



Forcepoint DLP

v9.0

Administrator Help

© 2022 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 14 October 2022

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

Contents

1 Overview.....	7
Forcepoint DLP basics.....	7
Forcepoint DLP appliances.....	8
Forcepoint DLP databases.....	8
What can I protect?.....	9
Data classification.....	10
Managing Forcepoint DLP.....	11
DLP in Forcepoint Web Security and Forcepoint Email Security.....	12
2 Navigating the system.....	13
Main options.....	14
Settings options.....	16
Deploy button.....	17
Global and status icons.....	18
3 Initial Setup.....	21
Entering a subscription key.....	22
Defining general system settings and notifications.....	23
Configuring system modules.....	24
Configuring the protector.....	24
4 Viewing Status.....	27
Viewing the Dashboard.....	27
Monitoring system health.....	30
Viewing endpoint status.....	33
Changing table properties.....	34
Viewing mobile device status.....	35
Applying column filters.....	36
Viewing deployment status.....	37
5 Viewing Incidents and Reports.....	39
The report catalog.....	40
Viewing the incident list.....	69
Data Loss Prevention reports.....	92
Mobile devices reports.....	104
Discovery reports.....	107
6 Policies Overview.....	111
What's in a policy?.....	112
Viewing policies.....	113
Selecting items to include or exclude in a policy.....	122
7 Configuring the Email DLP Policy.....	125
Configuring outbound and inbound email DLP attributes.....	126
Defining email DLP policy owners.....	130
Identifying email DLP trusted domains.....	131
8 Configuring the Web DLP Policy.....	133
Web DLP policy configuration overview.....	134
Configuring web DLP policy attributes.....	134

Selecting web DLP policy destinations.....	139
Defining web DLP policy owners.....	140
9 Configuring the Mobile DLP Policy.....	143
Mobile DLP policy configuration overview.....	143
Configuring mobile DLP attributes.....	144
Defining policy owners.....	148
10 Using Predefined DLP and Discovery Policies.....	151
Adding a predefined DLP or discovery policy.....	151
Changing the selected DLP or discovery policies.....	153
Changing policy industry or region settings.....	154
11 Creating Custom DLP Policies.....	155
Custom Policy Wizard - General.....	156
Custom Policy Wizard - Condition.....	156
Custom Policy Wizard - Severity and Action.....	161
Custom Policy Wizard - Source.....	164
Custom Policy Wizard - Destination.....	165
Rule Wizard - Finish.....	169
Selecting a content classifier.....	169
Managing rules.....	175
Managing exceptions.....	176
12 Classifying Content.....	181
Content classifier menu bar.....	183
Manually deleting fingerprinting classifiers.....	185
Details pane.....	186
Patterns & Phrases.....	189
File Labeling.....	194
File properties.....	196
Scripts.....	198
File fingerprinting.....	200
Database fingerprinting.....	217
Database Fingerprinting Wizard - Scheduler.....	230
Imported fingerprinting.....	233
Machine learning.....	235
Creating a rule from a content classifier.....	239
13 Defining Resources.....	241
General resources.....	242
Cloud resources.....	242
Endpoint resources.....	244
Remediation resources.....	245
User directory entries.....	245
Custom user directory groups.....	246
Custom users.....	248
Custom computers.....	249
Networks.....	249
Domains.....	250
URL categories.....	251
Business Units.....	251
Endpoint Devices.....	252

Endpoint Applications.....	253
Endpoint Application Groups.....	254
Endpoint Printers.....	256
Remediation.....	257
14 Creating Discovery Policies.....	277
Creating a discovery policy.....	278
Scheduling the discovery scan.....	280
Performing file system discovery.....	281
Performing SharePoint discovery.....	282
Performing Domino discovery.....	282
Performing Box discovery.....	283
Performing database discovery.....	284
Performing Exchange discovery.....	285
Performing Outlook PST discovery.....	285
Performing endpoint discovery.....	286
Viewing discovery status.....	287
Viewing discovery results.....	287
Updating discovery.....	288
Configuring discovery incidents.....	288
Copying or moving discovered files.....	288
15 Scheduling Discovery Tasks.....	293
Sorting and filtering tasks.....	293
Scheduling network discovery tasks.....	297
Emailing discovery task status reports.....	330
Configuring cloud discovery scans.....	331
Adding or editing a cloud discovery scan.....	333
Scheduling endpoint discovery tasks.....	333
16 Viewing Forcepoint DLP Logs.....	339
Filtering log data.....	339
Printing and exporting logs.....	340
The Forcepoint DLP traffic log.....	340
The Forcepoint DLP system log.....	343
The Forcepoint DLP audit log.....	343
17 General System Settings.....	347
Setting reporting preferences.....	348
Backing up the system.....	351
Exporting incidents to a file.....	354
Configuring endpoint settings.....	357
Remediation.....	361
Mail servers.....	363
Alerts.....	365
Archive storage.....	366
Services.....	368
Analytics.....	379
User directory settings.....	380
Archiving incident partitions.....	387
Updating predefined policies and classifiers.....	392
Entering subscription settings.....	395

18 Configuring Authorization.....	399
Defining administrators.....	399
Working with roles.....	404
Customizing your own administrator account settings.....	408
19 Managing Forcepoint DLP System Modules.....	409
Adding Forcepoint DLP system modules.....	410
Configuring protector services.....	432
Removing Forcepoint DLP modules.....	441
Balancing the load.....	441
20 Configuring Endpoint Deployment.....	445
Viewing and managing endpoint profiles.....	446
Configuring encryption for removable media.....	453
Selecting endpoint destination channels to monitor.....	456
Bypassing endpoint clients.....	458
Rearranging and deploying endpoint profiles.....	459
Using the endpoint client software.....	460
21 Troubleshooting.....	461
Discovery.....	461
Endpoint.....	462
Fingerprinting.....	463
Incidents.....	465
Miscellaneous.....	467
Performance.....	469
Linking Service.....	469
Online Help.....	471
Technical Support.....	471
A Appendix A: How Do I.....	473
Archive my incident data?.....	474
Configure a DLP policy?.....	474
Define an exception?.....	476
Filter incidents?.....	476
Fingerprint data?.....	477
Ignore sections of my document when fingerprinting?.....	478
Fingerprint specific field combinations in a database table?.....	480
Mitigate false positives in pattern or dictionary phrases?.....	481
Move from monitor to protect?.....	481

Chapter 1

Overview

Contents

- Forcepoint DLP basics on page 7
- Forcepoint DLP appliances on page 8
- Forcepoint DLP databases on page 8
- What can I protect? on page 9
- Data classification on page 10
- Managing Forcepoint DLP on page 11
- DLP in Forcepoint Web Security and Forcepoint Email Security on page 12

Forcepoint DLP protects organizations from information leaks and data loss at the perimeter and inside the organization, as well as in certain Infrastructure as a Service platforms.

- It includes an analytics engine that identifies and ranks high-risk incidents. Incidents generated by DLP policies across all core Forcepoint DLP components are evaluated to report on those with the highest data loss or data theft risk score.
- It can operate alone in the network, or be paired with Forcepoint Web Security or Forcepoint Email Security to provide a well-rounded security solution.

Forcepoint DLP Network prevents data loss through email and over web channels such as HTTP, HTTPS, and FTP.

- Includes Forcepoint DLP Email Gateway, which is deployed in Microsoft Azure to provide DLP policy enforcement for Microsoft Exchange Online
- Supports the scanning of content supplied by third-party solutions, such as Citrix FileShare, via the ICAP protocol

Use Forcepoint Data Discovery to learn the location of sensitive data within on-premises data centers and cloud hosted applications. It can scan data on file servers, email servers, databases, and content collaboration applications, such as Microsoft SharePoint and Box.

Forcepoint DLP Endpoint prevents data loss over endpoint channels, such as removable storage devices, mobile devices, browser uploads, email clients, and applications—for example, IM and file share clients.

- It can also discover and remediate sensitive data stored on laptop and desktop systems.
- The endpoint agent lets administrators analyze content within a user's working environment and block or monitor policy breaches as defined by the endpoint profiles.

Consult a Forcepoint sales representative for more information about the full range of Forcepoint DLP options.

Forcepoint DLP basics

Forcepoint DLP 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

- Identifying and ranking high-risk incidents to help prevent or remediate data loss and data theft

Forcepoint DLP has the following main components:

- The **management server** is a Windows-based machine that hosts the Forcepoint Security Manager and Forcepoint DLP software.
The management server provides the core information loss technology, capturing fingerprints, applying policies, and storing incident forensics. A deployment can include multiple Forcepoint DLP servers to share the analysis load, but there is only one management server.
- A **policy engine** resides on all Forcepoint DLP servers, Web Content Gateway servers, and Forcepoint Email Security appliances. Policy engines are also integrated with Windows, Mac OS X, and Linux endpoints running Forcepoint DLP Endpoint.
The policy engine is responsible for parsing data and using analytics to compare it to the rules in policies.
- The **analytics engine** resides on a 64-bit Linux machine.
It is used to identify potentially risky incidents, rank them with similar activity, and assign them a risk score.
- The **policy database** is a repository for Forcepoint DLP policies. For optimal performance, it is stored locally on each server (like the fingerprint database).

Forcepoint DLP appliances

Forcepoint DLP Network includes the option to use Forcepoint DLP Email Gateway, Web Content Gateway, or protector appliance.

- Forcepoint DLP Email Gateway is a virtual appliance for the Azure cloud infrastructure that can be used to protect data being sent through Exchange Online email
- Two kinds of Web Content Gateway appliances can be used to provide DLP over the web channel.
 - One is included with Forcepoint DLP Network. It decrypts SSL content and permits the use of custom policies and fingerprinting.
 - One requires Forcepoint Web Security. It decrypts SSL content and provides URL categorization, content security, web policy enforcement, and more.
- The protector is a soft appliance that intercepts and analyzes traffic on a variety of channels, such as email, HTTP, and FTP. (HTTP traffic is monitored but not enforced.) Forcepoint DLP also supports DLP content scanning with third-party proxies and data sharing solutions through the ICAP protocol.

A combined cloud and on-premises deployment of email DLP can be achieved using Forcepoint Email Security with the protector appliance. It is not possible, however, to deploy Forcepoint Email Security with Forcepoint DLP Email Gateway.

Forcepoint DLP databases

Forcepoint DLP 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 that it can be archived onto different physical disks. See *Archiving incident partitions* section.

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

To configure the size and location of the forensics repository, see *Configuring the forensics repository* section

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

Related concepts

[Archiving incident partitions](#) on page 387

Related tasks

[Configuring the forensics repository](#) on page 417

What can I protect?

Forcepoint DLP can control or monitor the flow of data throughout an organization. Administrators 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

Forcepoint DLP can be used with Forcepoint DLP Endpoint to secure all of the following (channels that require Forcepoint DLP Endpoint are marked with an asterisk [*]):

- Network and endpoint email***- Monitor or prevent sensitive information from being emailed in or outside of a domain from both network and endpoint computers.
- Mobile email**- Define what content can and cannot be synchronized to mobile devices—such as phones and i-pads—from network email systems. This protects data in case an employee’s mobile devices is lost or stolen.
- Web channels
 - FTP**- Monitor or prevent sensitive information from being uploaded to file transfer protocol (FTP) sites.
 - Plain text**- Monitor or prevent sensitive information from being sent via plain text (unformatted textual content).
 - HTTP/HTTPS**- Monitor or prevent sensitive information from being posted to a website, blog, or forum via HTTP. SSL decryption is performed by the Web Content Gateway module.
 - Endpoint HTTP/HTTPS***- Monitor or protect endpoint devices such as laptops from posting data over the Web.
- Endpoint applications***- 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 application file access monitoring*** - Monitor applications such as IM, cloud storage, and FTP clients that access and share sensitive data.
- Endpoint removable media***- Monitor or prevent sensitive information from being written to a removable device such as a USB flash drive, CD/DVD, or external hard disk.

Forcepoint DLP Endpoint 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.
 - Specify a list of IP addresses, hostnames or IP networks of computers that are allowed as a source or destination for LAN copy.
 - Intercept data copied from an endpoint client to a network share.
 - 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*** - Monitor or prevent sensitive data from being printed on local or network printers from endpoint client machines.

Comprehensive monitoring of these channels can prevent data from leaving an organization via the most common means.

Related concepts

[Classifying Content](#) on page 181

[Defining Resources](#) on page 241

[Remediation](#) on page 257

Data classification

With Forcepoint DLP, administrators can use several methods to classify data:

- Use predefined scripts, dictionaries, file-types, and regular expression (regex) patterns to start classifying data right away.
 - Regex patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.
 - File properties classifiers identify data by file name, type, or size.
- Create customized scripts, dictionaries, file-types, regular expression patterns, and key phrases for specific (described) data. As a shortcut, edit an predefined classifier, then save it with a new name.
- Fingerprint (register) data. The power of fingerprinting 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.
The system can fingerprint 2 types of data: structured (databases) and unstructured (files and folders).
- Create machine learning classifiers by providing examples of the type of data that should be protected and should **not** be protected, 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.

For more information on content classification methods, including which is most and least accurate, see [Classifying Content](#) section.

Related concepts

- [File fingerprinting](#) on page 200
- [Database fingerprinting](#) on page 217
- [Scripts](#) on page 198
- [Classifying Content](#) on page 181

Managing Forcepoint DLP

The web-based user interface used for Forcepoint DLP configuration, management, and reporting is called the **Forcepoint Security Manager**. It has modules for web, email, and data security.

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

This document describes how to use the Data Security module of the Forcepoint Security Manager. The following options are available in the Security Manager toolbar:

- 1) Click the **Appliances** icon () on the Security Manager toolbar to open the Manage Appliances page.
- 2) Click the **User Details** icon () on the Security Manager to view the current user name or to log off.
- 3) Click the **Global Settings** icon () on the Security Manager toolbar to open the Security Manager Global Settings page. These settings apply to all installed Forcepoint modules (Web Security, Email Security, and Data Security).
- 4) Click the **Help** icon () to display product Help options for either the Security Manager or the active Forcepoint module (Web Security, Email Security, and Data Security). Select Help Contents or Explain This Page to open the associated embedded Help.

To access product modules, such as Web Security, Email Security, and Data Security, use the following steps:

- 1) At the top left of the screen, hover over the **Forcepoint logo**. A pull-down menu displays the available modules.
- 2) Click the name of the module. The selected module displays.

For more information about the Security Manager toolbar, see [Forcepoint Security Manager Help](#).

Related concepts

- [Navigating the system](#) on page 13

DLP in Forcepoint Web Security and Forcepoint Email Security

- With the DLP Module for Forcepoint Web Security, content on web channels is analyzed without the need to purchase a separate Forcepoint DLP subscription or a protector appliance.

The web channels covered by the DLP Module include HTTP, HTTPS, FTP, and FTP-over-HTTP. This allows administrators to prevent posts to websites, blogs, and forums as well as FTP sites.



Note

If the Forcepoint Web Security Cloud services license is displayed on the Subscriptions page, it refers to the Data Protection Service integration with the Forcepoint Web Security Cloud solution. This integration is not related to the Forcepoint DLP integration with the Forcepoint Web Security on-premises deployment solution.

The supported channels for the Data Protection Service integration with Forcepoint Web Security Cloud are: HTTP, HTTPS, and FTP over HTTP.

- Forcepoint Email Security includes data loss prevention over email channels. A separate Forcepoint DLP subscription, agent, or protector appliance is not required.



