMAIL agent</td>
</tr>
<tr>
<td><img src="image" alt="Fingerprint repository" /></td>
<td>Fingerprint repository</td>
</tr>
<tr>
<td><img src="image" alt="Endpoint server" /></td>
<td>Endpoint server</td>
</tr>
</tbody>
</table>
### Navigating the System

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
<td>Crawler</td>
</tr>
<tr>
<td>📡</td>
<td>Forensics repository</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
<td>Policy engine</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
<td>ICAP server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Status Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>🕵️‍♂️</td>
</tr>
<tr>
<td>Icon</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><img src="image" alt="print" /></td>
</tr>
<tr>
<td><img src="image" alt="cut-copy" /></td>
</tr>
<tr>
<td><img src="image" alt="paste" /></td>
</tr>
<tr>
<td><img src="image" alt="file-access" /></td>
</tr>
<tr>
<td><img src="image" alt="download" /></td>
</tr>
<tr>
<td><img src="image" alt="screen-capture" /></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><img src="image" alt="http" /></td>
</tr>
<tr>
<td><img src="image" alt="endpoint" /></td>
</tr>
<tr>
<td><img src="image" alt="ftp" /></td>
</tr>
<tr>
<td><img src="image" alt="im" /></td>
</tr>
<tr>
<td><img src="image" alt="printer" /></td>
</tr>
<tr>
<td><img src="image" alt="smtp" /></td>
</tr>
<tr>
<td><img src="image" alt="icap" /></td>
</tr>
<tr>
<td><img src="image" alt="web" /></td>
</tr>
<tr>
<td>Icon</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Details report</td>
</tr>
<tr>
<td>View</td>
</tr>
<tr>
<td>Print preview - Current, selected, or all filtered incidents</td>
</tr>
</tbody>
</table>

**Reporting**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details report</td>
<td></td>
</tr>
<tr>
<td>Summary report</td>
<td></td>
</tr>
<tr>
<td>Run</td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>Save As</td>
<td></td>
</tr>
<tr>
<td>Export to PDF</td>
<td></td>
</tr>
<tr>
<td>Export to CSV</td>
<td></td>
</tr>
<tr>
<td>Add scheduled task - accesses the Task Scheduler screen</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

**Print and Export**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to PDF</td>
<td></td>
</tr>
</tbody>
</table>
Navigating the System

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Export to CSV</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Print Preview</td>
</tr>
</tbody>
</table>

**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.

- The Information icon provides added details when clicked.

- 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.

![Breadcrumbs Image](image)

The Help system also includes breadcrumbs.
Adding a new user directory server

2. Select **Enabled** to use this user directory server for user import.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

Check boxes

Most check boxes used in the Data Security manager 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.

Pagination

In tables where there is more than one page of data (more than 100 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.
Initial Setup

Related topics:
- Entering your subscription key, page 24
- Defining general system settings, page 25
- Setting up notifications, page 28
- Configuring Web attributes, page 62
- Configuring outbound and inbound attributes, page 55
- Adding a predefined policy, page 75
- Configuring system modules, page 30
- Deploying your settings, page 34

If you have TRITON AP-WEB or TRITON AP-EMAIL installed, follow these steps:

1. Define the general system settings, such as user directories and alerts. (See Defining general system settings, page 25.)
2. Select and define attributes for your Web or email policy. (See Configuring Web attributes, page 62 and Configuring outbound and inbound attributes, page 55.)
3. Deploy your settings. (See Deploying your settings, page 34.)

If you have only TRITON AP-DATA, follow these basic steps:

1. Enter your TRITON AP-DATA subscription key. (See Entering your subscription key, page 24.)
2. Define the general system settings, such as user directories and alerts. (See Defining general system settings, page 25.)
3. Set up notifications. (See Setting up notifications, page 28.)
4. Configure system modules (protector deployments only). (See Configuring system modules, page 30.)
5. Create predefined policies. (See Adding a predefined policy, page 75.)
6. Deploy your settings. (See Deploying your settings, page 34.)
Basic instructions are provided in this chapter. For more detailed instructions, follow the links under Related topics.

**Entering your subscription key**

Before beginning to work with TRITON AP-DATA you must enter your subscription key:

1. Log on to the TRITON Manager and click **Data** to access the Data Security manager. 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 > General > System**.
   b. From the System pane, choose **Subscription**.
2. Browse to your subscription file, then click **Submit**. Your current subscription information is displayed, and the TRITON AP-DATA application restarts.
3. 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 TRITON AP-WEB or TRITON AP-EMAIL, your subscription information is communicated to the TRITON management server automatically.
Defining general system settings

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 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

In the TRITON Manager, 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 tab, you define the user directory to use for TRITON AP-DATA 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the user directory server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of directory from the drop-down menu: Active Directory, Domino, ADAM, or CSV file.</td>
</tr>
</tbody>
</table>
## Initial Setup

### Connection Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname of the user directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the user directory server.</td>
</tr>
<tr>
<td>User distinguished name</td>
<td>Enter a user name that has access to the directory server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user name.</td>
</tr>
<tr>
<td>Root naming context</td>
<td>Optionally, enter the root naming context that TRITON AP-DATA 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, the system begins searching at the top level of the directory service.</td>
</tr>
<tr>
<td>Use SSL encryption</td>
<td>Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.</td>
</tr>
<tr>
<td>Follow referrals</td>
<td>Select <strong>Follow referrals</strong> if you want TRITON AP-DATA to follow server referrals should they exist. A server referral is when one server refers to another for programs or data.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click this button to test your connection to the user-directory server.</td>
</tr>
</tbody>
</table>

### Directory usage

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get user attributes</td>
<td>Select this box if you want to retrieve user attributes from the directory server.</td>
</tr>
<tr>
<td>Attributes to retrieve</td>
<td>Enter the user attributes that you want the Data Security manager to collect for all users (comma separated).</td>
</tr>
</tbody>
</table>
| 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.                        |
| View Results                  | Click **View Results** to check the user information that was imported. **View Results** retrieves and displays the data entered in the Attributes to retrieve, Photo attributes to retrieve, and Sample email address fields. |
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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:

- *Configuring alerts*, page 385
- *Setting up email properties*, page 385

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>When an alert is sent to administrators, from whom should it be coming?</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom the alert is coming.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname of the outgoing SMTP mail server to use for scheduled alert notifications.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the mail server to use.</td>
</tr>
</tbody>
</table>
6. Complete the remaining fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Enter a subject for alerts. Click the right-arrow to select a variable to include in the subject, such as %Severity%.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Click <strong>Edit</strong> to select the recipients to whom alerts should be sent.</td>
</tr>
</tbody>
</table>

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.

---

### Setting up notifications

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

TRITON AP-DATA 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 202* and *Action Plans, page 189* 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>Enter the name of the person from whom notifications should be sent. This is the name that will appear in the email <strong>From</strong> field.</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom notifications should be sent.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Type the subject of the notification. This appears in the email <strong>Subject:</strong> 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% because it breached corporate policy.”</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>For fastest set up, select <strong>Standard</strong> and leave all the check boxes selected.</td>
</tr>
<tr>
<td></td>
<td>See <em>Notifications, page 202</em> if you want to customize notifications.</td>
</tr>
<tr>
<td>Display as</td>
<td>Select a display format from the drop-down list: HTML or plain text.</td>
</tr>
</tbody>
</table>

9. Click **OK** to save your changes.
Configuring system modules

When you install TRITON AP-DATA, the modules you install are automatically registered with the TRITON management server.

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

The TRITON management server has the following modules by default:

- Primary fingerprint repository
- Endpoint server
- Crawler (fingerprinting and discovery agent)
- Forensics repository
- Policy engine

If you have TRITON AP-WEB or TRITON AP-EMAIL, there are also modules for the Web Content Gateway and TRITON AP-EMAIL.

Protector-based solutions have the following modules:

- ICAP agent
- Policy engine
- Secondary fingerprinting repository

The protector is also a module itself.

If you added any other modules to your system—such as supplemental TRITON AP-DATA servers, agents, crawlers—these components appear in tree view as well.

To get TRITON AP-DATA up and running, all you have to do is configure the protector. You need only configure the other modules for non-default behavior. In
In some cases, the protector is not even required—as in some endpoint deployments and in TRITON AP-WEB deployments.

### Note
See the TRITON AP-DATA *Installation Guide* for instructions on installing TRITON AP-DATA modules.

## Configuring the protector

1. Select **Settings > Deployment > System Modules**.
2. If it is not already done so, then expand the tree in the content pane.
3. Click the protector module in the tree and input data in all the tabs offered:
   - **General tab**, page 31
   - **Networking tab**, page 32
   - **Local Networks tab**, page 33
   - **Services**, page 34

### General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name you gave the protector when you added it. Edit as desired.</td>
</tr>
<tr>
<td>Description</td>
<td>The description you gave the protector when you added it. Edit as desired.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select <strong>Enabled</strong> to activate this protector in your system. Though you have added the protector, it is not used until you select <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the machine hosting the protector (uneditable).</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the machine hosting the protector (uneditable).</td>
</tr>
</tbody>
</table>
### Initial Setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed by</td>
<td>Read-only field. Name or IP address of the TRITON management that should manage this protector.</td>
</tr>
<tr>
<td>Version</td>
<td>Read-only field. Version of the TRITON AP-DATA protector software.</td>
</tr>
</tbody>
</table>

### Networking tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default gateway</td>
<td>Enter the IP address 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). Associate the Default gateway to the Interface (next field) connected to its subnet/VLAN.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select which network interface this protector uses for the default gateway.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>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.</td>
</tr>
<tr>
<td>DNS suffixes</td>
<td>Enter the DNS suffix used by your organization, then click Add. If you have more than one DNS suffix, add them all.</td>
</tr>
<tr>
<td>Connection mode</td>
<td>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?</td>
</tr>
</tbody>
</table>
### 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. Relevant only for network interfaces.
- **Subnet mask** - Enter a subnet mask for the interface. Relevant only for network interfaces.
- **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 checkbox if you want to enable Virtual LAN support on this network. Note that this does not apply when HTTP in active (blocking) mode is applied to an inline configuration.

### Local Networks tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include all networks</td>
<td>Select this option 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.</td>
</tr>
</tbody>
</table>
| Include specific networks | Select this option 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 inbound, outbound, 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 431 for information on configuring protector services.

Deploying your settings

To deploy all the settings you configured in this chapter, click Deploy in the Data Security manager toolbar.
Part II
Securing Your Company’s Data
Once you have installed TRITON AP-DATA software and configured system settings, the next step is to create a policy.

Data Loss Prevention (DLP) policies enable you to monitor and control the flow of sensitive data throughout your organization. Depending on your TRITON AP-DATA configuration, you can set up policies to monitor information sent via email and over HTTP and HTTPS channels, and ensure all communications are in line with regulations and compliance laws as required. You can also monitor email being sent to users’ mobile devices.

There are 5 kinds of DLP policies:

- **Email policy.** You can enable a single email DLP policy that contains all attributes you wish to monitor in inbound and outbound messages. For each attribute (for example, the appearance of a defined key phrase), you define whether to permit or quarantine the message, and whether a notification should be sent. For more information, refer to *Configuring the Email Data Loss Prevention Policy*, page 53.

- **Web policy.** You can enable a single Web DLP policy that contains all attributes you wish to monitor in HTTP, HTTP, and FTP channels, and also specify websites to which sensitive data cannot be sent. For more information, refer to *Configuring the Web Data Loss Prevention Policy*, page 61.

- **Mobile policy.** You can enable a single mobile DLP policy that contains all attributes you wish to monitor in email being sent to users’ mobile devices. For each attribute (for example, the appearance of a defined key phrase), you define whether to permit or quarantine the message, and whether a notification should be sent. For more information, refer to *Configuring the Mobile Data Loss Prevention Policy*, page 69.
- **Predefined policy.** TRITON AP-DATA comes with a rich set of predefined policies that cover the data requirements for a wide variety of organizations. They include:
  - Acceptable use policies, such as cyberbullying, obscenities, and indecent images.
  - Content protection policies, such as Password Dissemination, Credit Cards, and Financial Information.
  - Regulations, compliance, and standards policies, such as PCI and federal regulations.
  - Data theft indicator policies, such as Suspected Malicious Dissemination and Disgruntled Employee.

For more information, refer to *Using Predefined Policies*, page 75.

- **Custom policy.** 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. For more information, refer to *Creating Custom DLP Policies*, page 79.

---

**Note**

You cannot delete or rename an email, Web, or mobile DLP policy, but you can enable or disable their attributes. Likewise, you cannot update all rules or exceptions in email or Web policies using the batch operations on the Manage Policies screen.

---

Although much of the policy creation process is performed through wizards, it’s important that you understand some key concepts before you get started.
What’s in a policy?

In TRITON AP-DATA, policies contain rules, exceptions, conditions (defined by content classifiers), and resources. This is true of predefined and custom policies.

**Related topics:**
- *Managing rules*, page 100
- *Adding exceptions*, page 101
- *Classifying Content*, page 107
- *Defining Resources*, page 171

<table>
<thead>
<tr>
<th><strong>Element</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>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? Rules can apply to a single breach or to the accumulation of breaches over a period of time. Standard rules create incidents every time a rule is matched. Cumulative rules accumulate matches over time and create incidents when a threshold is met. This is known as <em>Drip DLP</em>.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>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. You cannot add exceptions to cumulative rules, and exceptions themselves cannot be cumulative.</td>
</tr>
</tbody>
</table>
These components are the building blocks of a policy. When you create a policy from a policy template, it already contains rules, exceptions, classifiers, sources, destinations, and actions. When you create a policy from scratch, wizards prompt you for such information.

Discovery policies also contain discovery tasks. These describe where to perform the discovery. On networks, this may include a file system, SharePoint directory, database or Outlook PST file. If you’re performing endpoint discovery, it includes the exact computers to scan.

### Viewing policies

Select **Main > Policy Management > DLP Policies** or **Discovery Policies**, then click **Manage Policies** to view a list of policies that have been defined for your organization.

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.

**Tip**

If you haven’t created a policy yet, the list is empty. To create your first policy, select **Add > Predefined Policy** or **Add > Custom Policy** from the toolbar.

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.

---

**Tree icons**

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Level" /></td>
<td>Level (See <strong>Policy levels</strong>.)</td>
</tr>
<tr>
<td><img src="#" alt="Policy" /></td>
<td>Policy</td>
</tr>
</tbody>
</table>
### The policy toolbar

The policy toolbar provides many functions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New…" /></td>
<td>Create a new policy, rule, or exception.</td>
</tr>
<tr>
<td><img src="image" alt="Edit…" /></td>
<td>Edit the selected policy, rule, or exception.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete the selected policy, rule, or exception. The administrators that were directly assigned to this policy see it in their policy list as deleted. However, they continue to see old incidents that relate to this policy. If you do not want to see incidents for a deleted policy, clear the check box for the policy in your Incident report list.</td>
</tr>
<tr>
<td><img src="image" alt="Show disabled rules" /></td>
<td>Show or hide disabled rules in the policy tree.</td>
</tr>
</tbody>
</table>
| ![More Actions](image) | ● Batch Operations - lets you update or delete multiple items at once. For example,  
  ■ Select Update rules of current policy to change one or more rules in the selected policy at the same time. This overrides the settings in the policy and reduces time and effort involved in updating multiple settings.  
  ■ Select Update exceptions of current rule to change one or more exceptions in the selected rule at the same time. This overrides the settings in the rule.  
  ■ Select Update rules of multiple policies to make changes to selected rules or all rules across multiple policies.  
  ■ Select Update exceptions of multiple rules to change selected exceptions or all exceptions across multiple 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. |

---

**Icon** | **Description**
---|---
Rules |  
Exception |
Select a name from the policy tree to edit a policy’s properties.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The name for this policy.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the rule for this policy. If this box is unselected, the rule is present, but disabled.</td>
</tr>
<tr>
<td>Policy description</td>
<td>Enter a description for this policy.</td>
</tr>
</tbody>
</table>
| Policy owners    | If configured, policy owners receive notifications of breaches. To define an owner or owners for this DLP policy:  
  1. Click Edit.  
  2. Select one or more owners from the resulting box. See Selecting items to include or exclude in a policy, page 49 for instructions.  
  3. Click OK. |

Update rules of current policy

Use this screen to change multiple rules in a policy at once. You can change as many rules as you want. This overrides the settings in the policy and reduces time and effort involved in updating multiple settings.

1. Select Main > Policy Management > DLP Policies or Discovery Policies
2. Select Manage Policies.
3. Select the policy to modify.
4. From the toolbar, select **More Actions > Batch Operations > Update rules of current policy**.
5. In the Selected Rules box, select the rules that you want to modify.
6. In the Fields to Update box, select the fields to update.
7. For each field, update the properties in the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the selected rules. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of the selected rules. See <em>Custom Policy Wizard - Severity &amp; Action</em>, page 85 for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data you’d like to analyze. These sources are applied to all of the selected rules. See <em>Custom Policy Wizard - Source</em>, page 88 for more details. Any changes made here override all other configurations of source in the rule.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations that you want to analyze. These destinations are applied to all of the selected rules. See <em>Custom Policy Wizard - Destination</em>, page 88 for more details. Any changes made here override all other configurations of destination in the rule.</td>
</tr>
</tbody>
</table>

8. Click **OK**.

**Update exceptions of current rule**

Use this screen to change multiple exceptions in a rule at once. You can change as many exceptions as you want. This overrides the settings in the rule and reduces time and effort involved in updating multiple settings.

1. Select **Main > Policy Management > DLP Policies or Discovery Policies**
2. Select **Manage Policies**.
3. Select the rule to modify.
4. From the toolbar, select **More Actions > Batch Operations > Update exceptions of current rule**.
5. In the Selected Exceptions box, select the exceptions that you want to modify.
6. In the Fields to Update box, select the fields to update.
7. For each field, update the properties in the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the selected exceptions. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of the selected exceptions. See Custom Policy Wizard - Severity &amp; Action, page 85 for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data you’d like to analyze. These sources are applied to all of the selected exceptions. See Custom Policy Wizard - Source, page 88 for more details.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations that you want to analyze. These destinations are applied to all of the selected exceptions. See Custom Policy Wizard - Destination, page 88 for more details.</td>
</tr>
</tbody>
</table>

8. Click **OK**.

**Update rules of multiple policies**

On this screen, you can make changes to selected rules or all rules across all policies.

1. Select **Main > Policy Management > DLP Policies** or **Discovery Policies**
2. Select **Manage Policies**.
3. Select the policy to modify.
4. From the toolbar, select **More Actions > Batch Operations > Update rules of multiple policies**.
5. Select either **All rules** if you want to update all rules with your changes, or **Selected rules** if you want to update only a few.
6. In the Selected Rules box, select the rules that you want to modify. You can see which policies contain the rule.
7. In the Fields to Update box, select the fields to update.
8. For each field, update the properties in the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the rules in the current policy. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of the rules in this policy. See Custom Policy Wizard - Severity &amp; Action, page 85 for more details.</td>
</tr>
</tbody>
</table>
### Field | Properties
--- | ---
Source | Select the sources of data you’d like to analyze. These sources are applied to all of the rules in the policy. See [Custom Policy Wizard - Source, page 88](#) for more details.

Destination | Select the data destinations that you want to analyze. These destinations are applied to all of the rules in the policy. See [Custom Policy Wizard - Destination, page 88](#) for more details.

---

9. Click **OK**.

**Update exceptions of multiple rules**

On this screen, you can change selected exceptions or all exceptions across all rules.

1. Select **Main > Policy Management > DLP Policies** or **Discovery Policies**
2. Select **Manage Policies**.
3. Select the rule to modify.
4. From the toolbar, select **More Actions > Batch Operations > Update exceptions of multiple policies**.
5. Select either **All exceptions** if you want to update all exceptions with your changes, or **Selected exceptions** if you want to update only a few.
6. In the Selected Exceptions box, select the exceptions that you want to modify. You can see which rules contain the exception.
7. In the Fields to Update box, select the fields to update.
8. For each field, update the properties in the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the exceptions to the current rule. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of this rule’s exceptions. See <a href="#">Custom Policy Wizard - Severity &amp; Action, page 85</a> for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data you’d like to analyze. These sources are applied to all of this rule’s exceptions. See <a href="#">Custom Policy Wizard - Source, page 88</a> for more details.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations that you want to analyze. These destinations are applied to all of this rule’s exceptions. See <a href="#">Custom Policy Wizard - Destination, page 88</a> for more details.</td>
</tr>
</tbody>
</table>

9. Click **OK**.
Delete policies

On this screen, you can delete a batch of policies at once.

1. Select **Main > Policy Management > DLP Policies** or **Discovery Policies**
2. Select **Manage Policies**.
3. From the toolbar, select **More Actions > Batch Operations > Delete Policies**.
4. Select the policy or policies to delete. Click **Select All** to delete all of your policies.
5. Click **OK**.
6. When asked to confirm your action, click **Yes**.

Policy levels

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. (All 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 TRITON AP-DATA, 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,
TRITON AP-DATA 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 the Data Security manager, 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:

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Select the entity—such as computers or networks if you are selecting a source—to display in the <strong>Available List</strong> 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. See <em>Defining Resources</em>, page 171 for instructions.</td>
</tr>
<tr>
<td>Filter by</td>
<td>Typically too many entries are available to display on one page. Use the <strong>Filter by</strong> field to specify criteria by which to filter the list. If you enter “jones”, the system searches for any entry that contains the string “jones”. It is equivalent to searching “<em>jones</em>”. You can use additional wildcards in your filter string if desired. For example: “??” represents any single character, as in the example “file_?.txt”. Click the <strong>Apply filter</strong> button to apply the filter or the <strong>Clear</strong> button to clear it.</td>
</tr>
</tbody>
</table>
When you are selecting sources or destinations, you can either 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 drop-down list box, select **Predefined lists** if you want to select from lists; or select **Free text** to type the name of an item to include.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available items</td>
<td>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. If you chose Directory Entries in the Display field, hover over an item in this list to see all the fields that will be searched—login, full name, domain name, and email address.</td>
</tr>
<tr>
<td>Selected items</td>
<td>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, then highlight it on the left. Make sure the <strong>Include</strong> tab is active, and then click &gt;. If you want to exclude Bob_Computer, make sure the <strong>Exclude</strong> tab is active when you click &gt;. If you select more than 1000 items, you receive an error recommending you create a business unit instead. <strong>Tip:</strong> you can move a group of users, computers, networks, etc. into the <strong>Include</strong> box, then remove one user, computer, or network by highlighting it on the right and clicking <strong>Remove</strong>.</td>
</tr>
</tbody>
</table>
2. If you choose **Predefined lists**, complete the fields in the table above. If you choose **Free text**, a box appears:

![Free text](image)

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

By default, the system searches for all entities containing the word or words you type. For example, if you type “jones” for policy owner, it might return mjones@example.com, jjones@acme.com, and sjones@abc.com. Entering “jones” is equivalent to searching “*jones*”. Additional wildcards are allowed.

3. Click **OK**.
Configuring the Email Data Loss Prevention Policy

TRITON AP-DATA enables you to control how sensitive data moves through your organization via email. Depending on your deployment, you can protect outbound, inbound, or internal email from data loss, or all three.

To monitor email for sensitive data, you must have either the TRITON AP-EMAIL module or TRITON AP-DATA protector.

Note that the email DLP policy applies to network channels only. To monitor email on endpoint machines, such as laptops that are off-network, create a custom policy.

Tip
To get the full benefit of TRITON AP-DATA’S email capabilities, use the TRITON AP-EMAIL module. (This requires a subscription to TRITON AP-EMAIL and the Email DLP module.) The protector can monitor inbound and outbound email when it’s in monitoring mode.

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

To confirm that the registration was successful, click Email in the TRITON toolbar, and navigate to Settings > General > Data Security. If the status is “unregistered,”
To configure the email DLP policy

1. In the Data Security manager, select Main > Policy Management > DLP Policies > Email DLP Policy. A quick-start email data loss prevention (DLP) policy is provided.

2. On the Outbound tab, select and enable the attributes to monitor in outgoing email messages—for example message size or attachment type. Configure properties for those attributes. When the settings you configure are matched, the policy is triggered.

   See Configuring outbound and inbound attributes, page 55 for instructions on completing the fields.

3. Select the Inbound tab, then select and enable the attributes to monitor inbound email messages—for example questionable images. Configure properties for those attributes.

   Note

   If you want to monitor internal email messages, you must create a custom policy. On the Destination tab of the policy wizard, select Network or Endpoint Email, then select Direction > Internal.

4. Identify an owner or owners for the policy. See Defining policy owners, page 59 for instructions.

5. Identify trusted domains if any. See Identifying trusted domains, page 59 for more information.

6. Click OK.

   Note

   You cannot delete or rename your email policy, but you can enable or disable attributes.

   In this section, you define inbound and outbound email attributes. You define Internal DLP email through the custom policy wizard.
Configuring outbound and inbound attributes

Select one or more email attributes to include in the policy. For each, highlight the attribute and click **Enabled** in the right pane. Define properties in the right pane as well.

When the system detects a match for an attribute, it triggers the policy.

If you want to send notifications when there is a violation of a particular attribute setting, select the **Send Notification** check box. You can configure who receives the notifications by clicking the name of the notification, “Email policy violation.” Click this option to define the mail server, email subject, and message body, as well as other required properties.

By default, for inbound messages, policy owners receive notifications. For outbound messages, both policy owners and message senders receive them.

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. Actions are described in *Adding a new action plan*, page 190.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size</td>
<td>Select the size of email messages to monitor. For example, choose 25 MB if you want the system to analyze and enforce messages exceeding 25 MB, but you're not concerned about messages smaller than 25 MB, even if there is a match. The default size is 10 MB. Default severity: low. Available actions: quarantine (default), permit.</td>
</tr>
<tr>
<td>Regulatory &amp; compliance</td>
<td>Select the regulatory and compliance laws you need to enforce. These are applied to the regions you selected with the regulatory &amp; compliance option.</td>
</tr>
<tr>
<td></td>
<td>- Personally Identifiable Information (PII)</td>
</tr>
<tr>
<td></td>
<td>- Protected Health Information (PHI)</td>
</tr>
<tr>
<td></td>
<td>- Payment Card Industry (PCI DSS)</td>
</tr>
<tr>
<td></td>
<td>If you have not selected regions, an error pops up. Click “Select regions” to fix this.</td>
</tr>
<tr>
<td></td>
<td>Once you’ve selected a law, click its name to view or edit the specific policies to enforce. For example, in the PCI category, both Europe and US credit card policies are enforced by default. You might exclude the US credit card policy if you do not do business in the US. Applying only the policies you need improves performance and reduces resource consumption. Select a sensitivity for each policy.</td>
</tr>
<tr>
<td></td>
<td>- Wide is highly sensitive and errs on the restrictive side. To avoid leaking sensitive data, it is more likely to produce a false positive (unintended match) than a false negative (content that is not detected).</td>
</tr>
<tr>
<td></td>
<td>- Default balances the number of false positives and false negatives.</td>
</tr>
<tr>
<td></td>
<td>- Narrow is the least restrictive. It is more likely to let content through than to produce an unintended match.</td>
</tr>
<tr>
<td>Attachment name</td>
<td>One by one, enter the names of the exact files that should be monitored when they’re attached to an email message. Include the filename and extension. Click Add after each entry.</td>
</tr>
<tr>
<td></td>
<td>For example, add the file named confidential.docx. When that file is attached to an email message, the system detects it and either permits or blocks the message, or drops the attachment and sends the remaining message.</td>
</tr>
<tr>
<td></td>
<td>Note that Drop Attachments applies only to the TRITON AP-EMAIL module. If your email is being monitored by the protector and you select this option, it will be quarantined when a policy is triggered. Default severity: low.</td>
</tr>
<tr>
<td></td>
<td>Available actions: quarantine, permit, drop attachments (default)</td>
</tr>
</tbody>
</table>
## Configuring the Email Data Loss Prevention Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment type</td>
<td>Click <strong>Add</strong> to specify the types of files that should be monitored when attached to an email message, 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, enter search criteria to find the file type you want. The system searches in the file type group, description, and file type for the data you enter. If the file type does not exist, specify exact files of this type using the <strong>Attachment name</strong> attribute instead. Default severity: <strong>low</strong>. Available actions: <strong>quarantine, permit, drop attachments</strong> (default). <strong>Note:</strong> Drop Attachments applies only to the TRITON AP-EMAIL module. If your email is being monitored by the protector and you select this option, it will be quarantined when a policy is triggered.</td>
</tr>
<tr>
<td>Patterns &amp; phrases</td>
<td>Click <strong>Add</strong> to define key phrases or regular expression (RegEx) patterns that should be monitored. RegEx patterns are used to identify alphanumeric strings of a certain format. 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. Define whether to search for the phrase or RegEx pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields. Default severity: <strong>medium</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Acceptable use</td>
<td>Select the dictionaries that define unacceptable use in your organization. For example, if you want to prevent adult language from being exchanged by email, select Adult. TRITON AP-DATA includes dictionaries in several languages. Select the languages to enforce. Only terms in these languages are considered a match. For example, if you select the Adult dictionary in Hebrew, then adult terms in English are not considered an incident. Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce. You cannot add or delete terms from predefined dictionaries, but you can exclude them from detection if you are getting unintended matches. Select Main &gt; Content Classifiers &gt; Patterns &amp; Phrases, select the dictionary to edit, then enter the phrases to exclude. By default the policy is triggered by a single match from the dictionary or dictionaries you select. Default severity: medium. Available actions: quarantine (default), permit.</td>
</tr>
<tr>
<td>Questionable images</td>
<td>Select this attribute to prevent pornographic images from entering your organization. (This feature requires a separate Image Analysis module subscription). Pornographic images pose a legal liability to organizations in many countries. The system judges images based on the amount of flesh tone they contain. Default severity: low. Available actions: quarantine, permit, drop attachments (default).</td>
</tr>
<tr>
<td>Number of attachments</td>
<td>Specify the number of attachments to detect. Email messages with this number of attachments (or more) trigger the policy. The default number of attachments is 20. Default severity: low. Available actions: quarantine (default), permit</td>
</tr>
<tr>
<td>Number of destination domains</td>
<td>This option is available for outbound messages only. Sometimes you may want to block messages sent to multiple destination domains, because this may indicate spam. Specify the number of destination domains to detect. Email messages sent to this number of domains (or more) trigger the policy. The default number of domains is 25. Also, select which email fields to monitor (To, Cc, Bcc). To and Cc are selected by default. Default severity: low. Available actions: quarantine (default), permit</td>
</tr>
</tbody>
</table>
Defining policy owners

Policy owners can view and 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 email DLP policy:

1. Select the Policy Owners tab.
2. Click Edit.
3. Select one or more owners from the resulting box. See Selecting items to include or exclude in a policy, page 49 for instructions.
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.

See Notifications, page 202 for more information.

Identifying trusted domains

Trusted domains are, simply, those that you trust, such as the domain of a company you just acquired. Trusted domains do not need to be monitored, so they do not get analyzed by the system.

---

Note

Trusted domains apply to outbound email traffic only.

---

If you have domains that you do not want enforced:

1. On the Outbound tab, select Enable trusted domains.
2. Click Edit.
3. Browse for the domain or domains you trust.
4. Click OK.
Configuring the Web Data Loss Prevention Policy

TRITON AP-DATA lets you to control how and where users upload or post sensitive data over HTTP or HTTPS connections.

To monitor HTTP and HTTPS channels for sensitive data, you must have either the TRITON AP-WEB module, the TRITON AP-DATA protector, or the TMG agent.

Note that the web DLP policy applies to network channels only. To monitor HTTP/HTTPS on endpoint machines, such as laptops that are off-network, create a custom policy.

---

Tip

To get the full benefit of TRITON AP-DATA’S web capabilities, use the TRITON AP-WEB module. (This requires a subscription to TRITON AP-WEB.) The TRITON AP-WEB module accesses the Websense Database to categorize URLs, and it includes a built-in policy engine that speeds analysis.

---

The TRITON AP-WEB module is automatically configured to work with TRITON AP-DATA. The TRITON AP-WEB module registers with the TRITON management server when you install it.

---

Important

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

---

To confirm that the registration was successful, navigate to Settings > Deployment > System Modules. If all went well, you’ll see a module named, Web Content Gateway.
To configure the Web DLP policy

1. In the Data Security manager, select Main > Policy Management > DLP Policies > Web DLP Policy. A quick-start Web DLP policy is provided.

2. On the Attributes tab, select and enable the 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 62 for instructions on completing the fields.

3. Select the Destination tab, then specify the websites where you do not want your data sent. See Selecting Web destinations, page 66 for instructions.

4. Select the Policy Owners tab, then identify an owner for the policy. See Defining policy owners, page 68 for instructions.

5. Click OK.

Note

You can’t delete or rename your Web policy, but you can enable or disable its attributes.

Configuring Web attributes

Select one or more Web attributes to include in the policy. For each, highlight the attribute and click Enabled in the right pane. Define properties for each attribute in the right pane as well.

When the system detects a match for an attribute, it triggers the policy.

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. See Configuring the Web Data Loss Prevention Policy, page 61 for instructions.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post size</td>
<td>Disabled by default. Select the size of Web posts to monitor. For example, choose 100 KB if you want the system 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: <strong>low</strong>. Available actions: block (default), permit.</td>
</tr>
</tbody>
</table>
| 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. |
Configuring the Web Data Loss Prevention Policy

Data theft

Disabled by default.

The system protects against content being posted to the Web after your computer is infected. This complements the TRITON AP-WEB 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 communication** - Identifies transactions that are suspected to be malicious, based on analysis of traffic of known infected machines. This includes traffic thought to be malware phoning home or attempting to steal data. To use this feature, you must have TRITON AP-WEB installed and the Linking Service enabled. Because Linking Service is required, malware is not detected on endpoints.

- **Encrypted files - unknown format** - Searches for outbound files that were encrypted using unknown encryption formats, based on advanced pattern and statistical analysis of the data.

- **Encrypted files - known format** - Searches for outbound transactions comprising common encrypted file formats, such as password-protected Microsoft Word files.

- **Password files** - Searches for password files, such as a SAM database and UNIX/Linux password files.

- **Common password information** - Searches for password information in plain text by looking for common password patterns and using various heuristics.

- **IT asset information** - Searches for electronic data containing suspicious content, such as network data, software license keys, and database files.

- **Suspicious behavior over time** - Searches for activity considered to be potentially malicious, such as numerous posts in a designated period or numerous transactions containing encrypted data.

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**.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data theft</td>
<td>Disabled by default. The system protects against content being posted to the Web after your computer is infected. This complements the TRITON AP-WEB module which protects against infected content downloaded from the Web.</td>
</tr>
<tr>
<td>Malware communication</td>
<td>Identifies transactions that are suspected to be malicious, based on analysis of traffic of known infected machines. This includes traffic thought to be malware phoning home or attempting to steal data. To use this feature, you must have TRITON AP-WEB installed and the Linking Service enabled. Because Linking Service is required, malware is not detected on endpoints.</td>
</tr>
<tr>
<td>Encrypted files - unknown format</td>
<td>Searches for outbound files that were encrypted using unknown encryption formats, based on advanced pattern and statistical analysis of the data.</td>
</tr>
<tr>
<td>Encrypted files - known format</td>
<td>Searches for outbound transactions comprising common encrypted file formats, such as password-protected Microsoft Word files.</td>
</tr>
<tr>
<td>Password files</td>
<td>Searches for password files, such as a SAM database and UNIX/Linux password files.</td>
</tr>
<tr>
<td>Common password information</td>
<td>Searches for password information in plain text by looking for common password patterns and using various heuristics.</td>
</tr>
<tr>
<td>IT asset information</td>
<td>Searches for electronic data containing suspicious content, such as network data, software license keys, and database files.</td>
</tr>
<tr>
<td>Suspicious behavior over time</td>
<td>Searches for activity considered to be potentially malicious, such as numerous posts in a designated period or numerous transactions containing encrypted data.</td>
</tr>
</tbody>
</table>

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**.
### Configuring the Web Data Loss Prevention Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of uploaded file</td>
<td>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 <strong>Add</strong> after each entry. For example, add the file named <strong>confidential.docx</strong>. When that file is being posted, the system will detect it and either permit or block the post. The system can detect files even when they’ve been compressed into an archive, such as a .zip file. Default severity: <strong>low</strong>. Available actions: <strong>block</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Type of uploaded file</td>
<td>Disabled by default. Click <strong>Add</strong> 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 <strong>Name of uploaded file</strong> attribute instead. Default severity: <strong>low</strong>. Available actions: <strong>block</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Patterns &amp; phrases</td>
<td>Enabled by default. Click <strong>Add</strong> 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: <strong>medium</strong>. Available actions: <strong>block</strong> (default), <strong>permit</strong>. <strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

---

**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, the system will detect it and either permit or block the post. The system 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

Select one or more websites to include in the policy on the Destination tab. When the system detects that someone is posting sensitive data to those websites, it triggers the policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Sites</td>
<td>Select this option if you do not want sensitive data posted or uploaded to any website, without exception.</td>
</tr>
</tbody>
</table>

Related topics:
- Configuring the Web Data Loss Prevention Policy, page 61
- Selecting Web destinations, page 66
- Defining policy owners, page 68
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>websites that belong to the selected categories</td>
<td>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 &gt; General &gt; System &gt; 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.</td>
</tr>
</tbody>
</table>

- **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
Configuring the Web Data Loss Prevention Policy

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. See Selecting items to include or exclude in a policy, page 49 for instructions.
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.

See Notifications, page 202 for more.
Configuring the Mobile Data Loss Prevention Policy

TRITON AP-DATA lets you define what content can and cannot be sent to mobile devices—such as phones and i-pads—from network email systems. Most organizations employ such a policy to protect their data in case an employee’s mobile devices is lost or stolen.

The system analyzes content when users synchronize their mobile devices to their organization’s Exchange server. If content being pushed to the device breaches the organization’s mobile DLP policy, it is quarantined or permitted accordingly, whether that content is part of an email message, calendar item, or task.

Mobile policies are set for user directory entries (users and groups), business units, or custom users, not individual mobile devices. In other words, you can prevent sensitive data being sent to John Doe’s mobile devices, not to a particular device ID.

To use this feature, you must have a subscription to TRITON AP-ENDPOINT DLP, and you must install the mobile agent in your DMZ and connect it to both your Exchange server and the TRITON management server. (See Configuring the mobile agent, page 444 for more information.)

Note that the mobile DLP policy applies to mobile email only. To monitor network or endpoint email, configure an email DLP or custom policy, respectively.

To configure the mobile DLP policy

1. In the Data Security manager, select Main > Policy Management > DLP Policies > Mobile DLP Policy. A quick-start mobile data loss prevention (DLP) policy is provided.

2. On the Attributes tab, select and enable the attributes to monitor in email that is being synchronized to mobile devices from network Exchange servers—for example message size or attachment type. Configure properties for those attributes. When the settings you configure are matched, the policy is triggered. See Configuring attributes, page 70 for instructions on completing the fields.
3. Identify users that don’t need to be monitored (trusted users), if any.
4. Identify an owner or owners for the policy. See *Defining policy owners*, page 73 for instructions.
5. Click **OK**.

---

**Note**

You cannot delete or rename your mobile policy, but you can enable or disable attributes.

---

**Configuring attributes**

Select one or more email attributes to include in the policy. For each, highlight the attribute and click **Enabled** in the right pane. Define properties in the right pane as well.

When the system detects a match for an attribute, it triggers the policy.

If you want to send notifications when there is a violation of a particular attribute setting, select the **Send Notification** check box. You can configure who receives the notifications by clicking the name of the notification, “Mobile policy violation.” Click this option to define the mail server, email subject, and message body, as well as other required properties.

By default, policy owners receive notifications.

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
Configuring the Mobile Data Loss Prevention Policy

Levels and available actions are shown below for each attribute. Actions are described in *Adding a new action plan*, page 190.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size</td>
<td>Select the size of email messages to monitor. For example, choose 25 MB if you want the system to analyze and enforce messages exceeding 25 MB, but you're not concerned about messages smaller than 25 MB, even if there is a match. The default size is 10 MB. Default severity: low. Available actions: quarantine (default), permit.</td>
</tr>
</tbody>
</table>
| Regulatory & compliance      | Select the regulatory and compliance laws 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 law, click its name to view or edit the specific policies to enforce. For example, in the PCI category, both Europe and US credit card policies are enforced by default. You might exclude the US credit card policy if you do not do business in the US. 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. To avoid leaking sensitive data, 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.  
- Narrow is the least restrictive. It is more likely to let content through than to produce an unintended match. Default severity: high. Available actions: quarantine (default), permit. |
| Attachment name              | One by one, enter the names of the exact files that should be monitored when they’re attached to an email message. Include the filename and extension. Click Add after each entry. For example, add the file named confidential.docx. When that file is attached to an email message, the system detects it and either permits or quarantines the message. Default severity: low. Available actions: quarantine (default), permit. |
## Configuring the Mobile Data Loss Prevention Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Attachment type** | Click **Add** to specify the types of files that should be monitored when attached to an email message, 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, enter search criteria to find the file type you want. The system searches in the file type group, description, and file type for the data you enter.  
If the file type does not exist, specify exact files of this type using the **Attachment name** attribute instead.  
Default severity: **low**.  
Available actions: **quarantine** (default), **permit**. |
| **Patterns & phrases** | Click **Add** to define key phrases or regular expression (RegEx) patterns that should be monitored. RegEx patterns are used to identify alphanumeric strings of a certain format.  
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.  
Define whether to search for the phrase or RegEx pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields.  
Default severity: **medium**.  
Available actions: **quarantine** (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. |
Configuring the Mobile Data Loss Prevention Policy

Enable trusted users

Trusted users are those who you feel you don’t need to monitor. Trusted users do not get analyzed by the system.

If you have users that you do not want enforced:

1. Select Enable trusted users.
2. Click Edit.
3. Browse for the users, directory entries, and business units you trust.

Defining policy owners

Policy owners can view and 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 mobile DLP policy:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable use</td>
<td>Select the dictionaries that define unacceptable use in your organization. For example, if you want to prevent adult language from being exchanged by email, select Adult. TRITON AP-DATA includes dictionaries in several languages. Select the languages to enforce. Only terms in these languages are considered a match. For example, if you select the Adult dictionary in Hebrew, then adult terms in English are not considered an incident. Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce. You cannot add or delete terms from predefined dictionaries, but you can exclude them from detection if you are getting unintended matches. Select Main &gt; Content Classifiers &gt; Patterns &amp; Phrases, select the dictionary to edit, then enter the phrases to exclude. By default the policy is triggered by a single match from the dictionary or dictionaries you select. Default severity: medium. Available actions: quarantine (default), permit.</td>
</tr>
<tr>
<td>Questionable images</td>
<td>Select this attribute to prevent pornographic images from entering your organization. (This feature requires a separate Image Analysis module subscription). Pornographic images pose a legal liability to organizations in many countries. The system judges images based on the amount of flesh tone they contain. Default severity: low. Available actions: quarantine (default), permit.</td>
</tr>
</tbody>
</table>
Configuring the Mobile Data Loss Prevention Policy

1. Select the Policy Owners tab.
2. Click Edit.
3. Select one or more owners from the resulting box. See Selecting items to include or exclude in a policy, page 49 for instructions.
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.

See Notifications, page 202 for more information.
TRITON AP-DATA comes with a rich set of predefined policies that cover the data requirements for a wide variety of organizations. You can use the predefined policies as applicable for your industry and region, or you can refine the policies to meet your needs.

For more information about the predefined policies, refer to Predefined Policies and Classifiers.

---

**Warning**

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

---

### Adding a predefined policy

1. Select Main > Policy Management > DLP Policies (or Discovery Policies) > Add predefined policy.
2. If you are looking at the policy templates for the first time, a wizard appears. Complete the fields as follows:
   - **Welcome**
   - **Regions**
   - **Industries**
   - **Finish**

---

**Welcome**

The Welcome screen contains introductory information about Websense predefined policies. Click **Next** when you’re ready to proceed.
Regions

On 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.

Industries

1. On 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.

2. Click **Next**.

Finish

The **Finish** screen appears, summarizing your selections. Click **Finish**. Refer to **Policy list, page 76** for information on the resulting screen.

Policy list

The **Policy Library** screen shows 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.

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 **Use Policies**.

Many times, these predefined 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 can create custom policies using wizards as well. Refer to **Defining Resources, page 171** for information on creating policies for your network and endpoint.
Using Predefined Policies

Changing the policies you selected

To add predefined policies to the list you've chosen:

1. Select Main > Policy Management > DLP Policies (or Discovery Policies) > Add Predefined Policies.
2. Select the category of policy you want to change from the drop-down list, or select All categories.
3. Click View, then choose whether you want to see the most commonly used policies or all policies. This clears the previously selected policies so you can choose new ones, so you are asked to confirm the action.
4. Expand the tree in the left pane to view additional policy categories and the policy names themselves.
5. Highlight a policy name to view details about the policy in the right pane. This includes a description, and a list of the rules and exceptions it contains.
6. Select the policy or policies to add, and click Use Policies. The policies you chose are applied to your organization.

Changing your industry or region

To change the selected industries and regions for your policies:

1. Select Main > Policy Management > DLP Policies (or Discovery Policies) > Add Predefined Policies.
2. Select the category of policy you want to change from the drop-down list, or select **All categories**.

3. At the top of the screen, locate the sentence:
   Displaying policies from *n* industries in *n* regions.

4. To change industries, click the industries link.

5. To change regions, click the regions link.
Creating Custom DLP Policies

To create a custom policy, do the following:

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

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 Main > Policy Management > Resources.

Related topics:
- Managing rules, page 100
- Adding exceptions, page 101
- Defining Resources, page 171
Creating Custom DLP Policies

Custom Policy Wizard - General

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:
● Custom Policy Wizard - Condition, page 80

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The name for this policy.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the rule for this policy. If this box is unselected, the rule is present, but disabled.</td>
</tr>
<tr>
<td>Policy description</td>
<td>Enter a description for this policy.</td>
</tr>
<tr>
<td>Policy owners</td>
<td>If configured, policy owners receive notifications of breaches. To define an owner or owners for this DLP policy: 1. Click Edit. 2. Select one or more owners from the resulting box. See Selecting items to include or exclude in a policy, page 49 for instructions. 3. Click OK.</td>
</tr>
<tr>
<td>Use the policy name for the rule name</td>
<td>Every policy has one or more rules. A rule will automatically be added to this policy, based on the properties you set on subsequent pages of this wizard. Select this option if you want the rule for this policy to have the same name as the policy.</td>
</tr>
<tr>
<td>Use a custom name for the rule</td>
<td>Select this option to define a custom name for this rule, then enter a name and description for this rule.</td>
</tr>
</tbody>
</table>

Custom Policy Wizard - Condition

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:
● Classifying Content, page 107
● Custom Policy Wizard - Severity & Action, page 85

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.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 or classifiers to use. When you choose this option, indicate whether you want to trigger incidents when the threshold is matched in individual parts or the sum of all parts.  
    ■ **the transaction as a whole** - Select this if you want to trigger an incident if the sum of all matches in the transaction exceeds the threshold you set. For example, if you set a threshold of 3, then a transaction with 2 matches in the message body and one match in the subject line triggers an incident.  
    ■ **each part separately** - Select this if you want an incident triggered only when the threshold it reached in any one part of the transaction. For example, there would have to be 3 matches in the body or 3 in the subject line or other message part for an incident to be triggered. |
Initially, you may have no content classifiers or attributes defined. To add one, click Add, then select from the following:

- **Patterns & Phrases** - Select this option to add a regular expression, a key phrase, or a dictionary.
- **File Properties** - Select this option to add a file name, type or size to the condition.
- **Fingerprint** - Select this option to add a file or database fingerprint classifier to the condition.
- **Machine Learning** - Select this option to add a machine learning classifier to the condition. Machine learning lets you provide examples of the data that you want to protect, so the system can learn from them and identify items of a similar nature.
- **Transaction Size** - detect transactions of the specified size or larger.
- **Number of Email Attachments** - applies to email transactions only. Detect email messages with a certain number of attachments or greater
- **Number of Email Destinations** - applies to email transactions only. Detect messages sent to a specified number of domains or greater

To delete a condition from the rule, select the condition and click Remove.

**Threshold**

To edit a condition’s threshold, that is, the number of matches that trigger an incident, click a hyperlink in the Properties column. If you are working with dictionary classifiers, the weights of the dictionary’s phrases are taken into account when determining if a threshold is reached. See *Adding a dictionary classifier, page 120* for more information.

See also, *Viewing or editing conditions and thresholds, page 83.*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add or remove content classifiers or attributes to the condition. | Initially, you may have no content classifiers or attributes defined. To add one, click Add, then select from the following:  
  - **Patterns & Phrases** - Select this option to add a regular expression, a key phrase, or a dictionary.  
  - **File Properties** - Select this option to add a file name, type or size to the condition.  
  - **Fingerprint** - Select this option to add a file or database fingerprint classifier to the condition.  
  - **Machine Learning** - Select this option to add a machine learning classifier to the condition. Machine learning lets you provide examples of the data that you want to protect, so the system can learn from them and identify items of a similar nature.  
  - **Transaction Size** - detect transactions of the specified size or larger.  
  - **Number of Email Attachments** - applies to email transactions only. Detect email messages with a certain number of attachments or greater  
  - **Number of Email Destinations** - applies to email transactions only. Detect messages sent to a specified number of domains or greater  
  
  To delete a condition from the rule, select the condition and click Remove.  

**Threshold**

To edit a condition’s threshold, that is, the number of matches that trigger an incident, click a hyperlink in the Properties column. If you are working with dictionary classifiers, the weights of the dictionary’s phrases are taken into account when determining if a threshold is reached. See *Adding a dictionary classifier, page 120* for more information.

See also, *Viewing or editing conditions and thresholds, page 83.*

| Condition Relations | If you have more than one condition defined, indicate when the rule should be triggered. Either when:  
  - **All conditions matched** - All of the selected conditions must be met to trigger the rule.  
  - **At least one of the conditions matched** - one of the selected conditions must be met to trigger the rule.  
  - **Custom** - Lets you define under what condition you want the rule triggered.  

If you choose Custom, do the following:  
1. Double-click a condition name to add it to the formula box.  
2. Click the And, Or, or Not button to define a condition.  
3. Double-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.  

| | |
Creating Custom DLP Policies

**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 for marketing purposes. 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 key phrase 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.

**Viewing or editing conditions and thresholds**

Click a hyperlink in the Properties column to view and edit the properties of a condition line, including the name, description, threshold, type of matches and email fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content classifier name</td>
<td>The name for this content classifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this content classifier.</td>
</tr>
</tbody>
</table>
| Threshold                     | A condition’s threshold is the number of matches that trigger an incident. Select one of the following:  
  - At least - select the minimum number of matches that must be made. Valid values are 1-999.  
  - Between - select an exact range of matches that must be made. Valid values are 1-999.  
  - No match exists - trigger the rule if there are no matches. |
| Calculate the threshold       | Does not apply to fingerprinting. Define how the threshold numbers are calculated:  
  - Count only unique matches for the transaction  
  - Count all matches, even duplicates |
| Email Fields                  | Click Email Fields to view and select the email fields to search for this condition. |
Creating Custom DLP Policies

If you are working with fingerprint classifiers, there are more configurable options. See *Fingerprint classifiers* later in this topic.

If you are working with dictionary classifiers, the weights of the dictionary’s phrases are taken into account when determining if a threshold is reached. See *Adding a dictionary classifier*, page 120 for more information.

### Fingerprint classifiers

If you click the Properties link of a database classifier, you get a page with two tabs — General and Properties. The General tab is for field selection and the Properties tab is where you define the threshold and email fields described in the table above. If you highlight a database records classifier, the screen displays the field (or column) names of the table to which this classifier corresponds. Select the fields you want to have scanned. You can select up to 32 fields per table.

For endpoints, the number of fields you select for a database fingerprinting classifier can affect accuracy. For the most accurate results, you should scan 3 or more fields. If you want to scan only one field for this rule, Websense recommends that you set a minimum threshold of 5 to reduce the likelihood of unintended matches. (In other words, trigger an incident when there are 5 or more matches on this field.) If you do not, the system changes the threshold for you.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search the most common fields</td>
<td>Select to search email fields that pose the highest risk of a policy breach. The fields are searched for the key phrase, regular expression, or dictionary terms you specify. This is the default.</td>
</tr>
</tbody>
</table>
| Search specific fields | Select to search only specific fields of the email message. Choose one or more of the following:  
  - **Attachment** - search only in email attachments  
  - **Subject** - search only in the subject line of the email message  
  - **Body** - search only in the main body of the email message  
  - **From** - search only in the From field of the email message  
  - **To** - search only in the To field of the email message  
  - **Cc** - search only in the carbon copy field of the email message  
  - **Bcc** - search only in the blind carbon copy field of the email message  
  - **Other header** - search in headers that are not covered by the above options.  
  - **All headers** - Search in all headers not covered in the above options. This includes all standard headers—such as Date, Message-ID, or Importance—as well as non-standard headers (x-headers) added during the sending of an email. Some examples of x-headers are x-mailer, x-spam-reason, and x-originating-ip.  
  - **User-defined header** - Some users define their own x-headers to add custom information to the header part of email messages. For example, they might create an x-header such as “X-MyCompany: Copyright 2011 MyCompany”. If you have user-defined email headers, and you’d like to search for these, enter the header name here. |

If you are working with dictionary classifiers, the weights of the dictionary’s phrases are taken into account when determining if a threshold is reached. See *Adding a dictionary classifier*, page 120 for more information.
If you want to scan 2 fields, set the minimum threshold to 3 or more. (Trigger an incident when 3 or more field1/field2 combinations are detected.)

<table>
<thead>
<tr>
<th>Number of Fields Chosen</th>
<th>Minimum Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3 or more</td>
<td>1</td>
</tr>
</tbody>
</table>

**Note**
If you are defining a condition for both network and endpoint resources, the threshold is changed for the endpoint only. Network resources retain the threshold you define on the Properties tab.

For more information on creating fingerprint classifiers, see *Database fingerprinting*, page 144.

**Custom Policy Wizard - Severity & Action**

On this screen, define whether incidents should be triggered every time this rule is matched or for the accumulation of matches for a particular source over time.
Also define how matches are counted, the threshold for triggering the incident, the severity to assign breaches, and the action plan to apply.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an incident for every matched condition</td>
<td>Select this option if you want an incident generated every time a condition in this rule is matched. For example, if a user sends an email message containing sensitive content, then prints the message, you would like 2 incidents generated.</td>
</tr>
<tr>
<td>Accumulate matches before creating an incident (Drip DLP)</td>
<td>Select this option if you want the system to accumulate matches over time and create incidents when a threshold is met. When this option is selected, the system remembers user activity and generates incidents for matches that occur within a defined period. If you select this option, indicate the time period to monitor and whether to count matches or transactions. • Count transactions - tells the system to count incident transactions as they accumulate for a given source, even though each incident can have multiple triggers. • Count unique matches - tells the system to count violation triggers that accumulate for a source, but only triggers that are unique. For example, you create a rule that does not permit 10 different credit card numbers to be sent within 1 hour. If a user sends 1 message with 20 credit card numbers, 1 violation trigger is counted. But if the user sends 20 email messages with the same credit card number, no triggers are counted, because the numbers were not unique. • Count all matches - tells the system to count all violation triggers that accumulate for a source, even duplicates. In the example above, even if the user sent 20 messages with the same credit card number, 20 triggers are counted. Matches and transactions are counted individually for each source, such as user name or IP address, and they are counted only on the policy engine that detects them. Incidents are generated only when the threshold is met on a single policy engine. The system counts matches by default. Note that the time period is a sliding window. It resets every time a match is detected.</td>
</tr>
<tr>
<td>When there are more than: n matches/transactions</td>
<td>Define the threshold for triggering an incident. For example, trigger an incident when there are more than 3 matches. Note: If you selected the cumulative option and the threshold is not met, the match count is 0.</td>
</tr>
<tr>
<td>The severity is:</td>
<td>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.</td>
</tr>
</tbody>
</table>
Creating Custom DLP Policies

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 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 that use it.

Click the icon to create a new action plan. See *Action Plans*, page 189, for details.

Note that the action applies only to the match that exceeded the threshold—the one that created the incident—and subsequent matches. Initial matches are permitted.

### Advanced

Click **Advanced** to define severity at a more granular level. This option does not apply to TRITON AP-WEB customers.

1. Specify what to do if some matches/transactions are detected in the specified time period, but the threshold is not met. Do you want the system to continue counting?
2. Define parameters for the advanced configuration. 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.