Note

Neither the Forcepoint Web Security DLP Module nor Forcepoint Email Security includes all of the options presented in this Help document. For access to other options and channels, talk to your Forcepoint account representative about purchasing a full Forcepoint DLP subscription.

Chapter 2

Navigating the system

Contents

- [Main options on page 14](#)
- [Settings options on page 16](#)
- [Deploy button on page 17](#)
- [Global and status icons on page 18](#)

The Data Security module of the Forcepoint Security Manager is displayed in two panes:

- The left pane is called the **navigation** pane. Each item in the navigation pane offers a menu of options.

The navigation pane is divided into two sections:

- **Main** has options for creating and fine-tuning policies, performing discovery, managing incidents, and viewing system status and logs. See *Main options* section.
- **Settings** has options for administrating the system; performing system maintenance; and configuring endpoint deployment, settings, modules, and roles. See *Settings options* section.



Note

For Forcepoint Web Security or Forcepoint Email Security administrators, the tabs look slightly different. Options that require a full Forcepoint DLP subscription, such as discovery and endpoint, are not shown.

- To the right of the navigation pane is the **content** pane. The content pane displays the feature selected in the navigation pane.
 - The Dashboard is displayed in the content pane by default when an administrator logs on to the Data Security module of the Security Manager. It offers an overview of top Incident Risk Ranking cases, data loss prevention incidents, and discovery incidents over a specified time period. For details about the Dashboard and its contents, see *Viewing the Dashboard* section.
 - Breadcrumb links are displayed at the top of the content pane, showing the navigation path to the current page. Each item in the path is a link, which can be used to navigate back to previous pages.

In the image below, **Status** is selected in the navigation pane, and the **Status > Dashboard** page appears in the content pane.

Health Alert Summary

- Your subscription is valid
- 12 data loss prevention and mobile policies are configured
- 1 discovery policies are configured
- 8 missing essential configurations

Data Loss Prevention - Incidents collected over the last 24 hours

Incidents by Severity

Time Period	High	Medium	Low	Total
4:0 PM	0	0	0	0
8:12 AM	0	0	0	0
12:4 AM	0	0	0	0
4:9 AM	2	4	0	6
8:12 PM	4	0	0	4
12:4 PM	1	0	0	1

Related concepts

- [Deploy button on page 17](#)
- [Global and status icons on page 18](#)
- [Main options on page 14](#)
- [Settings options on page 16](#)
- [Viewing the Dashboard on page 27](#)

Main options

The Main tab of the navigation pane offers access to the following features. (Items marked with an asterisk (*) apply only to full deployments of Forcepoint DLP, and not to the Forcepoint Web Security DLP Module or to Forcepoint Email Security.)

Related concepts

- [Viewing Incidents and Reports on page 39](#)
- [Creating Discovery Policies on page 277](#)
- [Scheduling Discovery Tasks on page 293](#)
- [Classifying Content on page 181](#)
- [Defining Resources on page 241](#)
- [Viewing Status on page 27](#)
- [Viewing Forcepoint DLP Logs on page 339](#)

Related tasks

- [Creating Custom DLP Policies on page 155](#)

Status

- The **Dashboard** appears first when an administrator logs on to the Data Security module of the Forcepoint Security Manager. It provides an at-a-glance dashboard of the enterprise data loss prevention status. See *Viewing the Dashboard* section.
- **System Health** helps administrators to monitor Forcepoint DLP performance. See *Monitoring system health* section.
- **Endpoint Status*** shows a list of data endpoints that are registered with the management server, including information regarding an endpoint's discovery, profile and policy, and the host's system summary. See *Viewing endpoint status* section.
- **Mobile Status*** shows a list of mobile devices that are registered with the management server, including information regarding the owner, device type, and last sync time. See *Viewing endpoint status* section.

Related concepts

[Viewing the Dashboard](#) on page 27

[Monitoring system health](#) on page 30

Related tasks

[Viewing endpoint status](#) on page 33

Reporting

- **Data Loss Prevention** lets each administrator view and manage relevant data loss prevention incidents. Assign incidents to other administrators, view consolidated reports on incidents and information leaks, and schedule reporting tasks. The reports provide a complete picture of what's going on inside the network.
View incidents representing the highest risk to the organization along with their risk scores.
- **Mobile Devices*** shows information about mobile device incidents. Use this page to assign, view, and monitor mobile device incidents.
- **Discovery*** shows information about incidents that were detected through discovery scans. Use this page to assign, view, and monitor discovery incidents.

Policy Management

- Use **DLP Policies** to create or manage network or endpoint DLP policies. Create policies from scratch or use predefined policies.
- Use **Discovery Policies*** to create or manage discovery policies. Create policies from scratch or use a predefined regulatory template.
- Use **Content Classifiers** to describe the data to be protected. Classify data using patterns and phrases, file properties, file fingerprints, database fingerprint, or machine learning.
- Use **Resources** to define data sources and destinations to monitor and protect, endpoint devices or applications that may be in use, and the remediations or actions to take when a violation is discovered (such as block or notify).

Logs

- **Traffic Log** shows details of the traffic being monitored by Forcepoint DLP. See *The Forcepoint DLP traffic log* section.
- **System Log** offers a list of the events sent from system components, such as the Forcepoint DLP servers, protectors, and policy engines. See *The Forcepoint DLP system log* section.
 - **Audit Log** displays a list of actions that administrators have performed in the system. See *The Forcepoint DLP audit log* section.

Related concepts

- [The Forcepoint DLP traffic log](#) on page 340
[The Forcepoint DLP system log](#) on page 343
[The Forcepoint DLP audit log](#) on page 343

Settings options

Following are the options available under Settings. Items marked with an asterisk (*) do not apply to the DLP Module for Forcepoint Web Security or Forcepoint Email Security.

Related concepts

- [General System Settings](#) on page 347
[Archiving incident partitions](#) on page 387
[Main options](#) on page 14

Related tasks

- [Configuring Authorization](#) on page 399

General

- **Reporting:** Set reporting preferences, such as the number of incidents to include.
- **Backup:** Configure system backup settings, such as the path to the backup storage location and the number of copies to keep.
- **Incident Export:** Configure settings for incident export, such as where to save the export file.
- **Endpoint***: 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.
- **Mobile***: Define how the management server should manage the mobile devices covered by policy.
- **Remediation:** Define the location of the syslog server and mail release gateway used for remediation.
- **Mail Servers:** 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.

- **Alerts:** Define when to trigger alerts and whether the alerts should be sent to the syslog or emailed to an administrator.
- **Archive Storage:** Specify where to store the incident archives and how much disk space to allow.
- **Services:** Configure services such as Linking Service, Microsoft Information Protection decryption, CASB, File Labeling, and Risk-Adaptive Protection.
- **User Directories:** Define the user directories to use for Forcepoint DLP users and other policy resources such as devices and networks.
- **Archive Partitions:** Archive, restore, or delete partitions.
- **Policy Updates:** Install updates to Forcepoint DLP predefined policies.
- **Subscription:** View and update product subscription information.

Authorization

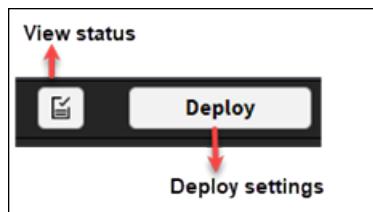
- **Administrators:** Set up and manage Forcepoint DLP administrators and assign roles.
- **Roles:** Edit access privileges or add new roles.
- **My Settings:** Configure personal settings, such as whether to get want system reminders about pending deployment.

Deployment

- **System Modules:** Manage system components such as Forcepoint DLP servers, fingerprint repositories, policy engines, cloud proxy service, and agents.
- **Endpoint Profiles***: Configure endpoint profiles.

Deploy button

In the Data Security module of the Security Manager, policy and configuration changes are saved to the management server as soon as an administrator clicks OK on a page. The changes are not activated, however, until they are deployed.



Click **Deploy** to implement policy changes (including changes to rules, exceptions, resources, content classifiers, and tasks) across all Forcepoint DLP components—the protector, agents, gateways, endpoint hosts, and so on.

- The button to the left of Deploy shows the status of the last deployment.
- Be sure to review configuration changes before clicking Deploy.
- To confirm the decision to deploy changes and initiate the deployment process, click **OK** when prompted.

While changes are being deployed, a table displays the dynamic status of the components that are being updated. While changes are being deployed across the

network, the status column updates for each module change from Processing to either Success or Failed.

Name	Status	Deployment Results
Forcepoint DLP Server on rsw2012dss	Success	All configuration settings were
Endpoint Server rsw2012dss	Success	All configuration settings were
Policy Engine rsw2012dss	Success	All configuration settings were
Forensics Repository rsw2012dss	Success	All configuration settings were
Primary Fingerprint Repository rsw2012dss	Success	All configuration settings were
Crawler rsw2012dss	Success	All configuration settings were
Forcepoint DLP Cloud Applications on ran-msdn-1	Success	All configuration settings were
Policy Engine ran-msdn-1-pe1	Success	All configuration settings were

Deploying changes can take time, and if a component is down or disconnected from the network, deployment to that specific component fails.

- Once the component becomes available again, it receives all pending updates.
- Any deployment failures are shown in the table.

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

Related concepts

[Troubleshooting](#) on page 461

Global and status icons

The following icons are used throughout the Forcepoint Security Manager to reflect status or offer assistance.

Severity and Incident Status

Icon	Description
	High
	Medium
	Low

Icon	Description
	New
	In Process
	Closed

System-wide

Icon	Description
	When a problem occurs, the Error icon is displayed at the top of the page with an explanation.

Icon	Description
	When an update succeeds, the Success icon is displayed at the top of the page with a description of what has been done.
	Click the Information icon to get additional details.
	The Note icon marks additional, pertinent information displayed on a page to assist with configuration.

Chapter 3

Initial Setup

Contents

- [Entering a subscription key](#) on page 22
- [Defining general system settings and notifications](#) on page 23
- [Configuring system modules](#) on page 24
- [Configuring the protector](#) on page 24

For deployments that include the DLP Module for either Forcepoint Web Security or Forcepoint Email Security:

- 1) Define the general system settings, such as user directories and alerts. See *Defining general system settings and notifications* section.
- 2) Select and define attributes for the web DLP or email DLP policy. See:
 - *Configuring web DLP policy attributes*
 - *Configuring outbound and inbound email DLP attributes*
- 3) To deploy all of the configured settings, click **Deploy** in the Data Security toolbar.

For Forcepoint DLP deployments:

- 1) Enter the Forcepoint DLP subscription key. See *Entering a subscription key* section.
- 2) Define the general system settings, such as user directories and alerts, as well as notifications. See *Defining general system settings and notifications* section.
- 3) Configure system modules (protector deployments only). See *Configuring system modules* section.
- 4) Configure predefined policies. See *Adding a predefined DLP or discovery policy* section.
- 5) To deploy all of the configured settings, click **Deploy** in the Data Security toolbar.

Related concepts

[Configuring web DLP policy attributes](#) on page 134

[Configuring system modules](#) on page 24

Related tasks

[Defining general system settings and notifications](#) on page 23

[Configuring outbound and inbound email DLP attributes](#) on page 126

[Entering a subscription key](#) on page 22

[Adding a predefined DLP or discovery policy](#) on page 151

Entering a subscription key

To enable Forcepoint DLP configuration, enter a subscription key in the Data Security module of the Forcepoint Security Manager:

Steps

- 1) Log on to the Security Manager. If the Data Security module is not displayed by default, hover over the Forcepoint logo at the top of the Forcepoint header and select **Data** from the drop-down list.
 - a) If no subscription information has been provided, the subscription page appears automatically.
 - b) To navigate to the subscription page, select **Settings > General > Subscription**.

- 2) Browse to the subscription file, then click **Submit**. Current subscription information is displayed, and the Forcepoint DLP application restarts.
 Your subscription terms displayed on this page include the start and expiration dates (or “n/a” if you have a perpetual subscription), the number of subscribed users, and the modules and services to which you subscribe.

- 3) If the subscription is about to expire, a notice appears on this screen. Click**Update** to update the subscription. To update the Data Security subscription:
 - a) Open the Forcepoint Security Manager console, and navigate to **Data > Settings > General > Subscription**.
 - b) Click **Update**, and browse to the new XML file you received as part of fulfillment.
 - c) Select the file, and click **OK**
 - d) Click **OK** again to save the new file.
 - e) Re-deploy:
 After the update, you are forced to log off of the Security Manager and then log on again to see accurate information on the subscription screen. The **Deploy** button is active at the top of the screen. Click **Deploy**. The subscription now updated to all Policy Engines in your deployment.

- 4) If the deployment includes the Web Content Gateway, log on to the Content Gateway manager and:
 - a) Navigate to the **Configure > My Proxy > Subscription > Subscription Management** tab.
 - b) Enter the Forcepoint DLP Network subscription key and click **Apply**.
 - c) Navigate to the **Configure > My Proxy > Basic > General** tab, then click **Restart** button to restart Content Gateway.



Note

With Forcepoint Web Security or Forcepoint Email Security, subscription information is communicated to the management server automatically.

Related reference

[Entering subscription settings](#) on page 395

Defining general system settings and notifications

Before creating and managing DLP policies, use the **Settings** pages in the Data Security module of the Security Manager to:

Steps

- Configure user directory server settings. This makes it possible for administrators to resolve user details during analysis and enhance the details displayed with the incident.
See *User directory settings* section, and *Adding or editing user directory server information* section.
- Set up alerts. This determines when administrators receive alerts from the system, such as when a subscription is about to expire or disk space is reaching its limit.
See *Alerts* section, and *Setting up email properties* section.

**Note**

The same outgoing mail server is used for alerts, notifications, scheduled tasks, and email workflow. If the server is changed for one function, it is changed for all of them.

- (*Forcepoint DLP only*) Set up notifications. Notifications are email messages that are sent when policy breaches are discovered.
Forcepoint DLP offers a built-in notification template, “Default notification,” that can be edited as required. 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 an action plan to use it.
See *Notifications* section, and *Adding a new message* section.

Related concepts

[User directory settings](#) on page 380

[Notifications](#) on page 273

Related tasks

[Adding or editing user directory server information](#) on page 381

[Alerts](#) on page 365

[Setting up email properties](#) on page 365

[Adding a new message](#) on page 273

Configuring system modules

When Forcepoint DLP is installed, each of its agents, components, and modules is automatically registered with the management server.

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

The 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 Forcepoint Web Security or Forcepoint Email Security, there are also modules for the Web Content Gateway and Forcepoint Email Security.

Protector-based solutions have the following modules:

- ICAP agent
- Policy engine
- Secondary fingerprinting repository The protector is also a module itself.

If other modules have been added to the system—such as supplemental Forcepoint DLP servers, agents, crawlers—these components appear in tree view as well.

To get a basic Forcepoint DLP deployment up and running, the only component that needs to be configured is the protector. In some cases, the protector is not even required—as in some endpoint deployments and in Forcepoint Web Security deployments.



Note

See the [Forcepoint DLP Installation Guide](#) for instructions on installing Forcepoint DLP modules.

Related concepts

[Managing Forcepoint DLP System Modules](#) on page 409

Related tasks

[Configuring the protector](#) on page 24

Configuring the protector



Note

Refer to *Configuring Forcepoint DLP system modules* section for information on the default settings of system modules.

Steps

- 1) In the Forcepoint Security Manager, go to the **Data > Settings > Deployment > System Modules** page.
- 2) Expand the tree in the content pane, if needed.
- 3) Click the protector module in the tree and provide the information requested on the following tabs:
 - a) *Edit Protector: General tab*
 - b) *Edit Protector: Networking tab*
 - c) *Edit Protector: Local Networks tab*
 - d) *Edit Protector: Services tab*

Related concepts

[Edit Protector: Services tab](#) on page 426

Related tasks

[Configuring Forcepoint DLP system modules](#) on page 411

[Edit Protector: General tab](#) on page 424

[Edit Protector: Networking tab](#) on page 424

[Edit Protector: Local Networks tab](#) on page 426

Chapter 4

Viewing Status

Contents

- Viewing the Dashboard on page 27
- Monitoring system health on page 30
- Viewing endpoint status on page 33
- Changing table properties on page 34
- Viewing mobile device status on page 35
- Applying column filters on page 36
- Viewing deployment status on page 37

The Data Security module of the Forcepoint Security Manager shows status information for various system components. Use this information to:

- Assess system performance.
- Find the connection status of various endpoint and mobile devices.
- View traffic trends to determine whether to fine-tune policy configuration. The following status options are available under **Main > Status**:
 - Dashboard
 - System Health
 - Endpoint Status
 - Mobile Status

On some status pages, the toolbar at the top of the content pane includes buttons on the right-hand side of the page that can be used to print status information, or export it to PDF or CSV file.

When information is exported to CSV, file contains all the rows in the main table, without paging. If the list is filtered, only the filtered records are exported.

Some pages offer the option to click a down arrow next to **Export to PDF** or **Print Preview** to define exactly what to export or print. Select the current item (such as the current endpoint host), the selected item, or all items.

Viewing the Dashboard

By default, the Dashboard opens every time an administrator accesses the Data Security module of the Forcepoint Security Manager. This page shows a comprehensive view of top Incident Risk Ranking cases, data loss prevention incidents, and discovery incidents over a specified time period.

From the Dashboard, administrators can see any system health alerts and act on them quickly and easily. Administrators can also view incidents by hostname and policy category to find out where the greatest risks lie.

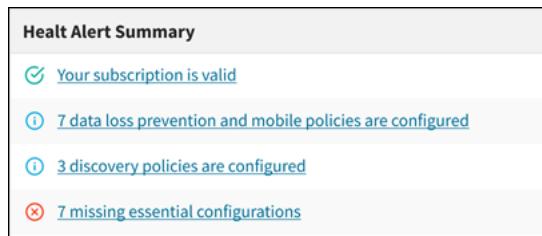


Note

The page displays only incidents that the current administrator is authorized to view. Adobe Shockwave Player is required.

Health Alert Summary

The summary at the top of the page shows subscription information, system messages, configuration gaps, and deployment updates.



Click on an alert to see further information or take action. 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.

SSL Certificate Alerts

The SSL certificate Alerts, added with v8.9.1, show a warning notification on the Dashboard about the upcoming expiration date or show an error notification on the Dashboard when the SSL Certificate expired, SSL certificate ca.cer file is missing, or SSL certificate ca.cer file corrupted.

The Alerts display one of the following messages:

- SSL Certificate ca.cer is about to expire in [x] days (DD/Mon/YYYY)
- SSL Certificate ca.cer has expired on DD/Mon/YYYY
- SSL certificate ca.cer file is missing
- SSL certificate ca.cer file is corrupt

The screenshot shows the Forcepoint DLP Status / Dashboard. A prominent yellow warning message states: "SSL certificate.ca.cer is about to expire in 1 day (14/Feb/2022). For information on how to renew the certificate, click Explain This Page." Below this, the "Health Alert Summary" section lists the following items:

- Your subscription is valid
- 4 data loss prevention and mobile policies are configured
- No discovery policies are configured
- 8 missing essential configurations

On the right side, there are two tables: "Business Value - Data collected over the last 24 hours (approximate)" and "Data Loss Prevention - Incidents collected over the last 24 hours".

Note

To resolve the DLP SSL Certificate expiring issue, you must have an updated DLP Certificate Authority (DLP ca.cer) or you have to renew the same. See the article [Forcepoint DLP CA.CER Certificate Expires Every 5 Years / DLP Certificate Recreation Procedure](#) for more information.

Business Value

Review the approximate amount of data collected over the last 24 hours:

Business Value - Data collected over the last 24 hours (approximate)

Inspected Web traffic:	10,238 (130 MB)
Inspected email messages:	131 (106 MB)
Messages delivered to mobile devices:	142 (35 MB)
Inspected discovery items:	1,235 (37 MB)
Endpoints:	215 of 346 are enabled (10 Jun. 2017, 10:41 AM)
Synchronized mobile devices:	12

- **Inspected Web traffic** shows the number of web transactions (including posts) analyzed, and the cumulative volume of the traffic in megabytes.
- **Inspected email messages** shows the number of email messages analyzed, and the cumulative size of the messages in megabytes.
- **Inspected mobile device messages** shows 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** shows 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 is approximately 5000 records.)
- **Connected endpoints** shows the number of endpoint clients connected to the system.

Data Loss Prevention Incidents

See the number of data loss prevention incidents that have been detected in the last 24 hours, as well as the following graphs:

- **Incident Risk Ranking - Top Cases** shows any cases found in the network with risk scores that exceed a configurable threshold.
 - Cases are groups of related incidents that, combined, indicate a risk to the organization.
 - Cases are assigned risk scores based on sophisticated security analytics.
 - The displays uses the risk threshold set on the **Settings > General > Reporting > Incident Risk Ranking** tab.
 Click the chart to view details on each case.
- **Incident Risk Ranking - Top Cases (last 7 days)** displays the number of cases above the risk threshold detected during each of the last 7 days. The height of the bars and the value shown inside represent the number of the risky cases for each date.
 Click a bar to drill down to the Incident Risk Ranking report for the selected date.
- **Incidents by Severity** displays the number of incidents that have entered the system in the last 24 hours by severity. These include all incidents that the system has detected.

Field	Description
High	Number of incidents that have been set to the most severe setting and should be handled immediately.
Medium	Number of incidents that have been set to the medium severity setting and should be handled soon.

Field	Description
Low	Number of incidents that have been set to the most lenient severity setting and should be handled.

- **Top 5 Policies** displays the policies that had the most incident violations, and the number of incidents in each of these policy categories.

The **Last data loss prevention incident** field provides the exact date and time the last incident was logged in Forcepoint DLP.

Click the **My data loss prevention incidents** link to open the incident summary page, where administrators can view and manage their assigned incidents.

Discovery Incidents

See the total number of discovery incidents detected by a Forcepoint Data Discovery scan, as well as the following graphs:

- **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** field provides the exact date and time the last incident was logged in Forcepoint DLP.

Click the **My discovery incidents** link to open the incident summary page, where administrators can view and manage their assigned incidents.

Monitoring system health

Use the **Data > Main > Status > System Health** page in the Forcepoint Security Manager to monitor the performance of Forcepoint DLP modules.

The tree view displays the names of all system modules, including servers and agents. Click a server or agent to ascertain its health.

For most components, the following information is displayed:

Chart	Description
System Summary	Information about the server, including operating system and version, time zone, and free disk space.
CPU Usage	The percentage of the CPU that is being used by the machine's processes over the specified time frame.
Memory Usage	The percentage of memory that is being used by the machine's processes over the specified time frame.

Forcepoint DLP servers include the following modules in the tree view:

- Primary fingerprint repository
- Endpoint server
- Policy engine

- OCR server (secondary Forcepoint DLP servers only)

Protectors, gateways, and agents include the following modules:

- Policy engine
- Secondary fingerprint repository

When a module is selected, information about the system health and performance of that module is shown. The right-hand part of the screen displays the statistics for events flowing through the system, showing how the system behaves with regards to traffic type (channels) and how busy the components are.

It also displays charts with information that can be used to help fine-tune the system and optimize Forcepoint DLP performance. The charts displayed depend on the module chosen:

- For protector:

Chart	Description
Packet loss and dropped transaction indication	Indicates the levels of packet loss and dropped transaction rates.
Number of events sent to analysis	The number of events sent for analysis by this protector in the specified time frame.
Load average	Average amount of work performed by the protector in the specified time frame. For optimum performance, the number on the chart should not exceed the number of available processors in the System Summary: for example, if the system load average is 3 and there are 2 available processors, the system might work slowly.
Memory usage	The percentage of memory used by machine processes.
Total Throughput	Total amount of traffic (in KB per second) monitored by the protector. This includes both interesting and non-interesting sessions.
Data sent to analysis throughput	Total amount of traffic (in KB per second) sent for analysis by this protector.

- For the policy engine:

Chart	Description
Analysis status	Displays the request load on the policy engine for analysis by time period.
DLP—number of analyzed events	Number of DLP events analyzed by this policy engine in the specified time frame.
DLP—number of incidents	Number of DLP incidents detected by this policy engine in the specified time frame.
Discovery—number of analyzed items	Number of discovery items analyzed by this policy engine in the specified time frame. This includes files, email messages, and database tables. This chart is available only for policy engines on Forcepoint DLP servers. If the policy engine on this computer does not handle discovery traffic, this report is empty.

Chart	Description
Discovery—number of incidents	Number of discovery incidents detected by this policy engine in the specified time frame. This chart is available only for policy engines on Forcepoint DLP servers. If the policy engine on this computer does not handle discovery traffic, this report is empty.

- For the fingerprint repository:

Chart	Description
Database fingerprint repository synchronization	Displayed only on the 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.
Secondary database fingerprint repository synchronization trend	Shows how much database data was synchronized from the primary repository to this one over time, in KB.
Number of fingerprinted files	Displays the total number of files fingerprinted in the specified time frame.
Number of fingerprinted database cells	Displays the total number of database cells fingerprinted in the specified time frame.

- For the endpoint server:

- Endpoint server load** displays the load on the endpoint server over the specified time period.
- Number of endpoints** shows the number of endpoint requests received by the endpoint server in the specified time frame.

- For the OCR server:

Chart	Description
Queue load	Shows the load of OCR server queue during the selected time period.
Number of textual requests	Shows the total number of OCR requests containing textual data during the selected time period.
Number of requests	Shows the total number of requests made to the OCR server during the selected time period.
Average image size	Shows the average size of images (in bytes) that were handled by the OCR server during the selected time period.
Average processing time	Shows the average processing time (in milliseconds) of images that were handled by the OCR server during the selected time period.

For each chart, use the **Display** drop-down list to select a time frame. 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 **Download Diagnostics** on the toolbar at the top of the content pane. A zip file

containing diagnostic information is downloaded to the specified location. This operation can take several minutes.

For all modules, an **Advanced** section is also available. Expand this section to view raw statistics supplied by the selected module.

Viewing endpoint status

Endpoint devices running Forcepoint DLP Endpoint 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. Filter down to locate servers that 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 DLP endpoints:

- 1) In the Forcepoint Security Manager, go to the **Data > Main > Status > Endpoint Status** page. The resulting screen lists all Forcepoint data endpoints registered with the management server. The list displays information for each endpoint, such as:

- Hostname of the endpoint client machine
- IP address of the endpoint client machine
- Logged-in Users (users who are currently logged into the endpoint)
- Last Update (last time that the endpoint checked for updates from the management server)
- Profile Name (name of the endpoint profile assigned to the endpoint)
- Whether endpoint clients are Synchronized or not synchronized with the latest management server updates. The sync status shows an "X" when the policy or profile version is not synchronized with the management server or when the endpoint's profile is not as it was set in the Manager.
- Discovery Status (whether a discovery process is currently idle or running on the endpoint) The discovery status shows N/A for endpoints that are not used in discovery, such as Linux endpoints.
- Client Status (whether endpoint clients are enabled or disabled via the Bypass option)

There are many other options available than displayed in the table by default. To customize the information shown in each column, or to view descriptions of the available data, see *Changing table properties* section.

There are also many options for filtering the data in the table. See *Applying column filters* section.

- 2) To drill down for further information about each endpoint, select an endpoint in the list. The profile name, fingerprinting version, and more are displayed.
- 3) To remove an endpoint from the list (such as one that no longer exists), select the endpoint and click **Remove**. If the endpoint is still active, it will automatically be added back when it sends status to the endpoint server.

Also use this page to:

- Search for a specific endpoint in the list.
Use the filtering option in the **Hostname** column header.
- Temporarily disable the selected endpoint
Click **Bypass Endpoint** (see *Bypassing endpoint clients*).
- View and edit system settings for endpoint clients

Click **Settings** (see *Configuring endpoint settings*).



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.

Related concepts

[Applying column filters on page 36](#)

Related tasks

[Configuring Endpoint Deployment on page 445](#)

[Bypassing endpoint clients on page 458](#)

[Changing table properties on page 34](#)

[Configuring endpoint settings on page 357](#)

Changing table properties

Click the Table Properties () button to customize the contents of an endpoint status report. Select the properties to display and choose the column width for each.

Column	Description
Apple Mail Plug-in Status	The status of the endpoint's plug-in. Possible statuses: <ul style="list-style-type: none"> ■ Enabled (for all logged-in users) ■ Disabled (for at least one logged-in user) ■ Unknown (for older endpoint version, or plug-in was never opened) ■ An empty status indicates that the endpoint machine operating system does not support the extension.
Client Installation Version	Version of the endpoint client software that is installed on the endpoint machine.
Client Status	Status of the endpoint client: enabled or disabled.
Discovery Status	The status of the discovery service on the endpoint.
Endpoint Server	Name of the server associated with this endpoint.
Files Scanned	The number of files that were scanned on the endpoint in the most recent scan.
Host Name	Host name of the endpoint machine.
IP Address	IP address of the endpoint machine.
Last Scan End Time	The time that the latest endpoint scan ended.
Last Scan Start Time	The time that the latest endpoint scan began.

Column	Description
Last Update	Last time the endpoint received updates from the management server (profiles, policies, etc.).
Logged-in Users	Users who have logged into the endpoint.
MAC Address	MAC address of the endpoint client machine.
Microsoft Information Protection	Whether Microsoft Information Protection (MIP) decryption and analysis is active or inactive.
Next Scan Time	The time scheduled for the next endpoint scan.
Policy Engine Version	Version of the policy engine machine that is associated with this endpoint.
Profile Name	The name of the endpoint profile on this machine.
Safari Extension Status	<p>The status of the endpoint's extension. Possible statuses:</p> <ul style="list-style-type: none"> ■ Enabled (for all users) ■ Disabled (for at least one user) ■ Unknown (for older endpoint version, or extension was never opened) <p>An empty status indicates that the endpoint machine operating system does not support the extension.</p>
Synced	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.

Viewing mobile device status

Use the **Data > Main > Status > Mobile Status** page in the Forcepoint Security Manager to view the status of all mobile devices and users connected to the system.

Initially, the page lists all mobile devices registered with the 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:

- 1) Click the Table Properties () button.
- 2) Select the properties to display and choose the column width for each.

Column	Description
Device ID	The Unique Device Identifier (UDID) associated with the device.
Device Type	The type of mobile device, for example, iPad or iPhone.
Email	The email address associated with this mobile device.
Last Sync Time	The date and time this mobile device last synchronized with the network email system.
User	The mobile device owner.
User Agent	The network protocol this mobile device uses to communicate with the Forcepoint DLP system (Touchdown, ActiveSync, etc.).