### Define matches

This option does not apply to TRITON AP-WEB 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.
Custom Policy Wizard - Source

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>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 49 for instructions on using the selector tool.</td>
</tr>
</tbody>
</table>
| Endpoints | - **Machine type** - Select the type of endpoint machines to analyze: laptops, static devices such as PC workstations, or all machines.  
- **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. |

Related topics:
- Custom Policy Wizard - Destination, page 88
- Sources and destinations, page 173

Custom Policy Wizard - Destination

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

The Destination page varies depending on your subscription. You may see:
- **Standard options**
- **TRITON AP-WEB mode**
- **TRITON AP-EMAIL mode**

For information on the file sizes that are support for the various destination channels, see File Size Limits in the Websense Technical Library.
Creating Custom DLP Policies

## Standard options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Email</strong></td>
<td>Select Network Email if you want to monitor email going through your network. By default, email is analyzed on all network destinations. Click Edit to select the destinations this policy should analyze, for example network computers or domains. (See Selecting items to include or exclude in a policy, page 49 for instructions on using the selector tool.) If you are using the TRITON AP-EMAIL module, click Direction to select the traffic to monitor: inbound, outbound, internal, or all 3. The protector monitor all traffic directed to them. All transactions are regarded as outbound.</td>
</tr>
<tr>
<td><strong>Endpoint Email</strong></td>
<td>Select Endpoint Email if you want to monitor email on endpoint machines (requires TRITON AP-ENDPOINT DLP). By default, email is analyzed on all endpoint destinations. Click Edit to select the domains this policy should analyze. (See Selecting items to include or exclude in a policy, page 49 for instructions on using the selector tool.) If you are using the TRITON AP-EMAIL module, click Direction to select the traffic to monitor: outbound or internal. (Outbound is the default.) You cannot monitor inbound email on endpoints. Note that protector can also define the email direction (as configured in: Settings &gt; Deployment &gt; System Modules &gt; Services &gt; SMTP &gt; SMTP Filter). Also note that if you choose a direction that is not configured under endpoint Email Domains, endpoint email traffic is not analyzed. Select Settings &gt; General &gt; System &gt; Endpoint &gt; Email Domains to define, in general, which directions may be monitored for endpoint email. Here, define which email directions should be enforced for this rule. For a complete list of endpoint email applications that TRITON AP-DATA supports, see TRITON AP-ENDPOINT DLP endpoint applications.</td>
</tr>
<tr>
<td><strong>Mobile Email</strong></td>
<td>Select Mobile Email if you want to monitor email that is being sent to users mobile devices, then select whose devices to monitor. You can select user directory entries (users and groups), business units, or custom users. By default all users’ email is analyzed when it is being synchronized to mobile devices. Click Edit to select the users to monitor. (See Selecting items to include or exclude in a policy, page 49 for instructions on using the selector tool.)</td>
</tr>
</tbody>
</table>

Data Security Manager Help ► 89
Creating Custom DLP Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Web            | Select this check box if you want to prevent or monitor users from posting sensitive data to networks, domains, business units, URL categories, directory entries, countries, or custom computers via any of the following Web channels:  
  ● FTP - file transfer protocol (FTP) sites  
  ● Chat - instant messenger applications  
  ● Plain text - unformatted textual content  
  ● HTTP - websites, blogs, and forums via HTTP  
  ● HTTPS - websites, blogs, and forums via secure HTTP  
  ● Endpoint HTTP - websites, blogs, and forums accessed by endpoint machines over HTTP  
  ● Endpoint HTTPS - websites, blogs, and forums accessed by endpoint machines over HTTPS  
  By default, posts to all Web destinations are analyzed. Click **Edit** to select the destinations to analyze.  
  See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool.  
  Note that several SaaS domains are excluded from analysis by default. You can exclude more domains as needed or remove some from the exclusion list. You can also customize the list of resources that are excluded from Web policies by default. For more information, see *Business Units, page 181*.  
  Click **Channels** to select or deselect individual Web channels.  
  For a complete list of endpoint browsers that TRITON AP-DATA supports, see *Selecting endpoint destination channels to monitor*.

| Endpoint Printing | Select this check box if you want to analyze files that endpoint users send to printers.  
  (Requires TRITON AP-ENDPOINT DLP.)  
  To select the printers to analyze click **Edit**.  
  See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool. |
Creating Custom DLP Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 49 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 .exe, .csv, .xls/xlsx, .pdf, .txt, .mht, and .doc/.docx files.  
  ● When files are saved to any other local folder, it analyzes all file types.  
The applications that the system supports out of the box are found in the Technical Library article, **TRITON AP-ENDPOINT DLP Applications**. You can also add custom applications. |
Creating Custom DLP Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Endpoint Removable Media     | 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 **Edit**.  
See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool.  
For a complete list of endpoint removable devices that TRITON AP-DATA supports, see *Selecting endpoint destination channels to monitor*.  
**Note:** If your endpoints are Linux-based, you cannot share removable media devices through NFS. |
| Endpoint LAN                 | 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, outbound traffic for all networks is covered—that is, traffic going from the endpoint to all LANs. To select a network to analyze, click **Edit**. See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool.  
With TRITON AP-DATA:  
- You can specify a list of IPs, hostnames, 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 the system does not resolve them. For this reason, if you want to block or allow access to a computer, you must specify it FQDN, hostname, mapped drive, and any other address the user might use. Alternatively, always block or allow access using hostname and inform your users to use hostname.  
- You can intercept data from an endpoint client.  
**Note:**  
- Endpoint LAN control is applicable to Windows File Sharing only.  
- If access to the LAN requires user credentials, files larger than 10 MB are handled as huge files which are only searched for file size, file name and binary fingerprint. Files smaller than 10 MB are fully analyzed. The huge file limit for other channels is 100 MB. |
TRITON AP-WEB mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit  | By default, Web channels are analyzed on all destinations. For TRITON AP-WEB, this includes:  
- **FTP** - file transfer protocol (FTP) or FTP-over-HTTP  
- **Web** - websites, blogs, and forums via HTTP and HTTPS  
Click **Edit** to select the destinations to analyze. See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool. |

TRITON AP-EMAIL mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit  | By default, all network email is analyzed in all directions: outbound, inbound, and internal.  
Click **Edit** to select the email destination to analyze. See *Selecting items to include or exclude in a policy, page 49* for instructions on using the selector tool. |

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.

Selecting a content classifier

On the Conditions tab of the custom policy wizard, you can add content classifiers or email attributes to the policy. Using content classifiers, you can classify account...
numbers, credit card numbers, industry terms, and similar items as sensitive data. Using attributes, you can identify the email components to monitor.

<table>
<thead>
<tr>
<th>Classifier type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Patterns &amp; Phrases</strong></td>
<td>Lets you classify data by regular expression patterns, key phrases, and dictionaries. RegEx patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.</td>
</tr>
<tr>
<td><strong>File Properties</strong></td>
<td>Lets you classify data by file name, type or size. File name identifies files by their extension. File type identifies files by metadata.</td>
</tr>
<tr>
<td><strong>Fingerprint</strong></td>
<td>Lets you fingerprint files or directories, including SharePoint directories, and database records directly from your database table, Salesforce table, or CSV file.</td>
</tr>
<tr>
<td><strong>Machine Learning</strong></td>
<td>Lets you provide examples of the data that you want to protect, so the system can learn from them and identify items of a similar nature.</td>
</tr>
<tr>
<td><strong>Transaction Size</strong></td>
<td>Lets you monitor transactions that exceed a size limit, such as email messages more than 10 MB.</td>
</tr>
<tr>
<td><strong>Number of Email Attachments</strong></td>
<td>Lets you monitor email messages containing multiple attachments.</td>
</tr>
<tr>
<td><strong>Number of Email Destinations</strong></td>
<td>Lets you monitor email messages being sent to multiple destination domains.</td>
</tr>
</tbody>
</table>

**Patterns & Phrases**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:

- **General tab**, page 94
- **Properties tab**, page 95

**General tab**

This page lists the content classifiers that you’ve added to this rule, if any. Search for existing classifiers, then select the classifier that applies to you. If you can’t find the
one you need, create a new classifier. Sort or filter columns to help you locate the classifier you need.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for</td>
<td>Enter a key term and click the magnifying glass to search for a content classifier that pertains to you. For example, enter credit card. You can include wildcards in your search, such as “credit*”.</td>
</tr>
<tr>
<td>New</td>
<td>Click New to add a new content classifier to the rule. You can add as many as you need. Select from the following classifier types:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Regular Expression</strong> - a string that is used to describe or match a set of strings, according to certain syntax rules. When the extracted text from a transaction is scanned, the system uses regular expressions to find strings in the text that match patterns for confidential information.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Key Phrase</strong> - an exact keyword or phrase (such as “top secret” or “confidential”) in content intended for an external recipient may indicate that classified information is being distributed. The system can block the distribution of this information.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Dictionary</strong> - a container for words and expressions belonging to the same language. Many dictionaries are built into TRITON AP-DATA, including lists for medical conditions, financial terms, legal terms, and credit card terms. You can create or customize a dictionary list that pertains to your line of business and then use this list in your policies. You can also assign each term a weight so when one term is detected, more points are given towards a threshold than when another term is detected.</td>
</tr>
</tbody>
</table>

**Properties tab**

Define the threshold and email fields in which the specific classifier will be searched.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>A condition’s threshold is the number of matches that trigger an incident. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>● <strong>At least</strong> - select the minimum number of matches that must be made. Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Between</strong> - select an exact range of matches that must be made. Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>● <strong>No match exists</strong> - trigger the rule if there are no matches.</td>
</tr>
<tr>
<td>Calculate the threshold</td>
<td>Define how the threshold numbers are calculated:</td>
</tr>
<tr>
<td></td>
<td>● Count only unique matches</td>
</tr>
<tr>
<td></td>
<td>● Count all matches, even duplicates</td>
</tr>
<tr>
<td>Email Fields</td>
<td>Click <strong>Email Fields</strong> to view and select the email fields to search for this condition.</td>
</tr>
</tbody>
</table>
Creating Custom DLP Policies

File Properties

General tab

The General tab lists all file property classifiers.

The Type column indicates whether the classifier is predefined or user-defined.

The Classifier Type indicates whether this is a file name, file type, or file size classifier. File-type classifiers group like files together. For example, office documents and pictures are 2 types of files. File-name classifiers identify files by file-name extension (such as *.docx) or the file name itself (such as myfile*.doc). And file-size classifiers identify files by their size. See File properties, page 123 for more details.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search in all the email fields</td>
<td>Select to search email fields that pose the highest risk of a policy breach. The fields are searched for the key phrase, regular expression, or dictionary terms you specify. This is the default.</td>
</tr>
<tr>
<td>Search only in these fields</td>
<td>Select to search only specific fields of the email message. Choose one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Attachment</strong> - search only in email attachments</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subject</strong> - search only in the subject line of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>Body</strong> - search only in the main body of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>From</strong> - search only in the From field of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>To</strong> - search only in the To field of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cc</strong> - search only in the carbon copy field of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bcc</strong> - search only in the blind carbon copy field of the email message</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other header</strong> - search in headers that are not covered by the above options.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>All headers</strong> - Search in all headers not covered in the above options. This includes all standard headers—such as Date, Message-ID, or Importance—as well as non-standard headers (x-headers) added during the sending of an email. Some examples of x-headers are x-mailer, x-spam-reason, and x-originating-ip.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>User-defined header</strong> - Some users define their own x-headers to add custom information to the header part of email messages. For example, they might create an x-header such as “X-MyCompany: Copyright 2011 MyCompany”. If you have user-defined email headers, and you’d like to search for these, enter the header name here.</td>
</tr>
</tbody>
</table>

Related topics:

- General tab, page 96
- Properties tab, page 97
Select the classifier you want to add to the policy’s rule.
Sort or filter columns to help you locate the classifier you need.

Properties tab

The Properties tab lets you configure the threshold.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Threshold   | A condition’s threshold is the number of matches that trigger an incident. Select one of the following:  
  - **At least** - select the minimum number of matches that must be made. Valid values are 1-999.  
  - **Between** - select an exact range of matches that must be made. Valid values are 1-999.  
  - **No match exists** - trigger the rule if there are no matches.  
| Calculate the threshold | Define how the threshold numbers are calculated:  
  - Count only unique matches  
  - Count all matches, even duplicates |

Fingerprint

There are 2 types of fingerprint classifiers that can be added: files or database records. The General tab displays all classifiers from both types. Sort or filter columns to help you locate the classifier you need.

If you highlight a database records classifier, the bottom of the screen displays the field (or column) names of the selected table. Select the fields you want to have scanned. You can select up to 32 fields per table.

For endpoints, the number of fields you select for a database fingerprinting classifier can affect accuracy. For the most accurate results, you should scan 3 or more fields. If you want to scan only one field for this rule, Websense recommends that you set a minimum threshold of 5 to reduce the likelihood of unintended matches. (In other words, trigger an incident when there are 5 or more matches on this field.) If you do not, the system changes the threshold for you.
If you want to scan 2 fields, then set the minimum threshold to 3 or more. (Trigger an incident when 3 or more field1/field2 combinations are detected.)

<table>
<thead>
<tr>
<th>Number of Fields Chosen</th>
<th>Minimum Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3 or more</td>
<td>1</td>
</tr>
</tbody>
</table>

Select the *Properties tab* to configure a threshold.

**Note**
If you are defining a condition for both network and endpoint resources, the threshold is changed for the endpoint only. Network resources retain the threshold you define on the Properties tab.

For more information on creating fingerprint classifiers, see *Database fingerprinting*, page 144.

**Properties tab**

Define the threshold and email fields in which the specific classifier will be searched.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>A condition’s threshold is the number of matches that trigger an incident. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>At least</strong> - select the minimum number of matches that must be made. Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Between</strong> - select an exact range of matches that must be made. Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No match exists</strong> - trigger the rule if there are no matches.</td>
</tr>
<tr>
<td>Email Fields</td>
<td>Click <strong>Email Fields</strong> to view and select the email fields to search for this condition.</td>
</tr>
</tbody>
</table>
Machine Learning

This page lists all the machine learning classifiers that are ready for use (finished processing). Select the classifier to use in this rule. To help you find the classifier you need, you can sort the columns by name, description, or accuracy. Click the down arrows to do so.

Accuracy denotes the accuracy expected for classifier matches, given the positive, negative, and all-documents examples provided and the complexity of the data.
Creating Custom DLP Policies

Transaction Size

Select the size of transactions to monitor. For example, for email channels, choose 25 MB if you want the system to detect email messages 25 MB or larger, but you’re not concerned about messages smaller than 25 MB, even if there is a match. For Web channels, choose 25 MB if you want to detect Web posts greater than or equal to 25 MB. The default size is 10 MB.

Number of Email Attachments

Select the number of attachments to monitor. For example, choose 10 if you want the system to detect messages with 10 or more attachments, but you’re not concerned about messages with fewer than 10, even if there is a match. The default number is 20.

Number of Email Destinations

Sometimes you may want to block messages sent to multiple destination domains, because this may indicate spam.

Specify the number of destination domains to detect. Email messages sent to this number of domains (or more) trigger the policy. The default number of domains is 25.

Also, select which email fields to monitor—the To field (To), copy field (Cc), or blind copy field (Bcc). To and Cc are selected by default.

This option applies to outbound email only.

Managing rules

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 a rule is created automatically. You do so by creating a content classifier and the system creates a rule from that.
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 170 for more information.)

When you are looking at a policy, you can click a rule in the tree view and select **Edit, Add > 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 **Add > Exception**. For information on adding exceptions, please see *Adding exceptions*.

### Adding exceptions

Most rules have exceptions.

In TRITON AP-DATA, exceptions and rules are tightly linked.

1. When there is a transaction, rules are evaluated.
2. If a rule is matched, its exception is evaluated, if any.
3. If the exception is matched, the exception action is taken.

In other words, exceptions are evaluated only when their rules are matched.

Unlike rules, exceptions cannot be cumulative.

You can highlight a rule or an exception from the toolbar to add an exception to a rule. On the **Main** tab under Policy Management, select DLP Policies or Discovery Policies. Click a rule and select **Add > Exception** from the toolbar.

Like policies, exceptions have levels that define execution priority order. See *Rearranging exceptions, page 102* 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.

Adding a new exception

Exceptions are very much like rules. To add a new exception, click a rule in the policy tree view and select Add > Exception. (You cannot add an exception to a cumulative rule.)

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:
- Custom Policy Wizard - General, page 80

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The name of the affected policy.</td>
</tr>
<tr>
<td>Rule name</td>
<td>The rule related to this exception.</td>
</tr>
<tr>
<td>Exception name</td>
<td>Enter a name for this exception.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this exception.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click to enable or disable this exception.</td>
</tr>
</tbody>
</table>

Exception Wizard - Properties

Related topics:
- Custom Policy Wizard - Source, page 88
- Custom Policy Wizard - Destination, page 88
- Custom Policy Wizard - Condition, page 80

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception Properties</td>
<td>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.</td>
</tr>
<tr>
<td>Condition</td>
<td>Select <strong>Condition</strong> if you want to change the condition parameters established for the rule, such as the content classifier, threshold, or condition relations.</td>
</tr>
<tr>
<td>Source</td>
<td>Select <strong>Source</strong> if you want to change the source of data defined for the rule.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select <strong>Destination</strong> if you want to change the destination of data defined for the rule.</td>
</tr>
</tbody>
</table>

| 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 Custom Policy Wizard - Condition, page 80 for explanations of the fields on this screen. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specify the exception you want to make for the rule’s source. For example, if a rule defined action plan “Audit only” for all computers, but you want to execute “Audit and notify” for laptops, click <strong>Edit</strong> then add laptops to the Available List. If you want to execute the “Audit and notify” for all laptops but John Smith’s, add John Smith’s laptop to the Exclude list. See <em>Custom Policy Wizard - Source, page 88</em> for explanations of the fields on this screen.</td>
</tr>
<tr>
<td>Destination</td>
<td>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 <em>Custom Policy Wizard - Destination, page 88</em> for explanations of the fields on this screen.</td>
</tr>
</tbody>
</table>
### Exception Wizard - Severity & Action

**Data Security Manager Help | TRITON AP-DATA | Version 8.0.x**

Related topics:
- *Custom Policy Wizard - Severity & Action, page 85*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 exception are of low importance. The policy breach is minor.  
- **Medium**: Incidents that match this exception are of medium importance. The policy breach is moderate.  
- **High**: Incidents that match this exception 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 **edit** 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 **create** icon to create a new action plan. See **Action Plans, page 189**, for details. |
| Advanced | This option does not apply to TRITON AP-WEB 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 to TRITON AP-WEB 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 rule you selected.
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 the Websense patented PreciseID fingerprinting technology; or you can provide examples of the type of data to protect so the system can learn from it and make decisions.

To classify your content:

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

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attributes</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Patterns &amp; Phrases</strong></td>
<td>Lets you classify data by regular expression patterns, key phrases, and dictionaries. RegEx patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.</td>
</tr>
<tr>
<td><strong>File properties</strong></td>
<td>Lets you classify data by file name, type or size. File name identifies files by their extension. File type identifies files by metadata.</td>
</tr>
<tr>
<td><strong>Fingerprints</strong></td>
<td></td>
</tr>
<tr>
<td><strong>File fingerprinting</strong></td>
<td>Lets you fingerprint files or directories, including Microsoft SharePoint and IBM Domino directories.</td>
</tr>
<tr>
<td><strong>Database fingerprinting</strong></td>
<td>Lets you fingerprint database records directly from your database table, Salesforce table, or CSV file.</td>
</tr>
<tr>
<td><strong>Machine Learning</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Machine learning</strong></td>
<td>Lets you provide examples of the data that you want to protect, so the system can learn from them and identify data of a similar nature.</td>
</tr>
</tbody>
</table>

Websense provides predefined classifiers for the most common use cases. These are described in **Predefined Policies and Classifiers**. 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 granularity of each content classifier.

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 the system does not analyze all types of data. For example, it does not analyze the metadata of plain text files or the data inside Windows .cab files.

If you are going to create a database fingerprinting classifier, read *Preparing for database fingerprinting*, page 146 and *Creating a validation script*, page 147. TRITON AP-DATA 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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>![icon]</td>
<td>Opens a dialog so you can create a new classifier of the selected type.</td>
</tr>
<tr>
<td>Delete</td>
<td>![icon]</td>
<td>Deletes the selected classifier. Be sure to check where the classifier’s used before deleting it. (See Where Used, below.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You can delete only one classifier at a time. If you’re deleting a fingerprint classifier and the crawler is unresponsive, you’re asked to delete the classifier manually. (See Manually deleting fingerprinting classifiers, page 111 for instructions.)</td>
</tr>
<tr>
<td>Create Rule from Classifier</td>
<td>![icon]</td>
<td>Creates a rule from the selected classifier and lets you mark it for use in an existing or new policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You can create a rule from only one classifier at a time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Creating a rule from a content classifier for more details on this shortcut.</td>
</tr>
<tr>
<td>Where Used</td>
<td>![icon]</td>
<td>Shows which policies, rules, and exceptions use this classifier.</td>
</tr>
</tbody>
</table>

The fingerprinting and machine learning classifiers have additional menu options.

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>![icon]</td>
<td>Begins the fingerprinting or machine learning scan. Alerts that the task will be moved into manual mode.</td>
</tr>
<tr>
<td>Pause</td>
<td>![icon]</td>
<td>Fingerprinting only. Pauses the scan.</td>
</tr>
</tbody>
</table>
In addition, the fingerprinting classifiers offer a Details pane on the right to show statistics about the scan and scheduler. See Details pane, page 111 for more information.

### Button Icon Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>![Stop Icon]</td>
<td>Stops the fingerprinting or machine learning scan. Alerts that the task will resume at the next scheduled time or the next time it is run manually.</td>
</tr>
</tbody>
</table>

More Actions

In addition to Create Rule from Classifier and Where Used, fingerprinting and machine learning classifiers offer a reporting option under More Actions:

**Download Fingerprinting Report** - Database fingerprinting only. Downloads a detailed report on fingerprinting activities.

**Download Machine Learning Report** - Machine learning classifiers only. Downloads a detailed report on machine learning processes. Using this report, you can:

- Understand the expected accuracy of the classifier (percentage of misclassified files). You can decide how to use the classifier or adjust the sensitivity as needed in the Details pane.

- Discover documents that were found when processing the positive examples folders but did not appear to belong there. Learn the accuracy of the classifier with and without these documents. Use the Details pane to indicate whether or not to ignore inconsistent examples.
Manually deleting fingerprinting classifiers

If the crawler is unresponsive for any reason when you delete a fingerprinting classifier from the management server, it is not alerted that you’ve deleted the classifier. When the crawler becomes responsive, it will continue to run the fingerprinting scan as scheduled and consume unnecessary resources.

To avoid these repercussions, you must manually delete the classifier from its associated crawler.

The Data Security manager warns you in this situation, and asks if you want to continue. If you do, manually delete the classifier as follows:

1. Identify the ID of the job to delete in one of two ways:
   a. View the TRITON AP-DATA System Log (Main > Status > System Log) and search for the entry stating the classifier was deleted. For example:
      The classifier Fingerprint_Name ID 8e76b07c-e8e5-43b7-b991-9fc2e8da8793 was deleted from the TRITON management server, but not from the crawler, Crawler_Name 10.201.33.1.
   b. Log onto the crawler machine associated with the discovery task.
      i. Switch to the %DSS_HOME%/DiscoveryJobs folder.
      ii. Search for the relevant classifier and ID by opening each job, one at a time, and examining the first line of its definition.xml file.
      For example, the first line of one file might show:
      <job type="fingerprinting" id="3178b4f9-96fe-4554-ad1d-eaa29fa23374" name="ora3" altID="168476">
      If your task was named “ora3”, then you know the ID is 3178b4f9-96fe-4554-ad1d-eaa29fa23374.

2. Delete the job:
   a. On the crawler machine identified above, switch to the %DSS_HOME%/packages/Services folder.
   b. Run the following command:
      Python WorkSchedulerWebServiceClient.pyc -o deleteJob -j #jobId#
      Where jobId is the ID number you identified in step 1.

Details pane

Fingerprinting and machine learning 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 less detail. Click the links, if offered, to see additional information on a particular statistic.
### Fingerprinting details

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

### Fingerprint Statistics

Statistics about the data that is used by the policies that include this classifier. This data was already fingerprinted and committed. (After a file is fingerprinted, it’s inserted to the fingerprint repository and then committed to be used as part of the classifier. Commit is done after stop, pause, each 2500 files, and the end of a run.)

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprinted files/records</td>
<td>The total number of analyzed items. Click the link to view a list of all the files that were fingerprinted, along with details such as fingerprint date, status, and version; folder and file name; and file size. (File version refers to the number of times a file has been fingerprinted. The first time a file is fingerprinted, the fingerprint is version 1. The second time, it is version 2, and so on.) To delete a fingerprint, select the file and click <strong>Delete</strong> on the toolbar.</td>
</tr>
<tr>
<td>Fingerprint size</td>
<td>The total size of analyzed items</td>
</tr>
<tr>
<td>Endpoint package size</td>
<td>The size of the endpoint package</td>
</tr>
<tr>
<td>Used space on endpoint</td>
<td>The total amount of disk space used on the endpoint</td>
</tr>
</tbody>
</table>

### Last Scan Statistics

Details about the last scan that was run or the current scan (if one is still running).

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned files</td>
<td>The total number of items detected in the last scan</td>
</tr>
<tr>
<td>Scanned size</td>
<td>The size of items detected in the scan, all totaled. (Does not apply to database scans.)</td>
</tr>
<tr>
<td>Scan/fingerprinting progress</td>
<td>The progress of the scan, in percentage completed</td>
</tr>
<tr>
<td>Fingerprinted files/records</td>
<td>The number of items sent to the policy engine’s fingerprint repository</td>
</tr>
</tbody>
</table>
### Last Scan Statistics
Details about the last scan that was run or the current scan (if one is still running).

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed files</td>
<td>The number of files that could not be fingerprinted for some reason—such as access to the folder was denied or the file was not found. Click the link to see why fingerprinting failed for these files.</td>
</tr>
<tr>
<td>Filtered-out files</td>
<td>The files that were not included in the scan because of the file filters you specified when you defined the task. (These files that were ignored by the crawler because they matched a filter.) Click the link to see the precise file type, age, or size filter that was matched.</td>
</tr>
<tr>
<td>Estimated total files/</td>
<td>An estimate of the total number of items</td>
</tr>
<tr>
<td>records</td>
<td></td>
</tr>
<tr>
<td>Estimated total size</td>
<td>An estimate of the total size of items</td>
</tr>
</tbody>
</table>
Machine learning details

**Active Classifier**
Details about the machine learning classifier that is currently active. The examples were processed, the system was trained, and the scan completed. This classifier may be used in a policy.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>Expected rate of unintended and undetected matches (false positives and false negatives).</td>
</tr>
<tr>
<td>Last successful scan time</td>
<td>The time and date of the last successful scan</td>
</tr>
<tr>
<td>All documents folder</td>
<td>Path to the all documents folder</td>
</tr>
<tr>
<td>Positive examples folder</td>
<td>Path to the positive examples folder</td>
</tr>
<tr>
<td>Negative examples folder</td>
<td>Path to the negative examples folder</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>How sensitive the classifier is when detecting matches—in other words, how closely content has to match the positive examples to be considered an incident.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Wide</strong> is highly sensitive and errs on the restrictive side.</td>
</tr>
<tr>
<td></td>
<td>To avoid leaking sensitive data, it is more likely to produce a false positive (unintended match) than a false negative (content that is not detected).</td>
</tr>
<tr>
<td></td>
<td>● <strong>Default</strong> balances the number of false positives and false negatives.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Narrow</strong> is the least restrictive. It is more likely to let content through than to produce an unintended match.</td>
</tr>
<tr>
<td>Ignore inconsistent examples</td>
<td>Indicates whether to ignore documents that do not appear to belong to the positive examples folder or to use them as positive examples anyway.</td>
</tr>
<tr>
<td></td>
<td>To view a list of inconsistent example documents, download the Machine Learning report.</td>
</tr>
</tbody>
</table>
## Current Scan Statistics
To keep the machine learning classifier up to date, you should periodically rescan your examples folders. This section shows statistics about the latest scan. If the scan succeeds, it becomes the active classifier. If it fails, the Active Classifier and Current Scan Statistics are different.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run time</td>
<td>The time and date that the machine learning process last ran</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the current content scan. Possible statuses include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pre-processing (n files)</strong> - The system is locating and counting all the files in the positive example files, negative example files, and all documents folder.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Processing (x%)</strong> - The system is processing files in the sample set. The percentage shows the progress made on the total number of files.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Training (x%)</strong> - The system is applying algorithms and learning from your positive, negative, and all-documents sample sets.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reprocessing (x%)</strong> - The system is reprocessing files or in the case of large sample sets, processing additional files. The percentage shows the progress made on the total number of files.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Retraining (x%)</strong> - The system is applying algorithms to learn from the new or broader scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Completed</strong> - The current scan succeeded and has become an active classifier that you can use.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Completed with warnings</strong> - The current scan succeeded and has become an active classifier that you can use, but there were a few warnings that you might want to address. To view the warnings, click <strong>More Actions</strong> and download the machine learning report.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Failed</strong> - The scan could not be completed and the classifier cannot be used. To view the errors that were encountered, click <strong>More Actions</strong> and download the machine learning report.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Paused</strong> - The scan was manually paused using the toolbar button.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Stopped</strong> - The scan was manually stopped using the toolbar button.</td>
</tr>
</tbody>
</table>

Note that the status shown here may be different from the status shown in the Status column if you click **Refresh** in one area but not the other.

| All documents folder       | Path to the all documents folder                                           |
| All my documents           | Number of documents in the all documents folder                            |
| Positive examples folder   | Path to the positive examples folder                                       |
| Positive examples          | Number of documents in the positive examples folder                        |
| Negative examples folder   | Path to the negative examples folder                                       |
| Negative examples          | Number of documents in the negative examples folder                        |
Patterns & Phrases

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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

1. Click **Main > Policy Management > Content Classifiers**.
2. Select **Patterns & Phrases**. Both user-defined and built-in patterns are shown. These are distinguished by the icons and the Type column. You can sort the list by this column. Refer to **Regular Expression Patterns** for details about each predefined classifier.

Also shown are the existing dictionary and key phrase classifiers, if any.

Click **New** to add a new regular expression, key phrase, or dictionary, **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, TRITON AP-DATA 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}[\-\]\d{4})\b

Because a regular expression file contains many internal attributes, if it is improperly written it can create many false-positive incidents, slow down the system, and impede analysis.

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 phrases 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, the system 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, the system 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 phrases 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 or editing a regular expression 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 > Patterns & Phrases**. Click **New** from the menu bar, then select **Regular Expression**.

2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this pattern, such as Visa card. If this is a predefined pattern, this is uneditable.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this pattern, such as Visa credit card patterns. If this is a predefined pattern, this is uneditable.</td>
</tr>
</tbody>
</table>
Classifying Content

3. Click **OK**.

To base a classifier on an existing classifier:

1. Click **Main > Policy Management > Content Classifiers > Patterns & Phrases**.
2. Click the classifier name that most closely resembles the classifier you want to create. Refer to **Regular Expression Patterns** for details about each predefined classifier.
3. Change any of the fields you want to change or add or remove exclude values to those that are uneditable.
4. 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 a Websense built-in pattern and save it under another name, then 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.
Adding a key phrase classifier

The presence of a keyword or phrase (such as “top secret” or “Project X”) in content intended for an external recipient may indicate that classified information is being leaked. TRITON AP-DATA enables you to block the distribution of this information by defining a key phrase classifier. No other protection features, such as fingerprinting, are required.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this key phrase classifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this key phrase.</td>
</tr>
<tr>
<td>Phrase to search</td>
<td>Enter the key word or phrase that might indicate classified information, up to 255 characters. Key phrases are case-insensitive. Leading and trailing white spaces are ignored. If you need to use slashes, tabs, hyphens, underscores, or carriage returns, define a regular expression classifier rather than a key word classifier.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

Unlike dictionaries, key phrases also identify partial matches. For example, the key phrase “uri” reports a match for “security”.

You can have up to 100 key phrase classifiers.

Adding a dictionary classifier

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

For your convenience, many dictionaries are built into TRITON AP-DATA. There are lists for medical conditions, financial terms, legal terms, credit card terms, geographical locations, and more.

In TRITON AP-DATA, 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.
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 > Patterns**.
2. Select **New > Dictionary**.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this pattern, such as Diseases.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this dictionary, such as Disease terminology.</td>
</tr>
</tbody>
</table>
| List of phrases to include | ● **Phrase**: 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.  
  ● **Weight** - For each phrase, select a weight, from -999 to 999. When matched with a threshold, weight defines how many instances of a phrase can be present, in relation to other phrases, before triggering a policy.  
  For example, if the threshold is 100 and a phrase’s weight is 10, an email message, Web post, or other destination can have 9 instances of that phrase before a policy is triggered, provided no other phrases are matched. If phrase A has a weight of 10 and phrase B has a weight of 5, 5 instances of phrase A and 10 instances of phrase B will trigger the policy.  
  The system also deducts the weights of excluded terms. Matches that should be excluded and are therefore not considered breaches are not accounted for in the summation of weight.  
  By default, if no weight is assigned, each phrase is given a weight of 1.  
  Thresholds are defined on the policy’s Condition tab.  
  Remove phrases by selecting them and clicking the **Remove** button. |

Remove phrases by selecting them and clicking the **Remove** button.
Classifying Content

4. Click **OK**.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Import                       | If you have many phrases to include, create a text file listing the phrases, then click **Import** and navigate to the text file. The text file must be of UTF8 format. In the text file:  
  - List each phrase on a separate line. The phrase can be up to 256 characters.  
  - Optionally, provide one weight per phrase on the same line.  
    - Separate the phrase and weight by a comma. Enclose the phrase in quotes (not required if there is no weight). For example, “private information”, 3  
    - Valid weights are from -999 to 999.  
    - If a phrase has no weight, it is assigned the default weight of 1.  
  - Each phrase must be distinct. (Repeated values are ignored.)  
  - You can include up to 5000 unique phrases. If you include more, only the first 5000 will be added to the list.  
  - White spaces are ignored.  
  - Slashes, tabs, hyphens, underscores, and carriage returns are included in the search.  
  - Common words are also included, unlike when fingerprint scans are performed.  
  **Sample file, custom_dictionary.txt:**  
  - “confidential”, 5  
  - “ProjectX”, 8  
  - “ProjectY”, 3  
  - 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                      | This field appears only when you are editing a predefined dictionary. 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 📌 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. |
File properties

Because classified data is often stored in specific file formats—such as PGP (encrypted) or Excel (xlsx)—TRITON AP-DATA 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 TRITON AP-DATA supports, see Supported File Formats.

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, the system 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 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.

**Note**

File properties classifiers do not work for the print channels (network or endpoint), because file property information cannot be extracted from printer drivers.

## 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.
Classifying Content

4. Complete the fields as follows:

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

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:

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

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this group of files, such as “Medium Files” or “Large Files”.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for these files.</td>
</tr>
<tr>
<td>File size</td>
<td>Define the size of the files.</td>
</tr>
<tr>
<td></td>
<td>● <strong>At least</strong> - Select this option if the file is always over a certain size, then specify the minimum size in KB.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Between</strong> - Select this option if the file is between 2 sizes, then specify the sizes in KB.</td>
</tr>
</tbody>
</table>

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, the system performs file-size, file-name, and binary-fingerprint checks for files of unlimited sizes.

---

**Scripts**

TRITON AP-DATA provides a list of built-in script classifiers that are written in a high-end development language that mimics natural language: Python. (See [NLP Scripts](#).)

Script 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, script classifiers are more accurate than regular expression classifiers. Scripts analyze both content and context using statistical analysis or decision trees.

Note that fingerprinting is better than scripts 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 script classifier. Scripts detect any valid credit card number. You may wish to use both with different levels of severity and different actions.
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 script content classifiers:

1. Click Main > Policy Management > Content Classifiers.
2. Select Patterns & Phrases.
3. Filter the Classifier Type column to display only scripts.

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 scripts, 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 predefined script

1. Click Main > Policy Management > Content Classifiers > Patterns & Phrases.
2. Click the name of the script you want to edit.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the script. If this is a user-defined script, you can modify the name.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the classifier. If this is a user-defined script, you can modify the description.</td>
</tr>
</tbody>
</table>
The presence of content intended for external recipients may indicate that classified information is being distributed via email and/or attachments. TRITON AP-DATA enables you to block the distribution of this information by fingerprinting files and directories and scanning data in motion for those fingerprints.

TRITON AP-DATA 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**.

   4. 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.

## File fingerprinting

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit parameter values</td>
<td>Select this check box if you want to edit the values of the script’s parameters. Refer to <a href="#">NLP Scripts</a> for details about the PreciseID script classifier you chose. Add a new value for each parameter as desired.</td>
</tr>
<tr>
<td>Exclude</td>
<td>Click <strong>Exclude</strong> if you want to exclude certain values from the classifier, then select either <strong>Pattern to exclude</strong> or <strong>List of phrases to exclude</strong> to define the pattern to exclude. Exclude should list exceptions to the rule.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pattern to exclude</strong> - Define the regular expression pattern to exclude. Click the information icon for a list of valid values.</td>
</tr>
<tr>
<td></td>
<td>- <strong>List of phrases to exclude</strong> - Enter a list of phrases to exclude, separated by commas. Click <strong>Add</strong> to add them to the list. These phrases, when found in combination with the script, affect whether the content is considered suspicious. Click <strong>Remove</strong> to remove selected strings from the list.</td>
</tr>
</tbody>
</table>

### Related topics:
- Managing TRITON AP-DATA, page 6
- File System Fingerprinting, page 128
- SharePoint Fingerprinting, page 132
- Domino Fingerprinting, page 136
- Classifying Content, page 107
2. Select **Fingerprints > File Fingerprinting**. 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 the links in the details pane to learn more about the fingerprinted files and folders. (See *Details pane*, page 111 for a description of the details pane.) You can also start, stop, or pause a fingerprinting task using buttons on the toolbar.

3. To create a fingerprinting classifier, select one of the following from the menu bar:
   - New > File System Fingerprinting
   - New > SharePoint Fingerprinting
   - New > Domino Fingerprinting
   A wizard opens.

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

---

**Note**

To import an existing fingerprinting classifier—one that has been exported and copied to a network location—select **Import** from the toolbar. See *Imported fingerprinting*, page 162 for more information.
File System Fingerprinting

File System Fingerprinting Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the files you are fingerprinting, such as “finance documents.”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this set of documents.</td>
</tr>
<tr>
<td>Crawler</td>
<td>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 drop-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.</td>
</tr>
<tr>
<td>Fingerprinting Mode</td>
<td>Select which type of fingerprinting to perform:</td>
</tr>
<tr>
<td></td>
<td>● Sensitive content - Select this option to identify the content files and documents to fingerprint.</td>
</tr>
<tr>
<td></td>
<td>● Ignored section - Select this option to identify parts of secured documents that the system should not analyze. This might include disclaimers, copyrights, and logos. Ignored sections are immediately enforced for every fingerprint. You do not need to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they’re fingerprinted.</td>
</tr>
<tr>
<td>Fingerprinting Method</td>
<td>Select a fingerprinting method:</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>● 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 1 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.</td>
</tr>
</tbody>
</table>

File System Fingerprinting Wizard Root Folder
When you click Next on this screen, TRITON AP-DATA tries to connect to the root folder using the given credentials. You are alerted if the attempt fails.
File System Fingerprinting Wizard - Scanned Files

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files and folders to scan</td>
<td>The files and folders included in the scan are listed in the box. By default, all files and folders in the root folder are included. Click Edit to modify the list. See Selecting items to include or exclude in a policy, page 49 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.</td>
</tr>
</tbody>
</table>

File System Fingerprinting Wizard - Scheduler

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this option to enable the fingerprint scan scheduler. If this is de-selected, you will be required to manually start fingerprint scans.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: once, daily, weekly, or continuously.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose Daily or Weekly, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run fingerprint scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait nn minutes between consecutive scans</td>
<td>If you select Continuously, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.</td>
</tr>
</tbody>
</table>

File System Fingerprinting Wizard - File Filtering
### Field System Fingerprinting Wizard - Export

This option appears only when you are creating a new classifier. Configure settings on this page if you want to use this classifier in policies on a disconnected network. Here you export this classifier to a network location. Later, you can copy it to the other network (using an external disk, for example) and import it using the **Import** option.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Type/Document Name</strong></td>
<td></td>
</tr>
<tr>
<td>Include file types/names</td>
<td>List the types of files to be fingerprinted, separated by semicolons. You can use the “<em>” or “?” wildcards. For example, “</em>.doc; *.xls; *.ppt; *.pdf”. Click <strong>File Types</strong> to select the type of files to include in the scan from predefined categories such as Office Documents or Bitmaps.</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well. Click <strong>File Types</strong> to select the type of files to exclude in the scan from predefined categories such as Office Documents or Bitmaps.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter by Age</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Search only for files that were modified:</td>
<td>Select this check box to filter files by age, then select the option that corresponds to the desired period. When you select this box, the default period is 24 months.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter by Size</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan only files larger than</td>
<td>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.</td>
</tr>
<tr>
<td>Scan only files smaller than</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note**

Files larger than 100 MB are fingerprinted for exact-matching. Two binary fingerprints are created: one with the first 100 MB, and another with the first and last 5 MB. When a large file is received, the first and last 5 MB are sent to analysis. They are compared to both of the fingerprints above to search for a match.
on the File Fingerprinting toolbar. See *Imported fingerprinting, page 162* for details. (The disconnected network must have a management server as well.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export fingerprints</td>
<td>Select this box if you want to export this fingerprint classifier for use in a disconnected network.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the export folder.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
<tr>
<td>Domain (optional)</td>
<td>Optionally, enter the domain name of the user you entered above.</td>
</tr>
<tr>
<td>Export folder</td>
<td>Enter the hostname or IP address (in UNC format) of the server where you want to store the classifier, then browse to the folder to use. The folder must be pre-existing. Example of UNC format: <code>\12.3.45.67</code> Note that a new folder is created in that directory every time the fingerprinting task is run. The folders are versioned and they can grow indefinitely. You are responsible for managing or deleting older versions as needed.</td>
</tr>
</tbody>
</table>

**File System 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.
SharePoint Fingerprinting

SharePoint Fingerprinting Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the documents you are fingerprinting, such as “finance documents.”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this set of documents.</td>
</tr>
<tr>
<td>Crawler</td>
<td>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 drop-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.</td>
</tr>
<tr>
<td>Fingerprinting Mode</td>
<td>Select which type of fingerprinting to perform:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Sensitive content</strong> - Select this option to identify the content files and documents to fingerprint.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Ignored section</strong> - Select this option to identify parts of secured documents that the system should not analyze. This might include disclaimers, copyrights, and logos. Ignored sections are immediately enforced for every fingerprint. You do not need to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they’re fingerprinted.</td>
</tr>
<tr>
<td>Fingerprinting Method</td>
<td>Select a fingerprinting method:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Content similarity</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Exact match</strong> - 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 1 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.</td>
</tr>
</tbody>
</table>

SharePoint Fingerprinting Wizard Site Root
When you click **Next** on this screen, the system tries to connect to the root-site using the given credentials. You are alerted if the attempt fails.
**SharePoint Fingerprinting Wizard - Scanned Documents**

### Field Description

**Documents to scan**
The documents 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 49 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 Fingerprinting Wizard - Scheduler**

### Field Description

**Enabled**
Select this option to enable the fingerprint scan scheduler. If this is de-selected, you will be required to manually start fingerprint scans.

**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.

Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.

**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 drop-down box and a time from the spinner.

**Wait nn 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 Fingerprinting Wizard - File Filtering**
Classifying Content

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Type/Document Name</strong></td>
<td></td>
</tr>
<tr>
<td>Include file types/names</td>
<td>List the types of files to be fingerprinted, separated by semicolons. You can use the “<em>” or “?” wildcards. For example, “</em>.doc; *.xls; *.ppt; *.pdf”. Click <strong>File Types</strong> to select the type of files to include in the scan from predefined categories such as Office Documents or Bitmaps.</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well. Click <strong>File Types</strong> to select the type of files to exclude in the scan from predefined categories such as Office Documents or Bitmaps.</td>
</tr>
<tr>
<td><strong>Filter by Age</strong></td>
<td></td>
</tr>
<tr>
<td>Search only for files that were modified:</td>
<td>Select this check box to filter files by age, then select the option that corresponds to the desired period. When you select this box, the default period is 24 months.</td>
</tr>
<tr>
<td><strong>Filter by Size</strong></td>
<td></td>
</tr>
<tr>
<td>Scan only files larger than</td>
<td>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.</td>
</tr>
<tr>
<td>Scan only files smaller than</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note**

Documents larger than 100 MB are fingerprinted for exact-matching. Two binary fingerprints are created: one with the first 100 MB, and another with the first and last 5 MB. When a large document is received, the first and last 5 MB are sent to analysis. They are compared to both of the fingerprints above to search for a match.

**SharePoint Fingerprinting Wizard - Export**

This option appears only when you are creating a new classifier. Configure settings on this page if you want to use this classifier in policies on a disconnected network. Here you export this classifier to a network location. Later, you can copy it to the other network (using an external disk, for example) and import it using the **Import** option.
Classifying Content

on the File Fingerprinting toolbar. See Imported fingerprinting, page 162 for details. (The disconnected network must have a management server as well.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export fingerprints</td>
<td>Select this box if you want to export this fingerprint classifier for use in a disconnected network.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the export folder.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
<tr>
<td>Domain (optional)</td>
<td>Optionally, enter the domain name of the user you entered above.</td>
</tr>
<tr>
<td>Export folder</td>
<td>Enter the hostname or IP address of the server where you want to store the classifier, then browse to the folder to use. The folder must be pre-existing. Note that a new folder is created in that directory every time the fingerprinting task is run. The folders are versioned and they can grow indefinitely. You are responsible for managing or deleting older versions as needed.</td>
</tr>
</tbody>
</table>

SharePoint 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.

Domino Fingerprinting

Domino Fingerprinting Wizard - General

With TRITON AP-DATA, you can fingerprint documents stored in an IBM Domino data management system.

Domino environments normally consist of one or more servers working together with data stored in Notes Storage Format (NSF) files. There are usually many NSFs on any given Domino server. Each entry in the NSF may have a title, one or more body fields, and attachments. For example:

- An NSF for email might have the fields: subject, to, from, bcc, body, and attachment.
● An NSF for inventory management might have the fields: catalog number, title, description, and expiration date.

A fingerprinting task treats the body of a document and each of its attachments as a separate item. This enables the system to show the full path down to the item inside a document that caused a breach.

---

**Important**

To use this feature, you must first:

- Install IBM Notes *before* installing TRITON AP-DATA. Notes must be on the same machine as the crawler. Be sure that the Notes installation is done for “Anyone who uses this computer.”
- Provide your Notes user ID file and password when prompted by the TRITON AP-DATA installer. This information is used to authenticate access to the Domino server for fingerprinting and discovery.
- Log onto Notes, one time only, and supply a user name and password. This user must have administrator privileges for the Domino environment. (Read permissions are not sufficient.)
- Connect to the Domino server from the Notes client.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the documents you are fingerprinting, such as “finance documents.”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this set of documents.</td>
</tr>
<tr>
<td>Crawler</td>
<td>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 drop-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 Domino server.</td>
</tr>
</tbody>
</table>
### Classifying Content

#### Fingerprinting Mode
Select which type of fingerprinting to perform:
- **Sensitive content** - Select this option to identify the content files and documents to fingerprint.
- **Ignored section** - Select this option to identify parts of secured documents that the system should not analyze. This might include disclaimers, copyrights, and logos.

Ignored sections are immediately enforced for every fingerprint. You do not need to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they’re fingerprinted.

#### 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 1 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.

### Domino Fingerprinting Wizard Server

**Data Security Manager Help | TRITON AP-DATA | Version 8.0.x**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino server to scan</td>
<td>Enter the hostname of the IBM Domino server that you want to scan—for example, <em>gumby</em>. Do not include the HTTP: prefix or leading slashes.</td>
</tr>
<tr>
<td>User name</td>
<td>When you click <strong>Next</strong> on this screen, the crawler tries to connect to the Domino server using credentials for the user indicated. These connection settings were provided when TRITON AP-DATA was installed on the Notes machine.</td>
</tr>
</tbody>
</table>

**Warning**

If this user has insufficient privileges for certain folders or NSF files on this server, those items will not be scanned.

To connect with different user credentials, run the TRITON AP-DATA installer on the Notes machine, select the **Modify** option, and upload a different user ID file.
## Domino fingerprinting Wizard - Scanned Documents

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document names are stored in the following field(s)</td>
<td>Enter the name of the field or fields that hold your document names. If you supply multiple field names, separate them with commas. For example: subject, docname, filename. By default, the “Subject” field is scanned.</td>
</tr>
</tbody>
</table>

| Documents and folders to scan | The documents 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 49](#) for instructions on using the selector tool. Note the following:  
  ● Document libraries are represented by folder icons. Click the folder icon with an arrow 🚶 to display the library one level up in the document management hierarchy. You can also click the breadcrumbs above the list to navigate to another level.  
  ● Domino documents are represented by file icons. Click a document to show its attachments.  
  ● Notes Storage Format (NSF) files are represented by an NSF icon. These can include one or many documents. Drill down an NSF by clicking it, or move it to the Include list to scan the entire NSF.  
  ● Attachments are represented by icons of a file with a paper clip. You can also specify the Notes views to scan. |

| Fields to scan | In Notes, just as document names are typically stored in the Subject field, document content is typically stored in the Body field. If your document content is stored in more than one field, enter the name of the fields, separated by commas. For example, "body, content, main". Attachments are the files that are attached to the document, such as graphic files, compressed files, word processing files, spreadsheets, and more. Indicate whether you want to scan the document content, file attachments, or both. Both are selected by default. |

## Domino Fingerprinting Wizard - Scheduler
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this option to enable the fingerprint scan scheduler. If this is de-selected, you will be required to manually start fingerprint scans.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: once, daily, weekly, or continuously.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>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. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait nn minutes between consecutive scans</td>
<td>If you select Continuously, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.</td>
</tr>
</tbody>
</table>

### Domino Fingerprinting Wizard - Document Filtering

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Document Name</td>
<td></td>
</tr>
<tr>
<td>Include names</td>
<td>Select <strong>Filter by Document Name</strong> to analyze content in document names. The file names and their paths are fingerprinted. List the exact document names to be fingerprinted, separated by semi-colons. You can use the “<em>” or “?” wildcards. For example, “top_secret</em>”.</td>
</tr>
<tr>
<td>Except</td>
<td>List the exact document names to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td>Filter by Age</td>
<td>Select this check box to filter documents by age, then select the option that corresponds to the desired period. When you select this box, the default period is 24 months.</td>
</tr>
<tr>
<td>Note:</td>
<td>The age of a document is the latest date of its body and all attachments.</td>
</tr>
<tr>
<td>Filter by Size</td>
<td></td>
</tr>
</tbody>
</table>
### Classifying Content

#### Domino Fingerprinting Wizard - Attachment Filtering

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Type</strong></td>
<td></td>
</tr>
<tr>
<td>Include file types</td>
<td>Select this option to look for specific attachments. List the types of files to be fingerprinted, separated by semicolons. You can use the “<em>” or “?” wildcards. For example, “</em>.doc; *.xls; *.ppt; *.pdf”.</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td><strong>Filter by Size</strong></td>
<td></td>
</tr>
<tr>
<td>Scan only files larger than</td>
<td>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.</td>
</tr>
<tr>
<td>Scan only files smaller than</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note**

Documents larger than 100 MB are fingerprinted for exact-matching. Two binary fingerprints are created: one with the first 100 MB, and another with the first and last 5 MB. When a large document is received, the first and last 5 MB are sent to analysis. They are compared to both of the fingerprints above to search for a match.
Domino Fingerprinting Wizard - Export

This option appears only when you are creating a new classifier. Configure settings on this page if you want to use this classifier in policies on a disconnected network. Here you export this classifier to a network location. Later, you can copy it to the other network (using an external disk, for example) and import it using the Import option on the File Fingerprinting toolbar. See Imported fingerprinting, page 162 for details.

(The disconnected network must have a management server as well.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export fingerprints</td>
<td>Select this box if you want to export this fingerprint classifier for use in a disconnected network.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the export folder.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
<tr>
<td>Domain (optional)</td>
<td>Optionally, enter the domain name of the user you entered above.</td>
</tr>
<tr>
<td>Export folder</td>
<td>Enter the hostname or IP address of the server where you want to store the classifier, then browse to the folder to use. The folder must be pre-existing. Note that a new folder is created in that directory every time the fingerprinting task is run. The folders are versioned and they can grow indefinitely. You are responsible for managing or deleting older versions as needed.</td>
</tr>
</tbody>
</table>

Domino 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.
Classifying Content

Database fingerprinting

TRITON AP-DATA lets you quickly connect to a database, retrieve records, and fingerprint them. It 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.

TRITON AP-DATA can also fingerprint a salesforce.com database that is hosted “in the cloud.”

In addition, TRITON AP-DATA 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. TRITON AP-DATA enables you to block the distribution of this information by defining database record fingerprints.

Related topics:
- Connecting to data sources, page 145
- Preparing for database fingerprinting, page 146
- Creating a validation script, page 147
- Selecting the data to fingerprint, page 150
- How matches are counted, page 152
- Data classification, page 5
- Creating a database fingerprint classifier, page 153
- Database Fingerprinting Wizard - General, page 155
- Database Fingerprinting Wizard - Data Source/Site, page 155
- Database Fingerprinting Wizard - Field Selection, page 157
- Database Fingerprinting Wizard - Scheduler, page 160
- Database Fingerprinting Wizard - Fingerprinting Type, page 161
- Database Fingerprinting Wizard - Finish, page 162
Connecting to data sources

In order to fingerprint a database, the TRITON AP-DATA server must be able to connect to the data source over a supported interface. TRITON AP-DATA supports the following database connection interfaces:

- Open Database Connectivity (ODBC)—Websense has certified support for the following ODBC-compliant databases:
  - Oracle 10g (ODBC driver 10.1.0.2.0)
  - Oracle Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (32- and 64-bit)
  - Microsoft SQL Server Express (SQL Server Express ODBC driver)
  - IBM DB2 9.5 (ODBC driver 8.2.9)
  - IBM Informix Dynamic Server 11.50 (IBM Informix ODBC driver 3.50)
  - MySQL 5.1 (ODBC driver 5.1.5)
    - Due to MySQL limitations, you must define “string” columns with UTF-8 encoding to fingerprint them.
  - Sybase ASE 15.0 (Sybase ODBC driver 15.0.0.152)
  - Teradata v13 and v14
- Salesforce.com
- CSV files (UNC path needs to be specified. For example, \\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. For best practice, be sure to test database connectivity before configuring content policies.

Supported field types

The system scans the following database field types:

- CHAR
- VARCHAR
- WCHAR
- WVARCHAR
- TINYINT
- SMALLINT
- INTEGER
- BIGINT
- DECIMAL
- NUMERIC
Preparing for database 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 or setting up database discovery, 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. Access the system’s ODBC Data Source Administrator.
   Windows 2012:
   a. Open Server Manager and expand the Tools menu.
   b. Select ODBC Data Sources 64-bit.
   Windows 2008:
   a. Navigate to C:\Windows\SysWOW64\ and run the executable file, odbcad32.exe
3. Click the User DSN tab and click Add.
   User DSNs are the most common type of DSN. They store information about how to connect to a specific data source. They may be used only by the current user on the current machine. To use a User DSN, you must be logged in as the TRITON AP-DATA Administrative User on the server running the relevant crawler.
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**.

7. If you selected a Sybase or DB2 driver in step #4:
   a. Stop all discovery tasks and fingerprinting jobs running on this machine.
   b. Open Windows Services Manager.
      
      Windows 2012:
      ○ Open Server Manager, expand the Tools menu, and select **Services**.
      Windows 2008:
      ○ Select **Start > Run** and type **services.msc**.
   c. Restart the service “Websense Data Task Scheduler.” In the services window, right-click **Websense Data Task Scheduler** and select **Restart**.

**Creating a validation script**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Fingerprinting cells with some values, such as multiple short values, can lead to multiple false-positive incidents. TRITON AP-DATA includes a mechanism that forwards database data to an external script for processing before fingerprinting.

**Validation script mechanism**

Each database fingerprints classifier can use a validation script. The validation script receives an input file containing the raw database data in a CSV format, and returns CSV data containing the information that should be fingerprinted.

Validation scripts must be designed to receive at least two parameters: An input path name and an output path name. An additional parameter, containing a configuration file path name, is optional.

The input file, received from TRITON AP-DATA, is a CSV file with a header row containing the database column names. Each line is delimited by a valid Windows line break (CRLF), and all values are double-quotes escaped. A sample package containing a sample input file, among other things, is available through Websense Technical Support.

The output file should be of the same format as the input file, but instead of using CRLF as the line delimiter, it uses CRCELF (2 Carriage-Return characters, and a Line-Feed character). An output sample file is available on the same package as the sample input file.

**Validating fingerprinting scans**

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 TRITON AP-DATA was installed (typically C:\Program Files\Websense\Data Security\ValidationScripts).
   - default_validation.bat.sample
Classifying Content

- default_validation.ini.sample

If you prefer to create your script from scratch, you can skip this step.

2. Name your new validation script using the following convention:

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

   where:
   - <classifier-name> is the name of the classifier on which the script will be implemented. Alternatively, the word “default” may be used, for scripts that are to be implemented on all classifiers that don't have specific scripts named after them.
   - bat is the extension for a batch file.
   - exe is the extension for an executable.
   - py is the extension for a python script.

   If the script requires a configuration file, then name the configuration file using the following convention:

   <classifier-name>_validation.[xml|ini]

   Place all files in the \ValidationScripts folder on the server where TRITON AP-DATA is installed (typically C:\Program Files\Websense\Data Security\ValidationScripts).

   Every validation script must be an executable or a batch file. If there is a need for an infrastructure element, for example the python interpreter, the operating system must be able to automatically initiate the element when the script is being called. To ensure the correct file association is configured, Websense recommends running the script from the command line, without reference to any other executable.

   __Note__

   Pay attention not to leave more than one executable or configuration file with the same name and different extension in the validation scripts directory.

3. The script should receive 2 command-line parameters from TRITON AP-DATA: the full path of a source file the system creates, and the full path where the system expects to find a destination file.
   - The first line of the source file includes the names of the columns that are available for fingerprinting. The remaining lines contain the data in those columns.
   - Your script should read and perform validation on the source file.
   - Your script should write the validated results to a destination file.
   - The destination file should be formatted in the same way as the source file—with the names of the columns that were fingerprinted on the first line. Note that the number of columns varies if your script adds or removes columns.
   - The destination file must use the name and path that received from TRITON AP-DATA.
Your script should return a return code of 0 if everything succeeded, and non-zero if there was a problem.

4. If you want your script to receive a configuration file, place it in the same location as the script, and name it with the same name as the script file followed by .xml or .ini. If this file is found, it is supplied as a third parameter to your script.

5. Create and run the fingerprinting classifier as described in Creating a database fingerprint classifier, page 153. Name the classifier with the name given in step 2.

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 the system 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 click 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.

Sample validation script

You can obtain a sample validation script from Websense Technical Support and modify it to suit your needs. The script contains the basic abilities required for most customers, such as removing NULL or single-character values from being fingerprinted.

The sample package contains the following files:

- default_validation.bat - Sample validation script
- validation_logic.py - Used by the sample validation script.
- default_validation.ini - Sample configuration file
- default_validation.ini.sample - An additional configuration sample file
- dictionary.txt - Sample dictionary file
- in.csv - Sample input file
- out.csv - Sample output file

The first 3 files are also included (with the .sample extension, for the batch and ini files) in the TRITON AP-DATA installation package.

The sample validation script is a production grade script, which is suitable for many customers. Install it by copying the default_validation.bat, validation_logic.py and the default_validation.ini files into the \ValidationScripts folder, which is located in the TRITON AP-DATA installation folder (typically C:\Program Files\Websense\Data Security\ValidationScripts).
Please note that although you can change the filenames of the `default_validation.bat` and `default_validation.ini` according to the conventions mentioned above, do not rename the `validation_logic.py` file. The `validation_logic.py` file must be present in the \ValidationScripts directory (typically `C:\Program Files\Websense\Data Security\ValidationScripts`) in its original form.

The validation script is predefined to make sure TRITON AP-DATA ignores:

- Numbers smaller than 10,000.
- Text strings containing fewer than 4 characters.
- Strings containing only zeros (i.e. "000000").
- Empty strings.
- Placeholders (NULL and similar values).
- Invalid SSNs in columns named 'ssn'.
- Invalid email addresses in columns named 'email'.

The following additions and changes can be configured through the `default_validation.ini` configuration file:

- It is possible to create a dictionary file that contains a list of strings for the validation script to remove. The file should be a line delimited UTF-16 file, and its path name should be written in the IgnoredDictionary configuration option in regular file system format. (For example c:\directory\dictionary.txt.) You can create UTF-16 files in Windows Notepad by saving the text with 'Unicode' encoding.

  The `default_validation.ini` file, which is part of the package, is a sample file containing such a definition. The `dictionary.txt` file is a sample dictionary file.

- You can use regular expressions to validate any column. To use this feature:
  - Add the column name, in lower case, to the columns parameter. Separate column names by semicolons.
  - Add a configuration section for the column by appending [column-name] to the file (again, lower case). This is the section header.
  - Add a RegExp parameter under the relevant (newly added) section header. Its value is a regular expression.

  The `default_validation.ini` sample file contains this type of validation for email addresses and social security numbers. These can be used as a reference.

---

**Note**

Additional configuration options are available. Contact Websense Technical Support for further assistance.
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 Patterns & Phrases, page 116 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 147*) 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:

<table>
<thead>
<tr>
<th>Column_A</th>
<th>Column_B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>AAAA</td>
</tr>
<tr>
<td>5678</td>
<td>AAAA</td>
</tr>
<tr>
<td>1234</td>
<td>AAAA</td>
</tr>
</tbody>
</table>

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 database fingerprint classifier

To classify your content by fingerprinting database records:

1. Click **Main > Policy Management > Content Classifiers**.
2. Select **Fingerprints > Database Fingerprinting**. 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 the links in the details pane to learn more about the fingerprinted records. (See *Details pane*, page 111 for a description of the details pane.) You can also start, stop, or pause a fingerprinting task using buttons on the toolbar.