Note

Some mobile devices do not use all of the available fields. In this case, the field for that device is empty.

To filter the data shown in the table, see [Applying column filters](#).

To drill down further, select a device in the list. The Details pane shows:

- Information about the device owner, such as phone number and email address. If the owner's full name is found in the user directory, this is also displayed.
- How many devices are registered to the owner
- Which device was last synchronized.

To remove a device from the list, select it and click **Remove**. To remove all devices at once, click **Remove All**.

Related concepts

[Configuring the Mobile DLP Policy](#) on page 143

[Applying column filters](#) on page 36

[Filter tab](#) on page 42

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Remediation](#) on page 361

Applying column filters

Endpoint and mobile device status information can be sorted, grouped, and filtered by column name (like Profile Name or Device Type). To sort a column, click the down arrow next to the column name, then choose an option:

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

To view the current filters in use, click the information ("i") 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: click this button to clear a single filter or all filters.

If there are too many items to fit on the page, browse the list using the Next, Previous, First, and Last buttons.

Viewing deployment status

After making policy configuration or settings changes, click **Deploy** to deploy the changes in the network.

Click the magnifying glass icon next to the Deploy button to display the Deployment Process page, which shows the status of the deployment. On this page, the Status column shows the deployment progress status, which can be:

- In progress
- Succeeded
- Failed

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

Error Handling

If you receive the following warning message on the Data Protection Service module:

This service is not connected to Forcepoint CASB. Incident reporting and policy enforcement will be affected for cloud channels. See "Explain this page" for more information.

This means that there is a connection issue, and DLP Cloud API and Cloud Data Discovery channels will not enforce DLP policies, and the DLP Cloud Proxy channel might not report incidents to the Forcepoint Security Manager.

To resolve this issue:

Check the log file, and determine which of the two possible error scenarios is relevant, and then proceed accordingly. Note that the exact content of the log messages might change.

Option 1: Two different CASB tenant IDs cannot be associated with the same Data Protection Service (global_tenant_id)

Log message:

`neo_tenants_status_code":526,"neo_tenants_status_message":"aborting since tenant_id (xxxxxxxxxxxx) already exists with different CASB Account ID:xxxxxxxxxxxx`

This indicates that the Forcepoint Security Manager is already connected to Forcepoint CASB using one CASB tenant ID, while Data Protection Service is trying to connect to Forcepoint CASB using a second CASB tenant ID.

In this case, the Security Manager successfully deploys the configuration to Data Protection Service, however the Forcepoint CASB cloud agents are not able to enforce DLP policies.

To see the CASB tenant ID associated with the Security Manager, go to **Services > Cloud Applications** tab, where it is listed at the top of the Module Connection Status section, or check the log file.

To fix the problem:

- 1) Reconnect Forcepoint Security Manager to Forcepoint CASB in the Cloud Applications tab, and check to make sure that the displayed CASB tenant ID is different than the one used before.
- 2) Click **Deploy**, and then check the Deployment page to make sure that the warning message about Data Protection Service is no longer displayed, and that the deployment is marked as successful.

If after reconnecting to Forcepoint CASB the same CASB tenant ID that prompted the warning is still displayed in the Cloud Applications tab, contact Forcepoint Support to request that your Security Manager connection to Forcepoint CASB and the Data Protection Service connection to Forcepoint CASB be associated with the same CASB tenant ID.

Option 2: Two different Data Protection Service (`global_tenant_id`) instances cannot be associated with the same CASB tenant ID

Log message:

```
neo_tenants_status_code":526,"neo_tenants_status_message":"aborting since casbTenantId (xxxxxxxxxxxxxx)
already exists with different tenantId:xxxxxxxxxxxxxx
```

This indicates that the CASB tenant ID is already associated with an instance of Data Protection Service (`global_tenant_id`), and Forcepoint Security Manager is now trying to connect it to an using a different Data Protection Service ID.

Contact Forcepoint Support to request that your Security Manager connection to Forcepoint CASB and the Data Protection Service connection to Forcepoint CASB be associated with the same CASB tenant ID.

Option 3: Other issues from Forcepoint CASB side

Errors originating on Forcepoint CASB cannot be resolved within Forcepoint DLP, and require you to contact Forcepoint Support for assistance.

As an example, the log message might includes the following message regarding absence of a required ID parameter:

```
casb_tenants_status_code":526,"casb_tenants_status_message":"Tenant id: xxxxxxxxxxxx has DPS but with no
sfAccountId (null/undefined)"
```

Related concepts

[Troubleshooting](#) on page 461

Chapter 5

Viewing Incidents and Reports

Contents

- [The report catalog](#) on page 40
- [Viewing the incident list](#) on page 69
- [Data Loss Prevention reports](#) on page 92
- [Mobile devices reports](#) on page 104
- [Discovery reports](#) on page 107

Use the **Main > Reporting > Data Loss Prevention**, **Mobile Devices**, or **Discovery** page in the Data Security module of the Forcepoint Security Manager to view and report on incidents. Review the incident list and details for individual incidents, or choose from a catalog of reports.

- **Recent Reports** shows the reports viewed most recently. The order of these reports changes with use.
- **Report Catalog** provides a list of all the reports that are available for a given area, both built-in and user-defined.



Note

What administrators can see depends on their permissions. See [Setting reporting preferences](#), for instructions on configuring settings for incidents and reports.

To learn about a report, click its name. To generate the report, click **Run**. To create a report:

- 1) Open an existing report. For example, Incidents (last 3 days).
- 2) Click **Manage Report > Edit Filter** to change the filters.
- 3) Click **Manage Report > Save As**.

Custom reports appear in the report catalog along with the built-in reports.

Related concepts

- [Viewing the incident list](#) on page 69
- [Data Loss Prevention reports](#) on page 92
- [Mobile devices reports](#) on page 104
- [Discovery reports](#) on page 107
- [Setting reporting preferences](#) on page 348

Related tasks

- [The report catalog](#) on page 40

The report catalog

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

- 1) In the Forcepoint Security Manager, go to the **Data > Main > Reporting > Data Loss Prevention, Mobile Devices, or Discovery** page.
- 2) 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*
 - *Mobile devices reports*
 - *Discovery reports*
- 3) Click a folder to expand it and see a list of related reports. Each report is marked with an icon:
 - marks detail reports of incident lists.
 - marks graphical summaries.
- 4) Click **Expand All** or **Collapse All** to expand or collapse all folders, or click **New Folder** to create a new folder.
- 5) Click the **Edit** to edit a folder name or **Delete** to delete a folder.
Predefined folders cannot be edited.
Click a report to read its description. When a report is selected, a menu bar appears, showing the following options:

Button	Icon	Description
Run		Run the selected report and display it.
Edit		Edit or apply filters to the report. See <i>Editing a report</i> .
Save As		Save the report with a new name.
Export to PDF		Export the report to a PDF file.
Export to CSV		Export the report to a CSV file.
Schedule a task		Schedule this report for automatic email delivery.
Delete		Delete the selected report. Predefined reports cannot be deleted.

There are additional buttons in the report catalog toolbar:

Button	Icon	Description
Scheduled Tasks		Used to create a schedule for emailing incident reports. Create a scheduled task, define sender and recipient names, and define the outgoing mail gateway.
Settings		Used to set preferences for incident lists and reports. For example, for data loss prevention incidents, define attachment size and forensics settings. For discovery incidents, set database thresholds. General settings, like filtering and printing, that apply to all types of incidents, can also be defined. For information on configuring these settings, see <i>Setting reporting preferences</i> .

Related concepts

[Scheduling a new task on page 67](#)
[Mobile devices reports on page 104](#)
[Discovery reports on page 107](#)
[Editing a report on page 41](#)
[Setting reporting preferences on page 348](#)

Related tasks

[Scheduling tasks on page 67](#)
[Setting preferences for data loss prevention reports on page 350](#)

Editing a report

Editing a report from the report catalog opens up to 3 tabs:

- *General tab* (displayed for all report types)
- *Filter tab* (displayed for summary and detail reports)
- *Table Properties tab* (displayed for detail reports only) Complete the fields as described in the linked sections.

Related concepts

[General tab on page 42](#)
[Filter tab on page 42](#)
[Table Properties tab on page 60](#)

General tab

Use the **General** tab of the Report Catalog > Edit Report page to configure basic report information, like the name, description, and number of items shown.



Note

For predefined trend reports, only the Show top field is configurable. All fields can be edited for custom trend reports.

Field	Description
Name	A unique name for the report.
Description	A description to help administrators understand the purpose of the report.
Which administrators can access the report:	Which administrators can access the report: <ul style="list-style-type: none"> ■ Only the Report owner ■ All administrators with access to the Data Security module of the Forcepoint Security Manager Forcepoint DLP
Show top	(<i>Summary reports only</i>) The number of items to display in the Top Items charts for this report (between 1 and 20). For example, display the top 5 policies in the Top Policies chart.

For custom trend reports, also specify the time period to cover. Select:

- **Last** to display trends for the last few days, then select the exact number of days.
- **Time period** to display trends for a set period, like “last month” or “current quarter,” then select the period from the drop-down list.
- **Exact dates** to display trends for a precise period, then select the From and To dates and times.

Related concepts

[Filter tab](#) on page 42

[Table Properties tab](#) on page 60

Filter tab

Use the **Filter** tab of the Report Catalog > Edit Report page to focus the report on the data that is most relevant to you. For example, apply the Action filter and display only incidents with the action Block. Apply as many filters as needed.

For each filter to apply:

- 1) Select the filters in the **Filter** by pane on the left.
- 2) Select **Enable filter** in the properties pane.
- 3) Apply properties to the filter in the 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*
- *Mobile Device filters*
- *Discovery filters*

Data Loss Prevention filters

Filter	Description
Action	<p>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.</p> <p>Incidents with the following actions can be displayed:</p> <ul style="list-style-type: none"> ■ Permitted ■ Blocked ■ Attachment(s) dropped ■ Quarantined ■ Encrypted with profile key ■ Encrypted with user password ■ Denied (confirmed) ■ Continued (confirmed) <p>In addition to the default actions, DLP actions configured in the Forcepoint Security Manager are listed (Forcepoint Email Security only).</p>
Application Name	Filter incidents by the name of applications found in the incidents. Select the applications to include in the report.

Filter	Description
Assigned to	<p>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 Security Manager. Assigned to selected administrators enables you to select specific administrators whose assigned incidents you want to display.</p>
Business Unit	Filter to filter incidents by the business unit to which they're assigned.

Filter	Description
Channel	<p>Limit which channels' incidents are displayed in the report. The list of available channels depends on channels configured in the Security Manager.</p> <p>If one or more email filters is selected, specify the email direction to display: inbound, outbound, or internal. Email direction is available only for those with the Forcepoint Email Security module, endpoint agent, or protector.</p> <p>For the endpoint application filter, select the operations to display in the report. For example, choose Paste to display all endpoint incidents where users pasted sensitive data into a document.</p> <p>It is also possible to view incidents from the Discovery channel or DLP Cloud Applications channels.</p> <p>Select DLP Cloud Applications to view incidents detected when users uploaded, downloaded, or shared files with cloud applications such as Office365 or Box. (Enable the Cloud Applications service at Settings > General > Services.)</p>
Classifier Matches	<p>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.</p> <p>Click Edit to add or remove content classifiers to the filter, then select a threshold for each.</p>
Classifier Type	<p>Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.).</p>
Destination	<p>Set the incident list to display only incidents that were directed at specific destinations.</p> <p>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".</p> <p>If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available.</p> <p>Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain.</p> <p>Complex filters can affect performance.</p> <p>See <i>Selecting items to include or exclude in a policy</i> for more details on using this selector.</p>

Filter	Description
Detected by	Display only incidents intercepted that were detected by specific Forcepoint DLP modules. Select each module to be displayed. The list of available modules depends on which modules were configured on the System Modules page.
Endpoint Type	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.

Filter	Description
Event Time	<p>Filter incidents by the date and time the policy engine first saw a transaction. An event is any transaction being analyzed. (An incident is an event that breaches policy.)</p> <p>Select a date range, then select a time of day.</p> <p>Date Range</p> <ul style="list-style-type: none"> ■ Last <i>n</i> days - Select this option to display incidents from the last <i>n</i> 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. <p>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.</p> <p>Time of Day</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>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.</p>

Filter	Description
File Name	<p>Filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click Add. Continue until all required file names have been added.</p> <p>Note that complex filters can affect performance.</p>
History	<p>Filter incidents by the date, administrator, or details contained on the incident History tab. For example, display all incidents that jdoe closed during March 2017.</p> <ul style="list-style-type: none"> ■ Select Filter by date to specify the date and time of the actions that were taken. Only actions during this period are included in the report. Select a date range and time of day. ■ Select Filter by administrator to specify the administrator who performed the listed workflow action. Enter the administrator name or names. Separate multiple names by commas. For example: Type "jdoe, bsmith" to view incidents that jdoe and bsmith acted on. ■ Select Filter by details to specify 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. <p>Enter the text for which to search. It is possible to search for all or part of the detail text. For example, enter "closed" to search for incidents that were closed during a certain period.</p> <p>As always, this filter depends on the other filters that have been selected, such as Incident Time and Ignored Incident. To filter only by history, define a large range for Incident Time, then define the history filter.</p> <p>Note that complex filters can affect performance.</p>
Ignored Incident	<p>Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.</p>
Incident Tag	<p>Filter incidents by a previously-defined tag. (See <i>Tagging incidents</i>). Select the tags by which to filter the report and click Add. Continue until all required tags have been added.</p> <p>These can be used to group incidents for external applications. Note that complex filters can affect performance.</p>

Filter	Description
Incident Time	<p>Filter incidents by the date and time they were written to the database. An incident is an event that breaches policy. (An event is any transaction being analyzed.)</p> <p>Select a date range, then select a time of day.</p> <p>Date Range</p> <ul style="list-style-type: none"> ■ Last n days - Select this option to display incidents from the last <i>n</i> 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. <p>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.</p> <p>Time of Day</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>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.</p>
Policy	Use the check boxes provided to set which policy's incidents are displayed in the incident list.

Filter	Description
Released Incident	Filter in or out SMTP incidents that have been released by an administrator (a reports remediation option).
Rule Name	Filter incidents by the rules they triggered.
Severity	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.