3. Click **New** from the menu bar then select **Database Table Fingerprinting**, **Salesforce Fingerprinting**, or **CSV File Fingerprinting**. A wizard opens. There are several pages in the wizard:
   - **General**
   - **Data Source (Table, CSV) or Site (SalesForce)**
   - **Field Selection**
   - **Scheduler**
   - **Fingerprinting Type**
   - **Export**
   - **Finish**

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

---

**Note**

To import an existing fingerprinting classifier—one that has been exported and copied to a network location—select **Import** from the database fingerprinting toolbar. See *Imported fingerprinting*, page 162 for more information.

---

**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 database fingerprinting*, page 146 for instructions.
Database Fingerprinting Wizard - General

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

- **Database table**, page 155
- **Salesforce site**, page 156
- **CSV file**, page 156

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

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the database records you are fingerprinting, such as “finance records.”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the database.</td>
</tr>
<tr>
<td>Crawler</td>
<td>From the drop-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.</td>
</tr>
</tbody>
</table>
### Database table

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Source Name</strong></td>
<td><strong>Data source name</strong> 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 Creating a Data Source Name (DSN) in Windows, page 146 for instructions. (For a list of supported databases and field types, see Connecting to data sources, page 145.) Click Refresh to refresh the list. Note that this DSN must be defined with the same user as the crawler you specified on the previous step.</td>
</tr>
<tr>
<td><strong>Database Credentials</strong></td>
<td><strong>Use data source credentials</strong> Select this option to use the name and password of the TRITON AP-DATA service account to access the database, that is the local administrator account that you defined when installing TRITON AP-DATA. Some databases allow you to use NT authentication to verify the login ID, so be sure the crawler’s credential is the one with the permission to access the database. Microsoft SQL Server allows you to use NT authentication or SQL Server authentication. If you’re using SQL Server authentication, select Use the following credentials instead.</td>
</tr>
<tr>
<td></td>
<td><strong>Use the following credentials</strong> Enter credentials defined in the database itself, such as the sa account. (Do not enter the network credentials.) • <strong>User name</strong> - Enter the user name of any user with “read” privileges to the database. • <strong>Password</strong> - Enter the password for this user. • <strong>Domain</strong> - Optionally, enter the domain for the entered user. If your database is using Windows authentication, include the domain name.</td>
</tr>
</tbody>
</table>

### Salesforce site

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salesforce site</td>
<td>Enter the URL of your organization’s Salesforce website, for example: <a href="https://emea.salesforce.com">https://emea.salesforce.com</a>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the Salesforce site.</td>
</tr>
</tbody>
</table>
This screen varies depending on whether you are defining a fingerprint for a database table, Salesforce site, or CSV file.

- **Database table or CSV file**, page 158
- **Salesforce site**, page 159
# Database table or CSV file

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select up to 32 fields from a table | Select this option if you want to select the fields to fingerprint.  
1. From the drop-down list, select the table that contains the fields of interest. CSV files are preselected.  
2. Select the field(s) you want to fingerprint. These correspond to columns in the table.  
You can select up to 32 fields for any given table.  
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 option 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**, the system 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 150*. For example, avoid fingerprinting short values, columns with repetitive values, and uninteresting or irrelevant values.
Note to Informix users

The system cannot fingerprint Informix tables that have names containing a backslash character; however, there is a workaround.

1. Select the **Select up to 32 fields from a table** option.
2. Select the desired table and fields.
3. Copy the query from the field labeled, **Selection as SQL query**.
4. Select the **Use the following SQL query to select records** option.
5. Paste the query into the box.
6. Surround the table name with double quotes. For example, SELECT "name","id","cc","phone" FROM "blade2\informix".custdb.
### Database Fingerprinting Wizard - Scheduler

**Salesforce site**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select up to 32 fields from a table</td>
<td>Select this option if you want to select the fields to fingerprint or choose a predefined database query. From the drop-down list, select the table from your Salesforce database that contains the fields of interest, or select a predefined query that can span multiple (joined) tables, such as “Sales this year.” If you select a predefined query, no other action is required. If you select a table, select the field or fields you want to fingerprint. These correspond to columns in the table. You can select up to 32 fields for any given table. Websense supplies the 10 most common Salesforce tables. You can query any of the tables that are used by salesforce.com using an API that Salesforce makes available publicly. You can view the SOQL query that was generated for your selection. This appears under <strong>Selection as SOQL Query</strong>. Click <strong>View Sample Data</strong> to make sure that the correct information is fingerprinted.</td>
</tr>
<tr>
<td>Use the following SOQL query to select records</td>
<td>Select this option if you want to generate your own SOQL query. You can either type your own query or click <strong>Copy Above Query</strong> 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 <strong>View Sample Data</strong> to make sure that the correct information is fingerprinted. When you click <strong>Next</strong>, the system validates your SOQL query.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this check box if you want to schedule the fingerprinting scan to run automatically. De-select the box if you want to run the task manually.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select when you want to start this task: as soon as possible, every day at a certain time, weekly on a certain day, or continuously. Note that once a task starts, it continues until it is finished. You cannot pause or resume a fingerprinting task. All dates and times reflect the time zone of the crawler, not the administrator time zone.</td>
</tr>
</tbody>
</table>

**Once**
- **But not before:** Select this check box 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 drop-down box and a time from the spinner.

**Daily**
- **Start every day at:** Specify when you want to start the scan, for example, 2 a.m. Websense recommends you run fingerprint scans at night, after peak business hours.

**Weekly**
- Specify the days and hours in which you want to start the scan, for example, Monday, Wednesday, and Friday at 2 a.m.; Sunday at noon.

**Continuously**
- **But not before:** Select this check box 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 drop-down box and a time from the spinner.
- **Wait:** Designate how many minutes to wait between consecutive scans.

---

**Database Fingerprinting Wizard - Fingerprinting Type**
### Database Fingerprinting Wizard - Export

This option appears only when you are creating a new classifier. Configure settings on this page if you want to use this classifier in policies on a disconnected network. Here you export this classifier to a network location. Later, you can copy it to the other network (using an external disk, for example) and import it using the **New > Imported Fingerprinting** option. See *Imported fingerprinting, page 162* for details. (The disconnected network must have a management server as well.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export fingerprints</td>
<td>Select this box if you want to export this fingerprint classifier for use in a disconnected network.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the export folder.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
</tbody>
</table>
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, file name, 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.

### Imported fingerprinting

The system gives you the option of using an existing file or database fingerprinting classifier in policies on a disconnected network.

To do so, you export the fingerprinting classifier to a network location. You configure this while creating or editing the classifier. Later, you manually copy it to the disconnected network (using an external drive, for example), then import it using the **Import** option on the File Fingerprinting or Database Fingerprinting toolbar.

Note that you must reimport the classifier every time the fingerprinting task is run. The import is incremental, so only changes to the fingerprints are imported.

To import a fingerprinting classifier:

1. Click **Main > Policy Management > Content Classifiers**.
2. Select **Fingerprints > File Fingerprinting** or **Fingerprints > Database Fingerprinting**.
3. Click **Import** from the toolbar. A wizard opens. There are several pages in the wizard:
   - **Import Source**
Import Fingerprint Wizard - Import Source

Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Enter the name of a user who has access to the folder where the classifier you want to import resides.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
<tr>
<td>Domain (optional)</td>
<td>Optionally, enter the domain name of the user you entered above.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select which crawler to use to perform this fingerprinting. Typically this would be the crawler that is closest in proximity to the file or database server.</td>
</tr>
<tr>
<td>Import from folder</td>
<td>Enter the hostname or IP address of the server where the classifier is stored, then browse to the folder to use.</td>
</tr>
</tbody>
</table>

Import Fingerprint Wizard - Properties

Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the new classifier. By default, this is the name of the original classifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this classifier. By default, this is the description of the original classifier.</td>
</tr>
</tbody>
</table>

Exported Classifier Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the classifier that was exported (uneditable)</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the classifier (uneditable)</td>
</tr>
<tr>
<td>Table name</td>
<td>Database fingerprinting only. The database table corresponding to the original classifier (uneditable)</td>
</tr>
<tr>
<td>Fingerprinted fields</td>
<td>Database fingerprinting only. The database fields that are configured to be fingerprinted in the original classifier (uneditable)</td>
</tr>
</tbody>
</table>
Import Fingerprint Wizard - Scheduler

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this check box if you want to schedule the fingerprinting scan to run automatically. De-select the box if you want to run the task manually.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select when you want to start this task: as soon as possible, every day at a certain time, weekly on a certain day, or continuously. Note that once a task starts, it continues until it is finished. You cannot pause or resume a fingerprinting task. All dates and times reflect the time zone of the crawler, not the administrator time zone.</td>
</tr>
</tbody>
</table>

Once
- **But not before:** Select this check box 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 drop-down box and a time from the spinner.

Daily
- **Start every day at:** Specify when you want to start the scan, for example, 2 a.m. Websense recommends you run fingerprint scans at night, after peak business hours.

Weekly
- Specify the days and hours in which you want to start the scan, for example, Monday, Wednesday, and Friday at 2 a.m.; Sunday at noon.

Continuously
- **But not before:** Select this check box 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 drop-down box and a time from the spinner.
- **Wait:** Designate how many minutes to wait between consecutive scans.

Import Fingerprint Wizard - Finish

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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, file name, 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.
Machine learning

Machine learning classifiers are for more advanced users. In them, you provide examples of the type of data that you want to protect and that you don’t want to protect, so the system can learn and identify sensitive data in traffic. These are called positive and negative training sets because the examples educate the system.

Unlike fingerprinting, the files do not need to contain parts of the analyzed files but can look similar or be on a similar topic. The system learns and recognizes complex patterns and relationships and makes decisions on them without exact include/exclude criteria that are specified in fingerprinting classifiers. Machine learning can even protect new, zero-day documents in this way.

Because machine learning classifiers are not looking for an exact match, they can handle a larger number of files.

---

**Note**

Machine learning classifiers can be used for unstructured file system data only. They cannot be used for database data or unstructured SharePoint or IBM Domino data.

---

Once you’ve created the classifier, the system assesses the expected number of unintended matches (false positives) and undetected content (false negatives) and provides an accuracy level.

The system supports 3 levels of machine learning classifiers:

- Explicit negative examples - For example, non-proprietary marketing plans as a negative example to propriety marketing plans.
- Non-explicit negative examples- For example, directories that do not contain marketing plans as negative examples to directories with proprietary marketing plan.
- Positive examples.

For tips and best practices for using machine learning, refer to [Introduction to Machine Learning for TRITON AP-DATA](#).
Creating a machine learning classifier

To create a machine learning classifier:

1. Click **Main > Policy Management > Content Classifiers**.
2. Select **Machine Learning**. A list of existing machine learning classifiers appears. You can expand the right pane to view more details, such as last run time, or you can collapse it to show fewer. Click the links in the details pane to adjust classifier settings or view more details. (See **Details pane**, page 111 for a description of the details pane.) You can also start, stop, or pause a machine learning process using buttons on the toolbar.
3. Click **New** from the menu bar. A wizard opens. There are several pages in the wizard:
   - **General**
   - **Credentials**
   - **Scanned Folders**
   - **Scheduler**
   - **Finish**

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

---

**Machine Learning Wizard - General**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a meaningful name for the machine learning classifier, such as “Engineering source code.”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the classifier.</td>
</tr>
</tbody>
</table>
# Machine Learning Wizard - Credentials

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawler</td>
<td>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 drop-down list, select which crawler to use to perform the scan. Typically this would be the crawler that is closest in proximity to the root folder containing your data.</td>
</tr>
</tbody>
</table>

**Network Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Enter a user name that has access to the root folder. This must be a user with administrative rights. Read permissions are not sufficient.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user.</td>
</tr>
<tr>
<td>Domain</td>
<td>Optionally, enter the domain name of the user you entered above.</td>
</tr>
</tbody>
</table>

**Root Folder**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root folder</td>
<td>Enter the root folder or root directory of the files and folders containing the positive, negative, and all-documents examples. For example, enter \Server\Public\shared if you want to scan \Server\Public\shared \User1, \Server\Public\shared \User2, and \Server\Public\shared \User3. You select the specific folders to scan on the Scanned Folders screen. A root folder is the highest folder in the hierarchy.</td>
</tr>
</tbody>
</table>
Machine Learning Wizard - Scanned Folders

These documents will be scanned and used for finding similar documents or parts of documents in the future.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive examples</td>
<td>Browse to a folder that contains examples of the type of textual data that you want to protect, so the system can learn from them and identify similar data in traffic. For example, if you want to protect proprietary source code written in Java, supply the path to the location of the proprietary source code. The examples in the folder should look similar. In other words, don’t include examples of all sensitive content in the same folder. Instead, create a new classifier for other types of content. For best results, there should be at least 50 examples in this folder.</td>
</tr>
<tr>
<td>Content type</td>
<td>From the pull-down list, select a type that best describes the content you want to protect; this must match the type of content in your positive examples folder. For example, select <strong>Java and C Source code</strong> if your examples contain engineering source code written in Java. This helps the system know how to interpret your data. Possible types include: • Java and C source code • Perl source code • F# source code • Patents • Software design documents • Movie manuscripts • Financial information - investments • Other If none of the types in the drop-down list applies to your content, select <strong>Other</strong>.</td>
</tr>
</tbody>
</table>
Classifying Content

### Machine Learning Wizard - Scheduler

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative examples</td>
<td>Browse to a folder that contains examples of textual data that is similar to but does not represent the data you want to protect. This folder must be dedicated to negative examples, and it cannot be a subdirectory of the positive examples. For example, if you are protecting proprietary source code, you might provide the location of publicly available source code. After learning, the system will create a classifier that can tell the proprietary source code apart from the non-proprietary. <strong>Note:</strong> If you selected “Other” in the Content Type field, you must provide either negative or all-documents examples to help the system better understand your needs. For best results, there should be at least 50 examples in this folder.</td>
</tr>
<tr>
<td>All documents</td>
<td>Optional. Select this option if you do not have a dedicated negative documents folder. Instead, navigate to a folder containing all types of documents in your network and endpoint traffic, and the system will determine good negative examples for you. The folder can contain both positive and negative examples. The system compares your positive examples to the documents in this folder and decides which files represent negative examples. If you select this option and provide negative examples, you improve the speed and accuracy of the classifier.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>But not before</td>
<td>By default, the machine learning process runs as soon as you complete this wizard. Select this option if you want to run the scan later, then specify the earliest time to run the scan. Note that only one machine learning classifier can be run at a time. If multiple machine learning classifiers are scheduled to run at the same time, they are run sequentially instead. Machine learning classifiers can be run at the same time as other types of classifiers.</td>
</tr>
</tbody>
</table>

### Machine Learning Wizard - Finish

A summary of this machine learning classifier appears. It lists the name of the data, the Crawler being used to perform the scan, the root folder, the content type, and the user logon. It also shows the positive, negative, and all-documents examples you provided and schedule information.

When you click **Finish**, a new classifier is created.
Unless otherwise configured in the scheduler, the scan task is run immediately.

Creating a rule from a content classifier

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content classifier</td>
<td>The content classifier from which you are creating a rule. This field is not editable.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of content classifier: PreciseID Pattern, Key Phrase, etc. This field is not editable.</td>
</tr>
<tr>
<td>Rule name</td>
<td>By default, the name of this rule is the name of the classifier. Enter a new name if desired.</td>
</tr>
<tr>
<td>Add this rule to an existing policy</td>
<td>Select this option to add this rule to an existing policy.</td>
</tr>
<tr>
<td>Add this rule to a new policy</td>
<td>Select this option to create a new policy for this rule.</td>
</tr>
</tbody>
</table>

- Policy Type - Select the type of policy to which you want to add this rule: data loss prevention or discovery.
- Policy Name - Select the exact policy to which you want to add this rule.
- Policy Type - Select the type of policy to create: data loss prevention or 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 one level defined.) For more information, see Policy levels.
- Policy Owners - Click Edit to select a policy owner or owners from a list.
Defining Resources

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 TRITON AP-DATA, 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**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sources and Destinations</strong></td>
<td></td>
</tr>
<tr>
<td><strong>User directory entries</strong></td>
<td>Users or groups that may be a source or destination of sensitive data. These entries are imported from your user directory.</td>
</tr>
<tr>
<td><strong>Custom user directory groups</strong></td>
<td>Groups who may send or receive sensitive data besides the standard groups in your user directory. These groups are derived from custom LDAP queries.</td>
</tr>
<tr>
<td><strong>Custom users</strong></td>
<td>Users not in your user directory who may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Custom computers</strong></td>
<td>Computers not in your user directory that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Networks</strong></td>
<td>Networks that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Business Units</strong></td>
<td>Business units that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Domains</strong></td>
<td>Domains that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>URL categories</strong></td>
<td>URL categories that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Endpoint Devices</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>Endpoint devices that may be the source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Endpoint Applications</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>Applications that may be a source or destination of your sensitive data on endpoint machines.</td>
</tr>
<tr>
<td><strong>Endpoint Application Groups</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>Application groups that may be a source or destination of sensitive data on endpoint machines.</td>
</tr>
<tr>
<td><strong>Endpoint Printers</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>Printers that may be a source or destination of sensitive data.</td>
</tr>
<tr>
<td><strong>Remediation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Action Plans</strong></td>
<td>The action to take when a breach is discovered.</td>
</tr>
<tr>
<td><strong>Remediation scripts</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>The external script to run when a breach is discovered.</td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td>The notification message to send when a breach is discovered, the person to send it to, and the format.</td>
</tr>
</tbody>
</table>

*Not included with TRITON AP-WEB. Requires a TRITON AP-ENDPOINT DLP subscription.*
Sources and destinations

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 IBM Domino. CSV files are also supported. These users, groups, and computers are possible sources or destinations of sensitive information in your organization.

Shown are the name of the user or group, the type of entry (user or group), the name of the directory server from which the entries were imported, and the distinguished name (DN) of the entry. A DN is the name that uniquely identifies the entry in the directory. It is made up of attribute=value pairs, separated by commas.

There are likely too many users and groups to display on 1 screen. Use the Search for field to filter the display to just users and groups that meet certain criteria. You can
filter user directory entry resources by entering 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: All, Computer, Group, User, or OU. For users, the system searches the Name, Login Name, Email, and DN fields. For groups, it searches the Name, Email, and DN fields. For other types of entries, it searches only the Name and DN.

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.

---

**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 user directory groups

Use this screen to add or manage theoretical groups derived from existing user directory entries. Create groups by filtering the user directory with advanced LDAP queries. The group is in effect a view into the user directory; however, it does not modify the user directory in any way.

This option is useful for targeting precise user directory attributes and compound conditions. For example, you can define a group of all users whose manager’s name starts with the letter A.

---

**Tip**
In addition to user directory groups, you can create groups of TRITON AP-DATA resources. These can contain user directory entries as well as non-user directory resources such as URL categories, geo-locations, custom users, and custom computers. Such groups are referred to as business units. Refer to **Business Units, page 181** for more information.
To add a custom user directory group to a policy, you must first add it to a business unit, then select the business unit as a source or destination when configuring rules. The group objects are recalculated every time the user directory is synchronized with the system.

To create a custom user directory group:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the group</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the group</td>
</tr>
<tr>
<td>User directory</td>
<td>If you have more than one user directory configured in the system, select which one you want to query.</td>
</tr>
</tbody>
</table>
Defining Resources

176

3. Click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Query            | Enter an LDAP query that will search the specified user directory and filter it to create a custom grouping. For example, to create a group of objects where the Department, Company, or Description attribute is Sales, enter: 

```
(| (department=Sales) (company=Sales) (description= Sales))
```

The query must use LDAP filter syntax. The filter format uses a prefix notation.

```
filter = "(" filtercomp ")"
filtercomp = and / or / not / item
and = "&" filterlist
or = "|" filterlist
not = "!" filter
filterlist = 1*filter
item = simple / present / substring extensible
simple = attr filtertype value
filtertype = equal / approx / greater / less
equal = "="
approx = "~=
greater = ">=
less = "<="
extensible = attr [":dn"] [:" matchingrule] ":=" value / [":dn"] ":=" value
present = attr "=*"
substring = attr "=" [initial] any [final]
initial = value
any = "*" *(value "*")
final = value
Nested operations:

```
(| (\&\&((K1\&\dots) (K2\&\dots)) (\&\&((K3\&\dots) (K4\&\dots))))
```

**Note:** Not all user directory entries can be retrieved. Only those that Websense imports during user directory import are supported: users, groups, and computers. Queries are refreshed whenever you reimport user directory.

| View Sample Data | Click this button to view a sampling of the data in this group, such as entry names, types, and distinguished names (DNs). Use this sample to make sure that the correct information is being retrieved. |
Custom users

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

To add a custom user:
1. Click New.
2. Complete the fields as follows:

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

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname for the computer.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Enter a fully-qualified domain name for the computer (for example, myhost.example.com).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this computer.</td>
</tr>
</tbody>
</table>

3. Click OK.

Note
If this computer is an endpoint machine that you’ll be adding to an endpoint profile, be sure to include an FQDN as well as an IP address.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network you are adding.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this network.</td>
</tr>
<tr>
<td>Network address / Subnet mask</td>
<td>Select this option 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).</td>
</tr>
<tr>
<td>IP address range / To</td>
<td>Select this option to enter the IP address range for the network (for example, 192.168.0.0 to 192.168.255.255).</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Enter name for this domain. You can enter a concrete domain name that is the name of a specific computer—like <a href="http://www.example.com">www.example.com</a>. Or you can use wildcards that indicate a group of computers—for example, <em>.example.com, w</em>.example.com, www-?.example.com.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this domain.</td>
</tr>
</tbody>
</table>

3. Click OK.

For expedience, you can also import a list of domains. To do so:
1. Create a text or CSV file listing the domains of interest.
   - The file must be in UTF8 format.
   - The file must be of a .TXT or .CSV file type, not just include the .TXT or .CSV extension.
   - List each domain name on a separate line.
   - Optionally, provide a description for each domain on the same line.
     - Separate the name and description by a comma.
     - If the description contains commas, place the description text in quotes.
       For example:
       mycompany.com,Corporate domain
       mypartner.com,PartnerA domain
       myvendor.com,"VendorA, translation vendor for manuals"
       ...
2. Click Import on the Domains toolbar.
3. Browse to the file you created.
4. Click OK.
If a domain in the .TXT or .CSV file is already in the domain list, the description from the file will be used.

---

**Note**

By default, the system excludes predefined SaaS domains from Web DLP policies’ destinations list. The domains are part of a business unit called Excluded Resources. You can add domains and other resources to the business unit or remove them by clicking the business unit name and editing it.

Refer to *Business Units*, page 181 for more information.

---

**URL categories**

If you are using TRITON AP-WEB, 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 the system does not monitor URL categories on endpoint Web channels.)

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 the system 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 TRITON AP-WEB, 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. TRITON AP-WEB 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. See *Configuring URL categories and user names*, page 390 for more information.
Business Units

Use this screen to define or manage custom groups that can be sources or destinations of information in your organization. For example, a business unit could comprise all Marketing personnel in the domain codivision.com.

Unlike Custom user directory groups, business units can contain any TRITON AP-DATA resource. These can include user directory entries such as users and groups. They can also include non-user directory resources such as URL categories, geographical locations, custom users, custom computers, networks, domains, and printers.

When you create a business unit, you add resources to it. You can then assign it to a policy so that only these resources are permitted to send or receive data of a particular type.

If a business unit includes computers and users but a policy applies only to users, the system applies the policy only to users in the business unit.

To define a business unit:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this organization grouping or business unit.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this business unit.</td>
</tr>
</tbody>
</table>
| Display     | From the drop-down list, select the item you want to add to the business unit. Options include:  
  - Directory Entries  
  - Custom Computers  
  - Domains  
  - Networks  
  - Custom Users  
  - Countries  
  - Custom User Directory Groups  
The entry you select appears in the **Available List** grouping at the bottom of the screen.  
Note that Countries applies only to Web destinations, not sources or any other destination channel. This option lets you specify which countries can receive data via Web posts. |
Defining Resources

1. Click **OK**.

TRITON AP-DATA includes a predefined business unit called Excluded Resources. By default, it includes a list of SaaS domains, such as salesforce.com, that are typically excluded from Web policies and rules. You can add domains and other resources to the business unit or remove them by clicking the business unit name and editing it.

This business unit is automatically added to the destination exclude list for every new Web policy or rule. (In other words, new Web DLP policies and rules are not applied to the resources in this business unit.)

When you create a policy or rule, you can exclude all resources in the business unit, or add or remove resources from the exclude list as needed.

### Endpoint Devices

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter name for this type of device, such as “R&amp;D devices”</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this type of device.</td>
</tr>
<tr>
<td>Value</td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Click OK.

**Endpoint Applications**

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 the Technical Library article, [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 > Cloud Application**.
2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this application, such as Microsoft Word.</td>
</tr>
</tbody>
</table>
| Initiated by | If you are adding a Windows desktop application, enter the name of its executable file, such as “winword.exe”.  
If you are adding a Mac or Windows Store app, enter the app name. For example, enter Microsoft.SkypeApp* for the Windows Store Camera app.  
If you are adding a cloud application, enter its URL. |
| 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.                  |
Defining Resources

Field | Description
--- | ---
Trusted application | Select **Trusted Application** to indicate that the system does not need to enforce this application. Trusted applications are permitted to write any type of information to a removable media device—such as a USB drive. They are also permitted to copy any type of data to a remote shared drive on a network. You can specify up to 50 trusted endpoint applications. If necessary, a trusted application can be configured to represent multiple applications. Contact Technical Support for assistance if this is required. Note that there are no trusted cloud applications.

Screen capture | From the drop-down list, select the action to take when end users try to capture screens from this application. Screen captures are not analyzed for content. They are either blocked and audited, permitted and audited, or permitted as you specify here.

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.

### Endpoint Application Groups

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

**Note**

This section applies only to customers with the endpoint agent known as TRITON AP-ENDPOINT DLP. If you have TRITON AP-WEB, it does not apply to you.
Websense provides a list of application groups that group applications in like categories. Below are the application groups and the operations monitored on them by default in Windows environments. You can select other operations as needed.

<table>
<thead>
<tr>
<th>Type</th>
<th>Copy/Cut</th>
<th>File Access</th>
<th>Paste</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsers</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>CD Burners</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Storage</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Encryption Software</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Office Applications</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online medical</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>P2P</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Packaging Software</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portable Devices</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SaaS (online)</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

To view a list of the application groups, select **Main > Resources > Endpoint > Endpoint Application Groups**. You can filter your view on the Applications column and/or the Endpoint Operations column.
To define your own application group, click **New > Application Group** or **New > Cloud Application Group**. See *Adding custom application groups*, page 187 for instructions.

## Endpoint Printers

This screen displays endpoint printers that are monitored by the system. Each printer is associated by a name, type (auto-detected or user-defined), and print server (IP address or hostname).

Initially, only printers that are detected by the system are shown.

If desired, you can add printers to the list—both local and network printers that may be connected to endpoints.

To add a printer:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the printer or group of printers you’re adding. Example: HP-6050 or All HP printers.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this printer or group of printers.</td>
</tr>
<tr>
<td>Value</td>
<td>Specify exactly which printer or printers to include in this setting. Wildcards are supported.</td>
</tr>
<tr>
<td>Trusted endpoint printer</td>
<td>Select this check box if you do not want this endpoint printer to be monitored. If you check this box, all print jobs directed to this printer by endpoint users are permitted to go through without enforcement.</td>
</tr>
</tbody>
</table>

3. Click **OK**.

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

For data endpoints, the system analyzes text in the endpoint application before it is sent to the printer. The endpoint print solution is not print driver-dependent.

---

**Note**

If you have TRITON AP-WEB, this section does not apply to you.
Applying a column filter

Click the down arrow next to a column heading to apply a column filter. This lets you narrow down the list of application groups that you see in the table.

When you apply a filter to the Applications column, you’re prompted to select the applications you’re interested in viewing. If you select more than one, for example Notepad and Firefox, the system displays groups that have either of the applications. The OR operation is applied to the filter. If Notepad OR Firefox are in the group, display the group.

The same thing applies to the Endpoint Operations filter. When you apply a filter on this column, you’re prompted to select the operations you’re interested in viewing. If you select more than one, for example Download and Paste, the system displays groups that have either of the operations.

---

Note

If you combine column filters, the system displays only groups that match both filters. For example, (Notepad or Firefox) AND (Download or Paste).

Adding custom application groups

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

1. Click New > Application Group or New > Cloud Application Group. Applications include software packages like Microsoft Word and Excel that you install locally. Cloud applications are those accessed over the web.

2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the application group, such as Desktop Publishing.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the application group.</td>
</tr>
</tbody>
</table>
Once you've defined which information can go where, you can define what remediation to perform when a policy breach is discovered.
Action Plans

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit only</td>
<td>This action plan, the default, is designed for mild breaches. It permits all activity on all channels and logs incidents in the audit log. If configured, it also generates notifications.</td>
</tr>
<tr>
<td>Audit and Notify</td>
<td>Audit incidents from all channels, and if configured, generate notifications.</td>
</tr>
<tr>
<td>Block all</td>
<td>This action plan is designed for severe breaches. It blocks all incidents on all channels, audits them, and if configured, generates notifications. It requires a subscription to Websense Data Protect.</td>
</tr>
<tr>
<td>Drop Email Attachments</td>
<td>Drop email attachments that breach policy.</td>
</tr>
</tbody>
</table>

**Note**

The predefined action plans use the Default notification. You can edit the action plans to use a different notification—see *Notifications, page 202* and *Adding a new message, page 202* for details.

When you add rules or exceptions 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*
- *TRITON AP-WEB mode*
- *TRITON AP-EMAIL mode*, page 195

**Standard options**

1. Click **New**.
2. Enter an action plan name and description.
3. On the Data Loss Prevention tab, complete the fields as follows. See *Possible actions*, page 192 for a description of each possible action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Channels</strong></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Select an action to take when a breach is discovered on network email channels.</td>
</tr>
<tr>
<td>Mobile email</td>
<td>Select an action to take when a breach is discovered in content being sent to a user’s mobile device.</td>
</tr>
<tr>
<td>FTP</td>
<td>Select an action to take when a breach is discovered over FTP.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>Select an action to take when a breach is discovered over HTTP or secure HTTP.</td>
</tr>
<tr>
<td>Chat</td>
<td>Select an action to take when a breach is discovered over chat.</td>
</tr>
<tr>
<td>Plain text</td>
<td>Select an action to take when a breach is discovered via plain text.</td>
</tr>
<tr>
<td><strong>Endpoint Channels</strong></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Select an action to take when a breach is discovered on endpoint email.</td>
</tr>
<tr>
<td>Application control</td>
<td>Select an action to take when a breach is discovered on an endpoint application such as Word.</td>
</tr>
<tr>
<td>Removable media</td>
<td>Select an action to take when a breach is discovered on an endpoint device such as a thumb drive.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>Select an action to take when a breach is discovered on an endpoint device over HTTP or secure HTTP.</td>
</tr>
<tr>
<td>LAN</td>
<td>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.</td>
</tr>
<tr>
<td>Printing</td>
<td>Select an action to take when a breach is discovered on a local or network printer that is connected to an endpoint.</td>
</tr>
</tbody>
</table>
### Defining Resources

**Audit incident**
Select this check box if you want the system to log incidents in the incident database.

**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

**Include forensics**
When you audit an incident, you can capture forensics if desired. Forensics include information about the transaction that resulted in the incident, such as the contents of an email body: From:, To:, Cc: fields; attachments, URL category, hostname, file name, and more.
Forensics display in the incident report.

**Run remediation script**
Select this check box if you want the system to run a remediation script when an incident is discovered, then select the script to use from the drop-down list. See [Remediation scripts](#), page 197 for more information.

**Run endpoint remediation script**
Select this check box if you want the system to run an endpoint remediation script when an incident is discovered, then select the script to use from the drop-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 202 and [Adding a new message](#), page 202 for details.

**Tip:** There is a benefit to using the same template for each action plan. The system 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.
### Possible actions

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Allow data to be maneuvered based on your selection—for example, allow it to be printed or posted to a website.</td>
</tr>
<tr>
<td>Block</td>
<td>Deny or block data from being printed, posted, or emailed, depending on your selection.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Quarantine email messages containing sensitive data. Network email can be encrypted before it’s released. Select <strong>Encrypt on release</strong> to enable this feature. <strong>Note:</strong> When a mobile email message is released from quarantine, it is sent to the mobile device the next time the device is connected to the network.</td>
</tr>
<tr>
<td>Drop attachments</td>
<td>● Drops email attachments that are in breach of policy.</td>
</tr>
<tr>
<td></td>
<td>■ Applies to messages detected by the TRITON AP-EMAIL module.</td>
</tr>
<tr>
<td></td>
<td>■ Applies to rules that monitor data in “each part separately.”</td>
</tr>
<tr>
<td></td>
<td>● Quarantines email messages that:</td>
</tr>
<tr>
<td></td>
<td>■ Have a body breach, but not an attachment breach.</td>
</tr>
<tr>
<td></td>
<td>■ Have breaches in both the message body and attachment.</td>
</tr>
<tr>
<td></td>
<td>■ Are detected by agents other than TRITON AP-EMAIL, such as the protector.</td>
</tr>
<tr>
<td></td>
<td>■ Are detected when rules are monitoring data in “the transaction as a whole.”</td>
</tr>
<tr>
<td></td>
<td>■ Fail to drop attachments when indicated.</td>
</tr>
</tbody>
</table>
|                | **Note:** If a violation is found in a UUencoded attachment, the attachment is treated as email body and blocked rather than dropped. This is because additional content is placed between the attachments, including the attachment name. (UNIX-to-UNIX encoding (UUencoding) is a utility that most email applications use for encoding and decoding files.) Select **Encrypt on release** if you want quarantined messages to be encrypted before they’re released. If an attachment has been dropped, this option reattaches it and encrypts both the body and attachment before releasing the message. To release an incident, an administrator selects **Remediate > Release** on the incident details toolbar.
By default, all incidents are audited. Deselect the **Audit incident** check box if you do not wish to audit incidents.

If you subscribe to TRITON AP-DATA Discover, click the **Discovery** tab and complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run remediation script</td>
<td>Select this check box if you want the system to run a remediation script when an incident is discovered, then select the script to use from the drop-down list. See <em>Remediation scripts</em>, page 197 for more information.</td>
</tr>
<tr>
<td>Run endpoint remediation script</td>
<td>Select this check box if you want the system to run an endpoint remediation script when an incident is discovered, then select the script to use from the drop-down list.</td>
</tr>
</tbody>
</table>

1. Click **OK** to save your changes.
**TRITON AP-WEB mode**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| Audit incident      | Select this check box if you want TRITON AP-DATA 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 202* and *Adding a new message, page 202* for details. |

**Tip**: There is a benefit to using the same template for each action plan. The system 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.
TRITON AP-EMAIL mode

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Select an action to take when a breach is discovered on network email channels.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Permit</strong> - Let the message through.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Block</strong> - Deny or block the message or post.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Quarantine</strong> - Quarantine the message. Select <strong>Encrypt on release</strong> if you want the message to be encrypted before it’s released.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Drop attachments</strong> - Drops email attachments that are in breach of policy. Quarantines email messages that:</td>
</tr>
<tr>
<td></td>
<td>■ Have a body breach, but not an attachment breach.</td>
</tr>
<tr>
<td></td>
<td>■ Have breaches in both the message body and attachment.</td>
</tr>
<tr>
<td></td>
<td>■ Are detected by agents other than TRITON AP-EMAIL, such as the protector.</td>
</tr>
<tr>
<td></td>
<td>■ Fail to drop attachments when indicated.</td>
</tr>
<tr>
<td></td>
<td>NOTE: If a violation is found in a UUencoded attachment, the attachment is treated as email body and blocked rather than dropped. This is because additional content is placed between the attachments, including the attachment name.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Encrypt on release</strong> if you want quarantined messages to be encrypted before they’re released. If an attachment has been dropped, this option reattaches it and encrypts both the body and attachment before releasing the message.</td>
</tr>
<tr>
<td></td>
<td>To release an incident, an administrator selects <strong>Remediate &gt; Release</strong> on the incident details toolbar.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Encrypt</strong> - Encrypt the message.</td>
</tr>
<tr>
<td></td>
<td>In addition, you can create custom actions in the Email Security manager just for DLP policies. This gives you much more control over what happens to email that leaks sensitive data. For example, you can Bcc the original unfiltered message, delay message delivery until a certain date, or use IP address.</td>
</tr>
<tr>
<td></td>
<td>Custom TRITON AP-EMAIL actions are displayed here as well for your selection.</td>
</tr>
<tr>
<td></td>
<td>To create an action in the Email Security manager, select <strong>Policy Management &gt; Actions</strong>, click Add, then indicate that the action is to be used by DLP policies only.</td>
</tr>
<tr>
<td></td>
<td>With TRITON AP-EMAIL (on-premises mode), the Action option applies to all email directions.</td>
</tr>
<tr>
<td></td>
<td>For hybrid email, this option applies only to outbound email. (Inbound and Internal email is permitted, and an alert is sent to the TRITON AP-EMAIL administrator.)</td>
</tr>
</tbody>
</table>
4. Click **OK** to save your changes.

### Remediation scripts

Remediation scripts let you extend the functionality of discovery and data loss prevention.

---

**Note**

If you have TRITON AP-WEB or TRITON AP-EMAIL, this section does not apply to you.

---

**Related topics:**

- *Adding a new remediation script*, page 199
- *XML interface*, page 201
A remediation script is an executable that is run by a policy engine or an endpoint agent whenever an incident is triggered.

- **Endpoint Script** - Runs when endpoint incidents are triggered. 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, and it should be smaller than 5 MB.

- **Incident Management Script** - Runs on incidents selected in the Incident Report. To activate this script, open an incident under **Main > Reporting > Data Loss Prevention > Incidents**, then click **Remediate > Run Remediation Script** on the menu bar and select which script to run on that incident. This script can be used to automate tasks such as opening a CRM case. It is not executed automatically.
Defining Resources

- **Policy Script** - Runs when data loss prevention and discovery incidents are triggered. When a breach is discovered on a usage or discovery transaction, this script is run automatically. For example, it might encrypt data detected in discovery breaches or perform an action in a DRM system. 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 the network.

The system provides 3 scripts for network file system and endpoint discovery. These scripts can be used to copy or move content detected in breaches. See *Copying or moving discovered files*, page 221 for details.

For information on writing your own scripts, see *Creating Remediation Scripts* in the Websense Technical Library.

All 3 scripts are configured the same way in the Data Security manager. 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. For endpoint scripts, you can provide scripts for Windows, Linux, and Mac.

**Adding a new remediation script**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

---

**Warning**

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

---

1. Click **New** then select the type of script to create from the menu. For a description of each type of script, refer to *Remediation scripts*, page 197.
2. Enter a name for this remediation script.
3. Enter a description for this script.
4. Depending on the type of script, you can add up to 3 versions of this script: Windows, Linux, and Mac. When a breach is discovered on an endpoint, the system knows which version to run.
Select the tab for each operating system your endpoints run and complete the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable file</td>
<td>Browse to the executable file you want to run when certain incidents are detected. To change your selection, right-click Browse and select a new file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using a remediation script that copies files to a \ quarantined folder, be sure to exclude this folder from discovery scans.</td>
</tr>
<tr>
<td></td>
<td>Endpoint scripts must be smaller than 5 MB.</td>
</tr>
<tr>
<td>Arguments (optional)</td>
<td>Optionally, enter any arguments you want to include with the command. If the arguments are enclosed in quotation marks, separate arguments by a space. Instead of: “-e” “-o”</td>
</tr>
<tr>
<td>Additional Files</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Additional files are placed in the same folder as the script, and they are automatically downloaded by the endpoints.</td>
</tr>
</tbody>
</table>

5. 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 TRITON management server.
3. Click **OK** to continue.
5. If necessary, update the additional files in the same way.
6. Click **OK**.

For more information about writing a remediation script, refer to the Technical Library document, **Data Remediation Scripts**. This document describes:

- What interpreted languages you can use for the script
- The XML structure of discovery and DLP incidents
- How to supply remediation scripts with credentials in various operating systems
- Code samples
XML interface

TRITON AP-DATA 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:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analysisDetails</td>
<td>Root element.</td>
</tr>
<tr>
<td>transactionID</td>
<td>The internal transaction ID (unique ID that the system generates for every analyzed transaction).</td>
</tr>
<tr>
<td>action</td>
<td>The action taken (for example, permit or deny).</td>
</tr>
<tr>
<td>actionDetails</td>
<td>The action taken per destination.</td>
</tr>
<tr>
<td>violations</td>
<td>The detected violations, including the policy name and content.</td>
</tr>
<tr>
<td>name</td>
<td>Descriptive policy name</td>
</tr>
<tr>
<td>detectedValues</td>
<td>The matched sensitive content and its location (for example, email body or file attachment).</td>
</tr>
</tbody>
</table>
Notifications

Use this screen to define whom to notify when a breach is discovered. TRITON AP-DATA offers built-in notification templates—Default notification, Email policy violation, Web policy violation, and Mobile policy violation—that you can edit as required.

Click a message name to see its contents and define its recipients. You can edit the predefined notifications, or create a new one.

The system 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

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>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.</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom notifications should be sent. Maximum length: 1024 characters.</td>
</tr>
</tbody>
</table>
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). Note that if you change the mail server properties, it changes all occurrences of this server (such as alerts).

7. Complete the remaining fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td>Type the subject of the notification. This appears in the email <strong>Subject:</strong> 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% because it breached corporate policy.” Maximum length: 4000 characters.</td>
</tr>
<tr>
<td><strong>Recipients</strong></td>
<td>Define the recipient(s) for the notification. Click <strong>Edit</strong> to select business units or directory entries. Select <strong>Additional email addresses</strong> 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. For mobile incidents, do not send notifications to senders or senders’ managers. The incident was a result of someone synchronizing email to a mobile device; the message may have been permitted otherwise. Notifications can be sent only to people in your domain. If a recipient is out of your organization, the notification is not sent, no matter what is configured in a rule or action plan.</td>
</tr>
</tbody>
</table>
8. On the Notification Body tab, select a notification type and display format from the drop-down lists.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select the type of notification to send:</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td>Select <strong>Standard</strong> 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.</td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td>Select this option if you want to send a custom notification. Edit the default text as needed. The drop-down menu provides variables.</td>
</tr>
<tr>
<td><strong>Display as</strong></td>
<td>Select a display format from the drop-down list: HTML or plain text.</td>
</tr>
<tr>
<td><strong>Logo</strong></td>
<td>Displays the Websense logo, date, and time.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Displays the action taken when the breach was discovered.</td>
</tr>
<tr>
<td><strong>Message to user</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Incident details</strong></td>
<td>Displays incident details in the notification message.</td>
</tr>
<tr>
<td><strong>Violation triggers</strong></td>
<td>Attaches a list of rules violated by the breach.</td>
</tr>
<tr>
<td><strong>Include links so that recipients can perform operations on the incident</strong></td>
<td>Select this option if you want to include links in the notification so that administrators can perform workflow operations on the incident directly from it—operations such as assign, ignore, and escalate. (See sample links below this table.) Administrators can perform only the operations they have permission to perform from their role assignment. To enable the Release Incident operation, select the next option. Plain text notifications do not show links. To support this feature, you must create an email account for the TRITON AP-DATA system in Exchange. To avoid reconfiguration, make sure the credentials assigned to this mailbox do not expire. Once done, navigate to Settings &gt; General &gt; System &gt; Mail Servers and configure the incoming mail server. Use this mailbox for the system email address.</td>
</tr>
</tbody>
</table>
Allow recipients to release quarantined email from this notification

This option does not apply to TRITON AP-WEB customers.
Select this option if you want to allow message recipients to release blocked messages by replying to their notification message or by clicking the Release All link within the message.
See the knowledge base article, “Releasing blocked email in TRITON AP-DATA” for instructions on setting up the release by reply capability. You must configure options in both TRITON AP-DATA and Microsoft Exchange to enable it.

Attach policy-breach content
Attaches policy breach contents to the email message.

Important
To include links in notifications or to allow recipients to release messages, you must configure the incoming mail server to use to receive these requests. To do so, click Mail Server Settings on the toolbar. See Configuring mail servers, page 383 for more information.

9. Click OK to save your changes.

Below is an example of what users see at the bottom of their notification message. Here they can perform workflow actions on the incident and release the quarantined content.

Each link opens a window where you compose a message to the system’s notification server. This is how the workflow operation is communicated to the management server.
For example, if you click the link to change the status of an incident to High, a window like this appears:

The message is drafted for you, but you can add comments to display on the History tab of the incidents report. Do not delete the Comments section, even if you are adding no comments. If they appear, do not modify the To: field or the encryption codes at the bottom of the message. Without the encryption codes, workflow is not modified.

Click Send to notify the system of your request.

Successful changes are shown on the incident’s History tab. This includes the name of the administrator who performed the action, any comments that were added, and the action taken.

If there is an error processing the workflow request, you receive an error message or the error is saved in the syslog. Syslog errors are logged if the system experiences an internal error.
Discovery is the act of determining where sensitive content is located in your enterprise. A 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 discovery policy, page 209
2. Scheduling Discovery Tasks, page 225
Structurally, discovery policies are the same as data loss prevention 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 discovery task that describes where and when to perform the discovery, including specific network and endpoint computers to scan.

On networks, you can perform file system, database, or email discovery.

File Discovery comprises:

- **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.
- **Domino** - Scans documents in a data management system on a IBM Domino server.
- **Box cloud** - Scans documents, folders, and accounts in Box cloud storage systems.

Database Discovery comprises:

- **Database** - Scans the organization’s database servers and detects confidential information that is defined as policy breaches in tables.

Email Discovery comprises:

- **Exchange** - Scans the organization’s Microsoft Exchange server and identifies data in breach of policies.
- **Outlook PST** - Scans Outlook folders and detects confidential information that is defined as policy breaches in PST data files.

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

Discovery policies are different from data loss prevention 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.

Microsoft FCI map maps discovery policies with Microsoft File Classification Infrastructure rules. This identifies data on Windows Server 2012 machines that is in breach of policy so it can be remediated by FCI rules.
Creating a discovery policy

1. Select Main > Policy Management > Discovery Policies.
2. Click Manage Policies.
3. In the toolbar, click Add.
4. Select either Predefined Policy or Custom Policy.
5. If you select Predefined Policy, a wizard appears.
   a. Click Next and select the geographical regions to cover.
   b. Click Next and select the industries to cover.
   c. The Finish screen appears, summarizing your selections. Click Finish. The TRITON AP-DATA policy database is updated and a confirmation message appears. The policies you selected appear in a list.
   d. 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.)
6. If you select Custom Policy, a policy wizard appears.
   a. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Enter a name for this policy.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the policy in your organization.</td>
</tr>
<tr>
<td>Policy description</td>
<td>Optionally, provide a description of this policy.</td>
</tr>
<tr>
<td>Policy owners</td>
<td>By default, no policy owners are included in the policy. To define a policy</td>
</tr>
<tr>
<td></td>
<td>owner(s), click Edit.</td>
</tr>
<tr>
<td></td>
<td>In the resulting box, select the people who should receive notification</td>
</tr>
<tr>
<td></td>
<td>in the event of a policy breach. Click the right-arrow to move them into</td>
</tr>
<tr>
<td></td>
<td>the Selected List. These are known as policy owners.</td>
</tr>
<tr>
<td></td>
<td>See Selecting items to include or exclude in a policy, page 49 for</td>
</tr>
<tr>
<td></td>
<td>instructions on using the selector tool.</td>
</tr>
</tbody>
</table>
b. Click **Next**.

c. Define the **Condition** in which a breach of this rule should be considered an event. Specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the policy name for the rule name</td>
<td>This option is a default selection. A rule will be created for the new policy you are creating. This option allows the rule name to be the same as the policy name for easier identification.</td>
</tr>
<tr>
<td>Use a custom name for the rule</td>
<td>Select this option if you do not want the rule name to be the same as the policy name. When you select this option, you can add a custom <strong>Rule name</strong> and optionally, a <strong>Rule description</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This rule monitors</td>
<td>Specify if this rule should monitor <strong>specific data</strong> or <strong>all activities</strong> in the transaction as a whole or each part separately.</td>
</tr>
<tr>
<td>Add</td>
<td>Select this button to add one of the following content classifiers or attributes to the condition you are creating:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Patterns &amp; phrases</strong>: Follow the Select a Content Classifier wizard and choose one from the list of existing classifiers or build your own. Toggle between the General and Properties tabs to complete the information and click <strong>OK</strong>. See <strong>Patterns &amp; Phrases</strong>, page 94 for details.</td>
</tr>
<tr>
<td></td>
<td>● <strong>File Properties</strong>: Select file properties to add to this policy. Click <strong>OK</strong>. See <strong>File Properties</strong>, page 96 for details.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Fingerprint</strong>: Select the fingerprint classifier to use for this policy. Click <strong>OK</strong>. See <strong>Fingerprint</strong>, page 97 for details.</td>
</tr>
<tr>
<td>Remove</td>
<td>Select a Content Classifier and click <strong>Remove</strong> to not include it in the condition you are defining.</td>
</tr>
<tr>
<td>Condition Relations</td>
<td>Select an answer for the question: <em>When do you want to trigger the rule?</em> Choose one option from the following:</td>
</tr>
<tr>
<td></td>
<td>● <strong>All conditions are matched</strong></td>
</tr>
<tr>
<td></td>
<td>● <strong>At least one condition is matched</strong></td>
</tr>
<tr>
<td></td>
<td>● <strong>Custom</strong></td>
</tr>
<tr>
<td></td>
<td>If you select the Custom option, you get additional descriptions and options to make your choices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d.</td>
<td>Click <strong>Next</strong> to define the <strong>Severity &amp; Action</strong> for incidents that match this rule and to specify the action plan to be taken. Click <strong>Advanced</strong> to further specify the severity according to the number of matched conditions.</td>
</tr>
<tr>
<td>e.</td>
<td>Click <strong>Next</strong> to complete the wizard.</td>
</tr>
<tr>
<td>f.</td>
<td>Click <strong>Finish</strong> to create the new rule and add it to MyPolicy.</td>
</tr>
</tbody>
</table>

Like data loss prevention policies, you can add rules and exceptions to discovery policies. The procedure is the same. See **Managing rules, page 100** and **Adding exceptions, page 101** for instructions.
Scheduling the scan

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

For more information, see Scheduling Discovery Tasks, page 225.

Performing file system discovery

To perform discovery on a network file system:

1. Prepare your file server as described in the Data Security Deployment Guide.
2. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)
3. Select Main > Policy Management > Discovery Policies.
4. Under Network Discovery Tasks, select Add network task > File Discovery > File System Task.
5. Complete the fields on the screen and click Next to proceed through a wizard. For details on each screen, see the sections below:
Performing SharePoint discovery

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

To perform discovery on SharePoint folders:

1. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)
2. Select Main > Policy Management > Discovery Policies.
3. Under Network Discovery Tasks, select Add network task > File Discovery > SharePoint Task on the toolbar.
4. 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 236
   b.  SharePoint Discovery Task Wizard - Site Root, page 237
   c.  SharePoint Discovery Task Wizard - Scanned Documents, page 237
   d.  SharePoint Discovery Task Wizard - Scheduler, page 237
   e.  SharePoint Discovery Task Wizard - File Filtering, page 239
   f.  SharePoint Discovery Task Wizard - Advanced, page 240
   g.  SharePoint Discovery Task Wizard - Finish, page 240
Creating Discovery Policies

5. Deploy your changes by clicking Yes when prompted.

6. Discovery will take place at the time and day you scheduled in step 4d. To start it immediately, click Start. A message indicates when the scan finishes.

7. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.

Performing Domino discovery

To perform discovery on documents on an IBM Domino server:

1. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)

2. Select Main > Policy Management > Discovery Policies.

3. Under Network Discovery Tasks, select Add network task > File Discovery > Domino Task on the toolbar.

4. Complete the fields on the screen and click Next to proceed through a wizard. For details on each screen, see the sections below:
   a. Domino Discovery Task Wizard - General, page 260
   b. Domino Discovery Task Wizard - Server, page 261
   c. Domino Discovery Task Wizard - Scanned Documents, page 262
   d. Domino Discovery Task Wizard - Scheduler, page 262
   e. Domino Discovery Task Wizard - Policies, page 263
   f. Domino Discovery Task Wizard - Document Filtering, page 264
   g. Domino Discovery Task Wizard - Attachment Filtering, page 264
   h. Domino Discovery Task Wizard - Advanced, page 265
   i. Domino Discovery Task Wizard - Finish, page 265

5. Deploy your changes by clicking Yes when prompted.

6. Discovery will take place at the time and day you scheduled in step 4d. To start it immediately, click Start. A message indicates when the scan finishes.

7. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.

Related topics:

- Scheduling Discovery Tasks, page 225
- Creating a discovery policy, page 209
- Scheduling network discovery tasks, page 229
- Domino tasks, page 259
Performing Box cloud discovery

To perform discovery on files in Box cloud storage:

1. If you will use Internet Explorer to configure the Box discovery task, do the following. This is not required for other browsers.
   a. Select Settings > Internet Options.
   b. Select the Privacy tab.
   c. Click the Sites button.
   d. Enter the web address www.box.com and click Allow.
   e. Click OK.
2. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)
3. Select Main > Policy Management > Discovery Policies.
4. Under Network Discovery Tasks, select Add network task > File Discovery > Box Cloud 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. Box Cloud Discovery Task Wizard - General, page 241
   b. Box Cloud Discovery Task Wizard - Permissions, page 241
   c. Box Cloud Discovery Task Wizard - Scanned Accounts, page 242
   d. Box Cloud Discovery Task Wizard - Scheduler, page 242
   e. Box Cloud Discovery Task Wizard - Policies, page 243
   f. Box Cloud Discovery Task Wizard - File Filtering, page 244
   g. Box Cloud Discovery Task Wizard - Advanced, page 245
   h. Box Cloud Discovery Task Wizard - Finish, page 245
6. Deploy your changes by clicking Yes when prompted.
7. Discovery will take place at the time and day you scheduled in step 4d. To start it immediately, click Start. A message indicates when the scan finishes.
8. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.
Performing database discovery

To perform discovery on a database:

1. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)
2. Select Main > Policy Management > Discovery Policies.
3. Under Network Discovery Tasks, select Add network task > Database Discovery > Database Task from the drop-down list.
4. 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 246
   b. Database Discovery Task Wizard - Data Source Name, page 247
   c. Database Discovery Task Wizard - Scheduler, page 248
   d. Database Discovery Task Wizard - Policies, page 248
   e. Database Discovery Task Wizard - Table Filtering, page 249
   f. Database Discovery Task Wizard - Advanced, page 249
   g. Database Discovery Task Wizard - Finish, page 250
5. Deploy your changes by clicking Yes when prompted.
6. Discovery will take place at the time and day you scheduled in step 4c. To start it immediately, click Start. A message indicates when the scan finishes.
7. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.

Related topics:
- Scheduling Discovery Tasks, page 225
- Creating a discovery policy, page 209
- Scheduling network discovery tasks, page 229
- Database tasks, page 245
Performing Exchange discovery

To perform discovery on email on a Microsoft Exchange server:

1. Prepare your Exchange server as described in the Data Security Deployment Guide.

2. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)

3. Select Main > Policy Management > Discovery Policies.

4. Under Network Discovery Tasks, select Add network task > Email Discovery > Exchange Task from the drop-down list.

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 250
   b. Exchange Discovery Task Wizard - Mailboxes, page 252
   c. Exchange Discovery Task Wizard - Exchange Servers (online), page 251
   d. Exchange Discovery Task Wizard - Scheduler, page 253
   e. Exchange Discovery Task Wizard - Policies, page 253
   f. Exchange Discovery Task Wizard - Filtering, page 254
   g. Exchange Discovery Task Wizard - Advanced, page 254
   h. Exchange Discovery Task Wizard - Finish, page 255

6. Deploy your changes by clicking Yes when prompted.

7. Discovery will take place at the time and day you scheduled in step 4d. To start it immediately, click Start. A message indicates when the scan finishes.

8. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.
Performing Outlook PST discovery

PST files are Microsoft Outlook files that contain all the mail users get as well as all their contacts, calendar meetings, tasks, etc. PST files can contain data for more than 1 user.

To perform discovery on email on Outlook PST data files:

1. Create a discovery policy. (See Creating a discovery policy, page 209 for instructions.)
2. Select Main > Policy Management > Discovery Policies.
3. Under Network Discovery Tasks, select Add network task > Email Discovery > Outlook PST Task from the drop-down list.
4. Complete the fields on the screen and click Next to proceed through a wizard. For details on each screen, see the sections below:
   a. Outlook Discovery Task Wizard - General, page 255
   b. Outlook Discovery Task Wizard - Scanned Folder, page 256
   c. Outlook Discovery Task Wizard - Scheduler, page 256
   d. Outlook Task Discovery Wizard - Policies, page 257
   e. Outlook Discovery Task Wizard - Filtering, page 257
   f. Outlook Discovery Task Wizard - Advanced, page 259
   g. Outlook Discovery Task Wizard - Finish, page 259
5. Deploy your changes by clicking Yes when prompted.
6. Discovery will take place at the time and day you scheduled in step 4c. To start it immediately, click Start. A message indicates when the scan finishes.
7. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.

Related topics:
- Scheduling Discovery Tasks, page 225
- Creating a discovery policy, page 209
- Scheduling network discovery tasks, page 229
- Outlook PST tasks, page 255
Performing endpoint discovery

To perform discovery on endpoint systems:

1. Create a discovery policy. (See *Creating a discovery policy*, page 209 for instructions.)
2. Select **Main > Policy Management > Discovery Policies**.
3. Under Endpoint Discovery Tasks, select **Add endpoint task**.
4. 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 266
   b. *Endpoint Discovery Task Wizard - Endpoints*, page 266
   c. *Endpoint Discovery Task Wizard - Scheduler*, page 267
   d. *Endpoint Discovery Task Wizard - Policies*, page 267
   e. *Endpoint Discovery Task Wizard - File Filtering*, page 267
   f. *Endpoint Discovery Task Wizard - Advanced*, page 268
   g. *Endpoint Discovery Task Wizard - Finish*, page 268
5. Deploy your changes by clicking **Yes** when prompted.
6. Discovery will take place at the time and day you scheduled in step 4c.
7. To view and respond to discovery results, click **Main > Reporting > Discovery**. See *Viewing the incident list*, page 300 for information on reading these screens.
Creating Discovery Policies

Mapping FCI rules to discovery policies

To map FCI rules to discovery policies:

1. Create and enable a discovery policy. (See *Creating a discovery policy*, page 209 for instructions.)
2. Select **Main > Policy Management > Discovery Policies**.
3. Under Microsoft FCI Map, select **Map Microsoft FCI Rules**.
4. Map FCI rules to discovery policies.
   a. Select **Main > Policy Management > Discovery Policies**.
   b. Select **Map Microsoft FCI Rules**.
   c. See *Configuring FCI tasks*, page 269 for instructions on completing the map.
5. Enable and configure the FCI agent in System Modules.
   a. Navigate to **Settings > Deployment > System Modules**, and then click the FCI agent module.
   b. Enable the module and add a description if desired.
6. Deploy settings.

Viewing discovery status

To view the status of a discovery task:

1. Select **Main > Policy Management > Discovery Policies**.
2. Under Network Discovery Tasks, select **Manage 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.
Creating Discovery Policies

Viewing discovery results

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

See *The report catalog, page 272* and *Viewing the incident list, page 300* for information on reading these screens.

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

Updating discovery

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

To update a discovery task, double-click the discovery task under **Manage network tasks** and modify the schedule. 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 Reporting section for discovery:

1. Select **Settings > General > System > Reporting.**
2. Select the **Discovery** tab.
3. Complete the fields as described in *Setting preferences for discovery incidents, page 361.*
Copying or moving discovered files

You can copy or move sensitive content (files) when it is discovered. TRITON AP-DATA provides the following remediation scripts for the most common actions you may need to perform.

- **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.

- **MoveFiles** - 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.

Note the following:

- These remediation scripts are provided only for network file system discovery, discovery on endpoint systems and SharePoint.
- The scripts can be used for endpoint or policy remediation, but not for remediation instigated during incident management.
- Support for endpoint discovery is limited. The scripts assume that the endpoint always has access to the quarantine folder. If the quarantine folder is outside the network, the operations will not work.
- The scripts cannot be used for Exchange, Outlook PST, or database discoveries, and they cannot be used for local versions of SharePoint.
- These scripts are just common examples of what can be done with remediation scripts. You can write any remediation script you need to in order to perform an action on discovered incidents, such as encryption or DRM-integration.

See *Preparing and running the remediation scripts, page 222* for instructions on using these scripts.
Preparing and running the remediation scripts

1. Configure CopyFiles and MoveFiles

1. Open the scripts in Notepad. By default, they’re located in the RunCommands directory where TRITON AP-DATA is installed.

2. In the CopyFiles script, define the destination of the copied files in the “Location” field. This location should either be a network share accessible to all servers and/or endpoints running discovery in the form of a UNC path, or a local path on the server and/or endpoints running discovery. For example:
   - \InfosecServer1\Quarantine
   - c:\secure\quarantine.

   Using a network location is usually recommended but might not be possible if you are performing endpoint discovery on endpoints that are not always connected to the corporate network. When performing endpoint discovery and choosing a local quarantine, be sure to exclude that folder from all the discovery tasks to avoid triggering incidents on the quarantine.

   Notice that the remediation script does not perform any deletions from the quarantine location, so it is up to you to perform routine cleanup operations on this location.

3. In the MoveFiles script, define the destination of the moved files in the “Location” field. Refer to step 2 for requirements in this field.
   - DaysKeepActiveFiles - Number of days to keep files parameter.
   - QuarantineMsg - Stubbed file created by MoveFiles

4. In the Data Security manager, select Main > Policy Management > Resources > Remediation Scripts.

5. Select New > Endpoint Script or Policy Script.

6. Enter a name and description for one of the discovery scripts.

7. Browse to the executable file of interest: CopyFiles.py or MoveFiles.py. By default, they’re located in the RunCommands directory where TRITON AP-DATA is installed. Note that it is not necessary to complete the fields on the Linux tab of the Add Policy Remediation Script window.

8. 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. CopyFiles needs read permissions to all scanned files, and read/write permission to the archive (quarantine) folder. MoveFiles also needs write permissions to all scanned files.

9. Click OK.

Repeat steps 4-9 for the other script.

2. Add the remediation scripts to an action
Creating Discovery Policies

1. Select **Main > Policy Management > Resources > Action Plans**.
2. Select an action plan or select **New** from the toolbar.
3. On the **Discovery** tab, do one of the following:
   - Select the check box **Run remediation script**, and select the script to run.
   - Select the check box **Run endpoint remediation script**, and select the script to run for endpoint discovery.
4. Click **OK**.

### 3. Add the action plan to a policy

1. Select **Main > Policy Management > 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**.

### 4. Deploy your changes

The remediation script will run when 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.
Scheduling Discovery Tasks

Select Main > Policy Management > Discovery Policies to create or manage discovery policies for your organization.

You can manage policies and tasks from this page:

- **Create and manage policies** - used to add predefined policies as well as policies with custom policy owners, conditions, severity settings, and action plans.
- **Network discovery tasks** - used to set up discovery on network file systems, shared (SharePoint) directories, Domino servers, databases, Outlook PST data files, and Exchange servers.
- **Endpoint discovery tasks** - used to set up discovery on endpoint hosts.
- **Microsoft FCI map** - used to map discovery policies with Microsoft File Classification Infrastructure rules.

Related topics:

- **Scheduling network discovery tasks**, page 229
- **Scheduling endpoint discovery tasks**, page 266
- **File System tasks**, page 230
- **SharePoint tasks**, page 236
- **Domino tasks**, page 259
- **Box Cloud tasks**, page 240
- **Database tasks**, page 245
- **Exchange tasks**, page 250
- **Outlook PST tasks**, page 255
- **Configuring FCI tasks**, page 269

**Note**

This chapter applies only to customers with TRITON AP-DATA Discover. It does not apply those with TRITON AP-WEB.
Scheduling Discovery Tasks

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Ascending</td>
<td>Select this option to sort the table by the active column in ascending alphabetical order.</td>
</tr>
<tr>
<td>Sort Descending</td>
<td>Select this option to sort the table by the active column in descending alphabetical order.</td>
</tr>
<tr>
<td>Filter by (column)</td>
<td>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.</td>
</tr>
<tr>
<td>Clear filter</td>
<td>Select this option to clear the filter and display all tasks.</td>
</tr>
</tbody>
</table>

Buttons and controls

All discovery tasks have these options:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td><img src="image" alt="New icon" /></td>
<td>Creates a new discovery task.</td>
</tr>
<tr>
<td>Edit</td>
<td><img src="image" alt="Edit icon" /></td>
<td>Lets you edit the active discovery task. If your changes require deployment, the task changes to Stopped (deployment needed) status. When restarted, task starts from the beginning.</td>
</tr>
<tr>
<td>Delete</td>
<td><img src="image" alt="Delete icon" /></td>
<td>Deletes the highlighted discovery task.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Download icon" /></td>
<td>Downloads a detailed report on discovery scanning activities in CSV format.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td><img src="image" alt="Start icon" /></td>
<td>Starts a discovery scan.</td>
</tr>
<tr>
<td>Stop</td>
<td><img src="image" alt="Stop icon" /></td>
<td>Stops a discovery scan. When restarted, task starts from the beginning.</td>
</tr>
<tr>
<td>Pause</td>
<td><img src="image" alt="Pause icon" /></td>
<td>Pauses a discovery scan. When restarted, task starts from the last point it was paused.</td>
</tr>
<tr>
<td>Download Discovery Report</td>
<td><img src="image" alt="Download icon" /></td>
<td>Downloads a detailed report on discovery scanning activities in CSV format.</td>
</tr>
</tbody>
</table>
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.

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

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned items/tables/files</td>
<td>The total number of analyzed items, tables, or files.</td>
</tr>
<tr>
<td>Scanned size</td>
<td>The total size of analyzed items in MB. (Does not apply to database scans.)</td>
</tr>
<tr>
<td>Scanned mailboxes/records/computers/shares</td>
<td>Total number of analyzed mailboxes, records, computers, or shares (depending on the type of scan).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned items/tables/files</td>
<td>The total number of items, tables, or files detected in the scan. For scanned tables, this number shows how many records were scanned. It is limited by the sample size as well as the filter definition.</td>
</tr>
<tr>
<td>Scanned size</td>
<td>The size of items detected in the scan in MB, all totaled. (Does not apply to database scans.)</td>
</tr>
<tr>
<td>Scan progress</td>
<td>The progress of the scan, in percentage completed.</td>
</tr>
<tr>
<td>Analyzed items/tables/files</td>
<td>The number of items, tables, or files sent to the policy engine’s fingerprint repository.</td>
</tr>
<tr>
<td>Failed items/tables/files</td>
<td>The number of items, tables, or files that failed for various reasons. Click the link to see more details on failed items.</td>
</tr>
<tr>
<td>Filtered out items/tables/files</td>
<td>The items, tables, or files that were not included by the filters you specified in the task definition. Click the link to see more details on the items, tables, or files that were filtered-out.</td>
</tr>
<tr>
<td>Scanned mailboxes/records/computers/shares</td>
<td>The total number of mailboxes, records, computers, or shares that were scanned.</td>
</tr>
</tbody>
</table>
The Last Scan Statistics are derived as follows:

1. The crawler counts the number of items (such as tables) to scan. This is an estimate, because items might be added or removed while the process is running.
   - In this step, the crawler calculates the following values:
     - Estimated total tables
     - Estimated total records
2. The crawler counts the items that should be filtered out (not scanned).
3. The crawler begins the scan and analysis process.
   - It goes over all the items that should be checked. Some of them may be analyzed and some may not. It updates actual Scanned items/tables/records. It also updates the Failed items/tables/files and Analyzed items/tables/files.

### Manually deleting discovery tasks

If the crawler is unresponsive for any reason when you delete a discovery task from the management server, it is not alerted that you’ve deleted the task. When the crawler becomes responsive, it will continue to run the discovery scan as scheduled and consume unnecessary resources.

To avoid these repercussions, you must manually delete the task from its associated crawler.

Data Security manager warns you in this situation, and asks if you want to continue. If you do, manually delete the task as follows:

1. Identify the ID of the job to delete in one of two ways:
   a. View the Data Security System Log (Main > Status > System Log) and search for the entry stating the task was deleted. For example:
      ```
      The task Discovery_Name ID 8e76b07c-e8e5-43b7-b991-9fc2e8da8793 was deleted from the TRITON Manager, but not from the crawler, Crawler_Name 10.201.33.1.
      ```
   b. Log onto the crawler machine associated with the discovery task.
      i. Switch to the `%DSS_HOME%/DiscoveryJobs` folder.
      ii. Search for the relevant task and ID by opening each job, one at a time, and examining the first line of its `definition.xml` file.
For example, the first line of one file might show:

```xml
<job type="discovery" id="3178b4f9-96fe-4554-ad1d-eaa29fa23374" name="ora3" altID="168476">
```

If your task was named “ora3”, then you know the ID is 3178b4f9-96fe-4554-ad1d-eaa29fa23374.

2. Delete the job:
   a. On the crawler machine identified above, switch to the %DSS_HOME%/packages/Services folder.
   b. Run the following command:

   ```
   Python WorkSchedulerWebServiceClient.pyc -o deleteJob -j #jobId#
   ```

   Where jobId is the ID number you identified in step 1.

---

**Scheduling network discovery tasks**

Select **Main > Policy Management > Discovery Policies > Network Discovery 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 hostname if it is supplied, an FQDN if there is no hostname, and an IP address if there is no hostname or FQDN. The crawler does not search all of these, only the first property it encounters.

To add a new network task, click **New** then select the type of task to create from the menu. You can create any of the following types of discovery tasks:

- **File Discovery**
  - **File System tasks**, page 230
  - **SharePoint tasks**, page 236
  - **Domino tasks**, page 259
- **Box Cloud tasks**, page 240
- **Database tasks**, page 245
- **Exchange tasks**, page 250
- **Outlook PST tasks**, page 255
Scheduling Discovery Tasks

- Box Cloud tasks
- Database Discovery
  - Database tasks
- Email Discovery
  - Exchange tasks
  - Outlook PST tasks

A wizard appears.

---

**Important**

For best practice, only run discovery tasks on directories that are protected by an antivirus application and found to be clean. Running discovery tasks on files not known to be clean can lead to unexpected results such as a suspension or termination of the discovery tasks by the antivirus process. Running discovery tasks on files that were never scanned by an antivirus application can lead to a propagation of malware and viruses.

---

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**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the network server.</td>
</tr>
</tbody>
</table>

**File System Discovery Task Wizard - Networks**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>By default, discovery runs on no computers or networks. Click <strong>Edit</strong> to select the computers and networks to scan. See <em>Selecting items to include or exclude in a policy, page 49</em> for instructions on using the selector tool.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Click <strong>Advanced</strong> 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.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned folders</td>
<td>Select the shared folders you want to scan:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Administrative shares</strong> - Select this if you want to scan administrative share drives (sometimes known as hidden shares) such as C$ and D$.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Shared folders</strong> - Select this if you want to scan shared folders such as PublicDocs.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Specific folders</strong> - Select this if you want to scan specific folders, then enter the name(s) of the folder(s) to scan, separated by semicolons. Individual paths cannot exceed 256 characters including hostname or IP.</td>
</tr>
<tr>
<td>Method</td>
<td>Select the method of port scanning to use when scanning network shares:</td>
</tr>
<tr>
<td></td>
<td>- <strong>TCP</strong> - Select TCP if you want to scan the share drives using transmission control protocol.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ICMP</strong> - 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.)</td>
</tr>
<tr>
<td></td>
<td>If you want to use ICMP, configure your firewall to ignore the specific server running the crawler.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name of any user with network access to the specified computer/shares.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and confirm a password for this administrator.</td>
</tr>
<tr>
<td>Domain</td>
<td>Optionally, enter the domain name of the network.</td>
</tr>
</tbody>
</table>

---

**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.
Scheduling Discovery Tasks

File System Discovery Task Wizard - Scheduler

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the scheduler for the current task. Deselect <strong>Enabled</strong> 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.</td>
</tr>
<tr>
<td>Run scan</td>
<td>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.)</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose <strong>Daily</strong> or <strong>Weekly</strong>, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>If you select <strong>Once</strong> or <strong>Continuously</strong>, 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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait <em>nn</em> minutes between consecutive scans</td>
<td>If you select <strong>Continuously</strong>, this option appears. Select the number of minutes to wait between consecutive scans. (Each scan starts from the beginning.)</td>
</tr>
</tbody>
</table>

File System Discovery Task Wizard - Policies

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All discovery policies</td>
<td>Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies</td>
</tr>
<tr>
<td>Selected policies</td>
<td>Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.</td>
</tr>
</tbody>
</table>

File System Discovery Task Wizard - File Filtering
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Type</td>
<td>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.</td>
</tr>
<tr>
<td>Include file types</td>
<td>List the types of files to be scanned, separated by semi-colons. You can use the “<em>” or “?” wildcards. For example, “</em>.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: “<em>temp</em>. *”</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td>Filter by Age</td>
<td>Select this check box if you want to filter the files to scan by file age.</td>
</tr>
</tbody>
</table>
| Scan only files that were modified: | Then select one of the following options:  
- **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.  
- **From...To** - 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
Scheduling Discovery Tasks

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
</tbody>
</table>
| An average of (1-9999) Mbps | Select this option if you want to limit the bandwidth used for the discovery process to an average number of megabytes per second, then select the desired limit.  
This option does not control the network bandwidth per file. Large files might still consume the available network bandwidth for short periods of time.  
The option does, however, prevent strain on your file servers, network adapters, and on the TRITON AP-DATA system.  
While planning to use this feature, keep in mind the following:  
1. Each file will be downloaded as fast as the operating system will allow.  
2. Subsequent file operations can be paused to maintain average bandwidth utilization.  
3. Average bandwidth utilization is maintained across several file operations, not during single file operation.  
In addition, if the amount of data for discovery is big, consider placing the supplemental server with the crawler and policy engine closer to your data sources. This eliminates the need to copy large volumes of data across WAN links.  
Windows QoS can be configured to maintain throttling on a network level. |
| Full scan schedule | Select one of the following options 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 file access timestamps to be updated when files are scanned by Data Security. When this option is selected, the operating system controls the “Last Accessed” timestamp of scanned files.  
**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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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 - Site Root
- SharePoint Discovery Task Wizard - Scanned Documents
- 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
Scheduling Discovery Tasks

SharePoint Discovery Task Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the SharePoint server.</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Indicate where your data is located:</td>
</tr>
<tr>
<td></td>
<td>● Local - Select this option if you are performing discovery on a local or network SharePoint server.</td>
</tr>
<tr>
<td></td>
<td>● Online - Select this option if you are performing discovery on data residing in the cloud via SharePoint Online for Office 365.</td>
</tr>
</tbody>
</table>

SharePoint Discovery Task Wizard - Site Root

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Site root hostname     | ● Local - Enter the hostname of the SharePoint site root, such as http://gumby:1234/site_name. (Note that a site is different than a folder in SharePoint. Data Security supports only site-level URLs for this field.)  
  If you enter an IP address, your SharePoint administrator must add the IP address to an alternate access map. In SharePoint 2010, they should choose Central Administration > Alternate Access Mapping, and click Add Internal URLs. In SharePoint 2013, they should choose Central Administration > Configure alternate access mappings > Add Internal URLs.  
  ● Online - Enter the URL of the SharePoint site root—for example: http://comp.gumby.com.  
  Note: The system clock of the Data Security server running this task must be synchronized with the Internet time server within 5 minutes for connection to succeed. |
| User name              | Enter a user name that has access to the shared folder. This must be a user with administrative rights. Read permissions are not sufficient. |
| Password               | Enter and confirm a password for this user. |
| Domain                 | Optionally, enter the domain name of the network. |
### Scheduling Discovery Tasks

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 49 for instructions on using the selector tool.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>By default, discovery runs on no SharePoint sites. Click <strong>Edit</strong> to select the SharePoint sites to scan. See <a href="#">Selecting items to include or exclude in a policy</a>, page 49 for instructions on using the selector tool.</td>
</tr>
</tbody>
</table>

### SharePoint Discovery Task Wizard - Scheduler

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the scheduler for the current task. Deselect <strong>Enabled</strong> 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.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: once, daily, weekly, or continuously.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose <strong>Daily</strong> or <strong>Weekly</strong>, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>If you select <strong>Once</strong> or <strong>Continuously</strong>, 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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait (nn) minutes between consecutive scans</td>
<td>If you select <strong>Continuously</strong>, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.</td>
</tr>
</tbody>
</table>

### SharePoint Discovery Task Wizard - Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All discovery policies</td>
<td>Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.</td>
</tr>
<tr>
<td>Selected policies</td>
<td>Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.</td>
</tr>
</tbody>
</table>

### SharePoint Discovery Task Wizard - File Filtering
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Type</td>
<td>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.</td>
</tr>
<tr>
<td>Include file types</td>
<td>List the types of files to be scanned, separated by semi-colons. You can use the &quot;<em>&quot; or &quot;?&quot; wildcards. For example, &quot;</em>.doc; *.xls; *.ppt; *.pdf&quot;. 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 *.</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td>Filter by Age</td>
<td>Select this check box if you want to filter the files to scan by file age.</td>
</tr>
</tbody>
</table>
| Scan only files that were modified: | Select one of the following options:  
  - **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.  
  - **From...To** - 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
<tr>
<td>An average of (1-9999) Mbps</td>
<td>Select this option if you 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 TRITON AP-DATA system.</td>
</tr>
</tbody>
</table>
| Full scan schedule | Select one of the following options 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.

Box Cloud tasks

You can perform discovery on data stored in Box cloud. The discovery wizard has 8 pages:

- **Box Cloud Discovery Task Wizard - General**
- **Box Cloud Discovery Task Wizard - Permissions**
- **Box Cloud Discovery Task Wizard - Scanned Accounts**
- **Box Cloud Discovery Task Wizard - Scheduler**
- **Box Cloud Discovery Task Wizard - Policies**
- **Box Cloud Discovery Task Wizard - File Filtering**
- **Box Cloud Discovery Task Wizard - Advanced**
- **Box Cloud Discovery Task Wizard - Finish**
Box Cloud Discovery Task Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Crawlers that do not support Box Cloud discovery are grayed out (such as older versions).</td>
</tr>
</tbody>
</table>

Box Cloud Discovery Task Wizard - Permissions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Access</td>
<td>You must log onto Box in order to give Data Security access to your files.</td>
</tr>
<tr>
<td>1. If you are using Internet Explorer to configure this task, do the following. This is not required for other browsers.</td>
<td></td>
</tr>
<tr>
<td>■ Select Settings &gt; Internet Options.</td>
<td></td>
</tr>
<tr>
<td>■ Select the Privacy tab.</td>
<td></td>
</tr>
<tr>
<td>■ Click the Sites button.</td>
<td></td>
</tr>
<tr>
<td>■ Enter the web address <a href="http://www.box.com">www.box.com</a> and click Allow.</td>
<td></td>
</tr>
<tr>
<td>■ Click OK.</td>
<td></td>
</tr>
<tr>
<td>2. Click the Grant Access button.</td>
<td></td>
</tr>
<tr>
<td>3. You’re redirected to the Box website.</td>
<td></td>
</tr>
<tr>
<td>4. Log onto the Box account associated with your enterprise. Enter the email address (user name) and password of an account administrator and then click Authorize.</td>
<td></td>
</tr>
<tr>
<td>5. A Grant Access page appears in the Box interface.</td>
<td></td>
</tr>
<tr>
<td>6. Click Grant Access to Box to give TRITON AP-DATA permission to connect with your Box storage. With access, the system can read and write to all files and folders and manage the enterprise.</td>
<td></td>
</tr>
<tr>
<td>Box issues a security token to the TRITON management server and displays connection status.</td>
<td></td>
</tr>
<tr>
<td>7. On connection, you are returned to the Data Security manager to resume task configuration. Click Next to continue.</td>
<td></td>
</tr>
<tr>
<td>If Box fails to connect, you cannot move to the next page in the wizard. Try again, or try to log onto Box with different credentials.</td>
<td></td>
</tr>
</tbody>
</table>

Note: Box security tokens are valid for 60 days. Tasks that run with expired tokens complete with errors. In the Details pane for the task, the link for Scan Status explains: “Tokens are expired. Please re-enter credentials for the task.” If this happens, you must edit each Box task that uses the token and re-grant access.

Box Cloud Discovery Task Wizard - Scanned Accounts
**Scheduling Discovery Tasks**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All accounts</td>
<td>Select this option to scan documents and folders in all user accounts in the Box enterprise.</td>
</tr>
<tr>
<td>Selected accounts</td>
<td>Select this option to specify accounts to scan. Click <strong>Edit</strong> to select the user accounts or folders to scan. See <em>Selecting items to include or exclude in a policy</em>, page 49 for instructions on using the selector tool.</td>
</tr>
</tbody>
</table>

**Box Cloud Discovery Task Wizard - Scheduler**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the scheduler for the current task. Desselect <strong>Enabled</strong> 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.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: once, daily, weekly, or continuously.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose <strong>Daily</strong> or <strong>Weekly</strong>, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>If you select <strong>Once</strong> or <strong>Continuously</strong>, 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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait <em>nn</em> minutes between consecutive scans</td>
<td>If you select <strong>Continuously</strong>, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.</td>
</tr>
</tbody>
</table>

**Box Cloud Discovery Task Wizard - Policies**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All discovery policies</td>
<td>Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.</td>
</tr>
<tr>
<td>Selected policies</td>
<td>Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.</td>
</tr>
</tbody>
</table>
# Box Cloud Discovery Task Wizard - File Filtering

**Data Security Manager Help | TRITON AP-DATA | Version 8.0.x**

## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Include file types</strong></td>
<td>List the types of files to be scanned, separated by semi-colons. You can use the “<em>” or “?” wildcards. For example, “</em>.doc; *.xls; *.ppt; *.pdf” Click <strong>File Types</strong> 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 <strong>Include file types</strong> to *.</td>
</tr>
<tr>
<td><strong>Except</strong></td>
<td>List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td><strong>Filter by Age</strong></td>
<td>Select this check box if you want to filter the files to scan by file age.</td>
</tr>
</tbody>
</table>
| **Scan only files that were modified:** | Select one of the following options:  
  - **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.  
  - **From...To** - 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.
Box Cloud Discovery Task Wizard - Advanced

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
<tr>
<td>An average of (1-9999) Mbps</td>
<td>Select this option 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 network adapters and on the TRITON AP-DATA system.</td>
</tr>
</tbody>
</table>
| Full scan schedule | Select one of the following options 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.) |

Box Cloud Discovery Task Wizard - Finish

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Displays a summary of the Box cloud discovery task you just established.

Database tasks

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

In order to perform discovery on a database, the Data Security server must be able to connect to the data source over a supported interface. Websense has certified support for the following ODBC-compliant databases:

- Oracle 10g (ODBC driver 10.1.0.2.0)
- Oracle Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (32- and 64-bit)
- Microsoft SQL Server Express (SQL Server Express ODBC driver)
- IBM DB2 9.5 (ODBC driver 8.2.9)
- IBM Informix Dynamic Server 11.50 (IBM Informix ODBC driver 3.50)
- MySQL 5.1 (ODBC driver 5.1.5)

Due to MySQL limitations, you must define “string” columns with UTF-8 encoding to fingerprint them.
Scheduling Discovery Tasks

- Sybase ASE 15.0 (Sybase ODBC driver 15.0.0.152)
- Teradata v13 and v14

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. For best practice, be sure to test database connectivity before configuring content policies.

Data Security scans the following database field types:

- CHAR
- VARCHAR
- WCHAR
- WVARCHAR
- TINYINT
- SMALLINT
- INTEGER
- BIGINT
- DECIMAL
- NUMERIC
- REAL
- FLOAT
- DOUBLE
- TIME
- LONGVARCHAR

Performing database discovery

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 - Advanced
- Database Task Wizard - Finish
### Database Discovery Task Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the database server.</td>
</tr>
</tbody>
</table>

### Database Discovery Task Wizard - Data Source Name

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>Select the DSN for the database that you want to scan.</td>
</tr>
</tbody>
</table>

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 Creating a Data Source Name (DSN) in Windows, page 147 for instructions. (For a list of supported databases and field types, see Connecting to data sources, page 146.)

Click refresh to refresh the list.

Note that this DSN must be defined with the same user as the crawler you specified on the previous step.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use data source credentials</td>
<td>Select this option to use the name and password of the Data Security service account to access the database, that is the local administrator account that you defined when installing Data Security. Some databases allow you to use NT authentication to verify the login ID, so be sure the crawler’s credential is the one with the permission to access the database. Microsoft SQL Server allows you to use NT authentication or SQL Server authentication. If you're using SQL Server authentication, select Use the following credentials instead.</td>
</tr>
<tr>
<td>Use the following credentials</td>
<td>Enter credentials defined in the database itself, such as the sa account. (Do not enter the network credentials.)</td>
</tr>
<tr>
<td>● User name - Enter the user name of any user with “read” privileges to the database.</td>
<td></td>
</tr>
<tr>
<td>● Password - Enter the password for this user.</td>
<td></td>
</tr>
<tr>
<td>● Domain - Optionally, enter the domain for the entered user. If your database is using Windows authentication, include the domain name.</td>
<td></td>
</tr>
</tbody>
</table>
# Scheduling Discovery Tasks

## Data Security Manager Help

**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. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.

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 drop-down box and a time from the spinner.

Wait \( nn \) 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 option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.

Selected policies | Select this option 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. Column names are included in each chunk that is analyzed. Only column names containing fewer than 40 characters are supported.

Database Discovery Task Wizard - Advanced

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
<tr>
<td>An average of (1-9999) Mbps</td>
<td>Select this option 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 TRITON AP-DATA system.</td>
</tr>
<tr>
<td>Discovery sample</td>
<td>Select one of the following options to indicate whether you want Data Security to scan all records of each table, or just a segment.</td>
</tr>
<tr>
<td>● Segment scan to</td>
<td>Select this option to scan X records from the table (the X records are chosen randomly); this will not scan the entire table.</td>
</tr>
<tr>
<td>● Scan all records of each table</td>
<td>Select this option if you want to scan all records. This can affect performance.</td>
</tr>
</tbody>
</table>

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 (online)
- Exchange Discovery Task Wizard - Mailboxes
- Exchange Discovery Task Wizard - Scheduler
- Exchange Discovery Task Wizard - Policies
- Exchange Discovery Task Wizard - Filtering
- Exchange Discovery Task Wizard - Advanced
- Exchange Discovery Task Wizard - Finish

Exchange Discovery Task Wizard - General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the Exchange server.</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Indicate where your data is located:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Local</strong> - Select this option if you are performing discovery on a local or network Exchange server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Online</strong> - Select this option if you are performing discovery on data residing in the cloud via Exchange Online for Office 365.</td>
</tr>
</tbody>
</table>

Exchange Discovery Task Wizard - Exchange Servers (online)

If you selected **Online** for your data storage location, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>Enter the email address used for logging on to your Exchange Online account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and confirm a password for this account.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click this button to test connection with the Exchange server. If you cannot connect, you may have entered the wrong credentials.</td>
</tr>
</tbody>
</table>
Exchange Discovery Task Wizard - Exchange Servers (local)

If you selected **Local** for your data storage location, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-discovered</td>
<td>Select this box to perform discovery on the Exchange servers that were automatically detected by the Data Security system. Click <strong>See list</strong> to view the auto-discovered servers.</td>
</tr>
<tr>
<td>Custom</td>
<td>TRITON AP-DATA 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 hostname or IP address of the additional server and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name of an administrator with access to the Exchange servers.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and confirm a password for this administrator.</td>
</tr>
<tr>
<td>Domain</td>
<td>Optionally, enter the domain for the entered administrator user.</td>
</tr>
<tr>
<td>Connect using secure HTTP</td>
<td>Select this option if you want Data Security to connect to your Exchange server using HTTPS and SSL.</td>
</tr>
<tr>
<td><strong>Note:</strong> Not all Exchange servers are set up for HTTPS. By default, Exchange 2003 is configured for HTTP and Exchange 2007 and 2013 are configured for HTTPS. Check the settings on your Exchange server before selecting this option.</td>
<td></td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click this button to test connection with the Exchange server. If you cannot connect, you may have entered the wrong credentials.</td>
</tr>
</tbody>
</table>

Exchange Discovery Task Wizard - Mailboxes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailboxes</td>
<td>Click <strong>Edit</strong> to select the mailboxes to scan. See <em>Selecting items to include or exclude in a policy, page 49</em> for instructions on using the selector tool.</td>
</tr>
</tbody>
</table>

**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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: once, daily, weekly, or continuously.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose Daily or Weekly, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>But not before</td>
<td>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 drop-down box and a time from the spinner.</td>
</tr>
<tr>
<td>Wait nn minutes between</td>
<td>If you select Continuously, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.</td>
</tr>
<tr>
<td>consecutive scans</td>
<td></td>
</tr>
</tbody>
</table>

Exchange Discovery Task Wizard - Policies

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All discovery policies</td>
<td>Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.</td>
</tr>
<tr>
<td>Selected policies</td>
<td>Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.</td>
</tr>
</tbody>
</table>
### Exchange Discovery Task Wizard - Filtering

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Mailbox or Folder name</td>
<td>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.</td>
</tr>
<tr>
<td>Filter by Subject</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Filter by Age | Select this check box if you want to filter the scan by age. Then select one of the following options:  
  - **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...To** - 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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
</tbody>
</table>
Scheduling Discovery Tasks

**Field** | **Description**
--- | ---
An average of (1-9999) Mbps | Select this option if you 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 TRITON AP-DATA system.

Full Scan | Select one of the following options to indicate when you want to perform full discovery scans:
- **Only on 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**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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

**Outlook PST tasks**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

The wizard for creating discovery tasks for Outlook PST files has 7 pages:

- **Outlook Discovery Task Wizard - General**
- **Outlook Discovery Task Wizard - Scanned Folder**
- **Outlook Discovery Task Wizard - Scheduler**
- **Outlook Task Discovery Wizard - Policies**
- **Outlook Discovery Task Wizard - Filtering**
- **Outlook Discovery Task Wizard - Advanced**
- **Outlook Discovery Task Wizard - Finish**
**Outlook Discovery Task Wizard - General**

**Data Security Manager Help | TRITON AP-DATA | Version 8.0.x**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the PST file server.</td>
</tr>
</tbody>
</table>

**Outlook Discovery Task Wizard - Scanned Folder**

**Data Security Manager Help | TRITON AP-DATA | Version 8.0.x**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Credentials</strong></td>
<td></td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name of a user with access to the network location.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and confirm a password for this user.</td>
</tr>
<tr>
<td>Domain</td>
<td>Optionally, enter the domain name of the network.</td>
</tr>
<tr>
<td><strong>Outlook Folder</strong></td>
<td></td>
</tr>
<tr>
<td>Folder name</td>
<td>Enter the UNC path of the server containing the PST files you want to scan, then browse to the desired PST folder. For example: \10.0.0.1\Server\PSTFiles. If your PST files are saved in different subdirectories under the same folder, specify the root folder here.</td>
</tr>
<tr>
<td>Scan subdirectories</td>
<td>Select this option if your PST files are saved in different subdirectories under the same root folder. Data Security will scan the subdirectories as well.</td>
</tr>
</tbody>
</table>

**Note**

While TRITON AP-DATA can scan PST files that are encrypted, it cannot scan files larger than 1 GB.
Outlook 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. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.

Outlook Task Discovery Wizard - Policies

Field | Description
---|---
All discovery policies | Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.

Selected policies | Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.

Outlook Discovery Task Wizard - Filtering

PST files are Microsoft Outlook files that contain all the email users get as well as all their contacts, calendar meetings, tasks, etc. PST files can contain data for more than one user, so they can contain several mailboxes with several different folders—for example: Inbox, Outbox, and Personal.

On this page, you can configure Data Security to filter by mailbox or folder (e.g. scan only user1\inbox, user2\outbox); or you can filter by email subjects (e.g. include all email with the subject “Project Name” or exclude email messages with the subject “Personal”).

Data Security scans within the PST for email messages that were sent or received within the last 2 months or scan only email messages that are larger than x KB.
### Field Description

**Filter by Mailbox or Folder name**
Select this check box if you want to scan by mailbox or folder name, then indicate what names to include and exclude. Wildcards are allowed. This field specifies which folders and mailboxes Data Security should scan within the PST file, where the Scanned Folder page specifies where to look for the PST file or files.

Include
List the mailboxes or folders to be scanned, separated by semi-colons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf” To set Data Security to scan all mailboxes or folders, set Include to “*”.

Exclude
List the mailboxes or folders to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.

**Filter by Subject**
Select this check box if you want to scan by subject lines (among them email, calendar items, notes, contacts, etc.), then indicate what subjects to include and exclude.

**Filter by Age**
Select this check box if you want to scan by file age.

Scan only files that were modified:
Select one of the following options:
- **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.
- **From... To** - 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 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 the file is scanned.
Outlook Discovery Task Wizard - Advanced

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>No limit: Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
<tr>
<td></td>
<td>Limit to an average of (1-9999) Mbps: Select this option if you 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 PST file servers, network adapters, and on the TRITON AP-DATA system.</td>
</tr>
</tbody>
</table>

Full Scan Schedule

<table>
<thead>
<tr>
<th>Full scan schedule</th>
<th>Select one of the following options to indicate when you want to perform full discovery scans:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Only on policy update: Select this option if you want to perform full discovery only when a discovery policy changes.</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>● 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.)</td>
</tr>
</tbody>
</table>

Outlook Discovery Task Wizard - Finish

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

Domino tasks

With Data Security, you can perform discovery on documents stored in an IBM Domino Data Management System.

Domino environments normally consist of one or more servers working together with data stored in Notes Storage Format (NSF) files. There are usually many NSFs on any given Domino server.

A discovery task treats a document (body and attachments) as one unit. This way, a breach is reported even if the sensitive content is scattered in different parts of the document that individually wouldn’t cause an incident.
Although NSF repositories contain documents and email messages, Data Security performs discovery only on documents.

---

**Important**

To use this feature, you must first:

- Install IBM Notes before installing Data Security. Notes must be on the same machine as the crawler.
- Provide your Notes user ID file and password when prompted by the Data Security installer. This information is used to authenticate access to the Domino server for fingerprinting and discovery.
- Log onto Notes, one time only, and supply a user name and password. This user must have administrator privileges for the Domino environment. (Read permissions are not sufficient.)
- Connect to the Domino server from the Notes client.

---

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

- *Domino Discovery Task Wizard - General*
- *Domino Discovery Task Wizard - Server*
- *Domino Discovery Task Wizard - Scanned Documents*
- *Domino Discovery Task Wizard - Scheduler*
- *Domino Discovery Task Wizard - Policies*
- *Domino Discovery Task Wizard - Document Filtering*
- *Domino Discovery Task Wizard - Attachment Filtering*
- *Domino Discovery Task Wizard - Advanced*
- *Domino Discovery Task Wizard - Finish*
**Domino Discovery Task Wizard - General**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
<tr>
<td>Crawler</td>
<td>Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the network server.</td>
</tr>
</tbody>
</table>

**Domino Discovery Task Wizard - Server**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino server to scan</td>
<td>Enter the hostname of the IBM Domino server that you want to scan—for example, gumby. Do not include the HTTP: prefix or leading slashes.</td>
</tr>
<tr>
<td>User name</td>
<td>When you click Next on this screen, the crawler tries to connect to the Domino server using credentials for the user indicated. These connection settings were provided when Data Security was installed on the Notes machine.</td>
</tr>
</tbody>
</table>

**Warning**

If this user has insufficient privileges for certain folders or NSF files on this server, those items will not be scanned. To connect with different user credentials, run the Data Security installer on the Notes machine, select the Modify option, and upload a different user ID file.
Domino Discovery Task Wizard - Scanned Documents

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document names are stored in the following field(s)</td>
<td>Enter the name of the field or fields that hold your document names. If you supply multiple field names, separate them with commas. For example: subject, docname, filename. By default, the “Subject” field is scanned.</td>
</tr>
<tr>
<td>Documents and folders to scan</td>
<td>The documents 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 49 for instructions on using the selector tool. Note the following: ● Document libraries are represented by folder icons. Click the folder icon with an arrow to display the library one level up in the document management hierarchy. You can also click the breadcrumbs above the list to navigate to another level. ● Domino documents are represented by file icons. Click a document to show its attachments. ● Notes Storage Format (NSF) files are represented by an NSF icon. These can include one or many documents. Drill down an NSF by clicking it, or move it to the Include list to scan the entire NSF. ● Attachments are represented by icons of a file with a paper clip. You can also specify the Notes views to scan.</td>
</tr>
<tr>
<td>Fields to scan</td>
<td>Indicate whether you want to scan the document body, attachments, or all fields except these. ● If you select Scan document body, enter the name of the field or fields that hold your documents’ body text. By default, it is “Body.” If you supply multiple field names, separate them with commas. For example: body, content, main. ● If you select Scan all other fields, all fields except body, subject, and attachment are scanned.</td>
</tr>
</tbody>
</table>

Domino Discovery Task Wizard - Scheduler

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>Run scan</td>
<td>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.)</td>
</tr>
</tbody>
</table>
### Scheduling Discovery Tasks

**Field** | **Description**
---|---
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. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.

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 drop-down box and a time from the spinner.

Wait *nn* 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.)

#### Domino Discovery Task Wizard - Policies

**Field** | **Description**
---|---
All discovery policies | Select this option if you want all discovery policies to be applied in this scan. TRITON AP-DATA will search for data that matches the rules in all deployed policies.

Selected policies | Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.
## Domino Discovery Task Wizard - Document Filtering

Filters the document body.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Document Name</strong></td>
<td></td>
</tr>
<tr>
<td>Include names</td>
<td>Select <strong>Filter by Document Name</strong> to look for specific document names. List the exact document names for which to search, separated by semi-colons. You can use the “<em>” or “?” wildcards. For example, “top_secret</em>”. The crawler searches for file names and their complete paths.</td>
</tr>
<tr>
<td>Except</td>
<td>List the exact document names to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td><strong>Filter by Age</strong></td>
<td></td>
</tr>
<tr>
<td>Scan only for document that were modified:</td>
<td>Select this check box to filter documents by age, then select the option that corresponds to the desired period. When you select this box, the default period is 24 months. <strong>Note:</strong> The age of a document is the latest date of its body and all attachments.</td>
</tr>
<tr>
<td><strong>Filter by Size</strong></td>
<td></td>
</tr>
<tr>
<td>Scan only files larger than</td>
<td>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.</td>
</tr>
<tr>
<td>Scan only items smaller than</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Domino Discovery Task Wizard - Attachment Filtering

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Type</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Include file types     | Select this option to look for specific attachments. List the types of files to be fingerprinted, separated by semicolons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”.
| Except                 | List the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well.                                  |
| **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**

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.

### Domino Discovery Task Wizard - Advanced

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No limit</td>
<td>Select this option if you do not want to limit the bandwidth used for the discovery process.</td>
</tr>
</tbody>
</table>
Scheduling Discovery Tasks

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An average of (1-9999) Mbps</td>
<td>Select this option if you 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 the TRITON AP-DATA system.</td>
</tr>
</tbody>
</table>
| Full scan schedule | Select one of the following options 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.) |

---

**Domino Discovery Task Wizard - Finish**

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

Select **Main > Policy Management > Discovery Policies > Endpoint Discovery 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this discovery task.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the endpoint discovery task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this discovery task.</td>
</tr>
</tbody>
</table>

### Endpoint Discovery Task Wizard - Endpoints

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>By default, discovery will run on all endpoint machines. Click <strong>Edit</strong> to select the endpoint to scan. For instructions on using the selector tool. Note that Linux network mounts, files symbolic links, folders symbolic links, classifiers, and filters are not scanned. In addition, if you are running a remediation script that copies files to a quarantine folder on Windows endpoints, be sure to exclude this folder from the scan. You cannot run remediation scripts for Linux endpoints.</td>
</tr>
</tbody>
</table>

### Endpoint Discovery Task Wizard - Scheduler

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run scan</td>
<td>Select how often you want to run the scan process: daily or weekly.</td>
</tr>
<tr>
<td>Hours to perform the scan</td>
<td>If you choose <strong>Daily</strong> or <strong>Weekly</strong>, specify the hours in which you want to run the scan, for example, daily at 2 a.m. For best practice, run discovery scans at night, after peak business hours. Select more than one time period to indicate when the scan should continue running if it is unable to complete during the first slot. Scans are not run more than once a day even when multiple time slots are selected.</td>
</tr>
<tr>
<td>Scan only while computer is idle</td>
<td>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. For Windows endpoints, idle time is derived from the operating system. For Linux endpoints, the idle time is 10 minutes.</td>
</tr>
<tr>
<td>Pause scanning while computer is running on batteries</td>
<td>Select this check box if you want to pause discovery scanning if the endpoint computer switches to battery mode.</td>
</tr>
</tbody>
</table>
Endpoint Discovery Task Wizard - Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All discovery policies</td>
<td>Select this option if you want all discovery policies to be applied in this scan. The system will search for data that matches the rules in all deployed policies.</td>
</tr>
<tr>
<td>Selected policies</td>
<td>Select this option if you want only certain policies to be applied in this scan, then select the policies to apply.</td>
</tr>
</tbody>
</table>

Endpoint Discovery Task Wizard - File Filtering

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Type</td>
<td>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.</td>
</tr>
<tr>
<td>Include file types</td>
<td>List the types of files to be scanned, separated by semi-colons. You can use the “<em>” or “?” wildcards. For example, “</em>.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 *.</td>
</tr>
<tr>
<td>Except</td>
<td>List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.</td>
</tr>
<tr>
<td>Filter by Age</td>
<td>Select this check box if you want to filter the files to scan by file age.</td>
</tr>
<tr>
<td>Scan only files</td>
<td>Select one of the following options:</td>
</tr>
</tbody>
</table>
| 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.  
                        | • From...To - 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        | Select this box to scan only files larger than a certain size, then use the spinner to specify the size.                                  |
| larger than            |                                                                                                                                             |
| Scan only files        | Select this box to scan only files smaller than a certain size, then use the spinner to specify the size.                                  |
| smaller than           |                                                                                                                                             |

Endpoint Discovery Task Wizard - Advanced
Configuring FCI tasks

Microsoft File Classification Infrastructure (FCI) is a Windows Server feature that lets you tag files based on classification criteria so you can control access to it, perform remediation on it, and more. (See Microsoft documentation for more details.)

Data Security augments the data classification capabilities that this infrastructure provides. For example, it can identify and classify sensitive data, such as personally identifiable information (PII) or personal health information (PHI), using one of more than 1700 predefined data security policies.

You do not run or schedule discovery in the Data Security manager. Rather, you set up scheduling or real-time scanning in the Microsoft File Server Resource Manager (FSRM).

In the Data Security manager, you simply map discovery policies to FCI rules. You can map predefined policies or create new ones. When initiated, Data Security compares your content with the discovery policies. When a match is detected, it applies the FCI rule to the data.

Data Security increases the accuracy of content classification. You can tag files on your servers and leverage Data Security’s FCI capabilities to remediate or take actions to comply with regulations.
To integrate Data Security with Microsoft FCI, you must install one or more Data Security FCI agents on the machine that is acting as your file server. This machine must be running Windows Server 2012 and have File Server Resource Manager (FSRM) enabled.

See FCI agent in the Data Security Installation Guide for more information.

### Mapping FCI rules

Select **Main > Policy Management > Discovery Policies > Map Microsoft FCI Rules** to configure discovery using FCI technology. This page lists the FCI rules you’ve already configured and the discovery policies associated with them.

Select **Enable FCI Map** to enable all FCI tasks. You can disable particular FCI agents in System Modules.

To configure a new FCI rule:

1. Ensure the FCI map is enabled.
2. Click **Add** on the FCI page.
3. Enter the name of an existing FCI rule. This should be the name of a classification rule that you set up in Microsoft’s FSRM console. The name must be an exact match. It is case-sensitive.
4. Select when the rule should be applied. Options include:
   - **One or more of the following policies was matched** - Select this option when you want the system to apply the FCI rule to the data when one or more Data Security discovery policies is matched, and then select the policies of interest.
     
     Add policies to or remove policies from the list as needed.
     
     Click a policy name to define the incident severity that should trigger the apply action. You can select:
     
     - **Any** - Use this option to apply the FCI rule for all matches, regardless of their severity.
     - **Selected severities** - Select one or more severity levels to indicate when to supply the FCI tag.
       
       - **High** - Apply the tag for high-severity incidents.
       - **Medium** - Apply the tag for medium-severity incidents.
       - **Low** - Apply the tag for low-severity incidents.

---

**Note**

When you map more than one policy to an FCI rule, the rule is satisfied when any of the policies is breached.
■ **No other FCI rules using this classification property were triggered** -
   After you define a classification property in the Microsoft FSRM console, you
   build rules to apply these properties to your files. Multiple rules can contain
   the same property, but with different thresholds for example. Select this
   option if you want to apply the current rule when no other rules using the
   same property were triggered.

5. Click **OK**.

To delete a rule, select it and click **Remove**.
To view incidents and reports on incidents, select Main > Reporting > Data Loss Prevention, Mobile Devices, or 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.

- **Recent Reports** - The reports you’ve viewed most recently are displayed on the main reporting page in a section called Recent Reports. The order of these reports changes with use.
- **Report Catalog** - Click Report Catalog to view a list of all the reports that are available for a given area, both built-in and user-defined.

**Note**

What you can see depends on your permissions. See Setting reporting preferences, page 358 for instructions on configuring settings for incidents and reports.

To learn about a report, click its name. To generate the report, click Run.

Summary reports are graphical and contain colorful executive charts.

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

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

1. Select **Main > Reporting > Data Loss Prevention, Mobile Devices, or Discovery**.
2. From the reports main page, select **View Catalog**.

The resulting screen lists all of the reports that are available for a given area—both built-in and user-defined. For a description of each report, see:

- *Data Loss Prevention reports*, page 324
- *Mobile devices reports*, page 332
- *Discovery reports*, page 335

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 also click the **Edit** button to edit a folder name or **Delete** to delete a folder. Predefined folders cannot be edited.
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.

---

**Note**

The operations you can perform on folders and reports in the catalog depend on your privileges. Superusers can perform these functions on all user-defined reports and folders. Other users can perform these functions only on reports and folders they created.

---

<table>
<thead>
<tr>
<th><strong>Button</strong></th>
<th><strong>Icon</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td><img src="#" alt="Run Icon" /></td>
<td>Run the selected report and display it.</td>
</tr>
<tr>
<td>Edit</td>
<td><img src="#" alt="Edit Icon" /></td>
<td>Edit or apply filters to the report.</td>
</tr>
<tr>
<td>Save As</td>
<td><img src="#" alt="Save As Icon" /></td>
<td>Save the report with a new name.</td>
</tr>
<tr>
<td>Export to PDF</td>
<td><img src="#" alt="Export to PDF Icon" /></td>
<td>Export the report to a PDF file.</td>
</tr>
<tr>
<td>Export to CSV</td>
<td><img src="#" alt="Export to CSV Icon" /></td>
<td>Export the report to a CSV file.</td>
</tr>
<tr>
<td>Schedule a task</td>
<td><img src="#" alt="Schedule a task Icon" /></td>
<td>Schedule this report for automatic email delivery.</td>
</tr>
<tr>
<td>Delete</td>
<td><img src="#" alt="Delete Icon" /></td>
<td>Delete the selected report. Predefined reports cannot be deleted.</td>
</tr>
</tbody>
</table>
There are additional buttons in the report catalog toolbar:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Tasks</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td>Lets you set preferences for incident lists and reports. For example, for data loss prevention incidents, you can define attachment size and forensics settings. For 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 <em>Setting reporting preferences</em>, page 358.</td>
</tr>
</tbody>
</table>

**Editing a report**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the current report.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the current report.</td>
</tr>
<tr>
<td>Availability</td>
<td>Select who should have access to the current report:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Report owner</strong> - Select this option if you want only the report owner to have access to this report.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All administrators</strong> - Select this option if you want all Data Security administrators to have access to this report.</td>
</tr>
<tr>
<td>Show top</td>
<td>This option applies to summary 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.</td>
</tr>
</tbody>
</table>
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. One by one, select the filters to apply to this report.
2. For each filter, select Enable filter in the Filter Properties pane.
3. Apply properties to the filter by making selections in the Filter Properties pane.

The filters that are available vary depending on the type of report. Filters and their properties are described below.

- Data Loss Prevention filters, page 276
- Mobile Device filters, page 282
- Discovery filters, page 287
## Data Loss Prevention filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. You can display incidents with the following actions:  
  - Permitted  
  - Blocked  
  - Attachment(s) dropped  
  - Quarantined  
  - Encrypted with profile key  
  - Encrypted with user password  
  - Denied (confirmed)  
  - Continued (confirmed)  
  In addition to the default actions, DLP actions configured in the Email Security manager are listed (TRITON AP-EMAIL only). |
| Application Name     | The Application Name filter enables you to filter incidents by the name of applications found in the incidents. Select the applications to include in the report. |
| 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 the Data Security manager. 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’ incidents are displayed in the report. The list of available channels depends on channels configured in the Data Security manager.  
  If you choose one or more email filters, specify the email direction to display: inbound, outbound, or internal. Email direction is available only for those with the TRITON AP-EMAIL module, endpoint agent, or protector.  
  If you choose to apply the endpoint application filter, select the operations you want to display in the report. For example, choose Paste to display all endpoint incidents where users pasted sensitive data into a document. |
| Classifier Matches   | This filter enables you to display specific classifiers whose thresholds have been exceeded. For example, select a dictionary classifier with profanity in it, and set its threshold to 3. The report displays only incidents where more than 3 terms from this dictionary were detected.  
  Click Edit to add or remove content classifiers to the filter, then select a threshold for each. |
| 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.) |
### Viewing Incidents and Reports

**Destination**

The **Destination** filter sets the incident list to display only incidents that were directed at specific destinations.

Select **Enable filter** to select destinations from your resource list or enter them as free text. Choose which method you want to use from the drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”.

If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available.

Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain. Complex filters can affect performance.

See *Selecting items to include or exclude in a policy, page 49* 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 TRITON AP-DATA modules.

Select each module to be displayed. The list of available modules depends on which modules were configured on the Data Security manager 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 static device (such as workstations). In the **Filter Properties** pane, select the endpoint type.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The <strong>Destination</strong> filter sets the incident list to display only incidents that were directed at specific destinations. Select <strong>Enable filter</strong> to select destinations from your resource list or enter them as free text. Choose which method you want to use from the drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”. If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available. Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain. Complex filters can affect performance. See <em>Selecting items to include or exclude in a policy, page 49</em> for more details on using this selector.</td>
</tr>
<tr>
<td>Detected by</td>
<td>The <strong>Detected by</strong> filter sets the incident list to display only incidents intercepted that were detected by specific TRITON AP-DATA modules. Select each module to be displayed. The list of available modules depends on which modules were configured on the Data Security manager System Modules page.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The <strong>Endpoint Type</strong> filter enables you to filter incidents according to the type of endpoint client, e.g. laptop or static device (such as workstations). In the <strong>Filter Properties</strong> pane, select the endpoint type.</td>
</tr>
</tbody>
</table>
## Viewing Incidents and Reports

### Event Time

The Event Time filter lets you filter incidents by the date and time they were received in the system as events. An event is any transaction being analyzed. (An incident is an event that breaches policy.) Select a date range, then select a time of day.

**Date Range**

- **Last \(n\) days** - Select this option to display incidents from the last \(n\) days, then select the number of interest. For example, display incidents from the last 30 days.
- **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.
- **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists. For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30.

**Time of Day**

By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select From and choose a time range.

- **Entire day** - Select Entire day to show all incidents during the date range, no matter what time of day they took place.
- **From ... to ...** - Select this option to show only incidents from a specific period.

For example, if you select **Last 60 days** and **From 8 a.m. to 5 p.m.**, the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.

If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around.

### File Name

This filter enables you to filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click Add. Continue until you’ve added all you need.

Note that complex filters can affect performance.
Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
Viewing Incidents and Reports

Incident Time
This filter lets you filter incidents by the date and time they occurred. An incident is an event that breaches policy. (An event is any transaction being analyzed.)
Select a date range, then select a time of day.

Date Range
- Last \( n \) days - Select this option to display incidents from the last \( n \) days, then select the number of interest. For example, display incidents from the last 30 days.
- Time period - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.
- Exact date and time - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists. For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30.

Time of Day
By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select From and choose a time range.
- Entire day - Select Entire day to show all incidents during the date range, no matter what time of day they took place.
- From ... to ... - Select this option to show only incidents from a specific period.
For example, if you select Last 60 days and From 8 a.m. to 5 p.m., the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.
If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Use the check boxes provided to set which policy’s incidents are displayed in the incident list.</td>
</tr>
<tr>
<td>Released Incident</td>
<td>This filter enables you to filter in or out SMTP incidents that have been released by an administrator (a reports remediation option).</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Lets you filter incidents by the rules they triggered.</td>
</tr>
<tr>
<td>Severity</td>
<td>Use this filter to select the severity of incidents to display. Select <strong>High</strong> if you want to display incidents of high severity, and so on. Select as many severity levels as desired.</td>
</tr>
</tbody>
</table>
### Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td>The <em>Source</em> filter lets you view only incidents that were initiated by specific sources. You can select sources from your resource list or enter them as free text. Choose which method you want to use from the drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”. If you have a role in which source and destination information is hidden for privacy reasons, you can enter one or more source IDs. Note that the filter returns values from all columns describing the source, such as URL category, hostname, IP address, and domain. Complex filters can affect performance. See <em>Selecting items to include or exclude in a policy</em>, page 49 for more details on using this selector.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The <em>Status</em> filter enables you to select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. You cannot filter by statuses that have been deleted from the system.</td>
</tr>
<tr>
<td><strong>Top Matches</strong></td>
<td>The <em>Top Matches</em> 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.</td>
</tr>
<tr>
<td><strong>Total Size</strong></td>
<td>This filter enables you to select the size of incidents to display. You can display incidents greater than a certain size (in KB), or between 2 sizes.</td>
</tr>
<tr>
<td><strong>Violation Triggers</strong></td>
<td>The <em>Violation Triggers</em> filter lets you select which incident triggers to display in the incident list. In the field, enter a violation trigger of interest and click <strong>Add</strong>. Continue until you’ve added all you need. Note that complex filters can affect performance.</td>
</tr>
</tbody>
</table>

---

*Data Security Manager Help ➤ 281*
## Mobile Device filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The <em>Action</em> filter enables you to filter incidents by the action that was performed on the incident. Select the check box for each action to be displayed.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The <em>Assigned to</em> 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 the Data Security manager. Assigned to selected administrators enables you to select specific administrators whose assigned incidents you want to display.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>The <em>Business Unit</em> filter enables you to filter incidents by the business unit to which they’re assigned.</td>
</tr>
<tr>
<td>Classifier Matches</td>
<td>This filter enables you to display specific classifiers whose thresholds have been exceeded. For example, select a dictionary classifier with profanity in it, and set its threshold to 3. The report displays only incidents where more than 3 terms from this dictionary were detected. Click Edit to add or remove content classifiers to the filter, then select a threshold for each.</td>
</tr>
<tr>
<td>Classifier Type</td>
<td>The <em>Classifier Type</em> filter enables you to select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)</td>
</tr>
<tr>
<td>Destination</td>
<td>The <em>Destination</em> 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 drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”. If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available. Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain. Complex filters can affect performance. See <em>Selecting items to include or exclude in a policy</em>, page 49 for more details on using this selector.</td>
</tr>
<tr>
<td>Detected by</td>
<td>The <em>Detected by</em> filter sets the incident list to display only incidents intercepted that were detected by specific TRITON AP-DATA modules. Select each module to be displayed. The list of available modules depends on which modules were configured on the Data Security manager System Modules page.</td>
</tr>
<tr>
<td>Device Details</td>
<td>This filter lets you display incidents that match certain device criteria. 1. In the Field menu, indicate whether you want to filter by device name, ID, user agent, model, operating system, or type. 2. Indicate whether you want the field to contain a certain value or be empty. 3. Enter a value in the blank text box. 4. Click <em>Add</em>.</td>
</tr>
</tbody>
</table>
Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device User          | This filter lets you display only incidents for specific mobile-device users. You can choose users from your resource list or enter identifying information manually.  
If you choose to use the resource list:  
- Use the Display field to indicate whether you want to pick from directory entries, business units, or custom users.  
- Enter a search term in the Filter by field.  
- Click the filter button.  
- Select items from the available list. See Selecting items to include or exclude in a policy, page 49 for more details on using this selector.  
If you choose free text, type a name, email address, or other information in the text box. Note that complex filters can affect performance. |
| Event Time           | The **Event Time** filter lets you filter incidents by the date and time they were received in the system as events. An event is any transaction being analyzed. (An incident is an event that breaches policy.)  
Select a date range, then select a time of day.  
**Date Range**  
- **Last n days** - Select this option to display incidents from the last n days, then select the number of interest. For example, display incidents from the last 30 days.  
- **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.  
- **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists.  
For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30.  
**Time of Day**  
By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select From and choose a time range.  
- **Entire day** - Select Entire day to show all incidents during the date range, no matter what time of day they took place.  
- **From ... to ...** - Select this option to show only incidents from a specific period.  
For example, if you select Last 60 days and From 8 a.m. to 5 p.m., the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.  
If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around. |
### Viewing Incidents and Reports

**File Name**
This filter enables you to filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click Add. Continue until you’ve added all you need.

Note that complex filters can affect performance.

**History**
History lets you filter incidents by the date, administrator, or details contained on the incident History tab. For example, you might display all incidents that jdoe closed during March 2011.

- Select **Filter by date** if you are interested in the date and time of the actions that were taken on the incident. Only actions during this period are included in the report. Select a date range and time of day.

- Select **Filter by administrator** to filter by the administrator who performed the listed workflow action. Enter the administrator names that you want to view. Separate multiple names by commas. For example: Type “jdoe, bsmith” to view incidents that jdoe and bsmith acted upon.

- Select **Filter by details** to filter based on details shown on the incident’s History tab. Details are automatically added when a workflow action is taken, such as “incident assigned to jdoe.” If administrators add comments to the incident (Workflow > Add Comments), those are appended to the workflow details.

Enter the text for which to search. You can search for all or part of the detail text. For example, you might enter “closed” to search for incidents that were closed during a certain period.

As always, this filter depends on the other filters you define such as Incident Time and Ignored Incident. If you want to filter only by history, define a large range for Incident Time, then define the history filter.

Note that complex filters can affect performance.

**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 311). Select the tags by which to filter the report and click Add. Continue until you’ve added all you need.

You can use these tags to group incidents for external applications.

Note that complex filters can affect performance.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>This filter enables you to filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click Add. Continue until you’ve added all you need. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>History</td>
<td>History lets you filter incidents by the date, administrator, or details contained on the incident History tab. For example, you might display all incidents that jdoe closed during March 2011. Select <strong>Filter by date</strong> if you are interested in the date and time of the actions that were taken on the incident. Only actions during this period are included in the report. Select a date range and time of day. Select <strong>Filter by administrator</strong> to filter by the administrator who performed the listed workflow action. Enter the administrator names that you want to view. Separate multiple names by commas. For example: Type “jdoe, bsmith” to view incidents that jdoe and bsmith acted upon. Select <strong>Filter by details</strong> to filter based on details shown on the incident’s History tab. Details are automatically added when a workflow action is taken, such as “incident assigned to jdoe.” If administrators add comments to the incident (Workflow &gt; Add Comments), those are appended to the workflow details. Enter the text for which to search. You can search for all or part of the detail text. For example, you might enter “closed” to search for incidents that were closed during a certain period. As always, this filter depends on the other filters you define such as Incident Time and Ignored Incident. If you want to filter only by history, define a large range for Incident Time, then define the history filter. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>Ignored Incident</td>
<td>The Ignored Incident filter lets you filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td><strong>Incident Tags</strong> let you filter incidents by a tag you earlier defined. (See Tagging incidents, page 311). Select the tags by which to filter the report and click Add. Continue until you’ve added all you need. You can use these tags to group incidents for external applications. Note that complex filters can affect performance.</td>
</tr>
</tbody>
</table>
## Viewing Incidents and Reports

**Incident Time**
This filter lets you filter incidents by the date and time they occurred. An incident is an event that breaches policy. (An event is any transaction being analyzed.) Select a date range, then select a time of day.

### Date Range
- **Last n days** - Select this option to display incidents from the last \(n\) days, then select the number of interest. For example, display incidents from the last 30 days.
- **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.
- **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists.

For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30.

### Time of Day
By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select From and choose a time range.
- **Entire day** - Select Entire day to show all incidents during the date range, no matter what time of day they took place.
- **From ... to ...** - Select this option to show only incidents from a specific period.

For example, if you select Last 60 days and From 8 a.m. to 5 p.m., the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.

If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Time</td>
<td>This filter lets you filter incidents by the date and time they occurred.</td>
</tr>
<tr>
<td>Date Range</td>
<td>Select a date range, then select a time of day.</td>
</tr>
<tr>
<td>Date Range</td>
<td>- <strong>Last n days</strong> - Select this option to display incidents from the last (n) days, then select the number of interest. For example, display incidents from the last 30 days.</td>
</tr>
<tr>
<td>Date Range</td>
<td>- <strong>Time period</strong> - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.</td>
</tr>
<tr>
<td>Date Range</td>
<td>- <strong>Exact date and time</strong> - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists.</td>
</tr>
<tr>
<td>Policy</td>
<td>Use the check boxes provided to set which policy’s incidents are displayed in the incident list.</td>
</tr>
<tr>
<td>Released Incident</td>
<td>This filter enables you to filter in or out SMTP incidents that have been released by an administrator (a reports remediation option).</td>
</tr>
<tr>
<td>Rule Name</td>
<td><strong>Rule Name</strong> lets you filter incidents by the rules they triggered.</td>
</tr>
<tr>
<td>Severity</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Filter Description

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source             | The **Source** filter lets you view only incidents intercepted that were directed at specific sources. You can select sources from your resource list or enter them as free text. Choose which method you want to use from the drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”.
If you have a role in which source and destination information is hidden for privacy reasons, you can enter one or more source IDs.
Note that the filter returns values from all columns describing the source, such as URL category, hostname, IP address, and domain.
Complex filters can affect performance.
See *Selecting items to include or exclude in a policy, page 49* for more details on using this selector. |
| Status             | The **Status** filter enables you to select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. You cannot filter by statuses that have been deleted from the system.                   |
| Synced by          | Use this filter to display incidents on messages that were synchronized by a certain number of mobile-device users.
For example, you want to know when the same violating message was synchronized by more than 10 users.                                                  |
| Top Matches        | The **Top 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.                |
| Total Size         | This filter enables you to select the size of incidents to display. You can display incidents greater than a certain size (in KB), or between 2 sizes.                                                           |
| Transaction Type   | Use this filter to display only incidents of a certain type, then select the types: email, calendar event, or tasks.                                                                                      |
| Violation Triggers | The **Violation Triggers** filter enables you to select which incident triggers to display in the incident list. In the field, enter a violation trigger of interest and click **Add**. Continue until you’ve added all you need.
Note that complex filters can affect performance.                                       |
## Viewing Incidents and Reports

### Discovery filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assigned to</strong></td>
<td>The <strong>Assigned to</strong> filter enables you to filter incidents by the person to whom they are assigned. <strong>Unassigned</strong> displays all incidents that have not been assigned to any administrator. Because filters can be available for all administrators, checking the <strong>Assigned to current administrator</strong> check box displays incidents assigned to the administrator who is currently logged onto the Data Security manager. <strong>Assigned to selected administrators</strong> enables you to select specific administrators whose assigned incidents you want to display.</td>
</tr>
<tr>
<td><strong>Channel</strong></td>
<td>The <strong>Channel</strong> filter enables you to limit which channels’ incidents are displayed in the report. The list of available channels depends on channels configured in the Data Security manager. Email Direction is available only for those with the TRITON AP-EMAIL module, endpoint agent, or protector.</td>
</tr>
<tr>
<td><strong>Content Classifier Name</strong></td>
<td>The <strong>Content Classifier Name</strong> filter enables you to select which specific content classifiers should be displayed in the incident list.</td>
</tr>
<tr>
<td><strong>Content Classifier Type</strong></td>
<td>The <strong>Content Classifier Type</strong> filter enables you to select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)</td>
</tr>
<tr>
<td><strong>Date Accessed</strong></td>
<td>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. Incidents relating to the access dates you choose are shown in the report. You can display incidents for data that was accessed within the last x days, within a date range, or on exact dates. You can also specify time periods.</td>
</tr>
<tr>
<td><strong>Date Created</strong></td>
<td>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. Incidents relating to the creation dates you choose are shown in the report. You can display incidents for data that was created within the last x days, within a date range, or on exact dates. You can also specify time periods.</td>
</tr>
<tr>
<td><strong>Date Modified</strong></td>
<td>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. Incidents relating to the modify dates you choose are shown in the report. You can display incidents that transpired within the last x days, within a date range, or on exact dates. You can also specify time periods.</td>
</tr>
<tr>
<td><strong>Detected by</strong></td>
<td>The <strong>Detected by</strong> filter sets the incident list to display only incidents that were detected by specific TRITON AP-DATA modules. Select each module of interest. The list of available modules depends on which modules configured on the Data Security manager System Modules page.</td>
</tr>
<tr>
<td><strong>Discovery Task</strong></td>
<td>Use this filter to select the discovery tasks to display in the report.</td>
</tr>
<tr>
<td><strong>Discovery Type</strong></td>
<td>Use this filter to select the type of discovery to display in the report: File System, Endpoint, SharePoint, SharePoint Online, Database, Exchange, Exchange Online, Outlook PST, and/or Domino.</td>
</tr>
<tr>
<td><strong>Endpoint Type</strong></td>
<td>The <strong>Endpoint Type</strong> filter enables you to filter incidents according to the type of endpoint client, e.g. laptop or static device.</td>
</tr>
<tr>
<td>Filter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Time</td>
<td>This filter allows you to select a time for the incidents you want to display. For filter properties, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Last $nn$ days</strong> - Select this option if you want to display incidents from the last $nn$ days, then select the number of days from the spinner.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Time period</strong> - Select this option if you want to display incidents that transpired in a particular date range, then select the range from the drop-down list. Example: last 24 hours or this week.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Exact dates</strong> - Select this option if you want to display incidents that transpired during a specific period, then select the <strong>From</strong> and <strong>To</strong> dates from the drop-down lists.</td>
</tr>
<tr>
<td>Folder</td>
<td>This filter allows you to view incidents from a certain folder or folders. Type a valid folder name into the field box, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>File Name</td>
<td>This filter enables you to filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click <strong>Add</strong>. Continue until you’ve added all you need. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>File Owner</td>
<td>Use this filter to filter incidents by file owner. Type a valid owner name into the field box, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>File Permissions</td>
<td>Use this filter to filter incidents by file permissions. Type a standard Access Control List (ACL) permission into the field box (such as USER name, password, services, or roles), then click <strong>Add</strong>. The values apply to all file-system scanning and Windows shares. Split multiple rows by commas and single rows by colons. For example:</td>
</tr>
<tr>
<td>File Size</td>
<td>Use this filter to filter incidents by file size, then choose the size of the file to include in the report.</td>
</tr>
<tr>
<td>Folder Owner</td>
<td>Use this filter to filter incidents by folder owner. Type a valid owner name into the field box, then click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
Viewing Incidents and Reports

**History**
History lets you filter incidents by the date, administrator, or details contained on the incident History tab. For example, you might display all incidents that jdoe closed during March 2011.

- Select **Filter by date** if you are interested in the date and time of the actions that were taken on the incident. Only actions during this period are included in the report. Select a date range and time of day.
- Select **Filter by administrator** to filter by the administrator who performed the listed workflow action. Enter the administrator names that you want to view. Separate multiple names by commas. For example: Type “jdoe, bsmith” to view incidents that jdoe and bsmith acted upon.
- Select **Filter by details** to filter based on details shown on the incident’s History tab. Details are automatically added when a workflow action is taken, such as “incident assigned to jdoe.” If administrators add comments to the incident (Workflow > Add Comments), those are appended to the workflow details. Enter the text for which to search. You can search for all or part of the detail text. For example, you might enter “closed” to search for incidents that were closed during a certain period.

As always, this filter depends on the other filters you define such as Incident Time and Ignored Incident. If you want to filter only by history, define a large range for Incident Time, then define the history filter.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>History lets you filter incidents by the date, administrator, or details contained on the incident History tab. For example, you might display all incidents that jdoe closed during March 2011.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Use <strong>Host Name</strong> to filter incidents by the host on which they were detected. Type a valid hostname into the field box, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Ignored Incident</td>
<td>The <strong>Ignored Incident</strong> filter lets you filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td><strong>Incident Tags</strong> let you filter incidents by a tag you earlier defined. (See <strong>Tagging incidents</strong>, page 311). Select the tags by which to filter the report and click <strong>Add</strong>. Continue until you’ve added all you need. You can use these tags to group incidents for external applications. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>Incident Time</td>
<td>This filter lets you filter incidents by time. Use it to select the time for the incidents you want to display.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Use <strong>IP Address</strong> to filter incidents by the host on which they were detected. Type a valid IP address into the field box, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Locked</td>
<td>Use this filter to show incidents that are locked or unlocked. You have 2 options: <strong>Show only locked incidents</strong> - Select this option to show only incidents that have been locked. <strong>Exclude locked incidents</strong> - Select this option to show only unlocked incidents. Disable the filter if you want to display both locked and unlocked incidents. Locking an incident prevents it from being overwritten with new data in subsequent scans. (To lock an incident, choose <strong>Workflow &gt; Lock</strong> in the Discovery incident report.)</td>
</tr>
</tbody>
</table>
### Table Properties tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

1. Select the columns to display in the table for this report. The options vary depending on whether this is a Data Loss Prevention properties, Mobile Device properties, page 293, or a Discovery properties.

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.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox Type</td>
<td>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.</td>
</tr>
<tr>
<td>Policy</td>
<td>Use the check boxes provided to set which policy’s incidents are displayed in the incident list.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Lets you filter incidents by the rules they triggered.</td>
</tr>
<tr>
<td>Severity</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>The Status filter enables you to select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. You cannot filter by statuses that have been deleted from the system.</td>
</tr>
<tr>
<td>Top Matches</td>
<td>The Top 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.</td>
</tr>
<tr>
<td>Total Size</td>
<td>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.</td>
</tr>
<tr>
<td>Violation Triggers</td>
<td>The Violation Triggers filter enables you to select which incident triggers to display in the incident list. In the field, enter the list of violation triggers to be displayed, separated by commas. Note that complex filters can affect performance.</td>
</tr>
</tbody>
</table>
## Data Loss Prevention properties

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The action taken on the incident, as determined by the action plan.</td>
</tr>
<tr>
<td>Analyzed by</td>
<td>Displays the name of the server component that analyzed the incident.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Either Unassigned or the name of the administrator assigned to handle this incident. (See Assigning incidents, page 308.)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel where the incident occurred. Possible channels include:</td>
</tr>
<tr>
<td></td>
<td>● Email</td>
</tr>
<tr>
<td></td>
<td>● Web</td>
</tr>
<tr>
<td></td>
<td>● FTP</td>
</tr>
<tr>
<td></td>
<td>● Endpoint application</td>
</tr>
<tr>
<td></td>
<td>● Endpoint printing</td>
</tr>
<tr>
<td></td>
<td>● Network printing</td>
</tr>
<tr>
<td>Destination</td>
<td>The intended destination or destinations of the content that violated policy.</td>
</tr>
<tr>
<td>Details</td>
<td>Details about the incident. Shows the subject in an SMTP incident, the URL in a Web incident, etc.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the name of the TRITON AP-DATA device or component that detected this incident.</td>
</tr>
<tr>
<td>Endpoint type</td>
<td>The type of endpoint involved in the incident: PC, laptop, etc.</td>
</tr>
<tr>
<td>Email direction</td>
<td>This column displays the direction of the email message that triggers an incident:</td>
</tr>
<tr>
<td></td>
<td>● Inbound</td>
</tr>
<tr>
<td></td>
<td>● Outbound</td>
</tr>
<tr>
<td></td>
<td>● Internal</td>
</tr>
<tr>
<td></td>
<td>If you are using the TRITON AP-EMAIL module, endpoint agent, or protector to monitor email, then all 3 directions are possible.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The ID number assigned to the event or transaction.</td>
</tr>
<tr>
<td>Event time</td>
<td>The date the event occurred.</td>
</tr>
<tr>
<td>File name</td>
<td>The name and size of the attachment for this incident.</td>
</tr>
<tr>
<td>ID</td>
<td>The incident’s unique ID number.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td>Displays any incident tag set for the incident. (See Tagging incidents, page 311.)</td>
</tr>
<tr>
<td>Incident Time</td>
<td>The time and date the incident was detected.</td>
</tr>
<tr>
<td>Top Matches</td>
<td>The maximum number of violations triggered by any given rule in the incident.</td>
</tr>
<tr>
<td>Policy</td>
<td>The policies that were violated by the content.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the incident: High, Medium, or Low. You define severity in the Severity &amp; Action page of the Add rule wizard. For example: &gt;0 matches = Low severity; &gt;20 = Medium; &gt;400 = High. You can also change an incidents severity (see Changing incident severity, page 310).</td>
</tr>
<tr>
<td>Source</td>
<td>The source of the incident. Could be a person, computer, or other.</td>
</tr>
</tbody>
</table>
### Column | Description
--- | ---
Status | The status of the incident. For example:
- New
- In process
- Closed
- False Positive
- Escalated
You can also add and filter by up to 17 custom statuses. See *Changing incident status*, page 309.
Total size | The total size of the file or attachment involved, if any, in megabytes.
Violation Triggers | The information that created the breach.
## Mobile Device properties

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The action taken on the incident, as determined by the action plan.</td>
</tr>
<tr>
<td>Analyzed by</td>
<td>Displays the name of the server component that analyzed the incident.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Either Unassigned or the name of the administrator assigned to handle this incident. (See Assigning incidents, page 308.)</td>
</tr>
<tr>
<td>Destination</td>
<td>The intended destination or destinations of the content that violated policy.</td>
</tr>
<tr>
<td>Details</td>
<td>Details about the incident. Shows the subject in an SMTP incident, the URL in a Web incident, etc.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the name of the TRITON AP-DATA device or component that detected this incident.</td>
</tr>
<tr>
<td>Email direction</td>
<td>This column displays the direction of the email message that triggers an incident:</td>
</tr>
<tr>
<td></td>
<td>● Inbound</td>
</tr>
<tr>
<td></td>
<td>● Outbound</td>
</tr>
<tr>
<td></td>
<td>● Internal</td>
</tr>
<tr>
<td></td>
<td>If you are using the TRITON AP-EMAIL module, endpoint agent, or protector to monitor email, then all 3 directions are possible.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The ID number assigned to the event or transaction.</td>
</tr>
<tr>
<td>Event time</td>
<td>The date the event occurred.</td>
</tr>
<tr>
<td>File name</td>
<td>The name and size of the attachment for this incident.</td>
</tr>
<tr>
<td>ID</td>
<td>The incident's unique ID number.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td>Displays any incident tag set for the incident. (See Tagging incidents, page 311.)</td>
</tr>
<tr>
<td>Incident Time</td>
<td>The time and date the incident was detected.</td>
</tr>
<tr>
<td>Top Matches</td>
<td>The maximum number of violations triggered by any given rule in the incident.</td>
</tr>
<tr>
<td>Policy</td>
<td>The policies that were violated by the content.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the incident: High, Medium, or Low. You define severity in the Severity &amp; Action page of the Add rule wizard. For example: &gt;0 matches = Low severity; &gt;20 = Medium; &gt;400 = High. You can also change an incidents severity (see Changing incident severity, page 310).</td>
</tr>
<tr>
<td>Source</td>
<td>The source of the incident. Could be a person, computer, or other.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the incident. For example:</td>
</tr>
<tr>
<td></td>
<td>● New</td>
</tr>
<tr>
<td></td>
<td>● In process</td>
</tr>
<tr>
<td></td>
<td>● Closed</td>
</tr>
<tr>
<td></td>
<td>You can also add and filter by up to 17 custom statuses.</td>
</tr>
<tr>
<td></td>
<td>See Changing incident status, page 309.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Synced by</td>
<td>Use this filter to display incidents on messages that were synchronized by a certain number of mobile device users. For example, you want to know when the same violating message was synchronized to more than 10 phones or iPads.</td>
</tr>
<tr>
<td>Total size</td>
<td>The total size of the file or attachment involved, if any, in megabytes.</td>
</tr>
<tr>
<td>Violation Triggers</td>
<td>The information that created the breach.</td>
</tr>
</tbody>
</table>
### Discovery properties

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzed by</td>
<td>Displays the name of the server component that analyzed the incident.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Either Unassigned or the name of the administrator assigned to handle this incident. (See Assigning incidents, page 308.)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel where the incident occurred. Possible channels include:</td>
</tr>
<tr>
<td></td>
<td>● Email</td>
</tr>
<tr>
<td></td>
<td>● Web</td>
</tr>
<tr>
<td></td>
<td>● FTP</td>
</tr>
<tr>
<td></td>
<td>● Endpoint application</td>
</tr>
<tr>
<td></td>
<td>● Endpoint printing</td>
</tr>
<tr>
<td></td>
<td>● Network printing</td>
</tr>
<tr>
<td>Details</td>
<td>The details listed in the forensics Properties tab. Shows the subject in an SMTP incident, the URL in a Web incident, etc.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the name of the TRITON AP-DATA device or component that detected this incident</td>
</tr>
<tr>
<td>Discovery task</td>
<td>The discovery task that identified the incident.</td>
</tr>
<tr>
<td>Discovery type</td>
<td>The type of resource that was scanned: File System, Endpoint, SharePoint, SharePoint Online, Database, Exchange, Exchange Online, and/or Outlook PST.</td>
</tr>
<tr>
<td>Endpoint type</td>
<td>The type of endpoint involved in the incident: PC, laptop, etc.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The ID number assigned to the event or transaction.</td>
</tr>
<tr>
<td>Event time</td>
<td>The date the event occurred.</td>
</tr>
<tr>
<td>File extension</td>
<td>The file extension of the file that violated policy. For example: .docx or .pptx.</td>
</tr>
<tr>
<td>File full path</td>
<td>The full directory path of the file that violated policy.</td>
</tr>
<tr>
<td>File name</td>
<td>The name of the file that violated policy.</td>
</tr>
<tr>
<td>File owner</td>
<td>The owner of the file that contained the policy violation.</td>
</tr>
<tr>
<td>File size</td>
<td>The size of the file that violated policy.</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder of the file that violated policy.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the host on which the violation was detected.</td>
</tr>
<tr>
<td>ID</td>
<td>The incident’s unique ID number.</td>
</tr>
<tr>
<td>Ignored incident</td>
<td>The incidents marked as ignored.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td>Displays any incident tag set for the incident. (See Tagging incidents, page 311.)</td>
</tr>
<tr>
<td>Incident Time</td>
<td>The time and date the incident was detected.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the host on which the violation was detected.</td>
</tr>
</tbody>
</table>
Viewing Incidents and Reports

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the current report.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the current report.</td>
</tr>
</tbody>
</table>
| 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 TRITON AP-DATA 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 option if you want to display trends for the last few days, then select the exact number of days. |
From the data loss prevention, mobile devices, or 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 the selected task now (regardless of its schedule).

Scheduling a new task

1. Select Main > Reporting > Data Loss Prevention / Mobile Devices / Discovery.
2. Select Report Catalog > View Catalog.
3. Click Scheduled Tasks on the toolbar.
4. Click New on the toolbar.
5. On the General tab, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task name</td>
<td>Enter a name for the task you are scheduling.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select Enabled to enable the task for use.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the task.</td>
</tr>
<tr>
<td>Report type</td>
<td>Indicate whether you want to email a data loss prevention, mobile devices, or discovery report.</td>
</tr>
</tbody>
</table>
6. On the **Mail Settings** tab, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report name</td>
<td>Select a report from the drop-down list. This is the report that will be emailed on the schedule you define.</td>
</tr>
<tr>
<td>Report format</td>
<td>If you selected a details report, select whether you want the report delivered in PDF or CSV format. Summary reports are graphical, so they can be exported to PDF only.</td>
</tr>
<tr>
<td>Sender name</td>
<td>Enter the name of the person from whom the report should be sent. This is the name that will appear in the email <strong>From</strong> field.</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom the report should be sent.</td>
</tr>
<tr>
<td>Outgoing mail server</td>
<td>The outgoing mail server that’s been configured appears on screen. If you want to change the server used, click <strong>Edit</strong> (the pen icon). Please note that changing this setting changes the configuration for the entire system.</td>
</tr>
<tr>
<td>Subject</td>
<td>Type the subject of the message containing the report. This appears in the email <strong>Subject:</strong> line.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Define the recipient(s) for the notification. Click <strong>Edit</strong> to select to select users or groups from a user directory. Select <strong>Additional email addresses</strong> 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.</td>
</tr>
</tbody>
</table>
7. On the **Schedule** tab, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Select the date and time on which to start the schedule. This is the date and time of the TRITON AP-DATA Server.</td>
</tr>
</tbody>
</table>
| 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 options 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 drop-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. |

8. 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 the system to run the report and email it now:

1. Select **Main > Reporting > Data Loss Prevention / Mobile Devices / Discovery.**
2. Select **Report Catalog > View 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

To view a list of data loss prevention incidents from the last 3 or 7 days, and their details:

1. Select Main > Reporting > Data Loss Prevention.
2. From Recent Reports, select Incidents (last 3 days) or Incidents (last 7 days).

To view a list of mobile device incidents from the last 3, 7, or 30 days, and their details:

1. Select Main > Reporting > Mobile Devices.
2. From Recent Reports, select Mobile Incidents (last 3 days) or Mobile Incidents (last 7 days) or Mobile Incidents (last 30 days).

To view a list of discovery incidents and their details:

1. Select Main > Reporting > Discovery.
2. From Recent Reports, select Incidents.

The top portion of the resulting screens lists incidents, their status, the action taken, and many more details.

The incidents list is a table displaying all data loss prevention, mobile device, or discovery incidents. By default, incidents are sorted by their incident 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 318.)

Click the down arrow on column header to sort, filter, or group incidents by that column. (See Applying a column filter, page 318 for more information.) Or click Table Properties to change the columns that are displayed, their order, and their width. See Table Properties tab, page 290 for a description of each property.

Use the radio controls 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 304 for more information about 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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td></td>
<td>Click this button to manage the workflow of the selected incident, then select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Assign</strong> - Select this option to assign the incident to someone or mark it as unassigned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Lock</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Unlock</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Change Status</strong> - Select this option to change the incident status or change the status labels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Change Severity</strong> - Select this option to change the incident severity assignment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Ignore Incident</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Tag Incident</strong> - Select this option to associate an incident with a custom tag that you can later use in filters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Add comments</strong> - Annotate the incident.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Download Incident</strong> - Select this option to download an incident. This option applies only to data loss prevention incidents. You can download just one incident at a time. This option applies only to DLP and mobile incidents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Delete</strong> - Select this option if you want to delete incidents. Depending on the type of incident (network, endpoint, mobile, or discovery), you may be able to delete selected incidents, all incidents that match the filter criteria for the current report, or all incidents.</td>
</tr>
</tbody>
</table>

(See *Managing incident workflow*, page 307 for details on all of these options.)
<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediate</td>
<td><img src="." alt="+" /></td>
<td>This option does not apply to TRITON AP-WEB customers. Click this button to remediate the selected incident, then select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Release</strong> - Select this option to release the selected incidents (email messages) from quarantine. This option applies only to data loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>prevention incidents on network, endpoint, and mobile email channels. You can add a comment to the confirmation window for future reference if desired.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Run Remediation Script</strong> - Select this option to run a remediation script on the selected incident.  (See Remediating incidents, page 313 for details on both options.)</td>
</tr>
<tr>
<td>Escalate</td>
<td><img src="." alt="✉" /></td>
<td>Click this button to escalate the selected incident to a manager or other person:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Email to Manager</strong> - Select this option to email the incident to the manager of the person generated the policy breach.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Email to Other</strong> - Select this option to email the incident to another person for action.  (See Escalating incidents, page 315 for details on both options.)</td>
</tr>
<tr>
<td>Manage Report</td>
<td>N/A</td>
<td>Click this button to edit the filter or table properties applied to the current report, then select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Edit Filter</strong> - Select this option to edit the filters applied to the report—for example, choosing a longer time period or single channel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Table Properties</strong> - Select this option to customize the properties of the incident table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Save</strong> - Select this option to save the changes you made to current report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● <strong>Save As</strong> - Select this option to save the current report with a new name.  (See Managing incident reports, page 317. for details on all of these options.)</td>
</tr>
<tr>
<td>Settings</td>
<td><img src="." alt="⚙" /></td>
<td>Lets you set preferences for incident lists and reports. For example, for data loss prevention incidents, you can define attachment size and forensics settings. For discovery incidents, you can set database thresholds. You can also define general settings, like filtering and printing, that apply to all types of incidents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information on configuring these settings, see Setting reporting preferences, page 358.</td>
</tr>
</tbody>
</table>
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 304 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. Only the first 500 rules or 500 MB for the incident are displayed.
Viewing Incidents and Reports

- **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. Only the first 500 triggers or 500 MB for the incident are displayed.

  ![Note](checkmark.png)
  
  If there are more than 500 violation rules or triggers, go to the Forensics tab. There you can see the complete transaction, including violations.

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. You cannot exclude an incident source from an email or Web data loss prevention policy.

- **Disable Policies** - Select this option to disable a policy if it is not producing the desired effect. You cannot disable an email or Web data loss prevention policy; you can only disable attributes.

- **Disable Rules** - Select this option to disable a rule if it is not producing the desired effect. To disable attributes in an email or Web data loss prevention policy, highlight the policy, click **Edit**, then de-select **Enabled** for the desired attributes.

  See *Tuning policies, page 322* for more information.

**Forensics**

The **Forensics** tab shows information about the original transaction.

For data loss prevention incidents that occurred on an email or a mobile channel, it displays the message subject, from, to, attachments, and message body. You can click links for details about the source or destination of the incident, such as email address, manager, and manager’s manager. You can retrieve thumbnail photos, if configured. You can also open attachments. The bottom portion of the incident screen displays the message body.

For data loss prevention incidents that occurred on a Web channel, the forensics could include the URL category property.

For discovery incidents, forensics includes the hostname 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.

Forensics are stored in the `\forensics_repository\data` directory on the TRITON management server.

Note that the extracted text may appear slightly different from channel to channel. This is due to the way the policy engine works in different environments.
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 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, released, or assigned to someone. These are automatically generated when a workflow operation is performed.

This tab also displays comments that were added by administrators using the **Workflow > Add Comments** option.

Each event in the incident’s history is shown in a separate row. You can expand or collapse events to view details.
## Managing incident 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.
- **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.
- **Add Comments** - Select this option to comment on the incident. Comments are added to the incident history.
- **Delete** - Select this option to delete selected incidents (all types), all incidents in the current report (network, endpoint, and mobile DLP incidents only), or all incidents at once (mobile DLP and discovery only).

The following option is available only for data loss prevention and mobile incidents:

- **Download Incident** - Select this option to download a data loss prevention 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.

### Related topics:

- Assigning incidents, page 308
- Changing incident status, page 309
- Changing incident severity, page 310
- Ignoring incidents, page 310
- Tagging incidents, page 311
- Adding comments, page 311
- Downloading incidents, page 312
- Deleting incidents, page 312
● **Unlock** - Select this option to unlock a locked incident.

---

**Tip**

If the system is configured properly, you can also manage the workflow of incidents from the email notifications that you receive. To set this up, navigate to **Main > Resources > Notifications**, then on the Notification Body tab, select **Include links so that recipients can perform operations on the incident.** (Links work only in HTML notifications, not plain text.)

---

### Assigning incidents

You can assign specific administrators to an incident. When you do, other administrators—those to whom it has not been assigned—no longer have the ability to perform actions on this incident, with the exception of Superusers. Administrators with the proper role may still be able to view the incident however.

To assign an incident to someone for action:

1. Select the incident.
2. From the toolbar, select **Workflow > Assign**.
3. Select the **Assign to** option.
4. From the drop-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** option.
4. Add comments if desired.
5. Click **OK**.

### Locking and unlocking incidents

During 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.

There are 5 predefined statuses:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Label</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="flag_new.png" alt="New" /></td>
<td>New</td>
<td>An administrator has not acted on this incident yet.</td>
</tr>
<tr>
<td><img src="flag_in_process.png" alt="In Process" /></td>
<td>In Process</td>
<td>An administrator is reviewing this incident.</td>
</tr>
<tr>
<td><img src="flag_closed.png" alt="Closed" /></td>
<td>Closed</td>
<td>This incident was reviewed and closed by an administrator.</td>
</tr>
<tr>
<td><img src="flag_false_positive.png" alt="False Positive" /></td>
<td>False Positive</td>
<td>An administrator identified this incident as a false positive or unintended match.</td>
</tr>
<tr>
<td><img src="flag_escalated.png" alt="Escalated" /></td>
<td>Escalated</td>
<td>The incident was escalated to a manager or other person.</td>
</tr>
</tbody>
</table>

Although you cannot change these statuses, you can add and maintain up to 17 more. To add a new status:

1. Select **Workflow > Change Status > Edit Statuses**.
2. Click **New** in the resulting window.
3. Enter a name for the status. It must be unique and fewer than 32 characters.
4. Enter a description for the status, up to 1024 characters.
5. Select from one of 12 available flags. If you add more than 12 statuses, you must reuse a flag.
6. Click OK.

The new status is added to the top of the status list. Rearrange the order of the list by selecting a status and clicking the up or down arrow. The order is reflected in reports and in the incident list when it’s sorted by the status column.

Click a status name to edit its properties (predefined statuses are uneditable). If you rename a status, all incidents with that status are updated with the new name.

If you delete a status, incidents with that status retain their designation; however, the status is no longer available in report filters.

**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 TRITON AP-DATA. 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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="High" /></td>
<td>High. This breach is significant and may have a broad impact on the business.</td>
</tr>
<tr>
<td><img src="image" alt="Medium" /></td>
<td>Medium. This breach is moderate and should be reviewed.</td>
</tr>
<tr>
<td><img src="image" alt="Low" /></td>
<td>Low. This breach is insignificant.</td>
</tr>
</tbody>
</table>

**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, the Data Security manager 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. (You can select multiple if you want to apply the same tag to all.)
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**.

### Adding comments

If you want notes to appear in an incident’s history, add comments to it.

1. Select the incident. (You can select multiple if you want to apply the same comment to all.)
2. From the toolbar, select **Workflow > Add Comments**.
3. Enter the desired comment in the Comment field.
4. Click **OK**.
To view an incident’s history, select the incident and click the History tab. Comments are displayed along with workflow details when you expand a row.

**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.

**Deleting incidents**

With TRITON AP-DATA, you can delete incidents that are known to be false positives or that are the product of a policy that is no longer relevant to your organization. There may be other reasons as well, depending on your security policies and practices.

- You can delete selected incidents.
- For discovery and mobile DLP, you can delete all incidents at once. Choosing this option deletes all discovery incidents or all mobile DLP incidents in the system (depending on your selection).
- For network, endpoint, and mobile DLP, you can delete all the incidents in the current report. For example, you can create a report that lists all email incidents originating from your company president, and then delete all those incidents in a single batch operation.

To delete incidents, you must be a Global Security Administrator or Super Administrator.

---

**Important**

You cannot undo this action.

---

**To delete selected incidents:**

1. Select the incidents to delete.
2. From the toolbar, select *Workflow > Delete > Selected Incidents*.
3. When prompted, select a reason for the action—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.
4. Click **OK** to confirm the action.

**To delete all the incidents in the report** (network, endpoint, and mobile DLP only):
Viewing Incidents and Reports

1. Set your report filters as desired. To do so, select Manage Report > Edit Filter.
2. When the report contains all the incidents you want to delete and no more, select Workflow > Delete > Report Incidents from the toolbar.
3. When prompted, select a reason for the action—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.
4. Click OK to confirm the action.

**To delete all incidents** (discovery and mobile DLP only):

1. From the toolbar, select Workflow > Delete > All Mobile Incidents / All Discovery Incidents.
2. For mobile DLP, skip to step #3. For discovery, select a reason for the action when prompted—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.
3. Click OK to confirm the action.

If you are deleting mobile or network DLP incidents, you can continue working while the operation runs in the background.

When incidents are deleted, their forensics are deleted from the forensic repository.

If the system is set up to do so, an email message is sent to all configured recipients notifying them that incidents were deleted from the incident database.

Incident deletions are also logged in the Audit Log, showing who deleted the incidents, when, and why.

### Remediating incidents

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

- **Releaseing incidents**, page 314
- **Running remediation scripts on incidents**, page 315

**Note**

This section does not apply to TRITON AP-WEB customers.

Click this button to remediate the selected incident, then select one of the following:

- **Batch Release** - Select this option to release selected email incidents 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 mobile agent, protector, or TRITON AP-EMAIL module—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 > General > System > Remediation. By default, the release gateway is the agent that delivered the message to the policy engine for analysis (the mobile agent, protector MTA, or TRITON AP-EMAIL).

There are 2 ways to release an incident:

**From the Incident Details report**

1. Select the incident or incidents you want to release.
2. From the toolbar, select Remediate > Batch Release.
3. A confirmation screen appears. Add comments to the release operation if desired. Comments are displayed on the History tab of the incident forensics.
4. Click OK.

For mobile incidents, you’re asked to select the users to release the message to. (Many users may have had the same message blocked when they synchronized their email to their mobile devices.) You can release the blocked message to all users who tried to sync it, or to selected users. If desired, you can release the message to everyone who syncs this message in the future.

If the system is set up to do so, an email message is sent to all configured recipients notifying them that incidents were released from the incident database.

The release status (success or failure) is also logged in the Audit Log.

**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.

See the knowledgebase article, Releasing blocked email in TRITON AP-DATA, for information on configuring the release gateway and Microsoft Exchange or Active Directory settings.
Running remediation scripts on incidents

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 TRITON AP-DATA, then 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 Upon script execution change status to. Select the desired status from the drop-down list.
5. Click OK.

Escalating incidents

Click this button to escalate the selected incident to the manager of the person who caused the incident or to another person.

For data loss prevention incidents, the following options are available:

- **Email to Manager** - Select this option to email the incident to the manager of the person who violated policy.
- **Email to Other** - Select this option to email the incident to another person for action.

For 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 the manager of the person who generated the incident**

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 manager of the person who generated the incident. For most DLP incidents, this is the incident source—the person who tried to move sensitive data. For mobile incidents, it is the person who received sensitive data and tried to synchronize it to a mobile device.

   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 or accept the default. Click the right arrow to choose variables to include in the subject, such as “This is to notify you that an employee’s message was %Action% because it breached corporate policy.” Maximum length: 4000 characters.
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. Click the right arrow to choose variables to include, such as %Incident Time% or %Severity%.
8. Click **OK**.

The selected incidents are immediately emailed to the manager.

**Email incidents to another**

1. Select the incident or incidents you want to email.
2. Do one of the following:
   - For data loss prevention incidents, from the toolbar, select **Escalate > Email to Other**.
   - For 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. Click the right arrow to choose variables to include in the subject, such as “This is to notify you that an employee’s message was %Action% because it breached corporate policy.” Maximum length: 4000 characters.

5. For data loss prevention 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. Click the right arrow to choose variables to include, such as %Incident Time% or %Severity%.

8. Click **OK**.

The selected incidents are immediately emailed to the people you selected.

**Managing incident reports**

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 the current report.
- **Save As** - Select this option to save the current report with a new name.

Related topics:

- *Editing report filters*, page 318
- *Editing table properties*, page 318
- *Applying a column filter*, page 318
- *Saving reports*, page 320
Editing report filters

To change the filters that are applied to this report, select Manage Report > Edit Filter. See Filter tab, page 275 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 290 for a description of the columns.

Set the maximum number of incidents to be displayed per page (20 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Ascending</td>
<td>Sorts the column’s entries by A-Z, from top to bottom.</td>
</tr>
<tr>
<td>Sort Descending</td>
<td>Sorts the column’s entries by Z-A, from top to bottom.</td>
</tr>
<tr>
<td>Group by this Column...</td>
<td>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).</td>
</tr>
</tbody>
</table>
| Filter by this Column...| When this option is selected, a pop-up caption box appears enabling you to filter the column according to specific words or to filter the column to exclude specific words. In most cases, you can select one of the following options in the Must field:  
  - **Contain** - Select this option if you want only incidents containing a specific word to appear in the incident list. If an entry in this column contains the word you enter, it appears in the incident list. Entries that do not contain this word do not appear. For example, entering “jon” displays incidents for Mary Jones and Jonathan Smith. Entering “jon” in the Contains field is equivalent to entering “*jon*”.  
  - **Be equal to** - Select this option if you want only incidents that match the word you enter exactly to appear in the incident list. For example, if you enter “jon”, incidents for Jon Smith would appear, but those for Jonathan Smith would not.
  - **Be empty** - Select this option if you want to display only incidents in which the specified field is empty (contains no value). The results are displayed in the column with or without the specific words in the column.  
| 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.

When you select **Save As**, indicate whether you want the report saved in one of the existing report folders or in a new folder.

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 318** 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 or exporting incidents to PDF

There are many ways to view or print incidents. You can:

- view a Print Preview
- export the incident to a PDF file
- export the incident to a CSV file, import the CSV into your favorite program

You can export the current incident, selected incidents, or all filtered incidents to a PDF file.

If you choose to export all filtered incidents, you can select a range to export (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.

Related topics:

- Setting general preferences, page 359
Here’s an example of what an incident report looks like:

![Incident Report Example](image)

To configure how incidents are grouped when exported to PDF, see Setting general preferences, page 359.

### 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 > Reporting > Data Loss Prevention / Discovery.**
2. From Recent Reports, 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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

This option is for custom data loss prevention policies only. You cannot exclude source from an email or Web data loss prevention policy.

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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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**.

**Note**

You cannot disable an email or Web data loss prevention policy; you can only disable attributes.

### Disabling rules

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

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**.

To disable attributes in an email or Web data loss prevention policy, highlight the policy, click **Edit**, then de-select **Enabled** for the desired attributes.

# Data Loss Prevention reports

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

1. Select **Main > Reporting > Data Loss Prevention**.
2. From the reports main page, select **View Catalog**.

Listed below are descriptions of the most common reports:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident List</td>
<td>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. You can also view: <strong>Incidents by Severity</strong> - See detailed information about each incident in the order of severity.</td>
</tr>
<tr>
<td>Executive Dashboard</td>
<td>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.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Find out which policies were violated most frequently over the last 7 days. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Top Violated Policies</td>
<td><strong>Last 7 Days</strong> - View which policies were violated most frequently over the last 7 days.</td>
</tr>
<tr>
<td></td>
<td><strong>Leaks to Removable Media Devices</strong> - View which policies users are violating when they copy confidential information to removable devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Leaks to Chat &amp; Email Web Sites</strong> - View which policies users are violating when they post confidential information to chat and email websites.</td>
</tr>
<tr>
<td></td>
<td><strong>Leaks to Malicious Web Sites</strong> - View which policies users are violating when they post confidential information to malicious websites.</td>
</tr>
</tbody>
</table>
Viewing Incidents and Reports

User Risk Summary (All Incidents) | Find out which users generated the most incidents across all active Data Loss Prevention policies.
---|---
User Risk Summary (Data Theft Risk Indicators) | Learn which users are behaving suspiciously and performing potentially unsafe computer practices.

**Severity & Action**

Violations by Severity & Action | 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.
---|---
- **Last 7 Days** - View incidents by the actions (permit, block, notify) and severities from the last 7 days.
- **Credit Card Violations** - View credit card-related incidents by the actions and severities applied to them.
- **Violations of Personally Identifiable Information (PII)** - View Personally-Identifiable Information (PII) incidents by the actions and severities applied to them.

**Sources & Destinations**

Top Sources & Destinations | Find out who are the top violators involved in data leakage and the top domains where sensitive data was posted.
---|---
- **Last 7 Days** - View the top violators involved in data leakage and the top domains where sensitive data was posted from the last 7 days.
- **Leaks to Public Email Web Sites** - View the top violators involved in leaking data to public email websites and the top domains of those websites.
- **Leaks to Malicious Web Sites** - View the top violators involved in leaking data to malicious websites and the top domains of those websites.
- **Credit Card Number Violations** - View who attempted to leak credit card information in plain text and the top destinations to which this information was leaked.
- **PII Violations** - View who violated a Personally-Identifiable Information (PII) policy and the top destinations to which PII information was leaked.
- **PCI Violations** - View who violated a PCI policy and the top destinations to which PCI information was leaked.

**Trends**

Incident Trends (current and previous quarter) | View incident statistics for this quarter. Find out if the number of violations in your organization reduces over time.

**Status**

Incident Status (last 7 days) | View the status of all DLP incidents from the last 7 days.

**Geographical Location**

Web DLP - Destinations by Severity | View Web DLP incidents by the geographical location where they occurred. View the destinations of the most severe outbound Web incidents, by geographical region.

Click a folder to expand it and see a list of related reports. Click Run to generate the report.
**DLP 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 Data Security manager 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 > Reporting > Data Loss Prevention** or **Discovery**.
2. From the report catalog, select **Executive Dashboard**. Remember that all reports represent only incidents from to which the administrator has access.
3. Click **Run** to generate the report.

The dashboard includes the following sections:

- **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.

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 317 for more details.)

To schedule this report to be delivered by email, see **Scheduling tasks**, page 297.
**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 loss prevention risk:

1. Select **Main > Reporting > Data Loss Prevention**.
2. From the report catalog, expand the Risk Assessment folder and select **Top Violated Policies (last 7 days)**.
3. Click **Run** to generate the report.

**User risk summary (all incidents)**

This report shows the users who generated the most incidents across all active DLP policies.

It contains the user’s full name, login name, department, manager, title, and business unit according to details imported from the user directory.

It also shows incident counts by severity.

To view this report:

1. Select **Main > Reporting > Data Loss Prevention**.
2. From the report catalog, expand the Risk Assessment folder and select **User Risk Summary (All Incidents)**.
3. Click **Run** to generate the report.

**User risk summary (data theft risk indicators)**

This report shows which users generated the most incidents across all active Data Theft Risk Indicator policies, including suspicious user activity, indicators of compromise, and employee discontent.

Suspicious User Activity policies include:

- Data Sent During Unusual Hours
- Database Files
- Email to Competitors
- Malicious Concealment
- Password Dissemination
- Suspected Mail to Self
- Suspicious Data Apps
- Unknown File Formats Over Time
- User Traffic Over Time
Indicators of Compromise policies include:

- Malware Communication Detection
- Suspected Malicious Dissemination
- Encrypted Files
- Password Files

Employee Discontent policies include:

- Disgruntled Employee
- Resume for HR
- Resume for HR Israel
- Resume for HR Cyrillic

Users who violate these policies could pose a security risk to your organization.

This report contains the user’s full name, login name, department, manager, title, and business unit according to details imported from the user directory.

It also shows incident counts by severity.

To view the report:

1. Select Main > Reporting > Data Loss Prevention.
2. From the report catalog, expand the Risk Assessment folder and select User Risk Summary (Data Theft Risk Indicators).
3. Click Run to generate the report.

For details about the policies that this report includes, see Data Loss Prevention policies in the Websense Technical Library.

**Violations 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 > Reporting > Data Loss Prevention.
2. From the report catalog, expand the Severity and Action folder and select All Violations Severity & Action (last 7 days).
3. Click Run to generate the report.

**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
TRITON AP-DATA due to breach of policy or those who were most frequently meant to receive unauthorized information.

1. Select **Main > Reporting > Data Loss Prevention.**
2. From the report catalog, expand the Sources and Destinations folder and select **Top Sources & Destinations (last 7 days).**
3. Click **Run** to generate the report.

**Incident trends**

After TRITON AP-DATA has been running for a while, 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 > Reporting > Data Loss Prevention.**
2. From the report catalog, expand the Trends folder and select **Incident Trends (this quarter).**
3. Click **Run** to generate the report.

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 of 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.** To specify how many policies to include in the report’s Top Policies chart, select **Manage Report > Show Top Items.** For example, do you want to see the top 5 violated policies? The top 10?

---

**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.

---

**Incident status**

View the status of all DLP incidents from the last 7 days.
**Top policies by status**

This section shows the status of incidents from the policies that were violated the most often.

Both the bar chart and table show the number of incidents that are new, in process, and closed for each top policy.

Click a link in the table to see details for the incidents.

**Incident status by administrator**

This section shows the number of new, in process, and closed incidents for each administrator. Click a link in the table to see details for the incidents.
Incidents by geographical location

The system lets you monitor or enforce to which countries data can be sent via the Web channel. Geolocation reports display incidents by the geographical location where data was sent.

1. Select **Main > Reporting > Data Loss Prevention.**
2. From the report catalog, expand the **Geographical Location** folder.
3. Select **Web DLP - Destinations by Severity.**
4. Click **Run** to generate the report.
5. A map of the world appears. (The report is schematic, not an accurate representation of global regions.)
   This map shows outbound incidents that occurred over the Web channel by severity and the geographical region where content was destined.
   Highlighted areas indicate the destinations for the most severe incidents.
   For example, you might learn that users are trying to upload your most sensitive data to a website or restricted domain in eastern Europe.
6. Hover over a highlighted area to view more details about the incidents in that region. Click to drill down further.
The resulting screen shows the total number of incidents using the selected filter for the region.

7. Right-click and select **Print** to print a chart or right-click and select **Save As** to save the report—with filters applied—under a new name.

To enforce to which countries data can be sent:

- Add the geographical locations of concern to a rule’s Destination page. Select **Main > Policy Management > DLP Policies > Create Custom Policy**, then on the Destination page, click **Edit** under Web and select **Countries** in the Display field.
- Add geographical locations to a business unit (**Main > Policy Management > Resources > Business Units**), and then add the business unit to the rule.

## Mobile devices reports

To see a catalog of all reports that are available for mobile devices:

1. Select **Main > Reporting > Mobile Devices**.
2. From the reports main page, select **View Catalog**.
The resulting screen lists all of the reports that are available for mobile devices—both built-in and user-defined.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident List</td>
<td>View a list of all the mobile email incidents for a certain period of time—that is, incidents discovered when users synchronize their mobile devices to their network email systems. 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. See Viewing the incident list, page 300 for an explanation of how to read and customize reports like this one.</td>
</tr>
<tr>
<td>Top Violated Mobile Policies</td>
<td>Find out which mobile DLP policies were violated most frequently over the last 7 days, so you can assess the security risk to your organization.</td>
</tr>
<tr>
<td>Top Synced Messages (last 7 days)</td>
<td>Find out the messages that were synchronized to mobile devices most frequently. View a list of incidents with details such as the time the message was sent, the source and destination of the message, the severity and more.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Find out when personally identifiable information was being synchronized to mobile devices, the users performing the sync, and the action taken.</td>
</tr>
<tr>
<td>Mobile PII Violations</td>
<td>Find out when credit card information was being synchronized to mobile devices, the users performing the sync, and the action taken.</td>
</tr>
<tr>
<td>Mobile Credit Card Violations</td>
<td></td>
</tr>
</tbody>
</table>

Click a folder to expand it and see a list of related reports. Click **Run** to generate the report.

**Top violated mobile policies**

This report shows which mobile DLP policies were violated most frequently over the last 7 days, so you can assess the security risk to your organization.

The bar chart shows how many times the policies were violated.

The table shows how many devices were involved in each breach—that is, how many tried to synchronize email that violated those policies. It also shows whether each violation was a high, medium, or low security breach. This setting is determined by which attribute was matched.
Click a link to view details about each incident.

**Top synced messages**

This report shows the messages that were synchronized to mobile devices most frequently.

View a list of incidents with details such as the time the message was sent, the source and destination of the message, the severity and more. (These properties are configurable.) View the message itself under incident forensics.

See *Viewing the incident list, page 300* for an explanation of how to read and customize incident reports like this one.

**Mobile PII violations**

This report shows the severity of personally identifiable information incidents and the action taken.