Filter	Description
Source	<p>View only incidents that were initiated by specific sources. Select sources from the resource list or enter them as free text. Choose which method to use from the drop-down list. If a free text entry includes a comma, enclose the value in quotes. For example: "Doe, John".</p> <p>If there is a role in which source and destination information is hidden for privacy reasons, optionally enter one or more source IDs.</p> <p>Note that the filter returns values from all columns describing the source, such as URL category, hostname, IP address, and domain.</p> <p>Complex filters can affect performance.</p> <p>See <i>Selecting items to include or exclude in a policy</i> for more details on using this selector.</p>
Status	Select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. It is not possible to filter by statuses that have been deleted from the system.
Top Matches	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	Select the size of incidents to display. It is possible to display incidents greater than a certain size (in KB), or between 2 sizes.
Violation Triggers	<p>Select which incident triggers to display in the incident list. In the field, enter a violation trigger of interest and click Add. Continue until all required triggers have been added.</p> <p>Note that complex filters can affect performance.</p>

Mobile Device filters

Filter	Description
Action	Filter incidents by the action that was performed on the incident. Select the check box for each action to be displayed.
Assigned 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 Forcepoint Security Manager. Assigned to selected administrators enables you to select specific administrators whose assigned incidents you want to display.
Business Unit	Filter incidents by the business unit to which they're assigned.
Classifier Matches	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	Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)

Filter	Description
Destination	<p>Set 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".</p> <p>If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available.</p> <p>Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain.</p> <p>Complex filters can affect performance.</p> <p>See <i>Selecting items to include or exclude in a policy</i> for more details on using this selector.</p>

Filter	Description
Detected by	<p>Set the incident list to display only incidents intercepted that were detected by specific Forcepoint DLP modules. Select each module to be displayed. The list of available modules depends on which modules were configured on the Security Manager System Modules page.</p>
Device Details	<p>Display incidents that match certain device criteria.</p> <ol style="list-style-type: none"> <li data-bbox="861 481 1498 576">1) In the Field menu, indicate whether to filter by device name, ID, user agent, model, operating system, or type. <li data-bbox="861 618 1498 703">2) Indicate whether the field should contain a certain value or be empty. <li data-bbox="861 745 1326 777">3) Enter a value in the blank text box. <li data-bbox="861 819 1041 851">4) Click Add.
Device User	<p>Display only incidents for specific mobile-device users. Select users from the resource list or enter identifying information manually.</p> <p>When using the resource list:</p> <ul style="list-style-type: none"> <li data-bbox="861 1062 1473 1146">■ Use the Display field to indicate whether to pick from directory entries, business units, or custom users. <li data-bbox="861 1167 1367 1199">■ Enter a search term in the Filter by field. <li data-bbox="861 1220 1147 1252">■ Click the filter button. <li data-bbox="861 1273 1481 1326">■ Select items from the available list. See <i>Selecting items to include or exclude in a policy</i>. <p>For free text, type a name, email address, or other information in the text box. Note that complex filters can affect performance.</p>

Filter	Description
Event Time	<p>Filter incidents by the date and time the policy engine first saw a transaction. An event is any transaction being analyzed. (An incident is an event that breaches policy.)</p> <p>Select a date range, then select a time of day.</p> <p>Date Range</p> <ul style="list-style-type: none"> ■ Last n days - Select this option to display incidents from the last <i>n</i> 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. <p>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.</p> <p>Time of Day</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>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.</p>

Filter	Description
File Name	<p>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.</p> <p>Note that complex filters can affect performance.</p>
History	<p>Filter incidents by the date, administrator, or details contained on the incident History tab. For example, display all incidents that jdoe closed during March 2017.</p> <ul style="list-style-type: none"> ■ Select Filter by date to specify the date and time of the actions that were taken. Only actions during this period are included in the report. Select a date range and time of day. ■ Select Filter by administrator to specify the administrator who performed the listed workflow action. Enter the administrator name or names. Separate multiple names by commas. For example: Type "jdoe, bsmith" to view incidents that jdoe and bsmith acted on. ■ Select Filter by details to specify 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. <p>Enter the text for which to search. It is possible to search for all or part of the detail text. For example, enter "closed" to search for incidents that were closed during a certain period.</p> <p>As always, this filter depends on the other filters that have been selected, such as Incident Time and Ignored Incident. To filter only by history, define a large range for Incident Time, then define the history filter.</p> <p>Note that complex filters can affect performance.</p>
Ignored Incident	<p>Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.</p>
Incident Tag	<p>Filter incidents by a previously-defined tag (see <i>Tagging incidents</i>). Select the tags by which to filter the report and click Add. Continue until all required tags have been added.</p> <p>Use these tags to group incidents for external applications. Note that complex filters can affect performance.</p>

Filter	Description
Incident Time	<p>Filter incidents by the date and time they were written to the database. An incident is an event that breaches policy. (An event is any transaction being analyzed.)</p> <p>Select a date range, then select a time of day.</p> <p>Date Range</p> <ul style="list-style-type: none"> ■ Last n days - Select this option to display incidents from the last <i>n</i> 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. <p>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.</p> <p>Time of Day</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>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.</p>
Policy	Use the check boxes provided to set which policy's incidents are displayed in the incident list.

Filter	Description
Released Incident	Filter in or out SMTP incidents that have been released by an administrator (a reports remediation option).
Rule Name	Filter incidents by the rules they triggered.
Severity	Select the severity of incidents to display. Select High to display incidents of high severity, and so on. Select as many severity levels as desired.

Filter	Description
Source	<p>View only incidents that were directed at specific sources. Select sources from the resource list or enter them as free text. Choose which method to use from the drop-down list. If the free text includes a comma, enclose the value in quotes. For example: "Doe, John".</p> <p>If there is a role in which source and destination information is hidden for privacy reasons, optionally enter one or more source IDs.</p> <p>Note that the filter returns values from all columns describing the source, such as URL category, hostname, IP address, and domain.</p> <p>Complex filters can affect performance.</p> <p>See <i>Selecting items to include or exclude in a policy</i>.</p>
Status	Select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. It is not possible to filter by statuses that have been deleted from the system.
Synced by	<p>Display incidents on messages that were synchronized by a certain number of mobile-device users.</p> <p>For example, you want to know when the same violating message was synchronized by more than 10 users.</p>
Top Matches	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	Select the size of incidents to display. You can display incidents greater than a certain size (in KB), or between 2 sizes.
Transaction Type	Display only incidents of a certain type, then select the types: email, calendar event, or tasks.
Violation Triggers	<p>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.</p> <p>Note that complex filters can affect performance.</p>

Discovery filters

Filter	Description
Action	View only incidents with no action or specific actions (for example, Applied a file label).
Assigned 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 Forcepoint Security Manager. Assigned to selected administrators enables you to select specific administrators whose assigned incidents you want to display.
Channel	Limit which channels' incidents are displayed in the report. The list of available channels depends on channels configured in the Security Manager. Email Direction is available only for those with the Forcepoint Email Security module, endpoint agent, or protector.

Filter	Description
Content Classifier Name	Select which specific content classifiers should be displayed in the incident list.
Content Classifier Type	Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.).
Current Labels	Select incidents to display in the report according to the current labels on their files.
Date Accessed	To see when data in violation of policy was accessed, use this filter, then select dates and times. Display incidents for data accessed within the last x days, within a date range, or on exact dates. It is also possible to specify time periods.
Date Created	To see when a file in violation of policy was created, use this filter, then select dates and times. Display incidents for data created within the last x days, within a date range, or on exact dates. It is also possible to specify time periods.
Date Modified	To see when a file in violation of policy was modified, use this filter, then select dates and times. Display incidents for data modified within the last x days, within a date range, or on exact dates. It is also possible to specify time periods.

Filter	Description
Detected by	Set the incident list to display only incidents that were detected by specific Forcepoint DLP modules. Select each module of interest. The list of available modules depends on which modules configured on the System Modules page.
Discovery Task	Select the discovery tasks to display in the report.
Discovery Type	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.
Endpoint Type	Filter incidents according to the type of endpoint client, e.g., laptop or static device.
Event Time	Select incidents by the date and time the policy engine first saw the transaction. For filter properties, select one of the following:
	<ul style="list-style-type: none"> ■ Last nn days - Select the number of days from the spinner. ■ Time period - Select the range from the drop-down list. Example: last 24 hours or this week. ■ Exact dates - Select the From and To dates from the drop-down lists.
File Labeling Status	View incidents with specific labeling status(es), e.g., Labeling succeeded or Partially labeled.
File Name	Filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click Add . Continue until all required files have been added. Note that complex filters can affect performance.
File Owner	Filter incidents by file owner. Type a valid owner name into the field box, then click Add .

Filter	Description
File Permissions	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 Add . The values apply to all file-system scanning and Windows shares. Split multiple rows by commas and single rows by colons. For example: Unix user\ramon:rwx,Unix Group\developers:r-x,\Everyone:r--
File Properties	Select file properties to include in the report (for example, Protected by Microsoft Information Protection and Marked by Microsoft Information Protection).

Filter	Description
File Size	Filter incidents by file size, then choose the size of the file to include in the report.
Folder	View incidents from a certain folder or folders. Type a valid folder name into the field box, then click Add .
Folder Owner	Filter incidents by folder owner. Type a valid owner name into the field box, then click Add .
History	<p>Filter incidents by the date, administrator, or details contained on the incident History tab. For example, display all incidents that jdoe closed during March 2017.</p> <ul style="list-style-type: none"> ■ Select Filter by date to specify the date and time of the actions that were taken. Only actions during this period are included in the report. Select a date range and time of day. ■ Select Filter by administrator to specify the administrator who performed the listed workflow action. Enter the administrator name or names. Separate multiple names by commas. For example: Type "jdoe, bsmith" to view incidents that jdoe and bsmith acted on. ■ Select Filter by details to specify 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. <p>Enter the text for which to search. It is possible to search for all or part of the detail text. For example, enter "closed" to search for incidents that were closed during a certain period.</p> <p>As always, this filter depends on the other filters that have been selected, such as Incident Time and Ignored Incident. To filter only by history, define a large range for Incident Time, then define the history filter.</p> <p>Note that complex filters can affect performance.</p>
Host Name	Filter incidents by the host on which they were detected. Type a valid hostname into the field box, then click Add .
Ignored Incident	Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.

Filter	Description
Incident Tag	<p>Filter incidents by a previously defined tag (see Tagging incidents). Select the tags by which to filter the report and click Add. Continue until all required tags have been added.</p> <p>Use these tags to group incidents for external applications. Note that complex filters can affect performance.</p>
Filter	Description
Incident Time	<p>Filter incidents by the date and time they were written to the database. Select the time for the incidents to display.</p>
IP Address	<p>Filter incidents by the host on which they were detected. Type a valid IP address into the field box, then click Add.</p>
Labeled by DLP	<p>Select incidents to display in the report according to the labels that were added to their files by DLP.</p>
Locked	<p>Use this filter to show incidents that are locked or unlocked. There are two options:</p> <ul style="list-style-type: none"> ■ Show only locked incidents (and not unlocked incidents) ■ Exclude locked incidents (and show only unlocked incidents) Disable the filter to display both locked and unlocked incidents. <p>Locking an incident prevents it from being overwritten with new data in subsequent scans. (To lock an incident, choose Workflow > Lock in the Discovery incident report.)</p>
Mailbox Type	<p>This filter applies only to Exchange discovery.</p> <ul style="list-style-type: none"> ■ Select Private mailbox to display incidents from private mailboxes. ■ Select Public mailbox to display incidents from public mailboxes. Both can be selected at the same time.
Policy	<p>Use the check boxes provided to set which policy's incidents are displayed in the incident list.</p>
Previous Labels	<p>Select incidents to display in the report according to the labels that were on their files before the DLP action.</p>
Rule Name	<p>Filter incidents by the rules they triggered.</p>
Severity	<p>Select the severity of incidents to display. Select High to display incidents of high severity, and so on. Select as many severity levels as desired.</p>

Filter	Description
Status	Select which incidents to show by their status—for example, New, Closed, In Process, False Positive, or Escalated. It is not possible to filter by statuses that have been deleted from the system.
Top Matches	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	Select the size of incidents to display. Display incidents greater than a certain number of KB, or between x KB and y KB.
Violation Triggers	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.

Related concepts

[General tab on page 42](#)

[Table Properties tab on page 60](#)

[Selecting items to include or exclude in a policy on page 122](#)

Related tasks

[Tagging incidents on page 81](#)

Table Properties tab

Use the **Table Properties** tab of the **Report Catalog Edit Report** page to configure which columns appear in the report, and assign a width to each.

- 1) Use the check boxes to the left of the page to select the columns to display in the table for this report. The options vary depending on the type of table. See:
 - [Data Loss Prevention properties](#)
 - [Mobile Device properties](#)
 - [Discovery properties](#)
- 2) Use the arrows to the right of the page to adjust the order of the columns.
- 3) Use the fields in the Width column to adjust the width of each column as needed.
- 4) At the bottom of the page, specify the **Maximum number of incidents** to display on any one page.
- 5) Select a column name from the **Sort by** drop-down list to define which column is used to sort the table.
- 6) Indicate if you want to sort in ascending or descending order.

Data Loss Prevention properties

Column	Description
Action	The action taken on the incident, as determined by the action plan.
Analyzed by	Displays the name of the server component that analyzed the incident.
Assigned to	Either Unassigned or the name of the administrator assigned to handle this incident. (See <i>Assigning incidents</i> .)
Channel	The channel where the incident occurred. Possible channels include: <ul style="list-style-type: none"> ■ Email ■ Web ■ FTP ■ Endpoint application ■ Endpoint printing ■ Network printing
Destination	The intended destination or destinations of the content that violated policy.
Details	Details about the incident. Shows the subject in an SMTP incident, the URL in a Web incident, etc.

Column	Description
Detected by	Displays the name of the Forcepoint DLP device or component that detected this incident.
Endpoint type	The type of endpoint involved in the incident: PC, laptop, etc.
Email direction	This column displays the direction of the email message that triggers an incident: <ul style="list-style-type: none"> ■ Inbound ■ Outbound ■ Internal If you are using the Forcepoint Email Security module, endpoint agent, or protector to monitor email, then all 3 directions are possible.
Event ID	Unique number assigned to an event. An event is created for any transaction that traverses the Forcepoint DLP system.
Event time	The date and time the policy engine first saw a transaction.
File name	The name and size of the attachment for this incident.

Column	Description
ID	Unique number assigned to an incident. An incident is an event that violates a policy.
Incident Tag	Displays any incident tag set for the incident. (See <i>Tagging incidents</i> .)
Incident Time	The time and date the incident was written to the database.
Policy	The policies that were violated by the content.
Severity	The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incident's severity (see <i>Changing incident severity</i>).
Source	The source of the incident. Could be a person, computer, or other.
Status	<p>The status of the incident. For example:</p> <ul style="list-style-type: none"> ■ New ■ In process ■ Closed ■ False Positive ■ Escalated <p>You can also add and filter by up to 17 custom statuses. See <i>Changing incident status</i>.</p>
Top Matches	The maximum number of violations triggered by any given rule in the incident.
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

Column	Description
Action	The action taken on the incident, as determined by the action plan.
Analyzed by	Displays the name of the server component that analyzed the incident.
Assigned to	Either Unassigned or the name of the administrator assigned to handle this incident. (See <i>Assigning incidents</i> .)
Destination	The intended destination or destinations of the content that violated policy.
Details	Details about the incident. Shows the subject in an SMTP incident, the URL in a web incident, etc.

Column	Description
Detected by	Displays the name of the Forcepoint DLP device or component that detected this incident.
Email direction	<p>This column displays the direction of the email message that triggers an incident:</p> <ul style="list-style-type: none"> ■ Inbound ■ Outbound ■ Internal <p>If you are using the Forcepoint Email Security module, endpoint agent, or protector to monitor email, then all 3 directions are possible.</p>
Event ID	The ID number assigned to the event or transaction.
Event time	The date and time the policy engine first saw a transaction.
File name	The name and size of the attachment for this incident.
ID	The incident's unique ID number.
Incident Tag	Displays any incident tag set for the incident. (See <i>Tagging incidents</i> .)
Incident Time	The time and date the incident was written to the database.
Policy	The policies that were violated by the content.
Severity	The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incident's severity (see <i>Changing incident severity</i>).
Source	The source of the incident. Could be a person, computer, or other.
Status	<p>The status of the incident. For example:</p> <ul style="list-style-type: none"> ■ New ■ In process ■ Closed <p>You can also add and filter by up to 17 custom statuses. See <i>Changing incident status</i>.</p>

Column	Description
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 to more than 10 phones or iPads.
Top Matches	The maximum number of violations triggered by any given rule in the incident.
Total size	The total size of the file or attachment involved, if any, in megabytes.
Violation Triggers	The information that created the breach.