The top portion shows incidents by severity.

- The table shows how many high, medium, and low severity PII incidents occurred during email sync. Click a link to view details about each incident, such as the source and destination of the violating email message.
- The pie chart shows the percentage of PII violations that were of high, medium, and low severity.

Severity is determined by which attribute was matched.

The bottom portion of the report shows the actions taken for each PII incident. The bar chart and table both show how many PII incidents were quarantined or permitted. Click a link in the table to view details about each incident.

**Mobile credit card violations**

This report shows when credit card information was being synchronized to mobile devices, the users performing the sync, and the action taken.

The top portion shows incidents by severity.

- The table shows how many high, medium, and low severity credit card incidents occurred during email sync. Click a link to view details about each incident, such as the source and destination of the violating email message.
- The pie chart shows the percentage of credit card violations that were of high, medium, and low severity.

Severity is determined by which attribute was matched.
The bottom portion of the report shows the actions taken for each credit card incident. The bar chart and table both show how many credit card incidents were quarantined or permitted. Click a link in the table to view details about each incident.

## Discovery reports

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

1. Select **Main > Reporting > Discovery**.
2. From the reports main page, select **View Catalog**.

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

Listed below are descriptions of the most common:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident List</td>
<td>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.</td>
</tr>
<tr>
<td>Discovered Hosts</td>
<td></td>
</tr>
<tr>
<td>Hosts with credit card data</td>
<td>Find out which hosts contain credit card data, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Hosts with personally identifiable information</td>
<td>Find out which hosts contain personally identifiable information, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Hosts with PCI data</td>
<td>Find out which hosts contain PCI data, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Hosts with sensitive data</td>
<td>Find out which hosts contain sensitive information, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Laptops with sensitive data</td>
<td>Find out which laptops contain sensitive information, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Discovered Sensitive Data</td>
<td></td>
</tr>
<tr>
<td>Sensitive data on shared folders accessible by everyone</td>
<td>Find out was sensitive data was found in shared folders.</td>
</tr>
<tr>
<td>Sensitive data on file servers, SharePoint servers, and cloud servers</td>
<td>Find out was sensitive data was found on file, SharePoint, and cloud servers (for example, SharePoint 365 and Box).</td>
</tr>
<tr>
<td>Sensitive data on laptops</td>
<td>Find out was sensitive data was found on laptops</td>
</tr>
<tr>
<td>Sensitive data in databases</td>
<td>Find out was sensitive data was found in databases.</td>
</tr>
</tbody>
</table>
Sensitive data in private mailboxes | Find out was sensitive data was found in private mailboxes.
---|---
Sensitive data in public mailboxes | Find out was sensitive data was found in public mailboxes.

**Discovered Databases**

<table>
<thead>
<tr>
<th>Databases with credit card numbers</th>
<th>Find out which databases contain credit card numbers, and assess any violated policies on each database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases with personally identifiable information</td>
<td>Find out which databases contain personally identifiable information, and assess any violated policies on each database.</td>
</tr>
<tr>
<td>Databases with sensitive data</td>
<td>Find out which databases contain sensitive information, and assess any violated policies on each database.</td>
</tr>
<tr>
<td>Databases with PCI data</td>
<td>Find out which databases contain PCI data, and assess any violated policies on each database.</td>
</tr>
</tbody>
</table>

**Discovered Mailboxes**

<table>
<thead>
<tr>
<th>Mailboxes with credit card numbers</th>
<th>View which mailboxes contain credit card numbers, and assess any violated policies in each mailbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailboxes with personally identifiable information</td>
<td>View which mailboxes contain personally identifiable information, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Mailboxes with sensitive data</td>
<td>View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Mailboxes with PCI data</td>
<td>View which mailboxes contain PCI data, and assess any violated policies in each mailbox.</td>
</tr>
</tbody>
</table>

**Executive Dashboard**

| Dashboard | Provides an at-a-glance view of system metrics for information leaks in the system and the actions being taken on them. |

**Status**

| Incident status | View the status of all discovery incidents from the last 7 days. |

Click a folder to expand it and see a list of related reports. Click **Run** to generate the report.

**Discovery 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 Data Security manager 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 > Reporting > Discovery.
2. From the report catalog, select Executive Dashboard. Remember that all reports represent only incidents from to which the administrator has access.
3. Click Run to generate the report.

The dashboard includes the following sections:

- **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 317 for more details.)

To schedule this report to be delivered by email, see Scheduling tasks, page 297.

### 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 > Reporting > Discovery.
2. From the report catalog, expand the Discovered Sensitive Data folder and select one of the following reports:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data on file servers, SharePoint servers, and cloud servers</td>
<td>Find out what vulnerable data was most violated and where it is stored. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Sensitive data in private mailboxes</td>
<td>Find out which policies were violated most, and in which mailboxes the violations occurred. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Sensitive data in databases</td>
<td>Find out which policies were violated most, and in which databases the violations are located. Assess the security risk to your organization.</td>
</tr>
</tbody>
</table>
### Report Description

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailboxes with sensitive data</td>
<td>View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Hosts with sensitive data</td>
<td>Find out which hosts contain sensitive information, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Databases with sensitive data</td>
<td>Find out which databases contain sensitive information, and assess any violated policies on each database.</td>
</tr>
</tbody>
</table>

3. Click **Run** to generate the report.
Viewing Status and Logs

The Data Security manager enables you to keep track of TRITON AP-DATA 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**.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Ascending</td>
<td>Select this option to sort the table by the active column in ascending alphabetical order.</td>
</tr>
<tr>
<td>Sort Descending</td>
<td>Select this option to sort the table by the active column in descending alphabetical order.</td>
</tr>
<tr>
<td>Filter by (column)</td>
<td>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.</td>
</tr>
<tr>
<td>Clear filter</td>
<td>Select this option to clear the filter and display all tasks.</td>
</tr>
</tbody>
</table>

To view the current filters in use, 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 and log 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. The CSV contains all the rows in the main table, without paging. If the list is filtered, only the filtered records are exported.

On some screens, you can click the down arrow next to the **Export to PDF** or **Print Preview** button to define exactly what you want to export or print. You can select the current item (such as the current endpoint host), the selected item, or all items.

## Viewing the Today page

By default, the Today page opens every time you log onto the Data Security manager. This page shows a comprehensive view of data loss prevention incidents that occurred in the last 24 hours, and the total number of discovery incidents.

From the Today page, you can see any system health alerts and act on them quickly and easily. You can also view incidents by hostnames 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. Adobe Shockwave Player is required.

---

**Health Alert Summary**

The 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 Health Alert Summary is displaying missing essential configurations and actions, click the link to see further details and direct links to the required fixes.
Business Value

This section displays the approximate amount 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, and the cumulative volume of the traffic in megabytes.
- **Inspected email messages** - The number of email messages that were analyzed, and the cumulative size of the messages in megabytes.
- **Inspected mobile device messages** - The number of email messages that were analyzed when being sent to mobile devices from network Exchange servers, and the cumulative size of the messages in megabytes.
- **Discovery inspected items** - the number of files plus the number of database chunks scanned using network discovery, and the cumulative size of these items in megabytes. (A database chunk equals ~5000 records.)
- **Connected endpoints** - The number of endpoint clients connected to the system.
- **Synchronized mobile devices** - The number of mobile devices that have synchronized with the mobile agent in the last 24 hours (may be fewer than the number of registered devices).

Data Loss Prevention Incidents

**Data Loss Prevention Incidents** displays the number of data loss prevention 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Number of incidents that have been set to the most severe setting and should be handled immediately.</td>
</tr>
<tr>
<td>Medium</td>
<td>Number of incidents that have been set to the medium severity setting and should be handled soon.</td>
</tr>
<tr>
<td>Low</td>
<td>Number of incidents that have been set to the most lenient severity setting and should be handled.</td>
</tr>
</tbody>
</table>

- **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 loss prevention incident** field provides the exact date and time the last incident was logged in TRITON AP-DATA.

Clicking the **My data loss prevention incidents** link displays the incident summary screen where you can view and manage the incidents assigned to you.
Discovery Incidents

This section does not apply to TRITON AP-WEB.

**Discovery Incidents** displays the total number of discovery incidents detected by a TRITON AP-DATA discovery scan. Two graphs are included:

- **Top 5 Hosts**: 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 discovery incident** and **My discovery incidents** fields work the same as for data loss prevention incidents. (See above.)

Monitoring system health

The System Health screen enables you to monitor the performance of TRITON AP-DATA modules.

To view system health, select **Main > Status > System Health**.

The tree view displays the names of all protector appliances, TRITON AP-DATA servers, Web Content Gateway, TRITON AP-EMAIL, and mobile agents.

Click a TRITON AP-DATA server or agent to view the following charts in the right-hand part of the screen:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Summary</td>
<td>Information about the server, including operating system and version, time zone, and free disk space.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The percentage of the CPU that is being used by the machine’s processes over the specified time frame.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The percentage of memory that is being used by the machine’s processes over the specified time frame.</td>
</tr>
</tbody>
</table>

The System Summary and Memory Usage charts are also available for all protectors.

TRITON AP-DATA servers include the following modules in the tree view:

- Primary fingerprint repository
- Endpoint server
- Policy engine
- OCR server (secondary TRITON AP-DATA servers only)
Protectors and agents include the following modules:

- Policy engine
- Secondary 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:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protector</strong></td>
<td></td>
</tr>
<tr>
<td>Packet loss and dropped</td>
<td>Indicates the levels of packet loss and dropped transaction rates.</td>
</tr>
<tr>
<td>transaction indication</td>
<td></td>
</tr>
<tr>
<td>Number of events sent to</td>
<td>The number of events sent for analysis by this protector in the specified</td>
</tr>
<tr>
<td>analysis</td>
<td>time frame.</td>
</tr>
<tr>
<td>Load average</td>
<td>Average amount of work performed by the protector in the specified time frame.</td>
</tr>
<tr>
<td></td>
<td>For optimum performance, the number on the chart should not exceed the</td>
</tr>
<tr>
<td></td>
<td>number of available processors in the System Summary: for example, if the</td>
</tr>
<tr>
<td></td>
<td>system load average is 3 and there are 2 available processors, the system</td>
</tr>
<tr>
<td></td>
<td>might work slowly.</td>
</tr>
<tr>
<td>Memory usage</td>
<td>The percentage of memory used by machine processes.</td>
</tr>
<tr>
<td>Total Throughput</td>
<td>Total amount of traffic (in KB per second) monitored by the protector. This</td>
</tr>
<tr>
<td></td>
<td>includes both interesting and non-interesting sessions.</td>
</tr>
<tr>
<td>Data sent to analysis</td>
<td>Total amount of traffic (in KB per second) sent for analysis by this</td>
</tr>
<tr>
<td>throughput</td>
<td>protector.</td>
</tr>
<tr>
<td><strong>Policy Engine</strong></td>
<td></td>
</tr>
<tr>
<td>Analysis status</td>
<td>Displays the request load on the policy engine for analysis by time period.</td>
</tr>
<tr>
<td>DLP—number of analyzed</td>
<td>Number of DLP events analyzed by this policy engine in the specified time</td>
</tr>
<tr>
<td>events</td>
<td>frame.</td>
</tr>
<tr>
<td>DLP—number of incidents</td>
<td>Number of DLP incidents detected by this policy engine in the specified</td>
</tr>
<tr>
<td></td>
<td>time frame.</td>
</tr>
<tr>
<td>Discovery—number of analyzed</td>
<td>Number of discovery items analyzed by this policy engine in the specified</td>
</tr>
<tr>
<td>items</td>
<td>time frame. This includes files, email messages, and database tables. This</td>
</tr>
<tr>
<td></td>
<td>chart is available only for policy engines on TRITON AP-DATA servers. If the</td>
</tr>
<tr>
<td></td>
<td>policy engine on this computer does not handle discovery traffic, this report</td>
</tr>
<tr>
<td></td>
<td>is empty.</td>
</tr>
<tr>
<td>Discovery—number of</td>
<td>Number of discovery incidents detected by this policy engine in the</td>
</tr>
<tr>
<td>incidents</td>
<td>specified time frame. This chart is available only for policy engines on</td>
</tr>
<tr>
<td></td>
<td>TRITON AP-DATA servers. If the policy engine on this computer does not handle</td>
</tr>
<tr>
<td></td>
<td>discovery traffic, this report is empty.</td>
</tr>
</tbody>
</table>
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 view raw data for troubleshooting purposes, such as logs and system statistics, click the Download Diagnostics button on the toolbar. A zip file containing diagnostic information is downloaded to the location you specify. This operation can take several minutes.

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 TRITON AP-DATA system.

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fingerprint Repository</strong></td>
<td></td>
</tr>
<tr>
<td>Fingerprint repository</td>
<td>Displayed only on the TRITON 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.</td>
</tr>
<tr>
<td>synchronization</td>
<td></td>
</tr>
<tr>
<td>Number of fingerprinted</td>
<td>Displays the total number of files fingerprinted in the specified time frame.</td>
</tr>
<tr>
<td>files</td>
<td></td>
</tr>
<tr>
<td>Number of fingerprinted</td>
<td>Displays the total number of database cells fingerprinted in the specified time frame.</td>
</tr>
<tr>
<td>database cells</td>
<td></td>
</tr>
<tr>
<td><strong>Endpoint Server</strong></td>
<td></td>
</tr>
<tr>
<td>Endpoint server load</td>
<td>Displays the load on the endpoint server over the specified time period.</td>
</tr>
<tr>
<td>Number of endpoints</td>
<td>Number of endpoint requests received by the endpoint server in the specified time frame.</td>
</tr>
<tr>
<td><strong>OCR Server</strong></td>
<td></td>
</tr>
<tr>
<td>Queue load</td>
<td>Shows the load of OCR server queue during the selected time period.</td>
</tr>
<tr>
<td>Number of textual requests</td>
<td>Shows the total number of OCR requests containing textual data during the selected time period.</td>
</tr>
<tr>
<td>Number of requests</td>
<td>Shows the total number of requests made to the OCR server during the selected time period.</td>
</tr>
<tr>
<td>Average image size</td>
<td>Shows the average size of images (in bytes) that were handled by the OCR server during the selected time period.</td>
</tr>
<tr>
<td>Average processing time</td>
<td>Shows the average processing time (in milliseconds) of images that were handled by the OCR server during the selected time period.</td>
</tr>
</tbody>
</table>
Viewing mobile device status

To view the status of all mobile devices and users connected to the system:

1. Select **Main > Status > Mobile Device Status**.
   
   The resulting screen lists all mobile devices registered with the TRITON management server. The list displays information for each device, such as:
   - owner
   - device type (iPhone, Android phone)
   - last sync time
   
   To customize the information shown in each column, click the Table Properties ( ) button. Click here for descriptions of the information you can display.

   **Note**
   
   Some mobile devices do not use all of the available fields. In this case, the field for that device is empty.

2. To drill down further, select a device in the list. In the Details pane, you can view information about the device owner, such as his or her phone number and email address. If the owner’s full name is found in the user directory, this is displayed as well. (Otherwise, the full name field shows N/A.) The Details pane also shows how many devices are registered to the owner and which was last synchronized.

3. To remove a device from the list, select it and click **Remove**. To remove all devices at once, click **Remove All**.

Status is sent from the mobile agent to the TRITON management server in intervals between 1 and 60 minutes. This is configurable by clicking **Settings** in the toolbar.
Viewing endpoint status

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 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 > Endpoint Status**.
   
   The resulting screen lists all Websense data endpoints registered with the TRITON management server. The list displays information for each endpoint, such as:
   
   - hostname
   - IP address
   - logged-in users
   - last update time
   - profile name
   - synchronization status
   - discovery status (idle or running)

   To customize the information shown in each column or to view descriptions, click the Table Properties ( ) button. There are many other options available than displayed in the table by default. Click *here* for descriptions of the information you can display.

   **Note**
   
   The discovery status shows N/A for Linux endpoints, because data discovery is not supported on Linux. The sync status shows an “X” when the policy, fingerprint, or profile version is not synchronized with the management server or when the endpoint’s profile name is out of sync.

2. To drill down further on information for each endpoint, select an endpoint in the list. 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**.

Related topics:

- *Configuring endpoint settings, page 477*
- *Bypassing endpoint clients, page 482*
From this screen you can also do the following:

- To search for a specific endpoint in the list, in the **Find host** field enter the hostname and click the **Find** button.
- Click **Bypass Endpoint** to temporarily disable the selected endpoint. For more information, see *Bypassing endpoint clients*, page 482.
- Click **Settings** to view and edit the system settings for endpoints. For more information, see *Configuring endpoint settings*, page 477.

---

**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

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

The logs available in the Data Security manager enable you to analyze all events and actions in the manager, and to keep track of the traffic flowing through the TRITON AP-DATA system.

There are 3 different logs you can view:

- Traffic log, page 348
- System log, page 349
- Audit log, page 349

Traffic log

The traffic log contains details of the traffic being monitored by TRITON AP-DATA over specific periods and the action taken.

For the endpoint channel, the log displays only traffic that breaches policy.

To view the contents of the traffic log, select Main > Status > Traffic Log.

The list displays information, such as:

- Event ID
- Event Time
- Channel
- Action Taken

To customize the information shown in each column, click the Table Properties ( ) button. Click here for descriptions of the information you can display.

The Updated to field shows when the traffic log was last updated. To see the latest data, click Update Now.

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 TRITON AP-DATA 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 > Status > 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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Defines whether the action is an error, or is reported for informational purposes.</td>
</tr>
<tr>
<td>Status</td>
<td>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 <strong>Mark as Confirmed</strong>. To revert a confirmed action to new, select the event and click <strong>Mark as New</strong>.</td>
</tr>
<tr>
<td>Message</td>
<td>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. The Data Security manager 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.).”</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Date and time the action occurred.</td>
</tr>
<tr>
<td>Local Date &amp; Time</td>
<td>Date and time on the component where the action occurred.</td>
</tr>
</tbody>
</table>
| Topic     | ● **System**- Displays system messages reported by system components  
            ● **Configuration** - Displays messages reported by the system after a configuration action is executed (usually by an administrator) |
| Reporter  | Displays the system module’s name, for example TRITON AP-DATA 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. For example, it can show when administrators:

- Export incidents to a PDF or CSV file
- Email incidents to a manager or other recipient
- Make changes to a user account, such as user name or password
• View incident details such as trigger values and forensics
  (To set this up, select **Settings > General > Authorization > Administrators** and then select **Audit incident detail views**.)

The audit log allows you to investigate any unauthorized or irregular changes made to the system that might jeopardize employee privacy or breach your IT security compliance policy.

To view the Audit Log, select **Main > Status > 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.

To customize the information shown in each column, click the Table Properties ( ) button. Click here for descriptions of the information you can display. The default columns are shown below.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action ID</td>
<td>ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the <strong>Find Action ID</strong> field and clicking <strong>Find</strong>.</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Date and time the action occurred.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Name and user name of the administrator that initiated the action in the Data Security manager.</td>
</tr>
<tr>
<td>Access Role</td>
<td>Role of the administrator.</td>
</tr>
<tr>
<td>Topic</td>
<td>You can filter the Audit Log by topic types.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Administration</strong> - Displays actions performed by administrators during the designated period, such as adding a new access role or configuring user directories. Also displays actions made on administrators, such as adding a new administrator or changing an administrator’s permissions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log on/Log out</strong> - Displays log on and log out actions so you know which administrators where active during the designated period.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Status</strong> - Displays actions performed on status reports and logs, such as deleting an entry or creating an audit record.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Policy management</strong> - Displays actions performed on policies, such as updating predefined policies, editing quick policies, or creating a new policy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reporting</strong> - Displays actions performed on reports during the designated period, such as editing or creating a new report.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Incident management</strong> - Displays actions performed on incidents, such as deleting incidents.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Archiving</strong> - Displays actions performed on incident archives, such as deleting or restoring an archive.</td>
</tr>
<tr>
<td></td>
<td>• <strong>System modules</strong> - Displays actions performed on system modules, such as editing a configuration or adding a module.</td>
</tr>
<tr>
<td>Action Performed</td>
<td>Description of the action performed by the administrator—for example, “exported DLP incident to PDF file”</td>
</tr>
</tbody>
</table>
Table properties

Some status windows and logs allow you to configure the columns that are displayed. To customize a status or log’s summary table:

1. Navigate to the desired status window or log.
2. Click the Table Properties () button.
3. Select the columns to display in the table for this report.
4. Use the arrows to indicate the order of the columns.
5. Adjust the width as desired.
6. Specify the maximum number of incidents to display on any one page.
7. 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.

Note that the columns that are available depend on the status window or log you’re viewing.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Taken</td>
<td>The online action that was performed (allow or block).</td>
</tr>
<tr>
<td>Analysis Failed</td>
<td>Displays whether analysis failure occurred.</td>
</tr>
<tr>
<td>Analyzed By</td>
<td>Displays the name of the policy engine that analyzed the event.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>Displays whether analysis was cancelled.</td>
</tr>
<tr>
<td>Channel</td>
<td>Channel on which the event was intercepted, for example SMTP, HTTP, or FTP.</td>
</tr>
<tr>
<td>Classifier Time</td>
<td>Time spent analyzing all classifiers, in milliseconds. Includes the time spent processing dictionaries, scripts, key phrases, patterns, and fingerprints.</td>
</tr>
<tr>
<td>Client Installation Version</td>
<td>Version of the endpoint client software that is installed on the endpoint machine.</td>
</tr>
<tr>
<td>Client Status</td>
<td>Status of the endpoint client: enabled or disabled.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Fingerprint Latency</td>
<td>Time in milliseconds that the transaction spent in the policy engine waiting for structured fingerprint analysis.</td>
</tr>
<tr>
<td>Database Fingerprint Search Time</td>
<td>Time in milliseconds spent on searching for structured fingerprint data in this transaction’s content.</td>
</tr>
<tr>
<td>Description</td>
<td>The description provided for this item.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination of the event, for example an IP address or an email address.</td>
</tr>
<tr>
<td>Details</td>
<td>Header details from the event. 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.</td>
</tr>
<tr>
<td>Detected By</td>
<td>Displays the protector or agent that caught the event.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The Unique Device Identifier (UDID) associated with the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of mobile device, for example, iPad or iPhone.</td>
</tr>
<tr>
<td>Dictionary Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for dictionary analysis.</td>
</tr>
<tr>
<td>Dictionary Search Time</td>
<td>Time in milliseconds spent on searching for dictionary phrases in this event’s content.</td>
</tr>
<tr>
<td>Discovery Status</td>
<td>The status of the discovery service on the endpoint.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address associated with this mobile device.</td>
</tr>
<tr>
<td>Endpoint Server</td>
<td>Name of the server associated with this endpoint.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Unique traffic log event number.</td>
</tr>
<tr>
<td>Event Time</td>
<td>Date and time the event was detected.</td>
</tr>
<tr>
<td>Extraction Time</td>
<td>Time spent extracting text from the event, in milliseconds.</td>
</tr>
<tr>
<td>File Fingerprint Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for unstructured fingerprint analysis.</td>
</tr>
<tr>
<td>File Fingerprint Search Time</td>
<td>Time in milliseconds spent on searching for unstructured fingerprint data in this event’s content.</td>
</tr>
<tr>
<td>Files Scanned</td>
<td>The number of files that were scanned on the endpoint in the most recent scan.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the endpoint machine.</td>
</tr>
<tr>
<td>Host Name Resolution Time</td>
<td>Time in milliseconds spent on performing external resolution from IP to hostname on this event’s source or destination.</td>
</tr>
<tr>
<td>ID</td>
<td>The ID assigned to this mobile device.</td>
</tr>
<tr>
<td>IMEI</td>
<td>The International Mobile Equipment ID for this mobile device.</td>
</tr>
<tr>
<td>Incident</td>
<td>Displays a check mark if the event was determined to be an incident (a policy violation).</td>
</tr>
<tr>
<td>Incident Creation Time</td>
<td>Time spent creating an incident when a breach is detected, in milliseconds. If no incident was created, this field is “0”.</td>
</tr>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the endpoint machine.</td>
</tr>
<tr>
<td>Key Phrase Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for key phrase analysis.</td>
</tr>
<tr>
<td>Key Phrase Search Time</td>
<td>Time in milliseconds spent on searching for key phrases in this event’s content.</td>
</tr>
<tr>
<td>Last Scan End Time</td>
<td>The time that the latest endpoint scan ended.</td>
</tr>
<tr>
<td>Last Scan Start Time</td>
<td>The time that the latest endpoint scan began.</td>
</tr>
<tr>
<td>Last Sync Time</td>
<td>The date and time this mobile device last synchronized with your network email system.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Last time the endpoint received updates from the management server (profiles, policies, etc.).</td>
</tr>
<tr>
<td>Latency</td>
<td>Time the event spent in the policy engine waiting for analysis, in milliseconds—in other words, Processing Time + Incident Creation Time + Queue Time.</td>
</tr>
<tr>
<td>Logged-in Users</td>
<td>Number of users logged into the endpoint.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the endpoint client machine.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of this mobile device (iPhone2, Thunderbolt, etc.).</td>
</tr>
<tr>
<td>Next Scan Time</td>
<td>The time scheduled for the next endpoint scan.</td>
</tr>
<tr>
<td>OS</td>
<td>The mobile device operating system (Apple iOS, Nokia MeeGO, Windows Phone, etc.).</td>
</tr>
<tr>
<td>OS Language</td>
<td>The operating system language of this mobile device (C++, Linux, Java, etc.).</td>
</tr>
<tr>
<td>Owner</td>
<td>The owner of this mobile device.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number for this mobile device.</td>
</tr>
<tr>
<td>Policy Engine Version</td>
<td>Version of the policy engine machine that is associated with this endpoint.</td>
</tr>
<tr>
<td>Prescribed Action</td>
<td>The name of the action plan that was triggered.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>The name of the endpoint profile on this machine.</td>
</tr>
<tr>
<td>Regular Expression Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for regular expression analysis.</td>
</tr>
<tr>
<td>Regular Expression Processing Time</td>
<td>Time in milliseconds spent on all regular expression calculations performed on this event’s content.</td>
</tr>
<tr>
<td>Resolution Time</td>
<td>Time spent resolving user names for all sources and destinations in the event, in milliseconds.</td>
</tr>
<tr>
<td>Script Search Time</td>
<td>Time in milliseconds spent on all script classifications performed on this event’s content.</td>
</tr>
<tr>
<td>Search Time</td>
<td>Time it took to search the event for breaches, in milliseconds—in other words, Classifier Time + Extraction Time + Resolution Time.</td>
</tr>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the event content, for example a file or an email message.</td>
</tr>
<tr>
<td>Source</td>
<td>The source from which the event originated. This could be an email address or IP address or other source.</td>
</tr>
<tr>
<td>Synced</td>
<td>Indicates whether the endpoint is updated with the latest settings. The sync status shows an “X” when the policy, fingerprint, or profile version is not synchronized with the management server or when the endpoint’s profile name is out of sync.</td>
</tr>
<tr>
<td>Text Extraction Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for text extraction.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Displays whether analysis was stopped due to a timeout restriction.</td>
</tr>
<tr>
<td>Total Queue Time</td>
<td>Total amount of idle time, in milliseconds, that the event spent in internal queues.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of mobile device (iPhone, iPad, Android, etc.).</td>
</tr>
<tr>
<td>URL Categorization Time</td>
<td>Time in milliseconds spent on categorizing the destination URL of this event.</td>
</tr>
<tr>
<td>User</td>
<td>The mobile device owner.</td>
</tr>
<tr>
<td>User Agent</td>
<td>The network protocol this mobile device uses to communicate with the TRITON AP-DATA system (Touchdown, ActiveSync, etc.).</td>
</tr>
<tr>
<td>User Name Resolution Time</td>
<td>Time in milliseconds spent on performing external resolution from IP to user name on this event’s source.</td>
</tr>
<tr>
<td>User Resolution Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for user name resolution.</td>
</tr>
</tbody>
</table>
Part III

Administering the System
Configuring System Settings

In TRITON AP-DATA, many system settings are configurable. You can:

- Set preferences for reports
- Back up and restore the TRITON AP-DATA system
- Define parameters for exporting incidents to a file*
- Configure endpoint hosts*
- Configure mobile email devices (included with TRITON AP-EMAIL)
- Configure user directory settings
- Configure remediation*
- Configure incoming and outgoing mail servers
- Configure alerts
- Configure the incident archive
- Enter subscription details
- Configure URL categories and user name resolution

Related topics:
- Setting reporting preferences, page 358
- Backing up the system, page 362
- Exporting incidents to a file, page 367
- Configuring endpoints, page 369
- Configuring mobile device settings, page 371
- Configuring user directory settings, page 374
- Configuring remediation, page 381
- Configuring mail servers, page 383
- Configuring alerts, page 385
- Configuring the incident archive, page 387
- Entering subscription settings, page 389
- Configuring URL categories and user names, page 390
*These options are not included with TRITON AP-WEB or TRITON AP-EMAIL.

Access the system settings screens by selecting Settings > General > System.

### Setting reporting preferences

By going to Main > Reporting, you can view all of the incidents that TRITON AP-DATA has discovered in your organization over time. On the Settings tab you can set preferences for those reports.

For example, for data loss prevention incidents, you can define attachment size and forensics settings. For 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 > General > System.
2. Select the Reporting option from the System pane.
3. Complete the General, Data Loss Prevention, Discovery, and Mobile 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachments</td>
<td>Select the maximum number of report attachments (between 1-40) to append to each email notification message. By default, 40 attachments can be appended.</td>
</tr>
<tr>
<td>Maximum size of attachments</td>
<td>Select the maximum overall file size (between 1-20 MB) for the email notification message. By default, the maximum is 5 MB.</td>
</tr>
<tr>
<td>Zip incident and discovery reports</td>
<td>Select this box if you want to zip incident management and discovery reports in an archive to minimize the size of the notification message.</td>
</tr>
</tbody>
</table>

**Printing Incidents**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of incidents</td>
<td>If a list of TRITON AP-DATA incidents or reports gets very long, you can break it into groups. Use this option to specify the number of incidents or reports to <strong>Print Preview</strong> or <strong>Export to PDF</strong> at any given time. 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 export 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 export 1-200, 201-400, 401-600, or 601-700 incidents. If you prefer to export all incidents, you can enter an email address to which to send a PDF file.</td>
</tr>
<tr>
<td>No custom logo</td>
<td>Select this option if you do not want to add a logo to the report. By default, the TRITON AP-DATA logo appears on the first page of the report.</td>
</tr>
<tr>
<td>Add the following logo</td>
<td>Select this option to add a custom logo to the top of the first page in the report, then browse to the image file containing the logo. The image must be smaller than 5 MB. Supported file types include .png, .gif, .bmp, and .jpg. For best practice, upload an image that is 200x50 pixels. The system reduces larger images to this size and the resolution may be affected. When you upload a logo, it appears on the top right of the report, and the TRITON AP-DATA logo appears on the top left.</td>
</tr>
</tbody>
</table>
Configuring System Settings

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

### Setting preferences for data loss prevention incidents

To define settings for reviewing data loss prevention incidents:

1. Select the **Data Loss Prevention** tab.
2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No disclaimer</td>
<td>Select this option if you do not want to add a disclaimer to the bottom of the report. By default, no disclaimer appears in the report footer.</td>
</tr>
<tr>
<td>Add the following disclaimer</td>
<td>Select this option to add a disclaimer to the bottom of the report, then enter the disclaimer text. The disclaimer can be 2 lines; each line can be 150 characters. Disclaimers appear on every page in the report.</td>
</tr>
<tr>
<td><strong>Forensics</strong></td>
<td></td>
</tr>
<tr>
<td>Secure forensics with plain text</td>
<td>Select this option if you want forensics to appear in the report in plain text. This blocks forensics from being displayed in potentially malicious HTML.</td>
</tr>
<tr>
<td>Delete forensics for closed incidents</td>
<td>Select this option to delete forensics for incidents when their status is changed to “Closed.” This reduces the size of your forensics repository.</td>
</tr>
<tr>
<td>Note: Incidents that are already closed when you select this option are not deleted.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **OK** to save your changes.
Setting preferences for discovery incidents

To define settings for discovery incidents:

1. Select the **Discovery** tab.
2. Complete the fields as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum discovery incidents</td>
<td>Enter the maximum number (from 10,000-2,000,000) of incidents stored in the discovery database. (The Discovery Incidents screen enables assigning, viewing and monitoring these incidents.) Do not include commas.</td>
</tr>
<tr>
<td>Endpoint discovery incidents</td>
<td>TRITON AP-DATA 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.</td>
</tr>
<tr>
<td>Network discovery incidents</td>
<td></td>
</tr>
</tbody>
</table>

3. **Click OK** to save your changes.
Setting preferences for mobile incidents

To define settings for mobile incidents:
1. Select the Mobile tab.
2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep mobile incidents for</td>
<td>Select the number of days you’d like to keep incidents pertaining to mobile devices. You can choose between 1-999. By default, mobile incidents are kept for 90 days. Incidents older than this number are deleted from the incident database and no longer available for reporting.</td>
</tr>
</tbody>
</table>

3. Click OK to save your changes.

Backing up the system

You should back up your TRITON AP-DATA system periodically to safeguard your policies, forensics, configuration data, fingerprints, encryption keys, and more. (See Backup folder contents, page 365 for a complete list.)
To back up the TRITON AP-DATA system:

1. Select **Settings > General > System > Backup**.
2. Enter a path for the backup files and credentials for accessing the path.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Enter a path name where you want the backup stored. This is the root folder where the backup files are written. If you enter a local path, it is local to the TRITON management server. 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.</td>
</tr>
</tbody>
</table>

**Credentials (optional)**

If the TRITON AP-DATA administrator doesn’t have write privileges to the specified path, use these fields to specify the credentials to use for writing backups.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Enter the domain name of the remote backup location.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name for an administrator who has access to this path.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the user’s password.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the password a second time.</td>
</tr>
</tbody>
</table>

3. Configure backup settings as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many backup copies do you want to keep?</td>
<td>Every time you backup the system, the system uses another backup folder. To avoid using too many disk resources, indicate how many backup folders you want to keep. The system will rotate between these folders on subsequent backups. It overwrites the oldest folder with the new data. You can have between 1 and 60 backup folders. The default is 5.</td>
</tr>
</tbody>
</table>

| Include forensics                  | Select this option if you want to include incident forensics in the backup. These are the details stored in the incident database.             |
| Do not include forensics           | Select this option if you do not want to include incident forensics in the backup. The incident database can be quite large, and backing it up requires additional disk space. |

4. Click **OK** to save the settings.

5. To run the backup task, use Windows control panel as described in *Scheduling backups*, page 364.
If for some reason a backup fails, refer to the log file `CPSBackup.log` stored in the TRITON AP-DATA installation directory.

---

**Note**

The backup process consists of large transactions and you cannot stop a transaction in the middle. You must wait until the process is complete.

---

### Scheduling backups

**Windows Server 2008**

1. On the TRITON management server, go to **Start > Administrative Tools > Task Scheduler**.
2. In the Task Scheduler window, select **Task Scheduler Library**.
3. Right-click the **DSS Backup** task and select **Enable**.
4. Right-click **DSS Backup** again and select Properties, then select the Triggers tab.
5. Click **Edit**, and edit the schedule as required.
6. Click **OK** twice.

If requested, enter your administrator password for the TRITON management server machine to confirm the changes to the task.

To run the task immediately, right-click **DSS Backup** and select **Run**.

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 TRITON AP-DATA machines.
Monitoring backups

Every backup operation writes start and completion entries in the Data Security manager’s system log screen (Main > Status > System Log).

In addition, every backup operation writes an entry in the Windows event log. 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 Data Security manager database (containing policies, incidents and configuration)
- Forensics_repository: the (encrypted) forensic incidents information
- Crawlers: information on the discovery and fingerprinting crawlers
- Certs: certificate files used for communication between the Data Security manager and other TRITON AP-DATA network and endpoint agents.

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 TRITON 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 TRITON AP-DATA modules—servers, agents, protectors—are registered with the TRITON management server and the system is operating normally.
2. On the TRITON management server, open the Windows Control Panel and select *Add/Remove Programs* (Windows 2003) or *Programs > Uninstall a program* (Windows 2008).
4. When asked if you want to add, remove, or modify TRITON AP-DATA, select *Modify*.
5. Click *Next* until you get to the *Restore Data from Backup* screen.
6. Select the *Load Data From Backup* check box and click the *Browse* button to locate the backup file.
7. 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.)
8. 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.
9. Complete the restore wizard.
10. To review the restore activity, read the *DataRestore.log* file located in the backup folder (for example, MM-DD-YYYY-HH-MM-SS).

**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.
11. Log onto the Data Security manager and select **Deploy**.

---

**Note**

If the backup system contains many policies, it may take a while to load the policies and deploy them.

---

**Exporting incidents to a file**

To export incidents to a log file for analysis:

1. Select **Settings > General > System**.
2. Select the **Incident Export** option from the System pane.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export incidents to a file</td>
<td>Select this box to set up your incident export.</td>
</tr>
<tr>
<td>Path</td>
<td>Browse to the location where the incident report will be saved, e</td>
</tr>
<tr>
<td>File name</td>
<td>Type the name of the incident export file. The name must be fewer than 180 characters. File names cannot include the following characters: <code>/:*?&quot;&lt;&gt;|;</code>, &amp;%@#$%^&amp;*()+=-`{</td>
</tr>
<tr>
<td>Maximum number of files</td>
<td>Use the arrows to choose the maximum number (between 1-20) of log files you want to keep.</td>
</tr>
<tr>
<td>New file creation</td>
<td>Indicate how often you want to create a new incident export file.</td>
</tr>
<tr>
<td>When file size reaches</td>
<td>Click this option and select a file size (from 1-5MB) to create a new incident report file when the old file exceeds your specified size.</td>
</tr>
<tr>
<td>At the start of a new day</td>
<td>Click this option to create a new incident log file at 12:00 a.m. every day.</td>
</tr>
</tbody>
</table>

4. Click **OK** to save your changes.
Listed below are the fields that are exported and a description of their contents.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident ID</td>
<td>External incident ID.</td>
</tr>
<tr>
<td>Insert date</td>
<td>The incident insert date.</td>
</tr>
<tr>
<td>Source hostname</td>
<td>The incident source hostname.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The incident source IP.</td>
</tr>
<tr>
<td>Source full name</td>
<td>The incident source full name.</td>
</tr>
<tr>
<td>Source email</td>
<td>The incident source email.</td>
</tr>
<tr>
<td>Source DN</td>
<td>The distinguished name (DN) of the incident source. A DN is the name that uniquely identifies the entry in the directory. It is made up of attribute=value pairs, separated by commas.</td>
</tr>
<tr>
<td>Destinations list</td>
<td>A list of the incidents destinations, in the format of dest1;dest2;dest3…</td>
</tr>
<tr>
<td>Channel name</td>
<td>The channel name.</td>
</tr>
<tr>
<td>Max action taken</td>
<td>A readable action taken (e.g.: Blocked, Audited).</td>
</tr>
<tr>
<td>Urgency</td>
<td>Incident’s urgency, sometimes called sensitivity (e.g.: Moderate).</td>
</tr>
<tr>
<td>Policy category</td>
<td>A policy category for the current line (an incident can generate multiple lines).</td>
</tr>
<tr>
<td>Filenames</td>
<td>The filename or filenames related to the current incident policy, up to 1024 characters. In the format of [fn1;fn2;…;fnX].</td>
</tr>
<tr>
<td>Filenames trimmed</td>
<td>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.</td>
</tr>
<tr>
<td>Breached contents</td>
<td>The breach content of the incident for the current policy, up to 1024 characters, in the format of [content1;content2;…;contentX].</td>
</tr>
<tr>
<td>Breached content trimmed</td>
<td>True if the actual size of the previous filed is more than 1024 characters.</td>
</tr>
</tbody>
</table>
Configuring endpoints

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 > General > System.
2. Select the Endpoint option from the System pane.
3. Complete the fields as follows.

### General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectivity</strong></td>
<td></td>
</tr>
<tr>
<td>Test connectivity every</td>
<td>Select how often (between 1-60 minutes) endpoints test connectivity. Default is 5 minutes.</td>
</tr>
<tr>
<td>Check for updates every</td>
<td>Select how often (between 30 seconds and 24 hours) endpoints check for configuration updates. Default is 1 hour.</td>
</tr>
<tr>
<td>An endpoint is disconnected if no signal is received within</td>
<td>Define when (between 1-60 hours) the endpoint is determined to be disconnected. Default is 48 hours.</td>
</tr>
</tbody>
</table>

### Note

This section applies only to customers with Websense Data Endpoint. If you have TRITON AP-WEB, 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.
### Field | Description
--- | ---
Enable endpoint administrator password | If you do not want endpoint users to be able to un-install the endpoint client software or disable blocking or anti-tampering, select this check box. Anyone who tries to perform these functions will be prompted for a password. Enter the password here.

### Optical Media

| Field | Description |
--- | --- |
Permit third-party CD/DVD burning | The system monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications. It can monitor non-native Windows CD/DVD burner applications as well, but only blocks or permits operations without performing content classification. Select this option if you want to allow users to burn data to CD/DVD using third-party burner applications. Non-native CD/DVD blocking applies to CD, DVD, and Blue-ray read-write devices on Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 endpoints. Linux endpoint does not support CD/DVD burners.

### Email Domains tab

#### Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

| Field | Description |
--- | --- |
Internal email domains | Enter the email domains your organization uses internally. These must be internal domains from which your users can send email. Click Add to add each domain to the internal email domains list. To delete an existing domain from the list, select the domain and click Remove. **Important**: Do not leave the Domain field blank. If you do, endpoint email is not analyzed.

Outbound* | Monitor email traffic between a source domain listed on this page and any destination domain that is not listed.

Internal* | Monitor email traffic between any source and destination domain that are both listed on this page.

* On this tab, you define, in general, which directions may be monitored for endpoint email (for instance, only outbound). The direction or directions that are actually enforced are determined by the settings on the Destination page of a custom rule.

In the rule, if you choose a direction that is not allowable per the Email Domains setting, endpoint email traffic is not analyzed.
Disk Space tab

Configuring System Settings

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System file storage size</td>
<td>Reports the disk space that is used for storing system files on each endpoint.</td>
</tr>
<tr>
<td>Maximum log file size</td>
<td>Limit the size (between 16-100 MB) of the endpoint client’s log file. Default is 16MB.</td>
</tr>
<tr>
<td>Incident storage size</td>
<td>Specify the incident-storage disk space to allocate (between 10-2000 MB) for disconnected endpoints. Default is 100 MB.</td>
</tr>
<tr>
<td>File fingerprint storage size</td>
<td>Specify the disk space (between 1-1000 MB) to allocate for storage of directory and SharePoint fingerprints. Default is 50 MB.</td>
</tr>
<tr>
<td>Database fingerprint storage size</td>
<td>Specify the disk space (between 1-1000 MB) to allocate for storage of database fingerprints. Default is 250 MB.</td>
</tr>
<tr>
<td>Contained file storage size</td>
<td>Specify the disk space to allocate for storage of contained files. Default is 500 MB. Contained files are those that are held in temporary storage on an endpoint. Files are contained when you have chosen to prevent sensitive information from being written from an endpoint to a removable device—such as a USB flash drive, CD/DVD, or external hard disk—and an end user tries to copy a file to a forbidden device. See the Endpoint User’s Guide in the Websense Technical Library for more information.</td>
</tr>
<tr>
<td>Total allocated disk space</td>
<td>Reports the total amount of disk space being allocated for TRITON AP-DATA functions on each endpoint. This represents the sum of all settings in the Disk Space section.</td>
</tr>
</tbody>
</table>

Configuring mobile device settings

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:
- Configuring the mobile agent, page 444
- Configuring the Mobile Data Loss Prevention Policy, page 69
- Viewing mobile device status, page 345

The mobile agent enables you to choose what type of email content to sync to users’ mobile devices when they connect to the network. If content breaches your mobile policy, it is blocked or audited as configured.
Use this screen to define how the TRITON management server should manage the mobile devices covered by policy.

Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep released messages for</td>
<td>When the mobile agent accepts a release operation for a specific message, it stores it for 2 main purposes:</td>
</tr>
<tr>
<td></td>
<td>• To wait for the user’s device to sync, which triggers the actual release sequence in Exchange.</td>
</tr>
<tr>
<td></td>
<td>• To avoid any subsequent analysis for the same message by the same user syncing to a second device.</td>
</tr>
<tr>
<td></td>
<td>Indicate how long the mobile agent should preserve a release operation.</td>
</tr>
<tr>
<td></td>
<td>You can select between 3 and 30 days.</td>
</tr>
<tr>
<td></td>
<td>By default, released messages are stored for 14 days.</td>
</tr>
<tr>
<td></td>
<td>This number affects the size of your incident database. A large number requires more storage space than a small one.</td>
</tr>
<tr>
<td>Update status every</td>
<td>Indicate how often you want device status sent to the management server. Status includes the device owner and type, date of the last synchronization, date of incident detection, and more.</td>
</tr>
<tr>
<td></td>
<td>You can update status every minute, hourly, or any interval in between.</td>
</tr>
<tr>
<td></td>
<td>By default, status is sent every 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Status from all registered devices is sent to the management server in a single batch operation.</td>
</tr>
</tbody>
</table>
Configuring System Settings

Click **OK** to save your changes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Analyze the following components | Indicate which Exchange server components you want the mobile agent to analyze:  
  - **Email messages** - Select this to analyze all parts of an email message (Subject, Body, To, From, Attachments, etc.)  
  - **Calendar events** - Select this to analyze calendar items, including Subject, Location, Attendees, and Description.  
  - **Tasks** - Select this to analyze content in To-Do lists. By default, all message types are analyzed. |
| Trusted Devices              | Trusted devices are those you feel you don’t need to monitor. Trusted devices do not get analyzed by TRITON AP-DATA. If you have devices that you do not want enforced:  
  1. Select **Enable trusted devices**.  
  2. One by one, enter a user name and user agent for each trusted device, and then click **Add**.  
     - **User name** - The name of the device user, case insensitive. Do not include the domain name. For example, enter jdoe rather than mydomain\jdoe. If you leave this field blank, all people who use the device specified in the User agent field are trusted.  
     - **User agent** - a case-sensitive identifier used to identify the device operating system and email client software. Similar devices share the same identifier. If you leave this field blank, all devices for the specified users are trusted—for example, all mobile devices used by jdoe. If the device is connected to an Exchange server, you can find the user agent string using an interface such as Outlook Web App (OWA).  
  Click **Remove** to remove a device from the trusted device list. |
Configuring user directory settings

In the TRITON Manager, you define the LDAP user directory or directories 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 tab, you define the user directory to use for TRITON AP-DATA users and other policy resources such as devices and networks.

By defining user directories such as Microsoft Active Directory or IBM Domino servers for these purposes, you do not have to enter directory entries manually, and you know that you have the most current information available.

To configure user directories in the Data Security manager:

1. Select Settings > General > 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.

Note that user names with a “/” character cause an import failure from Domino user directories. Please contact Websense Technical Support if your user names contain these characters.

Adding a new user directory server

2. Select Enabled to use this user directory server for user import.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the user directory server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of directory from the drop-down menu: Active Directory, Domino, Active Directory Application Mode (ADAM), or Comma Separated Value (CSV) file.</td>
</tr>
</tbody>
</table>

4. If you select Comma Separated Value (CSV) file, complete the following fields.

<table>
<thead>
<tr>
<th>Connection Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Enter a path for the CSV file containing your user directory entries. Use Universal Naming Convention (UNC) format. For example, &lt;\SharedServer\Shared\Groups\Network&gt;.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the name of a user with access to this directory.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for this user.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click this button to test your connection to the file server.</td>
</tr>
</tbody>
</table>

---

**Important**

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 378 for details.

5. If you select, Active Directory, Domino, or Active Directory Application Mode (ADAM), complete the following fields:

<table>
<thead>
<tr>
<th>Connection Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname of the user directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the user directory server.</td>
</tr>
<tr>
<td>User distinguished name</td>
<td>Enter the distinguished name of a user that has access to the directory server. This is the LDAP attribute that uniquely defines this user account or user object. If your organization uses Active Directory, you can use the format “domain\username”. Otherwise, use the format “CN=User, OU=Department, DC=DomainComponent,DC=com”.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user name.</td>
</tr>
<tr>
<td>Root naming context</td>
<td>Enter the root context for the user directory server. This field is required for ADAM directories, but optional for Active Directory and Domino.</td>
</tr>
</tbody>
</table>
### Configuring System Settings

<table>
<thead>
<tr>
<th>Use SSL encryption</th>
<th>Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow referrals</td>
<td>Select this option if you want TRITON AP-DATA to follow server referrals, should they exist. A server referral is when one server refers to another for programs or data. For example, in large, complex Active Directory networks, one domain controller may refer to another to get the information it needs to complete an operation. 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.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click this button to test your connection to the user directory server.</td>
</tr>
</tbody>
</table>

### Directory usage

<table>
<thead>
<tr>
<th>Get user attributes</th>
<th>Select this box if you want to retrieve user information from the directory server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes to retrieve</td>
<td>Enter the user attributes that you want the Data Security manager to collect for all users. Separate attributes by commas. For example: title, manager, department.</td>
</tr>
</tbody>
</table>
| 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. |
| View Results        | Click **View Results** to check the user information that was imported. **View Results** retrieves and displays the data entered in the **Attributes to retrieve**, **Photo attributes to retrieve**, and **Sample email address** fields. |

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

---

**Note**

If you change your user directory settings at a later date, existing administrators become invalid unless you are pointing to an exact mirror of the user directory server. If the new server is not a mirror, you may not be able to distinguish between your new and existing users.
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 > General > 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. Only users with email addresses are imported.

1. Select Settings > General > System.
2. Click the User Directories option in the System pane.
3. You can import entries immediately or on a specified schedule. Select one of the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Now</td>
<td>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.)</td>
</tr>
<tr>
<td>Import daily/weekly at hh:mm</td>
<td>The Import daily/weekly at hh:mm link indicates the current schedule for user directory imports. Click this link to adjust the import schedule. See Scheduling import, page 378 for instructions.</td>
</tr>
</tbody>
</table>

**Note**

Imports from CSV files cannot be scheduled. You must click Import Now to import data from a CSV user directory.
Scheduling import

You can import user directory entries on a prescribed schedule, daily or weekly at set times. This ensures that the TRITON AP-DATA system is synchronized with your user directory service.

To schedule user directory import:

1. Navigate to Settings > General > System > User Directories.
2. Select the user directory to import.
3. Click the link in the top right corner of the user directory server list, Import daily/weekly at hh:mm.
4. Select Enabled to enable the scheduler. If this box is not selected, the user directory will remain static until you manually select Import Now from the User Directory Settings toolbar.
5. Select one of the following options:
   - **Daily** - Select this option to import user directory entries into the TRITON AP-DATA system on a daily basis. Use the down and up arrows to select the exact time of day in hours and minutes. Many users choose to synchronize the directories during off business hours.
   - **Weekly** - Select this option to import user directory entries into the TRITON AP-DATA system once a week, then select the day of the week and time of day to perform the import. Use the down and up hours to select the exact time of day in hours and minutes. Many users choose to synchronize the directories during off business hours.
6. Click OK.

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. Enter a user name and a password with access to this directory.
6. Click OK.
7. Each time you want to import user, group, or computer data from the CSV files, go to Settings > General > 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 1 element or none.

Groups file format

Each row in the groups.csv file should contain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>No</td>
<td>Group name</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>Yes</td>
<td>Description</td>
</tr>
<tr>
<td>memberOf</td>
<td>List of UUID</td>
<td>Yes</td>
<td>UUIDs of which this group is a member (can be empty)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>No</td>
<td>User name</td>
</tr>
<tr>
<td>Email</td>
<td>String</td>
<td>Yes</td>
<td>Email address (primary)</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>Yes</td>
<td>Description</td>
</tr>
<tr>
<td>UUID</td>
<td>String</td>
<td>Yes</td>
<td>UUID of the current user’s manager</td>
</tr>
<tr>
<td>memberOf</td>
<td>List of UUID</td>
<td>Yes</td>
<td>UUIDs of which this group is a member (can be empty)</td>
</tr>
</tbody>
</table>

Zero or more “additional attributes” fields

<table>
<thead>
<tr>
<th>String</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>attr:wsbn_title=/=/Manager</td>
<td>wbsn_title</td>
<td>Manager</td>
</tr>
<tr>
<td>aTTr:my amazing attr=/=/the value</td>
<td>my amazing attr</td>
<td>the value</td>
</tr>
<tr>
<td>“ATTR:name=/=value1,value2”</td>
<td>name</td>
<td>value1,value2</td>
</tr>
</tbody>
</table>
Configuring System Settings

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>No</td>
<td>Computer name (hostname)</td>
</tr>
<tr>
<td>FQDN</td>
<td>String</td>
<td>Yes</td>
<td>DNS fully qualified domain name</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>Yes</td>
<td>Description</td>
</tr>
<tr>
<td>memberOf</td>
<td>List of UUID</td>
<td>Yes</td>
<td>UUIDs of which this group is a member (can be empty)</td>
</tr>
</tbody>
</table>

For example:

379a287f-0a5c-40ff-85fd-fae3da462d03,gumby, 
gumby.example.com, print server,"7c9d4db6-1737-4b80-9e6e-
42f415300a05"

Configuring remediation

To define the location of the syslog server and mail release gateway used for remediation:

Note

If you have TRITON AP-WEB, this section does not apply to you.

Related topics:

- Remediation, page 188
1. Select Settings > General > System.
2. Click the Remediation option in the System pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Settings</td>
<td></td>
</tr>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname for the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for the syslog server.</td>
</tr>
<tr>
<td>Use syslog facility for these messages</td>
<td>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.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click Test Connection to send your syslog server a verification test message.</td>
</tr>
<tr>
<td>Release Gateway</td>
<td></td>
</tr>
<tr>
<td>Use the gateway that detected the incident</td>
<td>This option is selected by default. The gateway could be TRITON AP-EMAIL or the protector MTA, depending on your subscription.</td>
</tr>
</tbody>
</table>
| Use the following gateway: | Define a specific gateway to use when releasing quarantined email. The mail release gateway is used to deliver email messages that were blocked and subsequently released.  
- **IP address or hostname** - Enter the IP address or hostname for your mail release gateway.  
- **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 in Arcsight Common Event Format (CEF):

```
CEF:0|Websense|TRITON AP-DATA|8.0|{id}|DLP
Syslog|{severity}| act={action} duser={destinations} 
fname={attachments} msg={details} suser={source} 
cat={policyCategories} 
sourceServiceName={channel}analyzedBy={policyEngineName} 
loginName={name}sourceIp={ip} 
```

where:
- Signature ID = event ID
- act = action taken
- analyzedBy = sensor that detected traffic
- cat = policy categories
- suser = incident source
- duser = incident destinations
- loginName = login name or sAMAccount name
● msg = incident details
● fname = attachments
● sourcelp = source IP where data loss is occurring
● sourceServiceName = channel

### Configuring mail servers

When you configure the system to send incident notifications to administrators, you have the option to include links that permit the administrators to perform workflow operations on the incident. For example, they can click a link to change its severity to High or to escalate it to a manager. When an administrator clicks a link inside an email message, a compose message window appears.

The administrator clicks **Send** on this message to notify the TRITON AP-DATA system that a workflow operation has been requested.

Use the Mail Servers screen to set up the mail server that should be used to receive email requests for workflow updates—the incoming mail server—as well as the mail server that should be used for sending the notifications—the outgoing mail server. (The same outgoing server is used for alerts and scheduled tasks.)

To define the incoming and outgoing mail servers:

1. Select **Settings > General > System.**
2. Click the **Mail Servers** option in the System pane.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Mail Server</strong></td>
<td></td>
</tr>
<tr>
<td>Email protocol</td>
<td>Select the protocol to use for email retrieval. Most mail servers support both.</td>
</tr>
<tr>
<td></td>
<td>● <strong>POP3</strong> - Post Office Protocol 3</td>
</tr>
<tr>
<td></td>
<td>● <strong>IMAP</strong> - Internet Access Message Protocol</td>
</tr>
<tr>
<td>Use secure connection</td>
<td>Select this option to use the secure sockets layer (SSL) protocol to connect</td>
</tr>
<tr>
<td>(SSL)</td>
<td>your incoming mail server. This protects the content of the email from users</td>
</tr>
<tr>
<td></td>
<td>outside of your network.</td>
</tr>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname for your incoming mail server. This is the</td>
</tr>
<tr>
<td></td>
<td>email server address that collects and stores incoming email from administra-</td>
</tr>
<tr>
<td></td>
<td>tor notifications. These are the email messages that are sent to the system</td>
</tr>
<tr>
<td></td>
<td>when administrators try to update workflow operations from inside a notification email.</td>
</tr>
</tbody>
</table>
## Configuring System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the port number for your incoming mail server.</td>
</tr>
<tr>
<td>System email address</td>
<td>The email address to which workflow email requests should be sent—for example: <a href="mailto:DLPsystem@mycompany.com">DLPsystem@mycompany.com</a>. You must set up an email account on your mail server for this purpose. It should be a dedicated account, because the system deletes its contents regularly. Any email in this folder is lost. This email address automatically appears in the To: field of the email message when administrators click a workflow operation link. The exception to this is when the operation is Assign. Then the system email address appears in the CC field, because the To: field is the address of the assignee. The TRITON AP-DATA system periodically cleans this mailbox.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name of someone with access to the incoming mail server. This should be network credentials, not TRITON AP-DATA administrator credentials. The system needs to connect to this server to retrieve the workflow updates.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter this user’s password.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click <strong>Test Connection</strong> to test the settings you configured. The system tries to connect to the server you specified and returns a success or failure message when done. This can take several minutes.</td>
</tr>
</tbody>
</table>

### Outgoing Mail Server

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname for your outgoing mail server. This is the email server address that waits and listens for outgoing notifications and alerts. Note that if you change the outgoing mail server here, the mail server for scheduled tasks, notifications and alerts is affected.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for your outgoing mail server.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click <strong>Test Connection</strong> to test the settings you configured. When prompted, enter an email address where the system can send a test message. If you receive the message, then it was able to connect to the outgoing mail server successfully. This can take several minutes.</td>
</tr>
</tbody>
</table>

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

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 > General > 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
- Policy updates fail during upgrade
- The number of discovery incidents reaches its limit
- Disk space for the incident archive reaches its limit
- Disk space for the forensics repository reaches its limit
- Incidents have been deleted from the incident repository

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>When an alert notification is sent to administrators, from whom should the report be coming?</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom the notification will be coming.</td>
</tr>
<tr>
<td>Outgoing mail server</td>
<td>Enter the IP address or hostname for your outgoing mail server. This is the email server address that waits and listens for outgoing notifications and alerts. Note that if you change the outgoing mail server here, the mail server for scheduled tasks, notifications, and email workflow is affected.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for your outgoing mail server.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject line for the scheduled alert notifications.</td>
</tr>
<tr>
<td>Recipients</td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Click OK to save your changes.

**Editing outgoing mail server properties**

1. To define or edit the **Outgoing mail server**, click the 📝 icon. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname of the outgoing SMTP mail server to use for scheduled alert notifications.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the mail server to use. Click OK to save your changes.</td>
</tr>
</tbody>
</table>

2. Click OK to save your changes. Note that if you change the outgoing mail server here, the mail server for notifications is also changed.
Configuring the incident archive

The incident database is partitioned quarterly. Archiving partitions optimizes performance. To specify where to store the incident archives and how much disk space to allow:

1. Select **Settings > General > System**.
2. Click the **Incident Archive** option in the System pane.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store archive locally</td>
<td>Select this option if you want to store the incident archive on the local machine.</td>
</tr>
<tr>
<td>Archive folder</td>
<td>The location where your archive will be stored, Websense\archive. This is configured during installation and cannot be changed.</td>
</tr>
<tr>
<td>Maximum archive disk space</td>
<td>The maximum amount of disk space allocated for archive storage (editable). *See below for guidelines on estimating how much disk space you’ll require.</td>
</tr>
<tr>
<td>Store archive remotely</td>
<td>Select this option if you want to store the incident archive on a remote machine in your network.</td>
</tr>
<tr>
<td>Use existing storage location</td>
<td>Use the drop-down menu to select a previously configured storage location. Click <strong>Delete</strong> to remove unneeded locations.</td>
</tr>
<tr>
<td>Name new storage location</td>
<td>Select this option to define a new storage location. Enter a name for the new location.</td>
</tr>
<tr>
<td>IP address or hostname</td>
<td>Enter an IP address or hostname for the machine on which the storage will be located.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain name.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name needed for location access.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password needed for location access.</td>
</tr>
<tr>
<td>Archive folder</td>
<td>Type a folder name for the new archive. For example: Websense\archive. Do not include preceding or trailing backslashes. The folder is relative to the IP or hostname that you entered.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click <strong>Test Connection</strong> to make sure the TRITON AP-DATA server can access the storage location. This ensures the path is valid (hostname and folder) and also checks the access credentials.</td>
</tr>
</tbody>
</table>
4. Click **OK** to save your changes.

To archive partitions, select **Settings > General > Archive.**

**Disk space calculation**

The amount of disk space that you’ll need for the incident archive depends primarily on:

- **The total size of the transactions resulting in incidents**—in other words, the size of the email messages, HTTP posts, printed files, and so on, that violated policy.

Estimate total transaction size using the following formula:

\[(\text{number of incidents per quarter}) \times (\text{average transaction size}) \times 12\]

You multiply the product by 12, because the system allows 12 archived partitions or 3 years of data.

To see the number of incidents you’ve had this quarter, view the Incident Trends report (**Main > Reporting > Data Loss Prevention > Incident Trends**). To see the number and size of audited Web and email transactions, view the upper right corner of the Today page (**Main > Status > Today**).

- **The size of the metadata for the incidents**

The metadata kept for DLP incidents also influences the size of the incident archive. The metadata size can vary depending on the number of policies you use and the complexity of your incidents. Incident complexity is a factor of the number of policies, rules, content classifiers, and violation triggers that are involved. Generally, metadata takes no more than 10-20 bytes of information per incident. Use the Incident Trends report to gain visibility into the number of DLP incidents.

Estimate expected metadata size using the following formula:

\[(\text{number of incidents per quarter}) \times 20\ \text{bytes} \times 12\]

The total disk space you require then, is the sum of the first and second result.

Depending on these factors, an archive containing 100,000 incidents could be between 10-20 MB and 1 GB.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>If desired, enter a description for the archive location.</td>
</tr>
<tr>
<td>Maximum archive disk space</td>
<td>Select a limit on the storage drive for disk space used by the archive. *See below for guidelines on estimating how much disk space you’ll require.</td>
</tr>
</tbody>
</table>
### Entering subscription settings

When you install TRITON AP-DATA, data loss prevention over Web and email is automatically provided through the Websense V-Series appliance (TRITON AP-WEB and TRITON AP-EMAIL subscription required). For these deployments, subscription keys are entered in the Web and Email tabs of the TRITON Manager. You are not required to enter a subscription key on the Data tab.

To provide Web and email DLP through other means—such as the TRITON AP-DATA protector or TMG agent—you must have a TRITON AP-DATA subscription. You must also have a TRITON AP-DATA subscription to analyze images or protect DLP channels besides Web and email.

To provide the subscription key:

1. Log onto the Data Security manager. If you have installed an add-on DLP component—such as Image Analysis or the endpoint agent—you’re prompted to enter your subscription key.
2. 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 AP-DATA application restarts.

When you purchase an upgrade or change your subscription type, you must update your TRITON AP-DATA subscription file. If you do not, an error message displays when you try to use TRITON AP-DATA.

To update your TRITON AP-DATA subscription:

1. Select **Settings > General > 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 AP-DATA application restarts automatically.

**Related topics:**

- Subscription alerts, page 390
Subscription alerts

The health alert summary on the TRITON AP-DATA 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.

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 TRITON AP-DATA sales representative.

Configuring URL categories and user names

This section describes how to configure URL categories and user name resolution for TRITON AP-DATA reports and transaction analysis. Both functions depend on Websense Linking Service, a Web filtering component that is automatically installed with the AP-WEB module of the TRITON Manager.

The Websense Linking Service provides IP address to user name resolution for HTTP incidents. With this service, TRITON AP-DATA is able to display user names in incident reports rather than IP addresses.
In addition, the Linking Service allows TRITON AP-DATA to import Web Security’s preset and custom URL categories so you can add them as resources in your DLP policies. This enables you to map URLs to categories and view them in incident reports.

On this screen, you can make sure the connection to the Linking Service is intact, and you can configure how to use the URL categories and user names in TRITON AP-DATA.

1. Select **Settings > General > System**.
2. From the System pane, choose **URL Categories & User Names**.
3. The IP address and port of the Linking Service machine appears automatically upon installation.
4. Ensure **Enabled** is selected.
5. Click **Test Connection** to test the linking connection. A confirmation message is returned.
6. If connection fails, update the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>Enter the IP address or hostname of the Web Security manager machine.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the Web Security manager machine, by default: 56992.</td>
</tr>
</tbody>
</table>

7. Dynamic user name resolution and category mapping are enabled by default when you install TRITON AP-DATA. If you are experiencing significant latency during content analysis, edit the properties in the **Properties** box to limit the use of the Linking Service to the most important functions. Only change these settings if the connection between your data and web modules is poor.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Reports</td>
<td></td>
</tr>
<tr>
<td>Show user names in incident reports</td>
<td>Select this check box if you want user names to display in incident reports rather than IP addresses. This lets you determine more easily who is moving sensitive data.</td>
</tr>
<tr>
<td>Show URL categories in incident reports</td>
<td>Select this check box if you want URL categories to display in incident reports rather than URLs. For example, rather than displaying <a href="http://www.cnn.com">http://www.cnn.com</a>, reports might display News and Media. This lets you see the type of website to which your sensitive data is being sent.</td>
</tr>
</tbody>
</table>
8. Click **OK** to save your settings.

**Importing URL categories**

URL categories are automatically imported into TRITON AP-DATA when you first set up the TRITON Manager. However, the Websense Master Database is updated regularly. To obtain the latest categories, you should re-import them periodically.

To import URL categories:

1. Select **Main > Resources > URL Categories**.
2. Click **Update Now** in the toolbar.
Configuring Authorization

Select General > Authorization on the Settings tab to configure authorization for your system. This section of the Data Security manager lets you:

- View and edit administrators - the people who manage the TRITON AP-DATA system. (Note that administrators are defined under TRITON Settings.)
- Set up roles - such as the Super Administrator, Basic, and Auditor. Each role has different permissions
- Configure personal settings

Defining administrators

TRITON AP-DATA administrators configure security policies, view incidents, fine-tune system performance, and more. You may have one Super Administrator in your system, or you may have multiple administrators with different responsibilities. Administrators are added, managed, and deleted using the TRITON Settings > Administrators option in the TRITON toolbar. In this same area, you indicate which administrators have access to the TRITON AP-DATA module.
In the Data Security manager, you can view the users who administer the TRITON AP-DATA module, and you can define their roles, but you cannot add or delete administrators.

There are 3 types of TRITON AP-DATA administrators:

- **Local administrator** - defined via TRITON Settings and granted TRITON AP-DATA permissions. The administrator’s role is assigned in the Data Security manager.

- **Network administrator** - defined in an LDAP user-directory, added via TRITON Settings, and granted TRITON AP-DATA permissions. The administrator’s role is defined in the Data Security manager.

- **Network group administrator** - belongs to a user-directory group added via TRITON Settings and granted TRITON AP-DATA permissions. Each user-directory member of this group can log on to the TRITON Manager and work with the TRITON AP-DATA module. The group’s role is assigned in the Data Security manager.

User-directory group members can belong to more than one user-directory group. When such users log on to the system, they are automatically assigned a custom role with the combined permissions from all their groups. The role name that appears in the TRITON toolbar for these users is “Multiple Combined.”

Do to their nature, network group administrators do not have all the same capabilities as local and network administrators.

- **Assign/release incidents** - Network group administrators cannot be assigned incidents or release incidents.

- **Audit records** - Audit log records reflect the administrator who is currently logged on, not the administrator’s group.

- **Administrator management** - In the administrators screen, local administrators, network administrators, and user-directory groups are listed. Network group administrators are not displayed.

- **Policy owners** - Local and network administrators can be policy owners, as can network groups (provided they have a valid email address). Individual network group administrators cannot own policies.

- **Notifications** - Local and network administrators can receive notifications, as can network groups (provided they have a valid email address). Individual network group administrators cannot receive notifications.

- **Report owner** - Ownership on reports is given to specific administrators and not to user-directory groups. This ownership is given according to the administrator who is currently logged on, so even group members can own reports.

- **Saved configuration** - TRITON AP-DATA configurations are saved according to the currently logged on administrator. Data is saved for specific administrators and not for user-directory groups. This data can be saved for user-directory members that logged on as well.

- **Administrator reports** - Several reports in the Data Security manager show top values per administrator. In such reports, only specific administrators are displayed. User-directory groups are not displayed.
Viewing administrators

To view a list of TRITON administrators with access to the TRITON AP-DATA module:

1. Select **Settings > General > 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, roles, and permissions.
3. To view details about all TRITON AP-DATA administrators, click the PDF button on the administrator list screen. Choose **Summary** to export basic information about the modules, policies, and business units each administrator can access, or choose **Details** to export detailed information, including TRITON AP-DATA permissions. You can save or print the report as needed.
4. Select a user name to view or edit an administrator profile.
5. When administrators are first added to the system, you should click their names and assign them roles. TRITON administrators with TRITON AP-DATA access permissions are assigned the default role, which lets them do nothing other than access reporting and Today page. Global Security Administrators are assigned the Super Administrator role in TRITON AP-DATA.
6. See **Editing administrators, page 396** for more information.

Related topics:

- **Defining administrators, page 393**
- **Editing administrators, page 396**
- **Working with roles, page 398**
- **Adding a new role, page 400**
You cannot change administrator user names or email addresses, because these are defined in TRITON Settings; but you can modify administrators roles and access permissions within the TRITON AP-DATA module.

1. Select **Settings > General > Authorization**.
2. Click the **Administrators** option in the Authorization pane.
3. Select the user name for the administrator whose profile you want to edit. Note that changes to administrator profiles are recorded in the audit log.
4. Select a role for this administrator from the drop-down list. There are several default roles to choose from (see *Working with roles*, page 398 for a description), or you can click **New** to create a new role. Click **View Permissions** to view the permission settings for the role you choose.
5. Under Incident Management, indicate which incidents you want this administrator to be able to manage. By default, the administrator can manage all incidents from all policies and business units. Click the links to modify these settings. See the following sections for more information:
   - **Select Incidents**
   - **Select Policies**
   - **Select Business Units**
6. Select **Audit incident detail views** if you want to add a record to the audit log each time this administrator views incident details in the Incidents report.

The audit log is updated when the administrator clicks (and highlights) an incident in the report, and its details are displayed in the Preview pane (triggered values, properties, forensics, and history). The log is also updated when the administrator double-clicks an incident and opens its details in a new browser window.

If this administrator is assigned a role with permission to “perform operations on incidents,” then records are also added to the audit log when the administrator emails incidents to a manager or other recipient or exports incidents to a CSV or PDF file.

This option does not add a record when the administrator views the incident summary information that is displayed when he or she runs a report.

By default, administrators are not audited when they view incident details.

### Related topics:
- *Defining administrators*, page 393
- *Select Incidents*, page 397
- *Select Policies*, page 397
- *Select Business Units*, page 398
- *Working with roles*, page 398
- *Adding a new role*, page 400
Navigate to **Main > Status > Audit Log** to view the audit log.

---

**Note**

If local administrators are also defined as members of a user directory group, the permissions you assign here supercede those of the group.

---

7. Click **OK**.

### Select Incidents

When editing an administrator’s profile (see *Editing administrators*, page 396), you have the option to select which incidents you want this administrator to be able to manage. The administrator will be able to access the incident reports and remediate the incidents that you select.

- Select **All incidents** if you want the administrator to be able to manage all incidents from the selected policies and business units.
- Select **Only incidents assigned to this administrator** if you want the administrator to manage only those incidents assigned to him or her.

2. Click **OK**.

---

**Note**

Administrators cannot access incidents unless their role has Reporting permissions. If this administrator does not have a role with such permissions, the settings you apply here have no effect.

---

### Select Policies

When editing an administrator’s profile (see *Editing administrators*, page 396), you have the option to select which policies the administrator can manage. This affects which incidents the administrator can manage as well. The administrator will be able to access all DLP and discovery incidents for these policies.

- Select **All** if you want this administrator to manage all policies. If you choose **All**, all current and future policies (and their incidents) are accessible to this administrator.
- Select **Selected** to select which policies the administrator can access. Choosing **Select All** selects all the items listed in the current window, but future policies are not selected.
2. Click **OK**.

---

**Note**
The administrator must have a role that permits policy management. If he or she does not, the settings you apply here have no effect.

---

### Select Business Units

1. When editing an administrator’s profile (see *Editing administrators*, page 396), you have the option to select the business units for which this administrator will be able to access incidents. For example, you can configure the administrator profile so that the administrator can access only incidents from the Marketing and Sales business units.

   For most channels, like email and Web, administrators can view incidents generated by someone in the business unit. (A user in this business unit sent sensitive data in an email message.) For the mobile channel, they can view incidents that were destined to users in the business unit. (A user received sensitive data in email and tried to synchronize it to his mobile device.)

---

**Note**
Business Units applies only to data loss prevention incidents. Administrators can view discovery incidents from all business units.

---

- Select **All** if you want this administrator to access DLP incidents from all business units. If you choose **All**, all current and future business units (and their incidents) are accessible to this administrator.

- Select **Selected** to select which business units the administrator can access. Choosing **Select All** selects all the items listed in the current window, but future business units are not selected.

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

---

### Working with roles

Administrators are added and assigned module access permissions using the **TRITON Settings > Administrators** option in the TRITON toolbar. In that area, you can define a Global Security Administrator with Super Administrator access to all TRITON modules (TRITON AP-WEB, TRITON AP-DATA, and TRITON AP-EMAIL), and you can assign custom permissions to other administrators. For example, you can give an administrator access to the TRITON AP-DATA module or access along with the ability to modify access permissions for other accounts.
In the TRITON AP-DATA module, you fine-tune permissions by assigning administrators roles. Roles are specific to functions performed in the TRITON AP-DATA module.

For example, one administrator 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 Super Administrator requiring access to all.

This is where roles come into play. Roles define the access privileges for various administrative roles in your organization. By default, the following roles are defined:

- **Super Administrator** - can access all configuration and management screens in the TRITON AP-DATA module with read and write privileges. This is different from Global Security Administrators who have Super Administrator privileges to all TRITON modules.
- **System Administrator** - can access the system settings functions, the deployment options, and the Status screens. This role is designed for IT or infrastructure administrators responsible for installing and maintaining the system infrastructure.
- **Policy Manager** - can configure policies, qualify and assign incidents.
- **Incident Manager** - can access reports, incident details, and workflow. Manages incident handling.
- **Auditor** - can review policies, rules, and content classifiers for regulatory compliance.
- **Default** - default role for a new administrator. Can access only reports and the Today page.
- **Multiple Combined** - has privileges from several roles combined. This role applies only to network administrators who belong to multiple user-directory groups. When such administrators log onto the Data Security manager, the system automatically generates a custom role that unifies the roles of all their groups. Because they are system-generated, multiple combined roles are not listed on the roles screen. Administrators with this role see this role name in the toolbar when they log on.

You can edit access privileges for these default roles or you can add new roles. You can then assign a role to each of your system administrators.

1. Select **Settings > General > Authorization**.
2. Click the **Roles** option in the Authorization pane.
   The resulting screen lists all the 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 role.
4. To delete an role, select it then click **Delete**.

Note that changes to roles are recorded in the audit log.
Configuring Authorization

Adding a new role

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

To define a new role:

1. Click New on the Roles page toolbar.
2. Complete the fields as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the new role</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description for the role</td>
</tr>
</tbody>
</table>
| 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. |

Related topics:

- Viewing administrators, page 395
Configuring Authorization

**Data Security Manager Help**

**401**

### Configuring Authorization

Select the incident and reporting functions that this role should be able to access.

#### Data Loss Prevention & Mobile

- **Summary reports** - Select this option to give administrators with this role access to data loss prevention summary reports.
- **Detail reports** - Select this option to give administrators with this role access to data loss prevention 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 forensics** - 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 loss prevention or mobile incidents.

#### Discovery

Not included in TRITON AP-WEB or TRITON AP-EMAIL.

- **Summary reports** - Select this option to give administrators with this role access to discovery summary reports.
- **Detail reports** - Select this option to give administrators with this role access to 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 administrators with this role to be able to perform all escalation, remediation, and workflow operations on discovery incidents.

Check the **Send email notifications** box if you want administrators with this role notified when an incident is assigned to them.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td>Select the incident and reporting functions that this role should be able to access.</td>
</tr>
<tr>
<td><strong>Data Loss Prevention &amp; Mobile</strong></td>
<td></td>
</tr>
<tr>
<td>• Summary reports</td>
<td>Select this option to give administrators with this role access to data loss prevention summary reports.</td>
</tr>
<tr>
<td>• Detail reports</td>
<td>Select this option to give administrators with this role access to data loss prevention detail reports. When this option is selected, several more are made available:</td>
</tr>
<tr>
<td>■ View violation triggers</td>
<td>Select this option if you want the administrator to view the values that trigger violations.</td>
</tr>
<tr>
<td>■ View forensics</td>
<td>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.)</td>
</tr>
<tr>
<td>■ Hide source and destination</td>
<td>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.</td>
</tr>
<tr>
<td>■ Perform operations on incidents</td>
<td>Select this option if you want administrators with this role to be able to perform all escalation, remediation, and workflow operations on data loss prevention or mobile incidents.</td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
<td>Not included in TRITON AP-WEB or TRITON AP-EMAIL.</td>
</tr>
<tr>
<td>• Summary reports</td>
<td>Select this option to give administrators with this role access to discovery summary reports.</td>
</tr>
<tr>
<td>• Detail reports</td>
<td>Select this option to give administrators with this role access to discovery detail reports. When this option is selected, more are made available:</td>
</tr>
<tr>
<td>■ View violation triggers</td>
<td>Select this option if you want the administrator to view the values that trigger discovery violations.</td>
</tr>
<tr>
<td>■ Perform operations on incidents</td>
<td>Select this option if you want administrators with this role to be able to perform all escalation, remediation, and workflow operations on discovery incidents.</td>
</tr>
</tbody>
</table>

Data Security Manager Help ▶ 401
Configuring Authorization

Policy Management

Select the policy management functions this role should be able to perform:

- **Data loss prevention policies** - Can configure DLP policies for all channels as well as content classifiers and resources.
- **Discovery policies** - Can configure discovery policies, tasks, content classifiers, and resources.
- **Sample database records** - Can view sample database information when editing a database fingerprinting classifier, including database, Salesforce, and CSV classifiers. This is offered on the Field Selection page of the fingerprinting wizard when you define the records to fingerprint. It allows you to verify that you've set up the classifier as intended. See *Database Fingerprinting Wizard - Field Selection, page 158* for more details.

Administrators can always view sample data when creating a new classifier, but you may not want all administrators to view data set up by others. If you de-select this box, this option is grayed out for administrators with this role.

Status

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 TRITON AP-DATA servers and protectors.
- The **Endpoint Status** screen summarizes the results of endpoint connectivity tests. (Not included in TRITON AP-WEB or TRITON AP-EMAIL.)
- The **Traffic log** contains details of the traffic being monitored by TRITON AP-DATA 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 TRITON AP-DATA servers, protectors, or policy engines.
- The **Audit log** displays actions performed by administrators in the system.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Management</td>
<td>Select the policy management functions this role should be able to perform.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Data loss prevention policies</strong> - Can configure DLP policies for all channels as well as content classifiers and resources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Discovery policies</strong> - Can configure discovery policies, tasks, content classifiers, and resources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sample database records</strong> - Can view sample database information when editing a database fingerprinting classifier, including database, Salesforce, and CSV classifiers.</td>
</tr>
<tr>
<td></td>
<td>This is offered on the Field Selection page of the fingerprinting wizard when you define the records to fingerprint. It allows you to verify that you’ve set up the classifier as intended. See <em>Database Fingerprinting Wizard - Field Selection, page 158</em> for more details.</td>
</tr>
<tr>
<td></td>
<td>Administrators can always view sample data when creating a new classifier, but you may not want all administrators to view data set up by others. If you de-select this box, this option is grayed out for administrators with this role.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the status reports and logs to which this role should have access:</td>
</tr>
<tr>
<td></td>
<td>- The <strong>Today</strong> page shows system alerts, statistics, and an incident summary over the last 24 hours.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>System Health</strong> screen enables you to monitor the performance of TRITON AP-DATA servers and protectors.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>Endpoint Status</strong> screen summarizes the results of endpoint connectivity tests. (Not included in TRITON AP-WEB or TRITON AP-EMAIL.)</td>
</tr>
<tr>
<td></td>
<td>- The <strong>Traffic log</strong> contains details of the traffic being monitored by TRITON AP-DATA over specific periods, such as data that has breached policies and the actions taken.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>System log</strong> displays system events sent from different Websense components, for example TRITON AP-DATA servers, protectors, or policy engines.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>Audit log</strong> displays actions performed by administrators in the system.</td>
</tr>
</tbody>
</table>
3. Click **OK** to save your changes.

### Configuring personal settings

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

In case you do not want to receive system reminders such as “Deployment is needed,” The system provides a “Do not show this window again” option.

Use Personal Settings if want to restore the default setting.

1. Select **Settings > General > Authorization.**
2. Select the **My Settings** option on the Authorization pane.
3. Select Show all reminders.
4. Click **OK** to save your changes.
Archiving Incidents

The incident database is partitioned every 90 days. Periodically, you should archive the partitions to optimize performance.

The Data Security manager 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 the Data Security manager.

Select **Settings > General > 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 the **Settings** button 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.

If you are using Microsoft SQL Server Standard or Enterprise for your TRITON database, you can have a maximum of 8 online partitions (approximately 2 years). Refer to **Remote SQL Server machines, page 407** for special instructions.

If you are using SQL Server Express, you can have one active partition for the current quarter. In addition, you can have up to 4 online partitions (approximately 1 year), 4 restored partitions (1 year), and 12 archived partitions representing 3 years of records.
The columns in the archive list are sortable.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>An internally set identifying number for the partition beginning with the year. Click the incident partitions to select them for archiving.</td>
</tr>
</tbody>
</table>
| 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        | The first event logged in the archive.                                                                                                      |
| To          | The last event logged in the archive.                                                                                                         |
| # of Incidents | The number of incidents currently collected in the archive.                                                                                  |
| Location    | The location of the archive, whether local or at an external IP address.                                                                        |
| 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 from the top of the screen 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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>🗑️</td>
<td>Click this button to send a selected archive to offline storage. See <em>Archiving a partition</em>, page 408.</td>
</tr>
<tr>
<td>Restore</td>
<td>📦</td>
<td>Click this button to restore a selected archived partition. See <em>Restoring a partition</em>, page 409.</td>
</tr>
<tr>
<td>Delete</td>
<td>✗</td>
<td>Click this button to delete a selected partition. Note: partitions are permanently deleted. See <em>Deleting a partition</em>, page 409.</td>
</tr>
<tr>
<td>Settings</td>
<td>🍂</td>
<td>Click this button to go to a screen where you can define the archive size and the storage location. See <em>Configuring the incident archive</em>, page 387.</td>
</tr>
</tbody>
</table>
When you install TRITON AP-DATA on the TRITON management server, you specify whether to use a local or remote SQL Server database.

If you specify a remote database, you have the option to enable TRITON AP-DATA archiving. (Archiving is automatically enabled when you use a local database.)

When you archive incidents, they are initially stored in a temporary folder. If you are using a remote SQL Server database, you must specify the folder to use before you can archive incidents. (This is done during installation.) Both the database and the TRITON management server must have access to the temporary folder.

If you do not configure these settings when you install TRITON AP-DATA, you cannot manually archive incidents. If you try, the Data Security manager warns you that you have not fully configured archive settings, so archiving won’t work. If you set up automatic archiving, it fails and sends a message to syslog.

If you receive such messages, you must modify your installation to use the archiving feature, as follows:

1. Rerun the Websense installer.
2. Next to TRITON AP-DATA, select Modify.
3. Click Next until you reach the Incident Archiving page.
4. Select Enable TRITON AP-DATA archiving.
5. Enter the local or network path that SQL Server should use to access the temporary folder.
6. Enter the UNC path that the management server should use to access the temporary folder.
7. Provide network credentials.
8. Continue through the installation wizard.
9. Click Deploy in the Data Security manager to deploy your changes.

Note that you only configure the temporary archive folder in the installer. To configure the final location of the archive, select Settings > General > System > Incident Archive in the Data Security manager.

---

**Important**
The folder must already exist.
Archiving a partition

Incident partitions will automatically fill, but you can only keep 4 partitions online (if using SQL Server Express), and 8 partitions online (if using Microsoft SQL Server Standard or Enterprise). 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.
4. Click **OK** to continue.

The number of partition archives you can create depends on the size of the partition location.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>The year the partition was created.</td>
</tr>
<tr>
<td>ID</td>
<td>An internally set identifying number for the partition beginning with the year. Click the incident partitions to select them for archiving.</td>
</tr>
</tbody>
</table>
| 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         | The first event logged in the archive. |
| To           | The last event logged in the archive. |
| Archive location | 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. |
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 4 partitions (approximately 1 year of record) if using SQL Server Express or Microsoft SQL Server Standard or Enterprise. To restore incident partitions from their archives:

1. Select **Settings > General > 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 > General > 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, the system automatically creates a “private” archive when disk space is exceeded. Should it be necessary, please contact Websense Technical Support to retrieve the archive.
Updating Predefined Policies and Classifiers

For your convenience, Websense provides many predefined policies, content classifiers, and file types. Websense research teams stay abreast of regulations across many industries and keep the policies and classifiers up-to-date. Sometimes these elements are updated between product release cycles and you can update them to the latest by going to Settings > General > Policy Updates. See Related Topics for a complete list of the policies, classifiers, and file types provided at the time of this product’s release.

Viewing your update history

To view the history of your policy updates (including when updates were performed, what they contained, and more), navigate to Settings > General > Policy Updates in
the Data Security manager. This page lists the updates you’ve obtained to date along with their original version and new version.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The date you performed the update.</td>
</tr>
<tr>
<td>Administrator</td>
<td>The administrator who performed the update.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of policy that was updated. Standard Policies are those predefined by Websense and available to all customers. Custom policies are those that have been built just for your organization.</td>
</tr>
<tr>
<td>From Version</td>
<td>The version of policies, classifiers, and file types installed prior to the update.</td>
</tr>
<tr>
<td>To Version</td>
<td>The version of policies, classifiers, and file types installed during the update.</td>
</tr>
<tr>
<td>Details</td>
<td>A link to a PDF file containing the details of the update. The PDF contains general information, release notes (details about what changed), a snapshot of your policies and classifiers before they were updated, and a list of the components that were updated. Click the link to view the details.</td>
</tr>
<tr>
<td>File name</td>
<td>The name of the update file used to perform the update.</td>
</tr>
</tbody>
</table>

**Toolbar buttons**

You can install updates or restore them by clicking buttons in the toolbar:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Updates</td>
<td><img src="image" alt="Install Icon" /></td>
<td>Click this button to install the latest policy updates, content classifiers, and file types on your system. A wizard is launched. (See Installing policy updates, page 413 for instructions on using the wizard.)</td>
</tr>
<tr>
<td>Restore</td>
<td><img src="image" alt="Restore Icon" /></td>
<td>Click this button to restore your policies, content classifiers, and file types to the selected version. (See Restoring policies to a previous version, page 414 for instructions.)</td>
</tr>
</tbody>
</table>
Installing policy updates

Websense updates the predefined policies (adding policies or changing existing ones) on a regular basis. Websense also updates the predefined content classifiers and file types it supports.

To install the most recent updates:

1. Obtain a file containing the latest updates from MyWebsense.com.
   a. Log onto MyWebsense.
   b. Click the Downloads tab.
   c. Select Get Hotfixes & Patches.
   d. Select TRITON AP-DATA.
   e. Select the software version for which you’re applying the updates. If you’re not sure of the version, select Help > About from the Data Security manager.
   f. Download the .zip file that’s provided. Do not unzip it.
2. In the Data Security manager, navigate to Settings > General > Policy Updates.
3. Click Install Updates on the toolbar. (You will be able to view the contents of the update before committing to it.) A wizard launches.
4. When prompted, browse to the zip file.
5. Click Next.
6. You’re shown the version of your current policies and the new policies. To see what’s new in the update, click the link that’s provided at the top of the page.
7. Click Next to install the updated policies and content classifiers. Once you do, you cannot cancel the update (though you can later restore it).
8. The Update Process page shows you the progress of the update. It shows what it’s adding, what it’s deleting, what it’s updating.
9. When the updates have installed successfully and you’re ready to apply them, click Next.
10. A message confirms the update has completed successfully. Click the link to view a summary of the update.
11. Click Finish.
12. The summary screen appears with the details of this update listed in the table. See Viewing your update history, page 411 for a description of this page.
Updating Predefined Policies and Classifiers

Restoring policies to a previous version

Occasionally, you may find that the latest policies do not suit your needs. For example, a content classifier that was deleted by the update was used in one or more of your policies. You’d like time to modify your policies before installing the latest updates.

If necessary, you can restore your policies, classifiers, and file types to their previous version.

Warning
When you restore predefined components to a previous version, all current policies, classifiers, and other elements are overridden.

When you restore a policy that was customized by Websense, all changes you have made to other policies since you installed the custom policy are reverted, and all action plans created since that time are deleted.

To restore your policies:

1. In the Data Security manager, navigate to Settings > General > Policy Updates.
2. From the table, select the From Version to which you want to revert.
3. Click Restore on the toolbar.
4. Click OK to confirm you want to proceed.
5. The system restores your policy and classifiers to the version and date you selected. Progress indicators show whether components were restored successfully.
6. Click Close. The summary screen shows the date you restored the policies, the version you moved from, and the version you moved to. See Viewing your update history, page 411 for a description of this page.

Note that you cannot restore policies from an older version of TRITON AP-DATA. For example, if you are running TRITON AP-DATA v8.0, you cannot revert to policies from Data Security v7.8.

Related topics:

- Viewing your update history, page 411
- Installing policy updates, page 413
Determining the policy version you have

When you are upgrading or restoring policy versions, it is helpful to know what version you currently have.

To do so, navigate to **Settings > General > Policy Updates** in the Data Security manager. This page lists the updates you’ve obtained to date along with their original version and new version.

Your current version is the **To Version** with the latest date.
Managing System Modules

The System Modules screen lets you configure all the components in the TRITON AP-DATA network and distribute the load between them evenly.

To access this screen, select **Settings > Deployment > System Modules**.

If you are running TRITON AP-WEB, the only modules you’ll see listed on this screen are the TRITON management server and supplemental TRITON AP-DATA 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 TRITON AP-DATA 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.

Related topics:
- *Adding modules*, page 419
- *Configuring modules*, page 419
- *Balancing the load*, page 465
Each module and component is represented by an icon. Next to each module is a version number. This lets you see at a glance whether a particular module has been upgraded.

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.

If you have more than one TRITON AP-DATA 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 465 for details.
Adding modules

To add a new module, go to the machine where you want to install it and run the TRITON AP-DATA installation wizard. (See the TRITON AP-DATA Installation Guide for instructions.

When you install the module, you are asked to provide the FQDN or the IP address of the TRITON management server and the credentials for a TRITON AP-DATA 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 role, page 400 for information on system modules permissions.

Please note that if you install 2 stand-alone agents on the same machine, the system registers them twice (independently) and they appear in the system-modules tree as 2 separate computers.

In addition, if the IP address or hostname (FQDN) of a module should change after you’ve registered it, you must re-register the module to notify the TRITON management server of the change.

If you change both the IP address and the hostname of a module, you must re-register it twice, once after each change. If you re-register once after both changes, the TRITON 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

If you have TRITON AP-WEB, you may never need to configure modules. The TRITON AP-DATA servers are given a default configuration when they’re installed that usually suffices.
Managing System Modules

If you’re running a full TRITON AP-DATA 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.

Either way, you are welcome to customize your configuration settings any time to meet your needs.

To configure a TRITON AP-DATA module:

1. Select Settings > Deployment > System Modules.
2. Click the module of interest.
3. Complete the fields as shown in the sections below:

   - Configuring the management server
   - Configuring a supplemental TRITON AP-DATA Server
   - Configuring the fingerprint repository
   - Configuring the endpoint server
   - Configuring the crawler
   - Configuring the forensics repository
   - Configuring the policy engine
   - Configuring the optical character recognition (OCR) server
   - Configuring the protector
   - Configuring ICAP
   - Configuring the Web Content Gateway module
   - Configuring the TRITON AP-EMAIL module
   - Configuring the TMG agent
   - Configuring the integration agent
   - Configuring protector services
   - Configuring the mobile agent
   - Configuring the Microsoft FCI agent

---

**Note**

If you have TRITON AP-WEB, not all of these options apply to you.

---

**Configuring the management server**

The TRITON management server is installed automatically on the TRITON management machine and is the heart of the TRITON AP-DATA 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a new name for the TRITON management server if desired. Not to exceed 128 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the management server, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. This lets you see whether the module has been updated along with the others.</td>
</tr>
</tbody>
</table>

The management server includes many other components: a primary fingerprint repository, endpoint server, crawler, forensics repository, and policy engine. To configure these components on the management server, expand the management server on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- Configuring the fingerprint repository
- Configuring the endpoint server
- Configuring the crawler
- Configuring the forensics repository
- Configuring the policy engine
Configuring a supplemental TRITON AP-DATA Server

Supplemental TRITON AP-DATA servers include a secondary fingerprint repository, endpoint server, crawler, policy engine, and OCR server. To configure these components on a supplemental server, expand the supplemental server on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- Configuring the fingerprint repository
- Configuring the endpoint server
- Configuring the crawler
- Configuring the policy engine
- Configuring the optical character recognition (OCR) server

Note that you can delete a supplemental TRITON AP-DATA server, but you cannot delete the management server.

Configuring the fingerprint repository

In TRITON AP-DATA, the primary fingerprint repository is stored on the TRITON management server. The primary repository creates secondary repositories on protectors, Content Gateways, TRITON AP-DATA servers, and any other module with a policy engine. These contain structured (database) fingerprints and are updated frequently to remain current. File fingerprints are transmitted in real time so they are not stored in the secondary repository.

This page depends on whether you are editing a primary or secondary fingerprint repository.

- Primary Fingerprint Repository
- Secondary Fingerprint Repository
### Primary Fingerprint Repository

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of agent (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
</tbody>
</table>

#### Tuning Performance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum disk space</td>
<td>Select the maximum disk space that should be allowed for the fingerprint repository, in megabytes. Default: 50,000 MB.</td>
</tr>
<tr>
<td>Maximum cache size</td>
<td>Select the maximum amount of memory that the fingerprint repository should use to cache fingerprints, in megabytes. Default: 512 MB.</td>
</tr>
</tbody>
</table>

### Secondary Fingerprint Repository

Secondary fingerprint repositories contain structured data only (database fingerprints). File fingerprints are transmitted in real time so they don’t need to be stored on system modules other than the management server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of agent (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module, not to exceed 128 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
</tbody>
</table>

#### Repository Selection

Detect fingerprints from: Select a option 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 TRITON management server, but you can select any repository. Forcepoint 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 the system should use the fingerprinting memory, and schedule the synchronization based on your networking requirements.
Managing System Modules

Configuring the endpoint server

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:
- Adding an endpoint profile, page 468
- Configuring endpoint settings, page 477

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect</td>
</tr>
<tr>
<td></td>
<td>it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module, not to exceed 128 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed</td>
</tr>
<tr>
<td></td>
<td>(uneditable).</td>
</tr>
</tbody>
</table>

Tuning Performance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum cache size</td>
<td>Select the maximum amount of memory that should be allocated for the</td>
</tr>
<tr>
<td></td>
<td>fingerprint repository, in megabytes.</td>
</tr>
<tr>
<td>Continuously</td>
<td>By default, secondary repositories check for updates from the primary</td>
</tr>
<tr>
<td></td>
<td>continually (every 30 seconds). This ensures the secondary repository</td>
</tr>
<tr>
<td></td>
<td>machine always has the latest fingerprints.</td>
</tr>
<tr>
<td>Continuously except</td>
<td>If you want to exclude a certain time period from this I/O activity, select</td>
</tr>
<tr>
<td>between</td>
<td>Continuously except between and specify the blackout time period—for</td>
</tr>
<tr>
<td></td>
<td>example: peak business hours.</td>
</tr>
<tr>
<td></td>
<td>During this period, the secondary repository will not check with the</td>
</tr>
<tr>
<td></td>
<td>primary for updates. (Times are assumed to be in the database repository</td>
</tr>
<tr>
<td></td>
<td>zone.)</td>
</tr>
<tr>
<td></td>
<td>Limiting I/O can improve fingerprinting performance, but accuracy can</td>
</tr>
<tr>
<td></td>
<td>be affected, because the latest fingerprints may not be used.</td>
</tr>
</tbody>
</table>
Managing System Modules

Configuring the crawler

The crawler is the agent that performs fingerprint and discovery scans. You can have multiple crawlers in your TRITON AP-DATA system. To configure one, select it on the System Modules screen and complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
</tbody>
</table>

Related topics:
- File fingerprinting, page 127
- Database fingerprinting, page 145
- Scheduling network discovery tasks, page 229
- Scheduling endpoint discovery tasks, page 265

Configuring the 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. It is different from the incident database which contains information about the rules that were violated, violation triggers, and more.

To configure the forensics repository, select it on the System Modules screen and complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
</tbody>
</table>
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 TRITON AP-DATA system to manage high transaction volumes. Policy engines reside on:

- TRITON management server
- Supplemental TRITON AP-DATA servers
- Protectors
- Mobile agents
- Content Gateway machines
- TRITON AP-EMAIL machines

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 465 for more information.
Managing System Modules

Configuring the optical character recognition (OCR) server

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

Related topics:
- *Adding or editing an OCR server*, page 429
- *Monitoring system health*, page 342

The OCR server enables the system to analyze image files being sent through network channels, such as email attachments and Web posts. The server determines whether the images are textual, and if so, extracts and analyzes the text for sensitive content. There is no special attribute to configure within your policies. If sensitive text is found, the image is blocked or permitted according to your current policies.

The server can also be used to locate sensitive textual images during network discovery.

Note that handwriting is not supported; nor are images containing text that is skewed more than 10 degrees.

The OCR server is automatically included in supplemental TRITON AP-DATA server installations. To use optical character recognition, you must install a supplemental TRITON AP-DATA server.

To enable OCR analysis in your network:
1. Navigate to the System Modules page and edit the policy engine on each server or agent that will receive traffic that you want analyzed. For example, edit the policy engine on Web Content Gateway if you’ll be routing traffic through TRITON AP-WEB.

2. In each Edit window, select **Enable OCR** and indicate which OCR server (supplemental TRITON AP-DATA server) to use to extract text from images.

When OCR is enabled, images are sent to that OCR server for text extraction.

This includes the following image types.

- JBIG2- JBIG2 File Format (.jB2, .jbig2)
- MacPaint - MacPaint
- PC_Paintbrush - Paintbrush Graphics (PCX)
- BMP - Windows Bitmap
- JPEG_File_Interchange - JPEG Interchange Format
- PNG - Portable Network Graphics (PNG)
- GIF_87a - Graphics Interchange Format (GIF87a)
- GIF_89 - Graphics Interchange Format (GIF89a)
- TIFF - TIFF
- Scanned documents PDF - documents containing only scanned text.

All other PDF documents, including hybrid files containing both searchable text and scanned text, are sent to the default TRITON AP-DATA extractor, not the OCR server. Should the system fail to extract text from a PDF, it is forwarded to the OCR server.

---

**Tip**

If you have a PDF type that you want always routed to the OCR server, you can edit a configuration file known as, **extractor.config.xml**. Refer to this [knowledgebase article](#) for instructions.

The OCR server can analyze images that meet the following criteria:

- 32,000 x 32,000 pixels or less
- 300 DPI resolution for images with large text (10 point font and larger)
- 400-600 DPI for images with small text (9 point font or smaller)

On the system modules page you can configure the languages to analyze and fine-tune the module’s accuracy profile to optimize performance.

To view the status of your OCR servers, select **Main > Status > System Health**.
Adding or editing an OCR server

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
</tbody>
</table>
| Accuracy  | Indicate your tolerance for speed versus accuracy. There is a tradeoff between the two.  
  - **Fast** - Select this option if you have a high volume of images (the load level on your OCR server will be large), and you are concerned about performance. Only large, text-intensive images are sent for extraction; small images and documents that don’t contain much text are not extracted at all. This option enhances performance but is less accurate than the Accurate option.  
  - **Accurate** - Select this option if you have a small number of images (the load level on your OCR server will be small), then every textual image in your network is sent to the server for extraction. This affects performance, but provides the most accurate results. If response is inadequate—for example, browsers are timing out on the HTTP channel—change this setting to Fast or Balanced.  
  - **Balanced** - Select this option (the default) if you want a balance between accuracy and speed. |
| Languages | The system can analyze textual images in many languages. Select the ones that might appear inside your textual images.  
Note that some languages are included with TRITON AP-DATA. These are listed below this table. Other languages require a separate language package on your OCR server. Refer to the Technical Library article, “Installing the TRITON AP-DATA Language Pack.”  
If you select a language that is not included with the product and you do not have the language pack installed, matches in that language are not detected.  
Image analysis can be time consuming. Select fewer languages to optimize performance.  
In addition, false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce. |
Languages included with TRITON AP-DATA (no language pack required)

- Basque
- Belarusian
- Danish
- Dutch (Netherlands)
- Dutch (Belgium)
- English
- Finnish
- French
- Scottish Gaelic
- German
- German (new spelling)
- German (Luxembourg)
- Greek
- Hebrew
- Icelandic
- Irish
- Italian
- Norwegian
- Old English
- Old French
- Old German
- Old Italian
- Old Spanish
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Spanish
- Swedish
- Turkish
- Welsh
- Yiddish
Configuring the protector

Once registration is established between the protector and the TRITON 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.

Note that protectors include an ICAP server, policy engine, and secondary fingerprint repository. To configure these components on the protector, expand the protector on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- *Configuring the fingerprint repository*
- *Configuring the policy engine*
- *Configuring ICAP*
General tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

The General tab enables you to modify the basic settings of the protector.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the protector.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable this protector for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the protector.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The hostname of the machine hosting the protector (uneditable).</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the machine hosting the protector (uneditable).</td>
</tr>
<tr>
<td>Managed by</td>
<td>The name of the TRITON AP-DATA Server that is currently managing this protector (uneditable).</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others (uneditable).</td>
</tr>
</tbody>
</table>

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.
Managing System Modules

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default gateway</td>
<td>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.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select an interface to which packets for this route will be sent.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>To add a DNS server, type in the DNS Server IP address and click Add. The DNS Server is added to the list.</td>
</tr>
<tr>
<td>DNS suffixes</td>
<td>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.</td>
</tr>
<tr>
<td>Connection mode</td>
<td>Select one of the following connection modes from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Inline (Bridge)</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SPAN/Mirror Port</strong> - 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.</td>
</tr>
</tbody>
</table>

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**

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 TRITON AP-DATA 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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge name</td>
<td>The name of the inline bridge (editable)</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Set the Link Speed to either: <strong>10Mb/s</strong>, <strong>100 Mb/s</strong>, <strong>1000Mb/s</strong>, <strong>Auto</strong>.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Set Duplex Mode to either <strong>Half</strong>, <strong>Full</strong> or <strong>Auto</strong>.</td>
</tr>
</tbody>
</table>
Managing System Modules

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>The name of the interface</td>
</tr>
<tr>
<td>Status</td>
<td>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 option as necessary.</td>
</tr>
<tr>
<td>Mode</td>
<td>Set the interface’s Operation Mode to either Network or Monitoring.</td>
</tr>
<tr>
<td>Interface IP address</td>
<td>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.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Enter the subnet mask for the interface.</td>
</tr>
<tr>
<td>Link speed</td>
<td>Set the link speed to either: 10Mb/s, 100 Mb/s, 1000Mb/s, Automatic.</td>
</tr>
<tr>
<td>Duplex mode</td>
<td>Set duplex mode to either Half, Full or Automatic.</td>
</tr>
</tbody>
</table>
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 - inbound as well as outbound 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 inbound and which are outbound. These networks are referred as my networks while considering inbound/outbound/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.
Managing System Modules

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 (inbound, outbound, 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 450 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/HTTPS tab
- FTP tab
Managing System Modules

General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports used by this ICAP server. These are the ports over which the system should monitor ICAP transactions. Separate multiple values with commas. Example: 1333,1334</td>
</tr>
<tr>
<td>Allow connection to this ICAP Server from the following IP addresses:</td>
<td>Select whether you want this ICAP server to allow connections from All IP addresses or just Selected IP addresses. If you choose Selected IP addresses, enter the IP address to allow then click Add. Repeat this process until you’ve added all the IP addresses you want to allow.</td>
</tr>
</tbody>
</table>

HTTP/HTTPS tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select the mode in which you want to deploy the module:</td>
</tr>
<tr>
<td></td>
<td>● Monitoring - Monitor HTTP traffic but not block it.</td>
</tr>
<tr>
<td></td>
<td>● Blocking - Block HTTP actions that breach policy.</td>
</tr>
<tr>
<td>When an unspecified error occurs</td>
<td>Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed:</td>
</tr>
<tr>
<td></td>
<td>● Permit traffic - Allow HTTP traffic to continue unprotected.</td>
</tr>
<tr>
<td></td>
<td>● Block traffic - Stop all HTTP traffic until the problem is resolved.</td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td>Default violation message</td>
<td>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.</td>
</tr>
<tr>
<td>Default unspecified error message</td>
<td>Click the link to see the error message that is displayed when a URL is blocked due to an unspecified error.</td>
</tr>
</tbody>
</table>

FTP tab
Configuring the Web Content Gateway module

The Web Content Gateway is a Web proxy that is an integral part of TRITON AP-WEB solutions. If you have Web Filter & Security and you want to combine it with TRITON AP-DATA, you must have the Websense Content Gateway.

When you register the Websense Content Gateway with the TRITON 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/HTTPS tab**
- **FTP tab**

Note that Content Gateway modules include a policy engine and secondary fingerprint repository. To configure these components on the Web Content Gateway module, expand the module on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- **Configuring the fingerprint repository**
- **Configuring the policy engine**
### General tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed. (uneditable)</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others.</td>
</tr>
</tbody>
</table>

### HTTP/HTTPS tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select the mode in which you want to deploy the module:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Monitoring</strong> - Monitor HTTP and HTTPS traffic through the Websense Content Gateway but not block it.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Blocking</strong> - Block HTTP and HTTPS actions that breach policy.</td>
</tr>
<tr>
<td>When an unspecified error</td>
<td>Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed:</td>
</tr>
<tr>
<td>occurs</td>
<td>● <strong>Permit traffic</strong> - Allow HTTP and HTTPS traffic routed through the Websense Content Gateway to continue unprotected.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Block traffic</strong> - Stop all HTTP and HTTPS traffic through the gateway until the problem is resolved.</td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td>Display default violation</td>
<td>Select this option to display a default violation message in the user’s browser whenever a URL violation is detected. Click the link to view the message.</td>
</tr>
<tr>
<td>message</td>
<td></td>
</tr>
<tr>
<td>Redirect to URL</td>
<td>Specify the URL to which to redirect users when they try to access a website that violates policy.</td>
</tr>
</tbody>
</table>
Configuring the TRITON AP-EMAIL module

The TRITON AP-EMAIL module is pre-installed on your V-Series appliance. It filters inbound, outbound, and internal email messages for spam and viruses, and uses the TRITON AP-DATA module to analyze content.

TRITON AP-EMAIL is automatically registered with the TRITON management server when you enter its subscription key in Email Security manager. Registration occurs when you enter this key for your first TRITON AP-EMAIL appliance. The key is propagated for all subsequent TRITON AP-EMAIL appliances.

To complete the registration, be sure to click Deploy in the Data Security manager.

When registration is successful, you can see an TRITON AP-EMAIL module on the System Modules page.

In the TRITON AP-EMAIL module of the TRITON Manager, you configure this module to monitor email traffic or enforce it. Click the Email tab, then select Main > Policy Management > Policies and select the policy of interest. On the Edit screen, change “Operation mode” to Monitor or Enforce as needed.

In the Data Security manager, you define the action to take when a breach is discovered. Messages can be permitted, quarantined, encrypted and released, or have their attachments dropped. Select Main > Policy Management > Resources > Action Plans to configure these options.
To manage the TRITON AP-EMAIL module in the Data Security manager, select it on the System Modules screen and complete the fields as follows. Note that some are uneditable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (editable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (editable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed. (editable)</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others. (editable)</td>
</tr>
</tbody>
</table>

Note that TRITON AP-EMAIL modules include a policy engine and secondary fingerprint repository. To configure these components on the TRITON AP-EMAIL module, expand the module on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- Configuring the fingerprint repository
- Configuring the policy engine

**Configuring the TMG agent**

The TMG agent is installed on a server hosting Forefront Threat Management Gateway (TMG) 2010. To configure the agent, select it on the System Modules screen and the Edit TMG Agent window appears.

There are 2 tabs in the Edit TMG Agent window:

- General tab
- Advanced tab

The TMG agent does not include its own policy engine, so it has to be associated with one. By default, the agent is associated with all available policy engines, including those on the management server, supplemental servers, Web Content Gateway (when applicable), and other modules. Traffic going through the agent is routed to the first available policy engine for analysis. To select specific policy engines, click **Load Balancing** on the System Modules menu bar and then select the TMG agent.
Managing System Modules

General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others. (uneditable)</td>
</tr>
</tbody>
</table>

Advanced tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation mode</td>
<td>Select the mode in which you want to deploy the module:</td>
</tr>
<tr>
<td></td>
<td>● Monitoring - Monitor traffic through the TMG server but not block it.</td>
</tr>
<tr>
<td></td>
<td>● Blocking - Block actions that breach policy.</td>
</tr>
<tr>
<td>Display default message</td>
<td>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.</td>
</tr>
<tr>
<td>Display custom message</td>
<td>Select this button to use a custom message, then browse to the message to use. (This file must be fewer than 2800 characters.)</td>
</tr>
<tr>
<td>When an unspecified error</td>
<td>Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed:</td>
</tr>
<tr>
<td>occurs</td>
<td>● Permit traffic - Allow traffic routed through the TMG server to continue unprotected.</td>
</tr>
<tr>
<td></td>
<td>● Block traffic - Stop all traffic through the TMG server until the problem is resolved.</td>
</tr>
<tr>
<td>Display default message</td>
<td>Select this button to display a default message in the user’s browser when a URL is blocked due to an unspecified error. Click the link to view the message.</td>
</tr>
<tr>
<td>Display custom message</td>
<td>Select this button to use a custom message, then browse to the message to use. (This file must be fewer than 2800 characters.)</td>
</tr>
</tbody>
</table>

Configuring the integration agent

The integration agent allows third-party products to send data to TRITON AP-DATA
for analysis. It is embedded in third-party installers and communicates with TRITON AP-DATA via a C-based API. You can change the name and description of this module by selecting it from the System Modules screen. The FQDN and version are not configurable.

Note that the Integration agent does not support discovery transactions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others.</td>
</tr>
</tbody>
</table>

### Configuring the mobile agent

The mobile agent is a Linux-based appliance that lets you secure the type of email content that is synchronized to users’ mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

In your network, the appliance connects to the TRITON management server as well as to your Microsoft Exchange server to provide this function. Outside your DMZ, it connects to any Microsoft ActiveSync-compatible mobile device over 3G and wireless networks—devices such as i-pads, Android mobile phones, and i-phones.

Like the protector, the mobile appliance has an on-board policy engine and fingerprint repository to optimize content analysis.

The mobile agent is included in subscriptions to TRITON AP-DATA Gateway, TRITON AP-EMAIL, and TRITON AP-ENDPOINT.

No software has to be installed on your users’ mobile devices.

To configure the mobile agent, select it on the System Modules screen and complete the fields as follows:

There are 3 tabs in the Edit Mobile Agent window:
Managing System Modules

- General tab
- Connection tab
- Analysis tab

Note that mobile agents include a policy engine and secondary fingerprint repository. To configure these components on the mobile agent, expand the module on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- Configuring the fingerprint repository
- Configuring the policy engine
### General tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module, not to exceed 4000 characters.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others. (uneditable)</td>
</tr>
</tbody>
</table>

### Connection tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exchange Connection</strong></td>
<td></td>
</tr>
<tr>
<td>Use secure connection (SSL)</td>
<td>Select this box if you want to use Secure Sockets Layer (SSL) to provide communication security when connecting the mobile agent to your Microsoft Exchange server.</td>
</tr>
<tr>
<td>Hostname or IP address</td>
<td>Enter the IP address of your Microsoft Exchange server. The mobile appliance connects to this server to access email resources. The appliance acts as a reverse proxy to the Exchange server, making mobile devices unaware of the server.</td>
</tr>
</tbody>
</table>
| Port                 | The port number for the Microsoft Exchange server depends on whether you are using a secure connection:  
  ● If you select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 443.  
  ● If you do not select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 80. |
| Domain               | Optionally, enter the domain used to identify users in your organization. |
| **Mobile Devices Connection** |             |
| Use secure connection (SSL) | Select this box if you want to use Secure Sockets Layer (SSL) to provide communication security when connecting the mobile agent to your users’ mobile devices. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP address                                   | Select the IP address of the network interface card (NIC) that mobile devices should use to connect to this agent.  
This is a NIC on the mobile appliance or machine hosting the mobile agent. It is the IP address that the mobile agent will listen on. The list reflects all of the NICs found on the mobile appliance.  
Select **All IP addresses** to allow the agent to listen and accept connections from all available network interface IPs.  
**Note:** To modify the IP addresses available on the mobile agent machine, re-install and re-register the mobile agent. If you enter a user name in the installation wizard, the system resolves it to the correct IP address. |
| Port                                         | The port number for the Microsoft Exchange server depends on whether you are using a secure connection:  
- If you select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 443.  
- If you do not select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 80. |
| Use Forcepoint default security certificate   | To secure connection, users must set up their mobile devices to accept security certificates from the server.  
Select this option to use the default security certificate provided by Forcepoint. The default security certificate is a self-signed certificate automatically generated by Forcepoint.  
It enables SSL encryption to secure the ActiveSync public channel that is used by the mobile agent when communicating with mobile devices, but it does not rely on a well known Root CA for authentication.  
If you use this option, users may need to configure their mobile devices to accept all SSL certificates. Some devices, such as those using Windows Mobile 7, do not support this. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the following certificates</td>
<td>Select this option to secure the ActiveSync public channel using your own signed certificates, then upload the certificates to use. This option enables SSL encryption and CA authentication, so it is seamlessly accepted by all mobile devices. You must upload both a public certificate and its associated private key.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Public certificate</strong> - Upload the public certificate that the agent should use to identify itself to mobile devices. The signing CA can be a self-signed Root CA or subordinated (possibly untrusted) CA. If your certificate is signed by a subordinated CA, you must also upload its associated certificate chain file. (See <strong>Add chained certificate</strong> below.)</td>
</tr>
<tr>
<td></td>
<td>● <strong>Private key</strong> - Upload the private key that was used to generate the public certificate.</td>
</tr>
<tr>
<td></td>
<td>The certificate files must conform to these requirements:</td>
</tr>
<tr>
<td></td>
<td>● All files should be in .PEM file format.</td>
</tr>
<tr>
<td></td>
<td>● The .PEM files for the public certificate and private key must be separate. Concatenation is not supported.</td>
</tr>
<tr>
<td></td>
<td>● The files should not be encrypted or passphrase protected.</td>
</tr>
<tr>
<td></td>
<td>● You must follow a Certificate Signing Request (CSR) procedure when creating the files. Instructions are readily available online.</td>
</tr>
<tr>
<td>Add chained certificate</td>
<td>Select this option if your public certificate is signed by a subordinated certificate. The certificate chain, also known as the certification path, should be a list of all of the CA certificates between (but not including) the server certificate and the Root CA stored in the mobile devices. Each certificate in the list should be signed by the entity identified by the next. For example, the chained certificate should include numbers 2, 3, and 4 below, but not numbers 1 or 2.</td>
</tr>
<tr>
<td></td>
<td>1. Server certificate, signed by</td>
</tr>
<tr>
<td></td>
<td>2. Issuing CA 1, signed by</td>
</tr>
<tr>
<td></td>
<td>3. Intermediate CA 2, signed by</td>
</tr>
<tr>
<td></td>
<td>4. Intermediate CA 3, signed by</td>
</tr>
<tr>
<td></td>
<td>5. Root CA</td>
</tr>
<tr>
<td></td>
<td>The SSLCertificateChainFile file is the concatenation of the various PEM-encoded CA certificate files, usually in certificate chain order. In most cases, the CA organization you work with provides this file.</td>
</tr>
</tbody>
</table>
Managing System Modules

Analysis tab

The Microsoft File Classification Infrastructure (FCI) agent enables the system to augment the data classification capabilities inherent to Windows machines. If you plan to perform discovery on a Windows machine, install the FCI agent on it to optimize security.

To configure this agent, select it on the System Modules screen and complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select the mode in which you want to deploy the module:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitoring</strong> - Monitor traffic through the mobile agent but not block it. This is selected by default.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Blocking</strong> - Block actions that breach policy. (Note, to prevent disruption, traffic is permitted when there is an unspecified system error.)</td>
</tr>
<tr>
<td>Notify users of breach</td>
<td>Only available in blocking mode. Select this option if you want to notify users when an email message, task, appointment, or other item was blocked by the agent. You can enter the text to include in the email subject line and body, or you can click the right arrows and select from variables such as %From%, %Attachments%, and %Type%. Note: Before users can be notified of breaches, you must configure an outgoing mail server and sender details. To do so, navigate to Settings &gt; General &gt; System &gt; Alerts, and then select the Email Properties tab.</td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest email transaction to analyze, in bytes.</td>
</tr>
</tbody>
</table>

Configuring the Microsoft FCI agent

The Microsoft File Classification Infrastructure (FCI) agent enables the system to augment the data classification capabilities inherent to Windows machines. If you plan to perform discovery on a Windows machine, install the FCI agent on it to optimize security.

To configure this agent, select it on the System Modules screen and complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module (uneditable).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it. (Agents are enabled by default.)</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module (uneditable).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name given to the module when it was installed (uneditable).</td>
</tr>
<tr>
<td>Version</td>
<td>The version of this module. Lets you see whether the module has been updated along with the others.</td>
</tr>
</tbody>
</table>
Configuring protector services

Related topics:
- Configuring the policy engine, page 426
- Configuring SMTP, page 450
- Configuring HTTP, page 456
- Configuring FTP, page 459
- Configuring chat, page 461
- Configuring plain text, page 463

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
- Chat
- Plain text

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
Managing System Modules

General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports to monitor, separated with commas. Example: 1333,1334</td>
</tr>
<tr>
<td>Intelligent protocol discovery</td>
<td>Select this check box if you want the system 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.)</td>
</tr>
<tr>
<td>Mode</td>
<td>If the protector is operating in inline mode, select which of the following modes to use:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitoring bridge</strong> - In monitoring bridge mode, TRITON AP-DATA monitors and analyzes a copy of the traffic but does not enable policies to block transactions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mail Transfer Agent</strong> - Select this option to set the protector to MTA mode. You must configure your mail servers and clients to forward mail to the protector. Note that when functioning as an MTA, it is important to ensure you limit the networks monitored by the protector in order to prevent the protector from becoming an open relay.</td>
</tr>
<tr>
<td></td>