Discovery properties

Column	Description
Action	The action taken on the incident, as determined by the action plan.
Additional action	Additional executed actions, such as remediation scripts or notifications.
Analyzed by	Displays the name of the server component that analyzed the incident.
Assigned to	Either Unassigned or the name of the administrator assigned to handle this incident. (See <i>Assigning incidents</i> .)
Channel	The channel where the incident occurred. Possible channels include: <ul style="list-style-type: none"> ■ Email ■ Web ■ FTP ■ Endpoint application ■ Endpoint printing ■ Network printing
Current labels	The labels on a file after a labeling action.
Details	The details listed in the forensics Properties tab. Shows the subject in an SMTP incident, the URL in a Web incident, etc.
Detected by	Displays the name of the Forcepoint DLP device or component that detected this incident
Discovery task	The discovery task that identified the incident.
Discovery type	The type of resource that was scanned: File System, Endpoint, SharePoint, SharePoint Online, Database, Exchange, Exchange Online, and/or Outlook PST.

Column	Description
Endpoint type	The type of endpoint involved in the incident: PC, laptop, etc.
Event ID	The ID number assigned to the event or transaction.
Event time	The date and time the policy engine first saw a transaction.
File extension	The file extension of the file that violated a policy. For example: docx or pptx.

Column	Description
File full path	The full directory path of the file that violated a policy.
File labeling status	<p>The status of a labeling action, which can be one of the following:</p> <ul style="list-style-type: none"> ■ Labeling succeeded - All labels were successfully applied to the file. ■ Labeling failed - No labels were successfully applied to the file. ■ Partially labeled - Some labels were successfully applied and some were not, because of an error or labeling system guidelines (for example, only a higher-priority label can be applied). ■ File was not labeled - Labels were not applied either because the label already exists on the file, or because of labeling system guidelines (for example, only a higher-priority label can be applied). <p>Relevant only for endpoint discovery.</p>
File properties	Additional file properties. For example, files protected by Microsoft Information Protection can have “Marking” or “Protection” properties.
Sharing status	Indicates whether the file was shared internally or externally.
Shared with	Indicates whether the file was shared with everyone or with a list of users.
File name	The name of the file that violated a policy.
File owner	The owner of the file that violated a policy.
File owner's email address	The email address of the owner of the file that violated a policy.
File type	The type of the file that violated a policy.
File size	The size of the file that violated a policy.
Folder	The folder of the file that violated a policy.
Hostname	The name of the host on which the violation was detected.

Column	Description
ID	The incident's unique ID number.
Ignored incident	The incidents marked as ignored.
Incident Tag	Displays any incident tag set for the incident. (See Tagging incidents)
Incident Time	The time and date the incident was written to the database.
IP address	The IP address of the host on which the violation was detected.
Labeled by DLP	Labels applied to a file by Forcepoint DLP.
Locked	Indicates whether the incident is locked or unlocked. Locking an incident prevents it from being overwritten with new data in subsequent scans. (To lock an incident, choose Workflow > Lock in the Discovery incident report.)
Policy	The policies that were violated by the content.
Previous labels	The labels that were on a file before a labeling action.

Column	Description
Severity	The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incident's severity (see Changing incident severity).
Status	The status of the incident. For example: <ul style="list-style-type: none"> ■ New ■ In process ■ Closed ■ False Positive ■ Escalated You can also add and filter by up to 17 custom statuses. See Changing incident status .
Top Matches	The maximum number of violations triggered by any given rule in the incident.
Violation Triggers	The information that created the breach.

Related concepts

[Filter tab](#) on page 42

[General tab](#) on page 42

Related tasks

- [Assigning incidents](#) on page 77
- [Tagging incidents](#) on page 81
- [Changing incident severity](#) on page 80
- [Changing incident status](#) on page 78

Scheduling tasks

Use the **Report Catalog > Scheduled Tasks** page to view a list of scheduled tasks you've created or to schedule a new task.

To open the Scheduled Tasks page, go to the data loss prevention, mobile devices, or discovery report catalog page in the Forcepoint Security Manager and click **Scheduled Tasks** in the toolbar at the top of the content pane.

The task list shows 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. See *Scheduling a new task*.
- Click **Delete** to delete the selected task.
- Click **Run** to initiate the selected task now (regardless of its schedule), then confirm that you want to run the report.

Related concepts

- [Scheduling a new task](#) on page 67

Scheduling a new task

Use the **Reporting > Data Loss Prevention / Mobile Devices / Discovery > Report Catalog > Scheduled Tasks > Task Details** page in the Data Security module of the Forcepoint Security Manager to schedule a new task.

Use the 3 tabs to configure basic report information, mail settings for distributing the report, and the schedule to use for running the report.

- 1 On the **General** tab, complete the fields as follows:

Field	Description
Task name	Enter a name for the task you are scheduling.
Enabled	Select Enabled to enable the task for use.
Description	Enter a description for the task.
Report type	Indicate whether you want to email a data loss prevention, mobile devices, or discovery report.
Report name	Select a report from the drop-down list. This is the report that will be emailed on the schedule you define.

Field	Description
Report format	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.

- 2) On the **Mail Settings** tab, complete the fields as follows:

Field	Description
Sender name	Enter the name of the person from whom the report should be sent. This is the name that will appear in the email From field.
Sender email address	Enter the email address of the person from whom the report should be sent.
Outgoing mail server	The outgoing mail server that's been configured appears on screen. To change the server used, see <i>Mail servers</i> . Note that changing this setting changes the configuration for the entire system.
Subject	Type the subject of the message containing the report. This appears in the email Subject: line.
Recipients	Define the recipient(s) for the notification. Click Edit to select to select users or groups from a user directory. Select Additional email addresses if you want to send the report to someone not on your user directory list, then enter the email address. Separate multiple addresses with commas.

- 3) On the **Schedule** tab, complete the fields as follows:

Field	Description
Start	Select the date and time on which to start the schedule. This is the date and time of the Forcepoint DLP Server.

Field	Description
Recurrence	<p>Select this check box to set up a recurrence pattern for the task, then select the pattern:</p> <ul style="list-style-type: none"> ■ 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". <p>Select one of the following options if you specify a recurrence pattern:</p> <ul style="list-style-type: none"> ■ 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.

- 4) After completing your changes, click **OK**.

Related tasks

[Mail servers](#) on page 363

Viewing the incident list

To view a list of data loss prevention incidents from the last 3 or 7 days, and their details:

- 1) In the Forcepoint Security Manager, go to the **Data > Main > Reporting > Data Loss Prevention** page.
- 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*.)

Click the down arrow on column header to sort, filter, or group incidents by that column. (See *Applying a column filter*, for more information.) Or click **Table Properties**  to change the columns that are displayed, their order, and their width. See *Table Properties tab*, for a description of each property.

Use the table 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*, 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.

Related concepts

- [Managing incident workflow](#) on page 76
- [Remediating incidents](#) on page 83
- [Escalating incidents](#) on page 85
- [Managing incident reports](#) on page 86
- [Editing table properties](#) on page 87
- [Applying a column filter](#) on page 87
- [Table Properties tab](#) on page 60

Related tasks

- [Previewing incidents](#) on page 74
- [Tuning policies](#) on page 90

Toolbar buttons

There are several buttons on the incident toolbar:

Button	Icon	Description
Workflow		<p>Click this button to manage the workflow of the selected incident, then select one of the following:</p> <ul style="list-style-type: none"> ■ Assign - Select this option to assign the incident to someone or mark it as unassigned. ■ Lock - Select this option to lock the selected incident, preventing any further changes from future scans of the file. This option applies only to discovery incidents. ■ Unlock - Select this option to unlock a locked incident, allowing information from future scans to overwrite the current data. This option applies only to discovery incidents. ■ Change Status - Select this option to change the incident status or change the status labels. ■ Change Severity - Select this option to change the incident severity assignment. ■ Ignore Incident - Select this option to mark an incident as ignored or unmark an ignored incident. Mark an incident as ignored when you've reviewed it and no action is required. ■ Tag Incident - Select this option to associate an incident with a custom tag that you can later use in filters. ■ Add comments - Annotate the incident. ■ Download Incident - 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. ■ Delete - 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

Button	Icon	Description
		<p>incidents, all incidents that match the filter criteria for the current report, or all incidents.</p> <p>(See <i>Managing incident workflow</i> section for details on all of these options.)</p>
Remediate		<p>Click this button to remediate the selected incident, then select one of the following:</p> <ul style="list-style-type: none"> ■ Release - Select this option to release the selected incidents (email messages) from quarantine. This option applies only to data loss prevention incidents on network, endpoint, and mobile email channels. You can add a comment to the confirmation window for future reference if desired. Not supported for messages detected by Forcepoint Email Security Cloud. ■ Run Remediation Script <ul style="list-style-type: none"> - Select this option to run a remediation script on the selected incident. <p>(See <i>Remediating incidents</i> for details on both options.)</p>
Escalate		<p>Click this button to escalate the selected incident to a manager or other person:</p> <ul style="list-style-type: none"> ■ Email to Manager - Select this option to email the incident to the manager of the person generated the policy breach. ■ Email to Other - Select this option to email the incident to another person for action. <p>(See <i>Escalating incidents</i> for details on both options.)</p>

Button	Icon	Description
Manage Report	N/A	<p>Click this button to edit the filter or table properties applied to the current report, then select one of the following:</p> <ul style="list-style-type: none"> ■ Edit Filter - Select this option to edit the filters applied to the report—for example, choosing a longer time period or single channel. ■ Table Properties - Select this option to customize the properties of the incident table. ■ Save - Select this option to save the changes you made to current report. ■ Save As - Select this option to save the current report with a new name. <p>(See <i>Managing incident reports</i> for details on all of these options.)</p>
Settings		<p>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.</p> <p>For information on configuring these settings, see <i>Setting reporting preferences</i>.</p>

Button	Icon	Description
View		Lets you customize the view in your incident list. You can choose any of the following: <ul style="list-style-type: none"> ■ Incident list only - Removes the preview so that many more incidents can appear in the list. ■ Incident preview only - Removes the list so you can preview more of the incident. ■ Incident list and preview - Displays the incident list and the preview in the same window. Includes scroll bars on the incident list. ■ Open preview in a new window - Opens a preview of the incident in a new window, so you can view it in its entirety.
Print Preview		Display a preview of the current, selected, or all filtered incidents.
Export to PDF		Export the current, selected, or all filtered incidents to a PDF file.
Export to CSV		Export all filtered incidents to a CSV file (incidents from the current report).

To preview an incident and learn more about it, click on the table row of the incident in the Incidents List. See *Previewing incidents* for details on this portion of the window.

Related concepts

- [Managing incident workflow](#) on page 76
- [Remediating incidents](#) on page 83
- [Escalating incidents](#) on page 85
- [Managing incident reports](#) on page 86
- [Setting reporting preferences](#) on page 348

Related tasks

- [Previewing incidents](#) on page 74

Previewing incidents

Details of the selected incident appear at the bottom of the screen. In this preview, you can see:

- *Violations*
- *Forensics*

- [Properties](#)
- [History](#)

Steps

- 1) To see more of the preview, select **View > Incident Preview Only** or **View > Open Preview in New Window**.

Related concepts

[Violations](#) on page 75

[Forensics](#) on page 75

[Properties](#) on page 76

[History](#) on page 76

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.
- **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

If there are more than 500 violation rules or triggers, go to the Forensics tab. There you can see the complete transaction, including violations.

- 1) 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* for more information.

Related tasks

[Tuning policies](#) on page 90

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 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

- 1 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.

- **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.
- **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.)

Related tasks

- [Assigning incidents](#) on page 77
- [Changing incident status](#) on page 78
- [Changing incident severity](#) on page 80
- [Ignoring incidents](#) on page 80
- [Tagging incidents](#) on page 81
- [Adding comments](#) on page 81
- [Downloading incidents](#) on page 82
- [Deleting incidents](#) on page 82

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 another administrator:

- 1) Select one or more incidents. Note that if you want to assign *all* the filtered incidents, there is no need to make any selections.
- 2) From the toolbar, select **Workflow > Assign**.
- 3) Select the **Assign to** option.

- Select **Apply to selected incidents** to apply the action only to the incidents you selected in the list.
 - Select **Apply to all filtered incidents** to apply the action to all filtered incidents in the list.
- 4) Select the **Assign to** option.
- 5) From the drop-down list, select the person to whom to assign the incident.
- 6) Add comments if desired.
- 7) Click **OK**.

To mark an incident as unassigned after it's been assigned:

- 1) Select the incident.
- 2) From the toolbar, select **Workflow > Assign**.
 - Select **Apply to selected incidents** to apply the action only to the incidents you selected in the list.
 - Select **Apply to all filtered incidents** to apply the action to all filtered incidents in the list.
- 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 one or more incidents. Note that if you want to apply the action to *all* the filtered incidents, there is no need to make any selections.
- 2) From the toolbar, select **Workflow > Change Status**.
- 3) Select a new status from the menu.
- 4) Select a **Change Status** option:
 - Select **Selected incidents** to change the status of only the incidents you selected in the list.
 - Select **All filtered incidents** to change the status of all filtered incidents in the list.

There are 5 predefined statuses:

Flag	Label	Definition
	New	An administrator has not acted on this incident yet.
	In Process	An administrator is reviewing this incident.
	Closed	This incident was reviewed and closed by an administrator.
	False Positive	An administrator identified this incident as a false positive or unintended match.
	Escalated	The incident was escalated to a manager or other person.

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 Forcepoint DLP. 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 one or more incidents. Note that if you want to apply the action to *all* the filtered incidents, there is no need to make any selections.
- 2) From the toolbar, select **Workflow > Change Severity**.
- 3) Select a new severity from the menu.
- 4) Select a **Change Severity** option:
 - Select **Selected incidents** to change the severity of only the incidents you selected in the list.
 - Select **All filtered incidents** to change the severity of all filtered incidents in the list.

Possible severities include:

Icon	Definition
	High. This breach is significant and may have a broad impact on the organization.
	Medium. This breach is moderate and should be reviewed.
	Low. This breach is insignificant.

Ignoring incidents

Forcepoint 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 Forcepoint Security Manager does not display ignored incidents. If you no longer want the incident to be ignored, you can unmark it.

To mark or unmark an incident as ignored:

- 1) Select one or more incidents.



Note

If you want to apply the action to all the filtered incidents, skip this step and select the relevant option in a later step.

- 2) From the toolbar, select **Workflow > Ignore Incident**.
- 3) Select **Mark as ignored incident** or **Unmark as ignored incident**, as applicable.

- 4) Select an option:
 - Select **Selected incidents** to mark or unmark only the incidents you selected in the list.
 - Select **All filtered incidents** to mark or unmark of all filtered incidents in the list.
- 5) Click **OK**.

Tagging incidents

Administrators can optionally add a custom tag to an incident. The tag can be used to:

- Search and filter data.
For example, tag all incidents relating to Project ABC with the string “Project ABC”, then later apply a filter with the string “Project ABC” to view all incidents relating to the project.
- Tag incidents to group them together for external applications.

To tag an incident:

- 1) Select one or more incidents.
- 2) From the toolbar, select **Workflow > Tag Incident**.
- 3) Do one of the following:
 - Select **Apply to selected incidents** to apply the action only to the incidents you selected in the list.
 - Select **Apply to all filtered incidents** to apply the action to all filtered incidents in the list.
- 4) Enter the desired text string into the **Incident tag** field.
- 5) Add comments if desired.
- 6) Click **OK**.

Adding comments

To include notes in an incident’s history, add comments:

- 1) Select one or more incidents.
- 2) From the toolbar, select **Workflow > Add Comments**.
- 3) Do one of the following:
 - Select **Apply to selected incidents** to apply the action only to the incidents you selected in the list.
 - Select **Apply to all filtered incidents** to apply the action to all filtered incidents in the list.
- 4) Enter the notes in the **Comments** field.
- 5) Click **OK**.

To view an incident's history, select the incident and click the **History** tab. Expand a row to see comments and workflow details.

Downloading incidents

To download incident details:

- 1) Select the incident.
- 2) From the toolbar, select **Workflow > Download Incident**.
- 3) When prompted, click **OK** to confirm the action.

Deleting incidents

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) From the **Reason** menu, select a reason for the action.
- 4) Click **OK** to confirm the action.

To delete all report incidents:

- 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) From the **Reason** menu, select a reason for the action.
- 4) 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

Click this button to remediate the selected incident, then:

- Select **Release** to release selected email incidents from quarantine.
- Select **Run Remediation Script** to run a remediation script on the selected incident.

Related concepts

[Releasing incidents on page 83](#)

Related tasks

[Running remediation scripts on incidents on page 84](#)

Releasing incidents

This option is only available for blocked incidents sent from the protector or Forcepoint Email Security module—that is, for email transactions that have been quarantined. It is not supported for Forcepoint Email Security Cloud.

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. The quarantined email must be released within 1 week. After that, the message expires and can no longer be released.

All messages are released through the configured release gateway. You configure the release gateway at **Settings > General > Remediation**. By default, the release gateway is the agent that delivered the message to the policy engine for analysis (the protector MTA or Forcepoint Email Security).

There are 2 ways to release an incident: *From the Incident Details report* or *By replying to the notification message*.

Related concepts

[By replying to the notification message on page 84](#)

Related tasks

[From the Incident Details report on page 83](#)

From the Incident Details report

Steps

- 1) Select the incident or incidents you want to release.
- 2) From the toolbar, select **Remediate > 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**.

Next steps

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 > 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 *Releasing email blocked by Forcepoint DLP* on the Forcepoint support site 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 Forcepoint DLP, 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**.

Related concepts

[Remediation scripts on page 269](#)

Related tasks

[Adding a new remediation script on page 271](#)

Escalating incidents

Related topics:

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** sends the incident to the manager of the person who violated policy.
- **Email to Other** sends the incident to another person for action. For discovery incidents, you have the following option:
- **Email Incident** sends the incident to the person of your choice.

Related tasks

[Emailing incidents to the manager of the person who generated the incident](#) on page 85

[Email incidents to another](#) on page 86

Emailing incidents to the manager of the person who generated the incident

Steps

- 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.

Next steps

If you want to send a copy or blind copy to other people, enter their email addresses in the **Cc** and **Bcc** fields.

- 1) 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.
- 2) Select **Include original message as an attachment** if you want to attach the message.
- 3) Select **High importance** if this is a priority message.
- 4) Edit the predefined message body as desired. Click the right arrow to choose variables to include, such as %Incident Time% or %Severity%.
- 5) Click **OK**.

The selected incidents are immediately emailed to the manager.

Email incidents to another

If you want to send an incident to someone other than a predefined manager, you can do so.

- 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%.

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 then select:

- **Edit Filter** to edit the filters applied to the report—for example, choosing a longer time period or single channel.
- **Table Properties** to customize the properties of the incident table.
- **Save** to save the changes you made to the current report.
- **Save As** to save the current report with a new name.

Related concepts

[Editing table properties on page 87](#)

[Applying a column filter on page 87](#)

[Editing report filters on page 87](#)

Related tasks

[Saving reports](#) on page 89

Editing report filters

**Note**

You can also apply a filter by selecting the right arrow on a column header in the incident table and selecting **Filter by [column]**. (See *Applying a column filter* for more information.)

To change the filters that are applied to this report, select **Manage Report > Edit Filter**. See *Filter tab* for instructions on selecting filters and defining filter properties.

Related concepts

[Applying a column filter](#) on page 87

[Filter tab](#) on page 42

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* 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.

Related concepts

[Table Properties tab](#) on page 60

Applying a column filter

The column filter enables you to apply filters directly to the incident list without accessing the Manage Report menu to build a custom screen.

Column filters further filter the data provided in the incident list. This means that the column filter is applied on top of the main filter—the one created with the **Manage Report > Edit Filter** option.

For example: If the main filter is set to display only SMTP channel incidents, and the column filter is then set to display severity - high, only high severity SMTP incidents

are displayed. Column filters are not saved, so when a custom filter is applied, the column filter that was applied before it is lost.

Selecting the **Clear Column Filter** option clears the applied column filter and applies the selected main filter.

Arrow buttons on column headers enable users to quickly filter the displayed information. Below are instructions of how to filter the information in the columns.

To filter columns:

1) Click the down arrow button in a column header. A drop menu with 5 options appears. Different columns display different options.

2) Select from one of the following options:

Option	Description
Sort Ascending	Sorts the column's entries by A-Z, from top to bottom.
Sort Descending	Sorts the column's entries by Z-A, from top to bottom.
Group by this Column...	<p>Incidents in the incident list screens can be grouped, allowing an alternative filtered report.</p> <p>Grouping incidents enables deep drill down into a problem. For more information, refer to <i>Grouping incidents</i>.</p>
Filter by this Column...	<p>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.</p> <p>In most cases, you can select one of the following options in the Must field:</p> <ul style="list-style-type: none"> ■ 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). <p>The results are displayed in the column with or without the specific words in the column.</p> <p>Note: When a column is filtered, the header arrow turns blue.</p>
Clear Column's Filter	When this option is selected, all current and previous filters set for the column are cleared.

Related concepts

[Grouping incidents on page 89](#)

Saving reports

Steps

- 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](#), for additional information.

Related concepts

[Applying a column filter on page 87](#)

Deleting incidents

Only discovery incidents can be deleted. To delete one or more selected incidents:

- Do one of the following:
 - Locate an incident and mark the check box to its left.
 - Use the display and column filters to display only the incidents you want to delete, then select them all.
- 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

To view or print incidents, administrators can:

- View a Print Preview
- Export the incident to a PDF file
- Export the incident to a CSV file, then import the CSV into your favorite program 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**.

Here's an example of what an incident report looks like:

The screenshot shows a PDF document titled "Data Loss Prevention - Incidents (last 7 days)". It includes a header with the Forcepoint DLP logo, creation date (31 May, 2017), and generator (admin). A "Report Filter" section shows settings for ignoring incidents and filtering by the last 7 days. The main content is a table of incident details:

ID:	230815		
Severity:	<input checked="" type="radio"/> Medium	Status:	<input checked="" type="checkbox"/> New
Action:	Permitted	Event time :	2017-05-31 10:03:34
Channel:	<input checked="" type="checkbox"/> Network email	Incident time:	2017-05-31 10:03:34
Assigned to:	Unassigned	Total matches:	0
Incident tag:	N/A		
Detected by:	Protector on BBPtester		
Analyzed by:	Policy Engine BBPtester		
Source:			
Email address:	ranger@qaexch01.com		
Destination:			
Email Direction:	Outbound		
Email address:	test@spin.com		
Action Taken:	Permitted		
Attachments:	test.docx(30.7 KB)		
Transaction Size:	43.08 KB		

To configure how incidents are grouped when exported to PDF, see [Setting general reporting preferences](#).

Related tasks

[Setting general reporting preferences](#) on page 349

Tuning policies

At first, some of the incidents reported may not be useful. Use this information to fine-tune policies and rules to better suit the needs of the organization.

To tune a policy based on an incident:

Steps

- 1) Go to the Main > Reporting > Data Loss Prevention or Discovery page.
- 2) From Recent Reports, select **Incidents (last 3 days)**.
- 3) Select an incident. Its details are displayed in the bottom section of the page.
- 4) Click the **Tune Policy** button on the left side of the incident details toolbar.
- 5) Select one of the following options:
 - *Excluding source from rules*
 - *Disabling policies*
 - *Disabling rules*

Related concepts

[Excluding source from rules](#) on page 91

[Disabling policies](#) on page 91

[Disabling rules](#) on page 92

Excluding source from rules

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

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

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 deselect **Enabled** for the desired attributes.

Data Loss Prevention reports

A catalog of all available DLP reports can be found on the **Main > Reporting > Data Loss Prevention > Report Catalog** page.

Click a folder to expand it and see a list of related reports. Click **Run** to generate the report.

The most common reports are described below.

Incident List

Incidents (last 3 days, last 7 days, or last 30 days)	<p>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 Forcepoint software. Evaluate whether policy changes are needed.</p> <p>Select this report when to manage incident workflow, remediation, and escalation.</p> <p>It is also possible to view Incidents by Severity, which shows detailed information about each incident, ranked in severity order.</p>
---	--

Executive Dashboard

DLP Dashboard (last 7 days, current quarter, previous quarter)	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.
--	--

Risk Assessment

Top Violated Policies	<p>Find out which policies were violated most frequently over the last 7 days. Assess the security risk to your organization.</p> <ul style="list-style-type: none"> ■ Last 7 Days shows which policies were violated most frequently over the last 7 days. ■ Leaks to Removable Media Devices shows which policies users are violating when they copy confidential information to removable devices. <p>Note: Users can see only those policies for which they have authorization.</p>
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.
Incident Risk Ranking - Top Cases	<p>Shows up to 20 cases with the highest risk scores during the selected time period, along with details for those cases.</p> <p>Requires the Forcepoint DLP analytics engine on a Linux machine.</p>
My Cases	Shows the cases that you have flagged for later reference. Requires the Forcepoint DLP analytics engine on a Linux machine.

Severity & Action

Violations by Severity & Action	<p>See incidents by the actions (permit, block, notify) and severities applied to them. Compare the ways Forcepoint software enforces policies, and gain insight into potential policy changes.</p> <ul style="list-style-type: none"> ■ Last 7 Days shows incidents by the actions (permit, block, notify) and severities from the last 7 days. ■ Credit Card Violations shows credit card-related incidents by the actions and severities applied to them. ■ Violations of Personally Identifiable Information (PII) shows PII incidents by the actions and severities applied to them.
---------------------------------	---

Sources & Destinations

<p>Top Sources & Destinations</p>	<p>Find out who are the top violators involved in data leakage and the top domains where sensitive data was posted.</p> <ul style="list-style-type: none"> ■ Last 7 Days shows 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 shows the top violators involved in leaking data to public email websites and the top domains of those websites. ■ Leaks to Malicious Web Sites shows the top violators involved in leaking data to malicious websites and the top domains of those websites. ■ Credit Card Number Violations shows who attempted to leak credit card information in plain text and the top destinations to which this information was leaked. ■ PII Violations shows who violated a PII policy and the top destinations to which PII information was leaked. ■ PCI Violations shows who violated a PCI policy and the top destinations to which PCI information was leaked.
--	--

Trends

<p>Incident Trends (current and previous quarter)</p>	<p>View incident statistics for this quarter. Find out if the number of violations in your organization reduces over time.</p>
---	--

Status

<p>Incident Status (last 7 days)</p>	<p>View the status of all DLP incidents from the last 7 days.</p>
--------------------------------------	---

Geographical Location

<p>Web DLP - Destinations by Severity</p>	<p>View the destinations of the most severe outbound web incidents, by geographical region.</p>
---	---

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 Forcepoint DLP reports, you can view the dashboard any time or create a scheduled task to receive it periodically via email.

To access the dashboard:

Steps

- 1) Select Main > Reporting > Data Loss Prevention or Discovery.
- 2) From the report catalog, select Executive Dashboard.
- 3) Remember that all reports represent only incidents from to which the administrator has access.
- 4) Click Run to generate the report.

Next steps

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 for more details.)

To schedule this report to be delivered by email, see *Scheduling tasks*.

Related concepts

[Managing incident reports](#) on page 86

Related tasks

[Scheduling tasks](#) on page 67

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:

Steps

- 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.



Note

Users can see only those policies they are authorized to access.

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:

Steps

- 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, Deep Web URLs, and Email to Competitors, among others.
- Indicators of compromise policies include Suspected Malware Communication, Suspected Malicious Dissemination, and Password Files, among others.
- Employee discontent policies include Disgruntled Employee and CV and Resume in English, among others.

For details about the policies used to populate the report, see [Data Loss Prevention policies](#).

Users who violate these policies could pose a security risk to the organization.

This report contains the user's full name, login name, department, manager, title, and business unit, if available.

It also shows incident counts by severity. To view the report:

- 1) Go to the Main > Reporting > Data Loss Prevention > Report Catalog page.

- 2) Expand the Risk Assessment folder (if needed), then select **User Risk Summary (Data Theft Risk Indicators)**.
- 3) Click **Run** to generate the report.

Incident risk ranking

Cases are groups of related incidents that combined, indicate a risk to the organization—for example, incidents of data being sent to suspicious destinations or incidents occurring outside normal office hours.

Cases are assigned risk scores by a sophisticated, Linux-based analytics engine.