<td>If the protector is operating in SPAN mode, select which of the following modes to use:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitoring passive</strong> - In monitoring passive mode, TRITON AP-DATA monitors and analyzes a copy of all traffic but does not enable policies to block transactions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mail Transfer Agent</strong> - Select this option to set the protector to MTA mode. You must configure your mail servers and clients to forward mail to the protector. Note that when functioning as an MTA, it is important to ensure you limit the networks monitored by the protector in order to prevent the protector from becoming an open relay.</td>
</tr>
</tbody>
</table>

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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction Size</strong></td>
<td></td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Select <strong>Inbound</strong> if you want the system to monitor incoming email traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select <strong>Outbound</strong> if you want the system to monitor outgoing email traffic.</td>
</tr>
<tr>
<td><strong>Internal</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Internal</strong> if you want the system to monitor internal email traffic.</td>
</tr>
<tr>
<td><strong>Source’s Network</strong></td>
<td></td>
</tr>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s network filter. This tells TRITON AP-DATA 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 <strong>Add</strong>. Repeat this process for each network address you want to skip.</td>
</tr>
</tbody>
</table>

## SMTP Filter tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direction</strong></td>
<td></td>
</tr>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the SMTP filter.</td>
</tr>
<tr>
<td>Internal email domains</td>
<td>Enter the name of an internal email domain to monitor and click <strong>Add</strong>. Do this for each internal email domain that you want to monitor.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Select <strong>Inbound</strong> if you want the system to monitor incoming email traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select <strong>Outbound</strong> if you want the system to monitor outgoing email traffic.</td>
</tr>
<tr>
<td><strong>Internal</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Internal</strong> if you want the system to monitor internal email traffic.</td>
</tr>
</tbody>
</table>
## Source’s Email Address

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s email address filter. This tells the system to watch for messages sent from specific email address and not analyze those messages. Enter the email address to not analyze then click <strong>Add</strong>. Repeat this process for each email address you want to skip.</td>
</tr>
</tbody>
</table>

### Important

If you do not select a direction, only rules governing outbound traffic are applied.
Managing System Modules

Mail Transfer Agent (MTA) tab

This tab applies only to inline protector mode.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Mode</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>Select this mode if you want to monitor SMTP traffic only.</td>
</tr>
<tr>
<td>Blocking</td>
<td>Select this mode if you want to block SMTP traffic that breaches policy.</td>
</tr>
<tr>
<td>Permit traffic</td>
<td>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.</td>
</tr>
<tr>
<td>Block traffic</td>
<td>Select this option if you want to block all SMTP traffic in the event of an unknown error.</td>
</tr>
<tr>
<td>SMTP Settings</td>
<td></td>
</tr>
<tr>
<td>SMTP HELO name</td>
<td>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.</td>
</tr>
<tr>
<td>Set next hop MTA</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum message size</td>
<td>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.</td>
</tr>
<tr>
<td>Network address</td>
<td>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.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Enter the subnet masks corresponding to the network addresses you entered above.</td>
</tr>
<tr>
<td>Email Settings</td>
<td></td>
</tr>
<tr>
<td>Add the following footer</td>
<td>Enter the footer to add to email notifications to all email messages monitored by TRITON AP-DATA.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Select this option if you want to send notifications when there is a problem with email.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable redirection gateway</td>
<td>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 TRITON AP-DATA know where to send traffic that is supposed to be encrypted or is set to bypass analysis.</td>
</tr>
</tbody>
</table>

**Encryption**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that at least one of the following conditions is met</td>
<td>Select this box if you want the system 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.</td>
</tr>
<tr>
<td>Subject contains encryption flag</td>
<td>One way to inform TRITON AP-DATA 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.</td>
</tr>
<tr>
<td>X-header field name</td>
<td>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 the system to send messages to the encryption gateway.</td>
</tr>
</tbody>
</table>

**Bypass**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that at least one of the following conditions is met</td>
<td>Select this box if you want the system 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.</td>
</tr>
<tr>
<td>Subject contains Bypass Flag</td>
<td>Enter the flag to add to the email Subject field when Bypass is desired.</td>
</tr>
<tr>
<td>X-Header Field Name</td>
<td>In this field, specify the x-header field name that should signal the system to send messages to the redirection gateway.</td>
</tr>
</tbody>
</table>
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**

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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports to monitor, separated with commas. Example: 80,8080</td>
</tr>
<tr>
<td>Intelligent protocol discovery</td>
<td>Select this check box if you want the system 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.)</td>
</tr>
<tr>
<td>Mode</td>
<td>Select which of the following modes to use:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitoring bridge</strong> - In monitoring bridge mode, TRITON AP-DATA monitors and analyzes a copy of all HTTP traffic but does not enable policies to block transactions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Active bridge</strong> - In inline mode, TRITON AP-DATA monitors and blocks traffic according to HTTP policies configured.</td>
</tr>
</tbody>
</table>
### Traffic Filter tab

If you are using HTTP and SMTP in active bridge mode or monitoring mode, be sure to set the **Direction** mode to outgoing *only*!

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction Size</strong></td>
<td></td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Select <strong>Inbound</strong> if you want the system to monitor incoming HTTP traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select <strong>Outbound</strong> if you want the system to monitor outgoing HTTP traffic.</td>
</tr>
<tr>
<td>Internal</td>
<td>Select <strong>Internal</strong> if you want the system to monitor internal HTTP traffic.</td>
</tr>
<tr>
<td><strong>Source's Network</strong></td>
<td></td>
</tr>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s network filter. This tells the system 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.</td>
</tr>
</tbody>
</table>

If you are using HTTP and SMTP in active bridge mode or monitoring mode, be sure to set the **Direction** mode to outgoing *only*!
HTTP Filter tab

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.

### 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.

**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**.

Advanced tab

Select the mode to use for HTTP traffic:
- **Monitoring** - Monitor HTTP traffic only.
- **Blocking** - Block HTTP traffic that breaches policy.

**Field** | **Description**
---|---
Operation mode | Select the mode to use for HTTP traffic:
- Monitoring - Monitor HTTP traffic only.
- Blocking - Block HTTP traffic that breaches policy.

**Policy violation**

- **Display default message**
  Select this option 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 option 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.
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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports to monitor, separated with commas. Example: 20,2121</td>
</tr>
<tr>
<td>Intelligent protocol discovery</td>
<td>Select this check box if you want the system 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.)</td>
</tr>
</tbody>
</table>

Traffic Filter tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Size</td>
<td></td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td>Direction</td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Select Inbound if you want the system to monitor incoming FTP traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select Outbound if you want the system to monitor outgoing FTP traffic.</td>
</tr>
<tr>
<td>Internal</td>
<td>Select Internal if you want the system to monitor internal FTP traffic.</td>
</tr>
</tbody>
</table>
### Source’s Network

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s network filter. This tells the system 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 <strong>Add</strong>. Repeat this process for each network address you want to skip.</td>
</tr>
</tbody>
</table>
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

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports to monitor, separated with commas. Example: 20,2121</td>
</tr>
<tr>
<td>Intelligent protocol discovery</td>
<td>Select this check box if you want the system 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.)</td>
</tr>
</tbody>
</table>

### Traffic Filter tab

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Description</td>
<td></td>
</tr>
<tr>
<td>Transaction Size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td>Direction</td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Select <strong>Inbound</strong> if you want the system to monitor incoming FTP traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select <strong>Outbound</strong> if you want the system to monitor outgoing FTP traffic.</td>
</tr>
<tr>
<td>Internal</td>
<td>Select <strong>Internal</strong> if you want the system to monitor internal FTP traffic.</td>
</tr>
<tr>
<td>Source’s Network</td>
<td></td>
</tr>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s network filter. This tells the system 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 <strong>Add</strong>. Repeat this process for each network address you want to skip.</td>
</tr>
</tbody>
</table>

### Advanced tab
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**

### Configuring plain text

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Select the maximum amount of time to wait before forwarding content to the TRITON AP-DATA server, in milliseconds.</td>
</tr>
</tbody>
</table>
Managing System Modules

**General tab**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the module for use in your environment. Deselect it to disable it.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the module.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the module.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the ports to monitor, separated with commas. Example: 5222, 5333</td>
</tr>
</tbody>
</table>

**Traffic Filter tab**

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction Size</strong></td>
<td></td>
</tr>
<tr>
<td>Minimum transaction size</td>
<td>Select the smallest size transaction that you want the system to monitor, in bytes.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Select <strong>Inbound</strong> if you want the system to monitor incoming FTP traffic.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Select <strong>Outbound</strong> if you want the system to monitor outgoing FTP traffic.</td>
</tr>
<tr>
<td>Internal</td>
<td>Select <strong>Internal</strong> if you want the system to monitor internal FTP traffic.</td>
</tr>
<tr>
<td><strong>Source’s Network</strong></td>
<td></td>
</tr>
<tr>
<td>Enable filter</td>
<td>Select this check box to enable the source’s network filter. This tells the system 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 <strong>Add</strong>. Repeat this process for each network address you want to skip.</td>
</tr>
</tbody>
</table>

**Advanced tab**
You may have several policy engines in your TRITON AP-DATA system. There is one on each TRITON AP-DATA server; there is one on the protector; and if you have TRITON AP-WEB, there is one on the 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 > 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 342 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.

**Note**

Forcepoint recommends that you do not distribute the load to the TRITON management server.
### Defining load balancing distribution

Double-click a service to configure which policy engine should analyze it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The name of the service (uneditable)</td>
</tr>
<tr>
<td>TRITON AP-DATA Server</td>
<td>The host responsible for the service (uneditable).</td>
</tr>
<tr>
<td>Protector</td>
<td><strong>Note:</strong> You cannot balance the load with the TRITON management server.</td>
</tr>
<tr>
<td>Crawler</td>
<td></td>
</tr>
<tr>
<td>ICAP Server</td>
<td></td>
</tr>
<tr>
<td>Content Gateway</td>
<td></td>
</tr>
<tr>
<td>Integration agent</td>
<td></td>
</tr>
<tr>
<td>TMG agent</td>
<td></td>
</tr>
<tr>
<td>FCI agent</td>
<td></td>
</tr>
<tr>
<td>Mobile agent</td>
<td></td>
</tr>
<tr>
<td>Analyzed by</td>
<td>Select <strong>All available policy engines</strong> if you want the service analyzed by all available policy engines. The policy engine on the protector is available for the protector only. Select <strong>Selected policy engines</strong> 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.</td>
</tr>
<tr>
<td>Apply these settings to all of this agent’s services</td>
<td>Select this check box if you want to apply these settings to all of this agent’s services without having to configure each manually.</td>
</tr>
</tbody>
</table>
Configuring Endpoint Deployment

Deploying endpoint systems in your network requires a subscription to TRITON AP-ENDPOINT DLP. It is comprised of the following basic steps:

1. Installing the TRITON management server as described in the TRITON AP-DATA 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 the Data Security manager 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 > General > 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 > DLP / 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 > DLP / Discovery Policies, Custom Policy 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 > 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 > Reporting > Data Loss Prevention.) 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 482 for more information on this capability.
For information on what end users see on their machine, refer to “Using endpoint client software” in the Websense Technical Library. You can distribute this document to your end users as desired.

**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 TRITON AP-DATA 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 TRITON management server and supplemental Data Security servers. Endpoint servers receive incidents from, and send configuration settings to, endpoint clients.
Viewing and managing endpoint profiles

A default endpoint profile is automatically installed on the endpoint client, and you can add more profiles as needed. To view a list of existing endpoint profiles, select Settings > Deployment > Endpoint.

From this screen, you can add a new profile, delete an existing profile, rearrange existing profiles, backup and restore encryption keys, and configure endpoint settings. Use the toolbar buttons to perform these functions.

Select a profile from the list to view or edit its properties.

Configuring encryption for removable media

WebSense Data Endpoint provides 2 methods to encrypt sensitive data that is being copied on removable media devices. You can:

- **Encrypt with profile key**: Windows and Linux only. Encrypt with a password deployed in the endpoint profile. This is for users who will be on an authorized machine—one with the endpoint agent installed—when they try to decrypt files. Select **Encrypt with profile key** when configuring your action plans for endpoint removable media. The action defaults to permitted on Mac endpoints regardless of your action plan setting.

- **Encrypt with user password**: Windows only. Encrypt with a password supplied by endpoint users. This is for users who will be decrypting files from other machines—those without the endpoint agent installed. Select **Encrypt with user password** when configuring your action plans for endpoint removable media. The action defaults to permitted on Linux and Mac endpoints regardless of your action plan setting.

**Encrypt with profile key** is the most secure method of protecting data on USB devices. You provide an encryption key when you create endpoint profiles for each user or group of users. (See **Encryption tab**, page 472 for more details.) The endpoint automatically decrypts files for users whose profiles have the relevant key. Users do not need to supply a password. Administrators can backup and restore encryption
keys. See *Backing up encryption keys*, page 476 and *Restoring encryption keys*, page 476 for more details.

If you select the **Encrypt with user password** option, you allow endpoint users to set the password to use. They can view the files on their home machines or give the files (and the password) to another user. Although content is encrypted on Windows endpoints, it can be decrypted on any Windows or Mac machine. Users must run a Websense Decryption Utility that is included on the removable media device with the encrypted files, and they must provide the password to access the files. See the TRITON AP-ENDPOINT DLP User’s Guide in the Websense Technical Library for more information.

---

**Note**

In the case of CD/DVD media, the Data Security manager automatically promotes the encrypt action to block files being transferred if the destination is a CD writer.

---

**Adding an endpoint profile**

A default endpoint profile is automatically installed on the endpoint client, and you can add more profiles as needed. To view a list of existing endpoint profiles, select **Settings > Deployment > Endpoint**.

From this screen, you can add a new profile, delete an existing profile, rearrange

1. To create a new profile, select **New**. (To edit an existing profile, click a profile name in the list.).

---

**Note**

TRITON AP-DATA 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.
2. Complete the **General, Servers, Properties**, and **Encryption** tabs as described in the following sections.
3. 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. 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.

**Tip**

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**.

---

**Important**

If you add “custom computer” resources to the profile, make sure they have an FQDN defined as well as an IP address. Profiles can only be deployed to computers with a known FQDN.

---

**Servers tab**

This tab lists the endpoint servers installed in the system. Each TRITON AP-DATA 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 TRITON AP-DATA 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:

- **Interactive mode.** This refers to the user interface on the endpoint that is displayed to its local user.

- **Endpoint message templates.** 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 TRITON AP-DATA is installed. You can modify them as required. You can include up to 256 characters in each message. If you include more, the message is truncated in the client user interface.

  If desired, you can clone a file, rename it, and modify the messages. If you put the new file in the \msgFiles folder, the Data Security manager displays it as one of the template options. See [Customizing Data Endpoint messages](#) for more details.

- **Data loss prevention (DLP) policies.** This enables you to override settings on policies designed to prevent data loss.

To define properties settings:

1. Select the **Properties** tab.

2. Under Interactive Mode Options, do the following:

   a. Select **Remote bypass** to allow the endpoint user to disable the endpoint client. This action requires a bypass code from the administrator. (See [Bypassing endpoint clients](#), page 482 for additional information.)

   b. Select **Content scan alerts** to alert the endpoint user when content scanning is in progress. A popup caption appears on the endpoint’s screen.

      Note that content scan alerts are not displayed when data is copied to removable media using a desktop-less environment, such as an ssh terminal connection.

3. To change the default endpoint message template, check the **Set message template** box and select a new message template from the drop-down list.

4. Check **Disable blocking and encryption capabilities when policy violations are detected** to disable blocking and encryption of endpoint traffic. Even if a policy is specifically set up to block or encrypt 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

The Encryption feature allows legitimate users to transfer confidential information to
removable media (such as an external hard drive) 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 with profile key, 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 key.

Note
You can also set the action to Encrypt with user
password if you want users to be able to decrypt files from
other machines (those without the endpoint agent
installed). See Configuring encryption for removable
media, page 467 for additional information.

The strength of the encryption lies with the encryption algorithm and key length used
by the algorithm. The Data Security manager uses a 256-bit key length open source
AES encryption algorithm and a symmetric-key encryption to offer the safest and
easiest method to encrypt your sensitive information. The key is double encrypted and
cannot be used on a USB stick or any external device to decrypt data on unauthorized
PCs.

You must define an encryption key for each endpoint profile. The Data Security
manager 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 the Data
Security manager.
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**

The password should be at least 8 characters in length (maximum is 15 characters), and it should contain:

- At least one digit
- At least one symbol
- At least one capital letter
- At least one lowercase letter

The following example shows a strong password:

8%w@s1*F
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 that 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 window.
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

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.

To rearrange profiles:
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

Once you have defined all the settings for an endpoint profile, the profile can be deployed to the Websense Data Endpoints.

To deploy an endpoint profile:
1. In the Data Security manager, 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 347.
Backing up encryption keys

When TRITON AP-DATA 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:

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

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 472.

To restore encryption keys:

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 369.

### Monitoring endpoint removable media

You can monitor or prevent sensitive information being written from an endpoint to a removable media 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. Click **Endpoint Devices**.
3. Click **New**.

For more information, see *Defining Resources*, page 171.

Add the new resource to your endpoint policy:

1. Select **Main > Policy Management > DLP Policies**.
2. Click **Manage Policies**.
3. Do one of the following:
   - Click a policy and select **Add > Rule**
   - Click a rule and select **Edit**
4. Go to the **Destination** section for the rule.
5. Select **Endpoint Removable Media**, and click **Edit**.
6. Select Devices from the **Display** drop-down list.
7. Choose the devices to monitor for this policy, by selecting the device and clicking the > button to move it to the **Selected List**.
8. Click **OK**.

---

**Note**

If your endpoints are Linux-based, you cannot share removable media devices through NFS.
Selecting endpoint destination channels to monitor

Data Security Manager Help | TRITON AP-DATA | Version 8.0x

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 > DLP Policies.**
2. Click **Manage Policies.**
3. Do one of the following:
   - Click a policy and select **Add > Rule**
   - Click a rule and select **Edit**
4. Go to the **Destination** section for the rule.
5. You can select from the following:
   - **Email** - Select **Endpoint Email** to monitor outbound or internal email messages sent to the destinations you specify. By default this option covers all endpoint destinations. To select particular destinations, click **Edit** and select the destinations to watch.
     
     Note that the system analyzes all email messages sent from endpoint users, even if they send them to external Web mail services such as Yahoo.
     
     **Important**
     
     For endpoint email to be analyzed, you must specify one or more internal email domains. Navigating to **Settings > General > System > Endpoint** and then click the Email Domains tab. If no domain is listed, endpoint email is not analyzed.
     
     For Windows, TRITON AP-DATA can analyze endpoint email generated by Microsoft Outlook and IBM Notes. (Note that rules are not enforced on Notes messages if Notes is configured to send mail directly to Internet, rather than through the Domino server.)
     
     The system supports the desktop version of Outlook 2003, 2007, 2010, and 2013 but not the Windows 8 touch version. If you are using Outlook 2003, then Office 2003 SP3 must be installed. The system supports IBM Notes version 8.5.1, 8.5.2 FP4, and 8.5.3.
     
     For Mac OS X, the system can analyze endpoint email generated by Outlook 2008, Outlook 2011, and Apple Mail.
     
     - **Web** - Select **Endpoint HTTP/HTTPS** from the **Channels** 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.
When the endpoint analyzes data via the Web > Endpoint HTTP/HTTPS destination, it intercepts HTTP(S) posts as they are being uploaded within the browser. (It does not monitor download requests.)

For both Mac and Windows-based endpoints, the system analyzes posts from the following browsers:

- Internet Explorer versions 7 to 11
- Firefox versions up to 32
- Google Chrome 32-bit versions 26 to 38. (Windows endpoints using Chrome 33 or later must belong to a domain for the Data Endpoint Chrome extension to function.)

It also analyzes posts on Mac OS X from Safari 7.0.3. Prior to that, it analyzed posts on Safari versions on Mac OS X 10.7 or above.

The system does not support the HTTP destination channel on Linux endpoints.

For a list of supported browser versions, see the Certified Product Matrix.

Note that this destination is different from the Endpoint Application > Browsers destination which looks at the data as it is being copied, pasted, or accessed. The system can monitor these operations on most browsers, such as Internet Explorer, Firefox, Safari, and Opera.

It’s possible to see URL category information on the incident if the Websense Linking Service is active. (See Configuring URL categories and user names, page 390 for details.)

- **Endpoint printing** - Select this option to monitor data being sent from an endpoint machine to a local or network printer. The system supports drivers that print to a physical device, not those that print to file or PDF.

- **Endpoint application** - You can monitor or prevent sensitive data from being copied and pasted from an application such as Microsoft Word or a Web 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 .exe, .csv, .xls/xlsx, .pdf, .txt, and .doc/.docx files.
- When files are saved to any other local folder, it analyzes all file types.

The system can monitor copy and paste operations on most browsers, such as Internet Explorer, Firefox, Safari, and Opera.

---

**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.

---
The applications that the system supports out of the box are found in the Technical Library article TRITON AP-DATA Endpoint Applications. You can also add custom applications.

- **Endpoint removable media** - You can monitor or prevent sensitive data from being transferred to removable media. In the action plan, you define whether to block it, permit it, ask users to confirm their action, encrypt it with a profile key configured by administrators, or encrypt it with a password supplied by endpoint users. Here, define the devices to analyze.

  The system monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications. It monitors non-native Windows CD/DVD burner applications as well, but only blocks or permits operations without performing content classification.


  Linux endpoint does not support CD/DVD burners.

  On Windows 7, the system can also monitor unencrypted data being copied to Android devices through the Windows Portable Devices (WPD) protocol.

- **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 TRITON AP-DATA:
  - 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 copied from an endpoint client to a network share.
  - 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.

  Please note, if access to the LAN requires user credentials, files larger than 10 MB are handled as huge files which are only searched for file size, file name and binary fingerprint. Files smaller than 10 MB are fully analyzed.

  The huge files limit for other channels is 100 MB.

  All destination channels are supported on Windows endpoints.

  On Linux endpoints, only removable media is supported. The HTTP/HTTPS and email channels are not supported on Linux, nor are the print or LAN channels or endpoint applications.
On Mac, all destination channels except the print channel are supported, with the exceptions noted below.

<table>
<thead>
<tr>
<th>Destination Channel</th>
<th>Windows</th>
<th>Mac OS X</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Web HTTP/HTTPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Printing</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications*</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Removable media</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>LAN</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

*Cloud apps and screen capture operations are not supported on Mac endpoints. The cut, copy, paste, file access, and download operations are not supported for cloud apps on Windows endpoints when they are used through a Windows Store browser.

For more information on monitoring destinations and protecting data on endpoints, see *Custom Policy Wizard - Destination*, page 88.

**Bypassing endpoint clients**

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.
2. The dialog that appears contains a bypass ID. Have the end user report it to you.
3. In the Data Security manager, select **Main > Status > 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 TRITON AP-DATA Deployment Guide for details.

If desired, you can customize or choose another language for the bypass message that appears on the client. See Customizing Data Endpoint messages for more details.

### Updating the endpoint client

Endpoint clients check for updates to policies and profile settings at intervals specified in the endpoint global settings. For more information on configuring endpoint settings, see Configuring endpoint settings, page 477.

The end user can start an update check at any time by clicking Update on the Websense Data Endpoint screen.
Using the endpoint client software

Data Endpoint client software is installed on users machines according to settings in the Websense Endpoint Package Builder.

If the software was installed in interactive mode, an icon appears on the endpoint machine’s task bar.

For instructions on using the endpoint client software, visit the Websense Technical Library.
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 486
- Endpoint, page 486
- Fingerprinting, page 488
- Incidents, page 490
- Miscellaneous, page 491
- Performance, page 492
- Linking Service, page 493

This section lists common problems and their solutions. See the Related Topics box to choose a specific area of concern.
Troubleshooting

Discovery

This section lists problems related to discovery and their solutions.

**Discovery is configured to discover sensitive files but sensitive files are not found**

It could be that the TRITON AP-DATA 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 the Data Security manager from a machine on the domain, logged in with an account that has rights to view shares, or add the TRITON AP-DATA server to the domain.

Endpoint

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 the Data Security manager**

The TRITON AP-ENDPOINT DLP 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.

Related topics:

- User name does not display on endpoint list in the Data Security manager, page 486
- Endpoint shield does not display on the client computer, page 487
- Failed to deploy endpoint configuration, page 487
**Endpoint shield does not display on the client computer**

The TRITON AP-ENDPOINT DLP 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 TRITON AP-DATA 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 476* for instructions on how to perform these actions.
Fingerprinting

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 the Data Security manager.

Error details appear in the Status column when you select either:

Main > Policy Management> Content Classifiers > File Fingerprinting

or

Main > Policy Management > Content Classifiers > Database Fingerprinting


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 the Data Security manager.

1. Select Main > Policy Management> Content Classifiers > File Fingerprinting.
2. Double-click the classifier configured for the file.
3. Click the File Filtering tab.
4. Change parameters in the Filter by Size section of the screen.
5. 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 148 for more information on validation scripts.

**No connectivity to fingerprint database**

Connectivity to a fingerprint repository has been lost. Fingerprint repositories are located on all TRITON AP-DATA 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 TRITON 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

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 Discovery Dashboard even when incidents are set to ignored

Try deleting the incidents rather than ignoring them. Select Main > 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

If there are any off-box components in the TRITON AP-DATA installation and the TRITON AP-DATA servers are not on the domain, then all passwords and user names must match for the service accounts being used for TRITON AP-DATA.

For example, if the account Websense with a password of “Pa55word123” is being used as the service account on the Data Security manager, then the service account in use for any off-box TRITON AP-DATA-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 TRITON management
server, which will prevent incidents from being recorded to the archive folder on the TRITON management server.

**Incident export lacks Discovery incidents**

This is expected behavior. Incident export exports only data loss prevention 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**

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 the Data Security manager:

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 the instructions in Importing user entries from a CSV file, page 378.
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 the Data Security manager, 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

The system analyzed an HTTP request and determined you do not have sufficient system resources for transactions of this size. See the knowledge-base article “TRITON AP-DATA — 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

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 TRITON AP-DATA servers and TRITON management servers:

- \Program Files\Websense\*
- \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 TRITON AP-DATA 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 on improving performance.

Linking Service

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.

Websense Linking Service stops responding

In the Data Security manager, take these steps:
2. Make sure the Enabled check box is selected.
3. Click the Refresh icon to retrieve the latest linking service host and port settings. These settings can change.
4. Click Test Connection to verify that the Linking Service machine can be reached.

**System alerts that linking service is not accessible**

When your Websense software subscription includes both TRITON AP-WEB and TRITON AP-DATA modules, the 2 security solutions are integrated. A system alert appears on the Today page in the Data Security manager when the Websense Linking Service is not accessible or has been disabled.

When the Linking Service is working:
- Data security software gains access to user data gathered by Web security components.
- Data security software can access Master Database categorization information.

To configure the Linking Service, go to the Settings > General > System > URL Categories & User Names page in the Data Security manager.

**Buttons in TRITON security center module tray return error**

If you receive an error when you click Web Security in the Data Security manager, the administrator account that you use to log on to the Data Security manager may not have been granted permission to access Web Security manager. In order to change between TRITON Manager modules, an administrator must:
- Be added to the TRITON Settings > Administrators page
- Be given access to each module

The default TRITON administrator account, admin, does not have access to all the modules.

Super Administrators and Global Super Administrators can configure each administrator’s level of access to modules and features of the TRITON Manager.
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/](http://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.
Part IV

Appendices
Here is a selection of quick tips for some of the most common tasks and procedures in the TRITON AP-DATA 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?, page 499
- Configure a DLP policy?, page 500
- Define an exception?, page 501
- Filter incidents?, page 501
- Fingerprint data?, page 502
- Ignore sections of my document when fingerprinting?, page 503
- Fingerprint specific field combinations in a database table?, page 504
- Mitigate false positives in pattern or dictionary phrases?, page 505
- Move from monitor to protect?, page 505
- Perform discovery?, page 506

**Archive my incident data?**

Select Settings > General > 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 408*.

## Configure a DLP policy?

Data Security Manager Help | TRITON AP-DATA | Version 8.0.x

**To add a predefined policy**

TRITON AP-DATA comes with a rich set of predefined policies that cover the data requirements for a variety of regions and industries.

1. From the **Main** tab, select **Policy Management > DLP Policies**.
2. Under Custom Policies, select **Add predefined policy**.
3. Complete the Predefined Policy Wizard that appears. See *Adding a predefined policy, page 75* for more details.
4. Click **Deploy**.

**To create a quick policy**

If you are interested in Web, email, or mobile DLP alone, you can configure “quick policies”. If you are only concerned with one of these outbound channels, this is the easiest way to get started.

1. From the **Main** tab, select **Policy Management > DLP Policies**.
2. Under Quick Policies, select **Email DLP Policy**, **Web DLP Policy**, or **Mobile DLP Policy**, depending on your needs.
3. Enable the attributes of interest and click **OK**. See one of the following for instructions:
   - *Configuring the Email Data Loss Prevention Policy, page 53*
   - *Configuring the Web Data Loss Prevention Policy, page 61*
   - *Configuring the Mobile Data Loss Prevention Policy, page 69*
4. Click **Deploy**.

**To create a custom policy**

Once you get started, you may want to create custom policies for multiple channels. In custom policies you can configure advanced conditions and use complex features such as fingerprinting and machine learning.

1. From the **Main** tab, select **Policy Management > DLP Policies**.
2. Under Custom Policies, select **Add custom policy**.
3. Complete the wizard as described in *Creating Custom DLP Policies, page 79*.
4. Click **Deploy**.
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, click Manage Policies and expand your policy’s tree view (does not apply to email, Web, or mobile DLP policies).

- Click a rule and select Add > Exception from the drop-down menu.
- Highlight a rule and select Add > Exception from the toolbar.
- Click an exception and select Add > 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 102.

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 a report, open the report and just below the toolbar, select Manage Report > Edit Filter.

1. Select the filters to apply to the report. When you select a filter to apply, options appear in the Filter Properties pane.
2. Enable the desired filters, and then specify the 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.
3. Click Run when you’re done.
4. To save the report for later use, select Manage Report > Save As.

Applying column filters

The incidents list is a table displaying all data loss prevention or 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 **File Fingerprinting**.
3. Click **New** on the menu bar, and then select one of the following:
   - File System Fingerprinting
   - SharePoint Fingerprinting
   - Domino Fingerprinting
4. You’ll see the 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 *File fingerprinting*, page 127.

To fingerprint a database, Salesforce site, or CSV file:

1. Click **Main > Policy Management > Content Classifiers**.
2. Select **Database Fingerprinting**.
3. Click **New** on the menu bar, and then select one of the following:
   - Database Table Fingerprinting
   - Salesforce Fingerprinting
   - CSV File Fingerprinting
4. You’ll see the 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 *Database fingerprinting*, page 145.

**Ignore sections of my document when fingerprinting?**

For file 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 > File Fingerprinting**.
2. Click **New**, then choose the type of fingerprint to create: file system, SharePoint, or Domino.
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, the system 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.

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 **Database Fingerprinting**.
3. Click **New** from the menu bar, then choose **Database Table Fingerprinting**.
4. Work through the wizard as described in *Creating a database fingerprint classifier, page 154*. On the Field Selection page, select **Select up to 32 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 > DLP Policies > Manage 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 Fingerprint 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 options. For more information on setting up conditions, see Custom Policy Wizard - Condition, page 80.

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 Regular Expression 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.

To block SMTP traffic with the protector (explicit MTA):

1. Navigate to Settings > Deployment > 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.
6. Click **Deploy**.

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.
5. Click **Deploy**.

---

**Important**

To block HTTP traffic using the TRITON AP-DATA protector, the protector must be deployed in your network in inline bridge mode.

---

**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 ☛ 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 189 for more information.

---

**Perform discovery?**

To perform discovery:

1. Create a discovery policy. (See *Creating a discovery policy*, page 209 for instructions.)
2. Create a discovery task. **Main > Policy Management > Discovery Policies**.
3. Select **Add Network Task** or **Add Endpoint Task**.
4. 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 211
   - *Performing SharePoint discovery*, page 212
   - *Performing database discovery*, page 215
   - *Performing Exchange discovery*, page 216
Performing Outlook PST discovery, page 217
Performing Domino discovery, page 213
Performing endpoint discovery, page 218

7. Deploy your changes by clicking Yes when prompted.
8. Discovery will take place at the time and day you scheduled.
9. To view and respond to discovery results, click Main > Reporting > Discovery. See Viewing the incident list, page 300 for information on reading these screens.
Glossary

A

Analysis
The process that the TRITON AP-DATA 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 TRITON AP-DATA-generated code 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.

Database

A TRITON AP-DATA 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 manager

The graphical user interface that enables the security officer to manage the TRITON AP-DATA system, define and monitor the distribution of security policies, and view reports.

Event

An event is any transaction that traverses the TRITON AP-DATA system. Not all events are stopped by the TRITON AP-DATA 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.

External User

A user who is outside the organization or domain.

File System Directories

Registered directories on the corporate file server that contain files with classified content.

File Fingerprinter
A Data Security component that scans specified folders and submits files for fingerprinting to the Data Security DMS API.

**File Fingerprints**

Information that is protected by TRITON AP-DATA. The information will be recognized even after the original file has been deleted from the corporate file server.

**File Type**

A data format, such as .doc, .pdf, or .xls.

**Fingerprint Server**

A Data Security component that analyzes corporate file directories at predefined intervals and fingerprints files.

**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.

---

**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 the Data Security manager does not include incidents marked as ignored. Refer to “Filtering Incidents” to modify this setting.

**Incident**

An incident is a transaction or set of transactions that violate a policy. Depending on how you configure a rule, incidents can be created for every policy breach, or for matches that occur within a defined period.

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 hostname, 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.

**LDAP**

Lightweight Directory Access Protocol is the protocol standard over TCP/IP that is used by email clients to look up contact information. TRITON AP-DATA uses LDAP to automatically add users and groups to the data security database.

**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.

**Notification**

An email alert sent to the Security Officers and Content Owners, indicating that the information was addressed to an unauthorized recipient.

**Owner**

See Content Owner.

**Permissions**

Permissions define what a user is authorized to perform within the TRITON AP-DATA structure.

**Policy**

The system 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 system does when it comes across a transmission that meets the designated criteria.
Policy Category

TRITON AP-DATA 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.

R

Registering

The process of identifying a unique set of characteristics for a document’s contents. TRITON AP-DATA 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 TRITON AP-DATA 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.

System modules
These are the various components of TRITON AP-DATA. They are either hardware-based physical devices, like the protector; software components, like the Data Security manager and TMG agent; or virtual components like channels and services.

T

TMG Agent

A TRITON AP-DATA component that receives all Web connections from the network and forwards them to the TRITON AP-DATA Policy Engine. The TRITON AP-DATA TMG Agent then receives the analyzed information back from the TRITON AP-DATA Policy Engine and forwards it to the recipients on the Web.

Traffic

The transmission of email messages sent through the electronic mail system or uploaded to the Internet.

TRITON AP-DATA Administrator

A user who manages and maintains the TRITON AP-DATA system.

TRITON AP-DATA Server

The server that controls all aspects of the TRITON AP-DATA software.

TRITON management server

The Management Server is the TRITON AP-DATA component that includes all core technology and Websense fingerprinting servers, policy servers, and patented data loss prevention technology.

TRITON Manager

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. Also known as the TRITON Manager.

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 TRITON AP-DATA. 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.

**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 Reporting page. Views are very much like reports; they're graphical and contain colorful executive charts.
Websense® TRITON AP-DATA
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published 2013
Printed in the United States of America

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

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

For other copyright information, refer to:
● Trademarks
● Other Acknowledgements

Trademarks

Websense, TRITON, and ThreatSeeker are registered trademarks of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.


The following is a registered trademark of Novell, Inc., in the United States and other countries: Novell Directory Services.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

Firefox is a registered trademark of the Mozilla Foundation.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

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

Other Acknowledgements

Portions of this Websense Software may utilize the following copyrighted material, the use of which is hereby acknowledged:
antlr

Version 2.7.6
ANTLR 4 License
[The BSD License]
Copyright (c) 2012 Terence Parr and Sam Harwell
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
• Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

asm

Versions 3, 1.5.3
Copyright (c) 2000-2011 INRIA, France Telecom
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bash

Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.
TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.


The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.


You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's
users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).
The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).
However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.


You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor’s “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a
If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.


If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.
15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT
WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF
THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL
ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING
ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF
THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS
OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect
according to their terms, reviewing courts shall apply local law that most closely approximates an
absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of
liability accompanies a copy of the Program in return for a fee.

BeatBox

Copyright (c) 2000-2013, Simon Fell
Licensed under the GNU Lesser General Public License, Version 2.0; you may not use this file except in
compliance with the License. You may obtain a copy of the License at http://www.gnu.org/licenses/old-
licenses/gpl-2.0.html.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is
not allowed.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright hold-
er saying it may be distributed under the terms of this General Public License. The "Program", below, re-
fers to any such program or work, and a "work based on the Program" means either the Program or any
derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either
verbatim or with modifications and/or translated into another language. (Hereinafter, translation is includ-
ed without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are out-
side its scope. The act of running the Program is not restricted, and the output from the Program is covered
only if its contents constitute a work based on the Program (independent of having been made by running
the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any me-
dium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright
notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence
of any warranty; and give any other recipients of the Program a copy of this License along with the Pro-
gam.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty
protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.
If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyright-related interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

boost

Boost Software License - Version 1.0 - August 17, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of
machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

bouncycastle

Version 1.3.5
Copyright (c) 2000 - 2013 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

cglíb

Version 2.2
INRIA, France Telecom
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

See 4suite for the terms and conditions of the Apache License, Version 2.0. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0.

chardet

Licensed under the GNU Lesser General Public License, Version 2.1, February 1999
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications
and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification").

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

C) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the
free software distribution system which is implemented by public license practices. Many people have
made generous contributions to the wide range of software distributed through that system in reliance on
consistent application of that system; it is up to the author/donor to decide if he or she is willing to
distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this
License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by
copyrighted interfaces, the original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries, so that distribution is permitted
only in or among countries not thus excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public
License from time to time. Such new versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this
License which applies to it and "any later version", you have the option of following the terms and
conditions either of that version or of any later version published by the Free Software Foundation. If the
Library does not specify a license version number, you may choose any version ever published by the
Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions
are incompatible with these, write to the author to ask for permission. For software which is copyrighted
by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions
for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our
free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR
THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE
LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES
RISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT
LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES
SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE
WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

cURL

COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.
All rights reserved.
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby
granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Fpconst

Copyright (c) February 24, 2005. The Apache Software Foundation (http://www.apache.org/)
Gregory R. Warnes
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.
Apache License, Version 2.0, January 2004

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work.
to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and
You must cause any modified files to carry prominent notices stating that You changed the files; and
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices as required, within the Source form of any Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties of MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0.

gtk2

Version 2.4.13-24.el4/2.10.4-20.el5
Copyright (c) 1991, 1999, Free Software Foundation, Inc.
GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and change it if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library. The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must
be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.

But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License. 3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.
4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
DISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

HOWL

Version 0.1.8
HOWL is OSI Certified Open Source Software licensed under the BSD license.
Copyright (c) 2004, Bull S. A., All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

kernel

Version 2.6.18-348.1.1.el5
Copyright (c) January 23, 2013
Copyright (c) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301
Licensed under the GNU Lesser General Public License, Version 2.0; you may not use this file except in compliance with the License.
See BeatBox for the terms and conditions of the GNU Lesser General Public License, Version 2.0. You may obtain a copy of the License at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

libnids

Version 1.2
Copyright (c) June 1991. Free Software Foundation
nergal@avet.com.pl
Licensed under the GNU Lesser General Public License, Version 2.0; you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that is in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program,
the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c) Accompany it with the information you received as to the offer to distribute corresponding source code.

   (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an
explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Libpcap

Versions 0.9.8.20081128
The Regents of the University of California

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THE SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

libwbxml

Copyright (c) 1991, 1999, Free Software Foundation, Inc.

Licensed under the GNU Lesser General Public License, Version 3.0; you may not use this file except in compliance with the License.

GNU LESSER GENERAL PUBLIC LICENSE
0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

• a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

• b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.


The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

• a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

• b) Accompany the object code with a copy of the GNU GPL and this license document.


You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

• a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

• b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

• c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

• d) Do one of the following:

• 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

• 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.
•e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:
•a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.
•b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl.html.

libxml2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:
Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSH

Version 4.3p2-26.el5
Copyright (c) February 15, 2006. The Apache Software Foundation (http://www.apache.org/)
1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.
Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".
The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf
NO WARRANTY
BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR
THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MER-
CHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE
QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM
PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR
CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL
ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAG-
ES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT
LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUS-
TAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH
ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED
OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a
BSD-style license.

Cryptographic attack detector for ssh - source code
Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use
in source and binary forms, with or without modification, are permitted provided that this copyright notice
is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE
DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM
THE USE OR MISUSE OF THIS SOFTWARE.
Ariel Futoransky <futo@core-sdi.com>
<http://www.core-sdi.com>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
Modification and redistribution in source and binary forms is permitted provided that due credit is given
to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public
domain and distributed with the following license:
@version 3.0 (December 2000)
Optimised ANSI C code for the Rijndael cipher (now AES)
@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>
This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MER-
CHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THE-
ORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

OpenSSL
Copyright (C) 1998-2011 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the fol-
lowing disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following ac-
knowledgement:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http:/
/www.openssl.org/)
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products
derived from this software without prior written permission. For written permission, please contact opens-
ssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their
names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http:/
/www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DI-
RECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SER-
VICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product
includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation
was written so as to conform with Netscapes SSL.
This library is free for commercial and non-commercial use as long as the following conditions are aheared
to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES,
e., code; not just the SSL code. The SSL documentation included with this distribution is covered by the
same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the
library used. This can be in the form of a textual message at program startup or in documentation (online
or textual) provided with the package.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following
disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following ac-
knowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic
related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application
code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

This software is provided by Eric Young "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

org.dbunit

Version 2.2
Copyright (c) 1991, 1999, Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See gtk2 for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

org.richfaces.framework

Version 3.3.3.Final
Copyright (c) 1991, 1999, Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See gtk2 for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

org.richfaces.ui

Version 3.3.3.Final
Copyright (c) 1991, 1999, Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See gtk2 for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

org.springframework

Version 3.2.0
Copyright (c) 2002-2012, SpringSource, a division of VMware, Inc.
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.
See 4suite for the terms and conditions of the Apache License, Version 2.0. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0.

org.springframework.security

Version 3.0.7.
Copyright (c) 2002-2012, SpringSource, a division of VMware, Inc.
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.
See 4suite for the terms and conditions of the Apache License, Version 2.0. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0.

Pcre

Version 4.5-4.el4_6.6/6.6-2.el5_1.7

PCRE LICENCE
PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.
Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.
The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS
Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk
University of Cambridge Computing Service,
Copyright (c) 1997-2013 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT
Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright(c) 2010-2013 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER
Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright(c) 2009-2013 Zoltan Herczeg
All rights reserved.

THE C WRAPPER FUNCTIONS
Contributed by: Google Inc.
Copyright (c) 2007-2012, Google Inc.
All rights reserved.

THE "BSD" LICENCE
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or
promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PyYAML

Copyright (c) 2006 Kirill Simonov

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

twistedcore

Copyright (c) 2001-2006, Twisted Matrix Laboratories.

Allen Short
Andrew Bennetts
Apple Computer, Inc.
Benjamin Bruheim
Bob Ippolito
Canonical Limited
Christopher Armstrong
David Reid
Donovan Preston
Eric Mangold
Itamar Shtull-Trauring
James Knight
Jason A. Mobarak
Jonathan Lange
Jonathan D. Simms
Jp Calderone
Jorgen Hermann
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

twistedweb

Version 0.7.0
See twistedcore.

xstream

Version 1.2.1
XStream is open source software, made available under a BSD license.
Copyright (c) 2003-2006, Joe Walnes
Copyright (c) 2006-2009, 2011 XStream Committers
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of XStream nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright © 2001, Zolera Systems, Inc.
All Rights Reserved.
Copyright © 2002-2003, Rich Salz.
All Rights Reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.
Index

A
accumulate matches, 86
accuracy, 108
Action filter, 276, 282
Active Directory Application Mode
  user directory, 173, 375
ADAM
  see also - Active Directory Application Mode
add TRITON AP-DATA to domain, 486
adding exceptions, 102
administrators
  changing passwords, 403
defining, 393
ingoing, 396
viewing, 395
alerts
  configuring, 385
  preferences, 385
  setting up, 27
  setup, 27
application groups, online, 186, 187
Application Name filter, 276
applying column filters, 501
archive database, 3
Archive screen, 406, 408
archive storage, 387
  configuring, 387
archive threshold, 410
archiving a partition, 408
archiving incidents, 405, 499
Assigned to filter, 276, 282, 287
attachments, 359
audit log, 349
authorization
  see also - administrators
  overview
Available List, 50

B
backup
  folder contents, 365
  monitoring, 365
  scheduling, 364
  system, 362
blocking data, 505
Box Cloud
tasks, 239
Box cloud
  discovery, 214
Breadcrumbs, 19
built-in patterns, 119
Business Unit filter, 276, 282
business units, 181
  selecting, 398
C
changing passwords, 403
Channel filter, 276, 287
Channels icons, 17
chat
  configuring, 459
Classifier matches filter, 276, 282
Classifier type filter, 276, 282
classifiers
  see also - content classifiers; pattern classifiers
deleting, 111
file-name, 124
file-size, 124
file-type, 123
fingerprint, 84, 97, 111
fingerprinting, 111
manage, 116
menu bar, 109
upgrading, 411
view, 116
Clear Column’s Filter, 319
column filter, 318
applying, 187
computers, custom, 177
Condition Relations, 82
Condition tab, rule wizard, 80
configuration
  alerts, 385
  archive storage, 387
  authorization, 393
  chat, 459
crawler, 425
discovery incidents, 220
discovery incidents, 220
endpoint deployment, 465
endpoint server, 424
endpoints, 369
fingerprint repository, 422

Data Security Manager Help ▶ 553
forensics repository, 425
FTP, 457
HTTP, 455
ICAP, 437
integration agent, 443
ISA agent, 442
management server, 420
mobile agent, 444
mobile devices settings, 371
plain text, 460
policies, 500
policy engine, 426
protector, 431
protector services, 449
remediation, 381
SMTP, 449
supplemental TRITON AP-DATA servers, 421
system modules, 30, 419
URL categories, 390
user directory server settings, 25
user directory settings, 374
user names, 390
Websense Content Gateway agent, 439
configuring the OCR server, 427
Connection Settings, 375
communication issues, 489
content classifier
classifying content, 108
Content Classifier Name filter, 287
Content Classifier Type filter, 287
content classifiers, 93, 107
choosing, 108
classifying content, 107
creating, 107
creating rules, 170
menu bar, 109
Content Gateway
see also - Websense Content Gateway
content pane, 10
Content similarity, 129, 133, 138
copying discovered files, 221
count all matches, 86
count transactions, 86
count unique matches, 86
crawler, 30
configuring, 425
creating, 79
creating a data discovery policy, 209
creating a PreciseID fingerprint classifier, 166
creating content classifier rules, 170
credentials
TRITON AP-DATA, 419
CSV
importing domains, 179
CSV file
format - computers, 381
format - groups, 379
format - users, 380
formatting, 379
importing user entries, 378
action plans, 506
cumulative rules, 86
custom computers, 177
custom disclaimer, 360
custom logo, 359
Custom message, 440
custom policy, 38, 39, 79, 323
wizard, 80–93
custom user directory groups, 174
custom users, 177
Customer support, 495
customize patterns, 119
D
dashboard
data loss prevention, 326
exporting report, 326, 337
viewing, 326, 336
data
classifying, 339
data discovery
data buttons and controls, 226
incidents, setting preferences, 361
no incident created, 490
no incident export, 491
scan scheduling, 211
sensitive data reports, 337
data discovery policy
creating, 209
Data Discovery Tasks, 211
data loss prevention, 1
see also - DLP policies
dashboard, 326
incidents, 300, 341, 360
report filters, 276
reports, 291
Data Security manager
audit log, 349
Deploy button, 13
icons, 15
Main tab, 11
navigation, 9
system log, 349
traffic log, 348
viewing logs, 348
data source name
see also - DSN
data source names, 146
Data Source tab, database fingerprinting wizard, 155
data sources, connecting to, 145
data usage
  see also - data loss prevention
database discovery, 215
task wizard, 245
database fingerprinting, 144–162, 504
  connecting, 145
  creating, 153
  preparing, 146
database partition, 405
database tasks, 244
database, record chunking, 248
Date Accessed filter, 287
Date Created filter, 287
Date Modified filter, 287
Default email address error, 492
Define Matches, 87
defining
  exception, 501
  resources, 171
deleting
  incidents, 320, 490
  deleting a partition, 409
Deploy button, 13
deployment, 403
deployment status, 347
Destination filter, 277, 282
Destination tab, rule wizard, 88
destinations, 173
Detected by filter, 277, 282, 287
Device details filter, 282
Device owner filter, 283
dictionary classifier
  adding, 120
dictionary classifiers, 84
directory servers, 173
disclaimers, 503
disclaimers, custom, 360
discovered files, copying, moving or encrypting, 221
discovery
  Box cloud, 214
  configuring incidents, 220
database, 215
defined, 207
endpoint, 218
Exchange, 216
file system, 211
Lotus Domino, 213
Outlook, 217
report, 295
report filters, 287
results, 220
search pattern, 248
SharePoint, 212
status, 219
updating, 220
discovery incidents
  deleting, 490
discovery not on domain, 486
discovery policies, 207, 208, 209
Discovery Task filter, 287
discovery tasks
  endpoint, 225
  file system, 230, 259
  manually deleting, 228
  network, 225
  sorting and filtering, 226
Discovery Type filter, 287
DLP policies, 37, 208
  see also - custom policy; email DLP policy;
  mobile policy; regulatory and compliance
  policy; Web DLP policy
types of, 37
DN (Distinguished Name), 173
DNS suffixes, 433
domains, 178, 486
  adding, 178
  importing, 179
Domino, 173
  fingerprinting, 136–??
DSN, 246
  creating, 146

E
edit rules, 100
editing report filters, 501
Email destinations, 89
email DLP policy, 37, 53
email notifications, 191, 197
e-mail policy
  violation notification, 202
email properties, 385
  editing outgoing server, 386
Email to Manager, 316
Enable bypass mode, 435
encrypting discovered files, 221
encryption
  encryption tab, 472
  removable media, 467
  user password, 468
encrypting keys, 476
  backing up, 476
  removable media, 467
  restoring, 476
Index

endpoint
   applications, 183
   bypassing endpoint clients, 482
   configuring settings, 477
   configuring system settings, 369
   deployment, 465
   devices, 183
   endpoint channels, 90, 91, 92, 479
   overview, 465
   removable media, 478
   viewing status, 346
endpoint clients, 466
endpoint discovery, 218
   scheduling tasks, 265
   task wizard, 265–267
   tasks, 225
endpoint profiles, 466
   adding, 468
   deploying, 475
   Encryption tab, 472
   General tab, 469
   Properties tab, 471
   rearranging, 475
   Servers tab, 470
endpoint server, 30, 344, 466
   configuring, 424
endpoint shield not displayed, 487
Endpoint Type filter, 277, 287
Error 400, 492
Escalate, 303
event log, 490
Event Time filter, 278, 283, 288
events error, 491
Exact match, 129, 133, 138
Exception wizard
   general, 103
exception, adding, 102
exception, properties, 103
exceptions
   adding, 101
   adding new, 102
   defining, 501
   rearranging, 102
   updating multiple, 44
   updating selected, 46
exceptions, adding, 101
Exchange discovery, 216
   task wizard, 249–254
   tasks, 249
Exclude Source from Rules, 305
exclude tab, selector, 49
exclude values, 117
excluding items from a policy, 49
export
   dashboard report, 326, 337
export fingerprint
   database, 161
export fingerprints
   file system, 131
   Lotus Domino, 142
   SharePoint, 136
external channels
   defined, 4
F
fail closed
   content gateway FTP, 441
   content gateway HTTP, 440
   ICAP FTP, 439
   ICAP HTTP, 438
   ISA agent, 443
   protector HTTP, 457
   protector MTA, 453
fail open
   content gateway FTP, 441
   content gateway HTTP, 440
   ICAP FTP, 439
   ICAP HTTP, 438
   ISA agent, 443
   protector HTTP, 457
   protector MTA, 453
failing to import user directory, 491
failure to deploy endpoint, 487
false positives
   mitigating, 505
false positives, mitigating, 505
field combinations, fingerprinting, 504
Field Selection tab, database fingerprinting wizard, 157
file fingerprinting, 127
   Domino fingerprinting, 136
   file system fingerprinting, 128
   SharePoint fingerprinting, 132
file format
   computer, 381
   CSV, 379
   groups, 379
   users, 380
File Name filter, 278, 284, 288
File Owner filter, 288
File Permissions filter, 288
file properties, 123
File Size filter, 288
file system discovery, 211
file system task wizard, 230
file system tasks, 230
file-name classifier, 124
files and directories
fingerprinting, 127
file-size classifier, 124
file-type classifier, 123
filter
columns, 318
Filter by, 50
Filter by Age, 234
Filter by Size, 234
Filter by this Column..., 319
Filter by Type, 234
filtering incidents, 501
filtering tasks, 226
fingerprint
CSV files, 144
fingerprint repository, 153, 344
configuring, 422
primary, 30, 422
secondary, 422, 423
fingerprint repository, primary, 423
Fingerprinting
Lotus Domino, 136
fingerprinting
advice, 150
errors and problems, 488
field combinations, 504
ignored sections, 503
selected data, 150
validating, 147
fingerprinting classifiers, 111
database fingerprinting classifiers, 108
fingerprinting data
how to, 502
Fingerprinting Method, 129, 133, 138
Fingerprinting Mode, 129, 133, 138
Folder filter, 288
Folder Owner filter, 288
Force bypass, 435
forensics
webmail, 360
Forensics path, 426
forensics repository, 3, 30
configuring, 425
FQDN, 419, 444
FTP
configuring, 457

H
Help, 494
history
incident, 306
history filter, 279, 284, 289
Host Name filter, 289
hosts with sensitive data, 337
HTTP
configuring, 455

I
ICAP
configuring, 437
icons, tree, 41
ignore sections in fingerprint, 503
Ignored Incident filter, 279, 284, 289
Ignored section, 129, 133, 138
ignored sections, 503
import users failure, 491
importing a fingerprint classifier, 162
incident
changing severity, 310
changing status, 309
database, 405
forensics, 305
incident archive
disk space for, 387
location, 387
incident database, 3
archiving, 3
incident management, 315
Incident Tag filter, 279, 284, 289
Incident Time filter, 280, 285, 289
incidents
archiving, 405, 499
assigning, 308
data loss prevention, 341
deleting, 312, 320
discovery, 342
downloading, 312
escalating, 315
exporting to CSV, 321
exporting to file, 367
exporting to PDF, 321
filter, 300
filtering, 501
grouping, 320
ignoring, 310
locking, 308
managing views, 317
managing workflow, 307
missing, 490
not created, 490
Index

previewing, 304
printing, 321
releasing, 314
remediating, 313
report filters, 318
selecting, 397
setting preferences, 358
severity, 341
severity and action, 328
severity flags, 310
sources and destinations, 328
status flags, 309
tagging, 311
toolbar, 301
top policies, 341
trends, 329
unlocking, 308
viewing lists, 300
violated policies, 327
incidents and reports, 300
general preferences, 359
viewing, 271
incidents list, 300
incidents, released, 280, 285
include links in notifications, 204
include tab, selector, 49
including items in a policy, 49
initial setup, 23
Inline (Bridge) mode, 434
inline mode, 450
installing
    policy updates, 413
    template updates, 413
Integration agent, 444
integration agent
    configuring, 443
Intelligent protocol discovery, 450
invalid email addresses, 492
invalid monitoring policy, 492
IP Address filter, 289
ISA agent
    configuring, 442

K
key phrase classifiers, 120

L
LDAP servers, 377
LDAP users, 173
levels, adding, 47
levels, deleting, 49
levels, policy, 47
levels, rearranging, 49

Link Speed, 434
linking, 180
linking problems, 493
Linking Service problems, 493
linking service stopped responding, 493
load balancing, 462
defining distribution, 463
Locked filter, 289
locking incidents, 308
logos, custom, 359
Lotus Domino, 173
discovery, 213
fingerprinting, 123–143
tasks, 258
user directory, 173, 375
Lotus Domino fingerprinting, 136

M
machine learning classifier, 82, 165
machine learning details, 114
machine learning report, 110
Mail Transfer Agent, 450
Mailbox Type filter, 290
mailboxes with sensitive data, 337
Main tab
    Incidents & reports, 11
    Policy management, 11
    Status, 12
Manage Report, 303, 317
Management Server, 2
    overview, 2
management server
    configuring, 420
managing rules, 66, 100
matches, how counted, 152
Microsoft Active Directory
    user directory, 173, 374, 375
missing incidents, 490
mitigating false positives, 505
mobile
    incidents, setting preferences, 362
mobile agent
    configuring, 444
    mobile devices, 1, 4
    configuring settings, 371
    report filters, 282
    viewing status, 345
mobile DLP policy, 69
mobile policy, 37
    configuring, 69
    defining owners, 73
    violation notification, 202
module
    TRITON AP-DATA, 395
TRITON AP-DATA servers, 342
modules
adding, 419
managing, 417
Protectors, 343
Monitoring bridge, 450
Monitoring passive, 450
moving discovered files, 221
moving from monitoring to blocking, 505
my settings, 403

N
navigation, 9
navigation pane, 9
network discovery, 229
tasks, 225
tasks, scheduling, 229
tasks, types of, 229
Network Interfaces, protector, 433
network tasks
Box cloud, 239
database, 244
Exchange, 249
file system, 230
Lotus Domino, 258
Outlook PST, 254
SharePoint, 235
networks, 178
NLP policy error, 491
notifications
see also - notification messages
notification messages, 202, 314
creating, 202
setting up, 28
template, 202
notifications
including links in, 204
Number of owners filter, 286, 294

O
OCR server, 427
Online Application Group, 186, 187
online help, 494
outgoing mail server, 386
Outlook discovery, 217

P
partitions
archiving, 408
database, 405
deleting, 409
restoring, 409
password
changing, 403
passwords, changing, 403
pattern classifiers, 116
adding, 118
editing, 118
pattern matches
exclusions, 117
patterns, built-in, 119
personal settings, 403
photo attributes, 376
Phrase to search, 120
plain text
configuring, 460
policies
configuring, 500
data discovery, 209
disabling, 323
including and excluding items, 49
invalid monitoring, 492
levels, 47
Rule wizard, 80
selecting, 397
tuning, 322
policy, 402
adding attributes, 55
content classifiers, 40
contents, 39
creating, 40
custom, 39
data loss prevention, 323
deleting, 47
exceptions, 39
installing updates, 413
overview, 37
predefined, 39, 411, 413
resources, 40
restore to previous, 414
rules, 39
tree view, 41
updating, 43, 411
updating history, 411
updating multiple, 45
version, 415
viewing, 40
policy database, 2
policy engine, 2, 30, 343, 462
configuring, 426
overview, 2
Policy filter, 280, 285, 290
policy levels, 47
adding, 47
deleting, 49
rearranging, 49
Policy owners, 59, 73
Index

- defining, 68
- policy toolbar, 42
- PreciseID
  - file, 127
  - technology, 2, 5, 107, 144, 154
- PreciseID fingerprint classifier
  - creating, 166
- PreciseID fingerprinting classifier, creating, 153
- files and directories, 127
- overview, 5
- PreciseID patterns, 116–118
- Predefined lists, 51
- predefined policies, 37, 39, 75
- predefined templates
  - installing updates, 413
- printers
  - monitoring, 186
- Printing destinations, 90
- properties
  - incident, 306
- Properties tab, exception wizard, 103
- protecting data, 505
- Protector, 343
- protector, 2
  - blocking, 505
  - configuring, 431
  - monitoring, 505
- protector services
  - configuring, 449
- Protectors
  - modules, 343
- PST files, 217
- PST discovery task wizard, 254
- Python scripts, 125

<table>
<thead>
<tr>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>recurrence, 299</td>
</tr>
<tr>
<td>registration with servers, 419</td>
</tr>
<tr>
<td>regulatory and compliance policy, 38</td>
</tr>
<tr>
<td>Release Gateway, 382</td>
</tr>
<tr>
<td>released incidents, showing in report, 280, 285</td>
</tr>
<tr>
<td>RemEDIATE, 303</td>
</tr>
<tr>
<td>remediating incidents, 313</td>
</tr>
<tr>
<td>remediation, 188</td>
</tr>
<tr>
<td>- action plans, 189</td>
</tr>
<tr>
<td>- configuring, 381</td>
</tr>
<tr>
<td>- running scripts, 222</td>
</tr>
<tr>
<td>remediation scripts, 191, 197, 315</td>
</tr>
<tr>
<td>- adding, 199</td>
</tr>
<tr>
<td>- discovery, 222</td>
</tr>
<tr>
<td>- preparing, 222</td>
</tr>
<tr>
<td>- running, 222</td>
</tr>
<tr>
<td>types of, 198</td>
</tr>
<tr>
<td>writing, 200</td>
</tr>
<tr>
<td>removable media</td>
</tr>
<tr>
<td>- endpoints, 478</td>
</tr>
<tr>
<td>repetitive values, 152</td>
</tr>
<tr>
<td>report</td>
</tr>
<tr>
<td>- data loss prevention, 276, 291</td>
</tr>
<tr>
<td>- data loss prevention report</td>
</tr>
<tr>
<td>- discovery, 11</td>
</tr>
<tr>
<td>- details, 314</td>
</tr>
<tr>
<td>- discovery, 287, 295</td>
</tr>
<tr>
<td>- editing, 274</td>
</tr>
<tr>
<td>- mobile devices, 282</td>
</tr>
<tr>
<td>- saving, 320</td>
</tr>
<tr>
<td>report catalog, 272</td>
</tr>
<tr>
<td>report filters</td>
</tr>
<tr>
<td>- data loss prevention report, 276</td>
</tr>
<tr>
<td>- discovery report, 287</td>
</tr>
<tr>
<td>- editing, 318</td>
</tr>
<tr>
<td>- mobile devices report, 282</td>
</tr>
<tr>
<td>report menu bar, 273</td>
</tr>
<tr>
<td>Report owner, 274</td>
</tr>
<tr>
<td>reporting, 401</td>
</tr>
<tr>
<td>reports</td>
</tr>
<tr>
<td>- recurrence, 299</td>
</tr>
<tr>
<td>- saving, 320</td>
</tr>
<tr>
<td>- sensitive data, 337</td>
</tr>
<tr>
<td>- setting preferences, 358</td>
</tr>
<tr>
<td>- trend, 296</td>
</tr>
<tr>
<td>resource sources and destinations, 173</td>
</tr>
<tr>
<td>resources</td>
</tr>
<tr>
<td>- business units, 181</td>
</tr>
<tr>
<td>- custom computers, 177</td>
</tr>
<tr>
<td>- custom users, 177</td>
</tr>
<tr>
<td>- defining, 171, 172</td>
</tr>
<tr>
<td>- directory entries, 173</td>
</tr>
<tr>
<td>- networks, 178</td>
</tr>
<tr>
<td>- notification messages, 202</td>
</tr>
<tr>
<td>- overview, 171</td>
</tr>
<tr>
<td>- remediation scripts, 197</td>
</tr>
<tr>
<td>- terms and descriptions, 172</td>
</tr>
<tr>
<td>restoring a partition, 409</td>
</tr>
<tr>
<td>restoring encryption keys, 476</td>
</tr>
<tr>
<td>results</td>
</tr>
<tr>
<td>- discovery, 220</td>
</tr>
<tr>
<td>roles</td>
</tr>
<tr>
<td>- adding new, 400</td>
</tr>
<tr>
<td>- working with, 398</td>
</tr>
<tr>
<td>Rule wizard, 80</td>
</tr>
<tr>
<td>severity and action, 85</td>
</tr>
<tr>
<td>rules</td>
</tr>
<tr>
<td>- disabling, 323</td>
</tr>
<tr>
<td>- exceptions, 101, 501</td>
</tr>
<tr>
<td>- excluding, 323</td>
</tr>
</tbody>
</table>
managing, 66, 100
source, excluding, 323
source, including, 323
rules, editing, 100
running, 315
running a scheduled task, 299

S
scans
scheduling, 211
scheduled task
running now, 299
Scheduler tab, database fingerprinting wizard, 160
scheduling discovery, 211
Scheduling tasks
network discovery, 229
scripts, 125
search pattern, discovery, 248
selecting fingerprinting data, 150
selector, how to use, 49
Sensitive content, 129, 133, 138
sensitive data reports
data discovery, 337
viewing, 337
setting up alerts, 27
Settings tab, 12
deployment, 13
general, 13
setup, initial, 23
Severity & Action tab, exception wizard, 104
Severity & Action tab, rule wizard, 85
severity and action, 85
Severity filter, 280, 285, 290
severity, incident, 310
SharePoint
discovery, 212, 506
discovery task wizard, 236–239, 240–??, 240–244
fingerprinting, 132–136
tasks, 235
short values, 151
SMTP
agent, 30
configuring, 449
Sort Ascending, 319
Sort Descending, 319
Sorting and filtering tasks, 226
sorting tasks, 226
Source filter, 281, 286
Source tab, rule wizard, 88
sources and destinations, 173
SPAN mode, 450
SPAN/Mirror Port mode, 435
status
discovery, 219
status & logs
filtering data, 339
monitoring system health, 342
overview, 339
printing and exporting, 340
viewing deployment status, 347
viewing endpoint status, 346
viewing mobile devices status, 345
Status filter, 281, 286, 290
subscription alerts, 390
subscription settings
entering, 389
Support, Technical, 495
system
restore, 366
system backup, 362
system health, 342
system log, 349
system modules, 417
adding, 419
configuring, 419
OCR server, 427
permissions, 419
T
Table Properties, 290, 300
tasks
scheduling, 297
Technical support, 495
templates
installing, 413
templates, updating, 411
Today dashboard, 13
Today page, 340
toolbars, 42, 301
archive, 406, 412
incident, 301
incidents & reports, 301
policy, 42
report catalog, 274
TRITON, 374, 393
Top Matches filter, 281, 286, 290
Total Size filter, 281, 286, 290
traffic log, 348
transaction size, 100
Transaction type filter, 286
tree view, 342
trend report, 296
TRITON AP-DATA
credentials, 419
setting up, 23
TRITON AP-DATA module, 395
TRITON AP-DATA servers, 2
configuring, 421
endpoint deployment, 471
modules, 342
TRITON AP-WEB mode, 6
TRITON management server configuring, 420
modules, 30, 419
system backup, 362
system restore, 366
TRITON Manager, 1, 6
trusted domains, 59, 73

U
undetected events, 491
updates
  predefined templates, 413
  updating discovery, 220
URL categories, 180
  configuring, 390
  importing, 392
  updating, 180
user directory, 173
  configuring settings, 374
  entries, 173
user directory groups, custom, 174
user directory import failure, 491
user directory queries, 174
user directory servers
  adding new, 374
  configuring settings, 25
  rearranging, 377
user entries
  importing, 377, 378

V
importing from CSV, 378
users, custom, 177

T
validation scripts, 108
  fingerprinting, 147
  sample, 149
  template, 151, 152
Violated rules, 304
Violation triggers, 305
Violation Triggers filter, 281, 286, 290

W
warning message
  archive threshold, 410
Web attributes, 62
Web channels, 4, 6, 66, 90, 180
Web DLP policy, 37, 61
  configuring, 62
  disabling policies, 305, 323
  excluding rules, 305, 323, 324
  violation notification, 202
Web Mail Forensics, 360
Websense Linking Service problems, 493
Websense Content Gateway
  configuring agent, 439
  policy engine, 426
Workflow, 302
  workflow, managing, 307

X
XML interface, 201