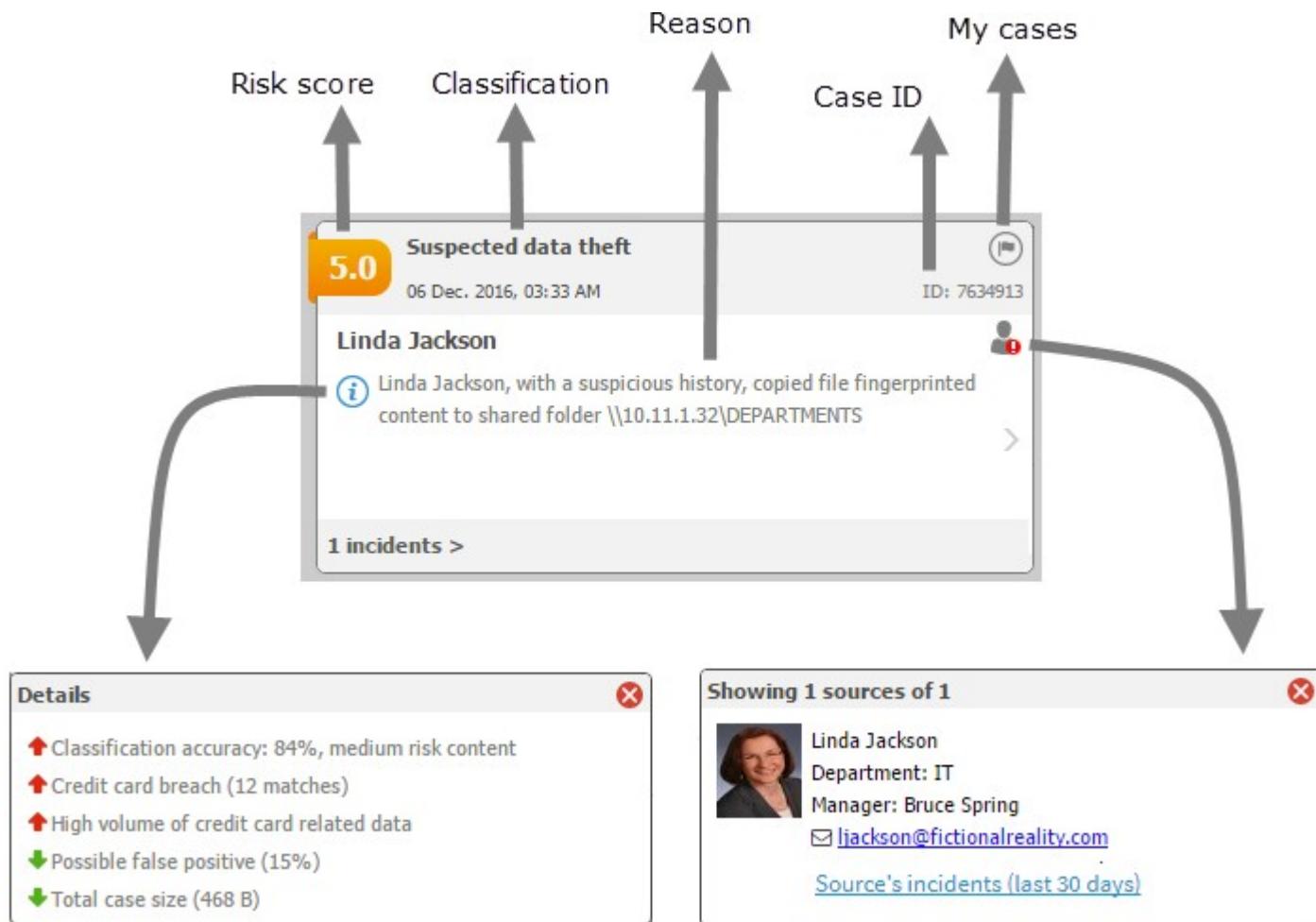
- The analytics engine is required to enable Incident Risk Ranking reports.
- After processing incidents, the analytics engine groups incidents from the same user that have the same classification to ensure that they are combined into the same case (and card), reducing the number of cases for investigators to review.
- Incidents within cases are ranked according to their number of matches, transaction size, content, breached policies and rules, date and time, and more.

For information on the analytical and statistical techniques used to rank and score incidents, see *Risk-Based DLP Incident Ranking* on the Forcepoint support site.

The Incident Risk Ranking report shows the cases with the highest risk scores during the specified time period, along with details for those cases. Specify the threshold for displaying cases on the **Settings > General > Reporting > Incident Risk Ranking** page in the Data Security module of the Security Manager. Up to 20 cases are shown. (See *Setting reporting preferences*.)

Only administrators with **Summary reports** permissions can view Incident Risk Ranking reports.

In Incident Risk Ranking reports, each case is represented by a card:



Cards show the following information:

- The **Risk score** assigned to the case, between 0 (lowest risk) and 10 (highest risk).

This score is derived by the analytics engine and can be used to assess the security risks in your organization. Scores are based on data accumulated over time. An incident with a score of 2.5 may not pose a high-risk on Monday, but when combined with other incidents from the same source over the week, it might be assigned a higher score. The sample case shows a risk score of 5.0.

See *What factors affect risk scoring?*, for more information about factors that influence the risk score.

- The **Classification** is one of the following:
 - Suspected data theft** - the incidents in this case may indicate an attempt to steal sensitive data. This is based on factors and indicators such as behavioral anomalies, user and system profiling, the sensitivity of the data, and the destination of the transaction.
 - Possibly broken business process** - the incidents in this case may be the result of business process deficiencies. For example, if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong. This classification is based on factors such as recurring patterns that could indicate common behavior.
 - Uncategorized (unknown)** - the incidents in this case do not fall into another classification.
- The **date and time** the case was opened is displayed under the classification. To see incident risk cases for other dates, use the time line shown above the case cards. Click a date to display incidents that occurred on that date. Use the scroll bar to see incidents for the previous week. The time line also shows the number of incidents scoring above the selected threshold each day. The picture below shows that there were 16 incidents above the threshold today (Monday).



- The **case ID** is a unique numeric identifier.

- Click the **My Cases** flag () to add a case to, or remove a case from, a personal case list.

Each administrator can have up to 200 cases in his or her My Cases list.

- The **source** that originated the incidents in the case: a person or machine and the LDAP role, if available.
 - Click the source icon to view a picture of the source, if available, along with details such as email address, phone number, manager, and in the case of computers, IP address and hostname.
 - Sources that are part of a high-risk resource list are indicated by an exclamation mark.
 - In the source pop-up window, click the **Source's incidents...** quick link to open a report showing incidents associated with the selected source over the last 30 days.
- The **reason** the case is included in the report. For example:

jbrown@gmail.com sent credit card and other sensitive content (almost 300 matches) to 3 common email addresses.

- To view case **details**, click the information () icon on the card.

Some detail descriptions show classification accuracy. Red up arrows flag indicators that increase a case's risk score. Green down arrows flag indicators that lower the risk score.

- Use the next/previous page () icons to see the next page of the card for more details.

The content varies by case. The second page shows the source and destinations relevant to the case (those that pose a risk) and any files that are involved.

- The **number of incidents** in the case are shown as a link on the bottom of the card.

Click this link to drill down to the current Incidents report, filtered according to the case, so you can investigate the incidents further. Under the link is a date range showing when the incidents occurred.

Related concepts

[What factors affect risk scoring?](#) on page 100

[Setting reporting preferences](#) on page 348

Toolbar

The toolbar at the top of the report offers access to the following additional features and functions:

- My Cases** shows the cases that you (the currently logged-on administrator) have flagged.
- Settings** opens the **Settings > General > Reporting** page, used to configure reporting preferences such as risk score threshold—for example, show only cases exceeding a score of 8.0.
- Export to PDF** exports all of the cases that are currently displayed to PDF.

What factors affect risk scoring?

Many factors and indicators contribute to the risk score displayed in the incident risk ranking reports. This section introduces some of the score's main components.

Impact

The **impact** of a case represents the potential damage of the breach, and is evaluated directly from the case's breached classifiers. The impact is used as a multiplier to increase the risk score. For example, a 20% increase in impact results in a 20% increase in risk score.

Marking a source as a privileged account increases the impact value, as breaches from privileged accounts may comprise highly sensitive information or evolve into a high-profile breach.

Risk indicators

Various indicators are used to assess the case's classification as active data theft, broken business process, false positive, and so on. The indicators take into account such factors as the user's history, statistics, the reputation of the destination, and the type of content, among others.

An active data theft case conveys the highest risk and requires urgent action.

High-risk users

Marking a source as a high-risk user affects the **data-theft probability**, but not the impact.

Cases with a high-risk user as the source have a higher data-theft probability.

My cases

This report shows the cases that you have marked with a flag for later reference. This is the same list that appears when you click **My Cases** on the Top Risks report toolbar.

Use My Cases as a temporal workbench area for tracking cases that you're working on.

This report can show all cases that you have flagged or only those from a specific date. Use the date filter in the filter pane to select which.

The screenshot shows a report interface with the following details:

- Header:** Dashboard > Incident Risk Ranking - Top Cases > My Incident Risk Ranking Cases
- Description:** Shows the cases that you have flagged for later reference.
- Filter Pane:**
 - All** (radio button selected)
 - Mon, 26 Sep 2016** (date filter)
 - 1 Cases**
 - Score 4+**

Your account must have a role with **Summary reports** permissions to view the My Cases report.

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.

Steps

- 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 Forcepoint DLP due to breach of policy or those who were most frequently meant to receive unauthorized information.

Steps

- 1) Go to the Main > Reporting > Data Loss Prevention page.
- 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 Forcepoint DLP 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) Go to the Main > Reporting > Data Loss Prevention page.
- 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

Forcepoint DLP can monitor or restrict data being sent via the Web to specific countries. Geolocation reports display incidents by the geographical location to which data was sent.

Use the **Main > Reporting > Data Loss Prevention** page in the Data Security module of the Forcepoint Security Manager to access geolocation reports:

- 1) From the report catalog, expand the **Geographical Location** folder.
- 2) Select **Web DLP - Destinations by Severity**.
- 3) Click **Run** to generate the report.

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.

Geographical Location: Web DLP - Destinations by Severity

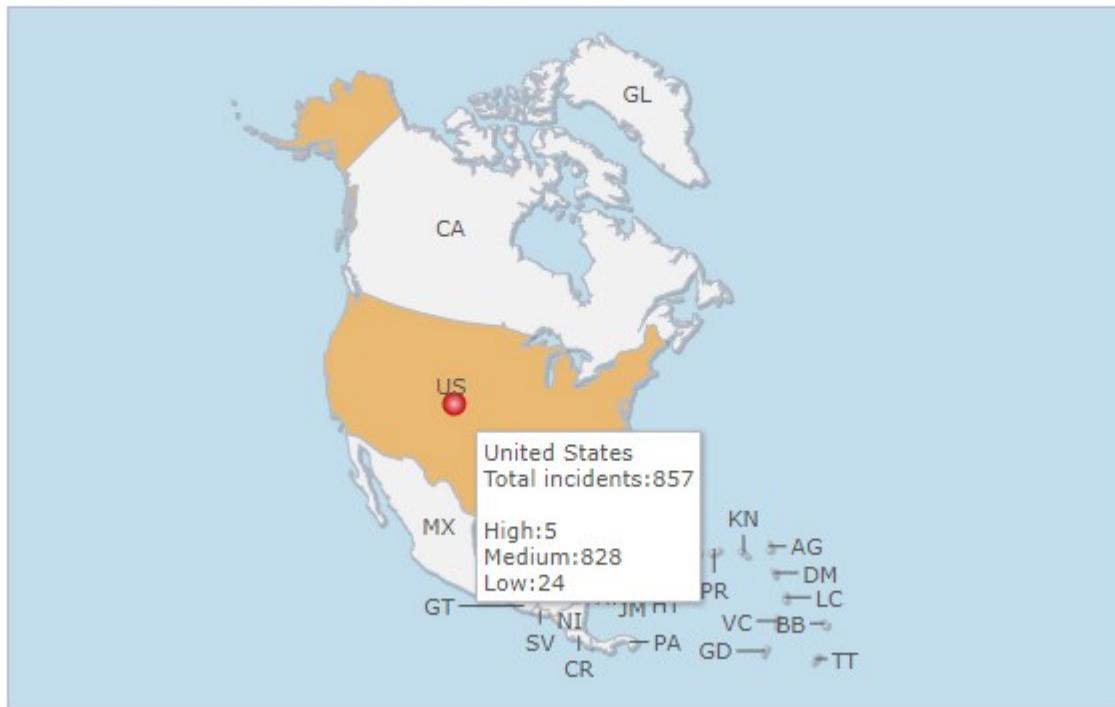
Shown are the destinations of the most severe Web DLP incidents by geographical region. Hover over a region to view details; click to drill down for more information.



- 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.
- 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.

Geographical Location: Web DLP - Destinations by Severity

Shown are the destinations of the most severe Web DLP incidents by geographical region. Hover over a region to view details; click to drill down for more information.



- 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 restrict data from being sent to specific countries:

- Add geographical locations to a policy's Destination page:
 - Go to the **Main > Policy Management > Manage Policies** page and open or create a custom policy.
 - On the Destination page, under Web, click **Edit**.
 - 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

Use the **Main > Reporting > Mobile Devices > Report Catalog** page to see a catalog of all reports—both built-in and user-defined—that are available for mobile devices:

Report	Description
--------	-------------

Incident List

Mobile Incidents (last 3, 7, or 30 days)	<p>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.</p> <p>See detailed information on each incident. Investigate the violated policies and the actions taken by Forcepoint software. Evaluate whether policy changes are needed.</p> <p>Select this report when you want to manage incident workflow, remediation, and escalation.</p> <p>See <i>Viewing the incident list</i>, for an explanation of how to read and customize reports like this one.</p>
--	---

Risk Assessment

Top Violated Mobile Policies	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.
Top Synced Messages (last 7 days)	<p>Find out the messages that were synchronized to mobile devices most frequently.</p> <p>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.</p>

Severity & Action

Mobile PII Violations	Find out when personally identifiable information was being synchronized to mobile devices, the users performing the sync, and the action taken.
Mobile Credit Card Violations	Find out when credit card information was being synchronized to mobile devices, the users performing the sync, and the action taken.

Click a folder to expand it and see a list of related reports. Click **Run** to generate the report.

Related concepts

[Viewing the incident list](#) on page 69

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*, for an explanation of how to read and customize incident reports like this one.

Related concepts

[Viewing the incident list](#) on page 69

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

Use the **Main > Reporting > Discovery > Report Catalog** page to see a catalog of all available discovery reports—both built-in and user-defined. The built-in reports are described below.

Click a folder to expand it and see a list of related reports. Click **Run** to generate the report.

Incident List

Incidents	<p>View a list of recent incidents, with detailed information on each incident. Evaluate whether policy changes are needed.</p> <p>Select this report when you want to manage incident workflow, remediation, and escalation.</p>
-----------	---

Discovered Hosts

Hosts with credit card data	Find out which hosts contain credit card data, and assess any violated policies on each host.
Hosts with personally identifiable information	Find out which hosts contain personally identifiable information, and assess any violated policies on each host.
Hosts with PCI data	Find out which hosts contain PCI data, and assess any violated policies on each host.
Hosts with sensitive data	Find out which hosts contain sensitive information, and assess any violated policies on each host.
Laptops with sensitive data	Find out which laptops contain sensitive information, and assess any violated policies on each host.

Discovered Sensitive Data

Sensitive data on shared folders accessible by everyone	Find out was sensitive data was found in shared folders.
Sensitive data on file servers, SharePoint servers, and cloud servers	Find out was sensitive data was found on file, SharePoint, and cloud servers (for example, SharePoint 365 and Box).
Sensitive data on laptops	Find out was sensitive data was found on laptops
Sensitive data in databases	Find out was sensitive data was found in databases.
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

Databases with credit card numbers	Find out which databases contain credit card numbers, and assess any violated policies on each database.
------------------------------------	--

Databases with personally identifiable information	Find out which databases contain personally identifiable information, and assess any violated policies on each database.
Databases with sensitive data	Find out which databases contain sensitive information, and assess any violated policies on each database.
Databases with PCI data	Find out which databases contain PCI data, and assess any violated policies on each database.

Discovered Mailboxes

Mailboxes with credit card numbers	View which mailboxes contain credit card numbers, and assess any violated policies in each mailbox.
Mailboxes with personally identifiable information	View which mailboxes contain personally identifiable information, and assess any violated policies in each mailbox.
Mailboxes with sensitive data	View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.
Mailboxes with PCI data	View which mailboxes contain PCI data, and assess any violated policies in each mailbox.

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.
-----------------	--

Discovery dashboard

Use the **Main > Reporting > Discovery > Discovery Dashboard** page to find:

- An overview of information leaks in the system
- What actions are being taken on the leaks
- Which channels are problematic
- 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.

View the dashboard in the Security Manager at any time, or create a scheduled task to receive it periodically via email.

To access the dashboard:

- 1) Go to the **Main > Reporting > Discovery > Report Catalog** page and expand the **Executive Dashboard** section, if needed.

2) Click Discovery 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:** the policies that were violated the most frequently and the number of times each was violated.
- **Top Items:** the hosts, mailboxes, and tables with the most violations, depending on the type of discovery performed.

Optionally:

- Export the dashboard report to a PDF file or view a Print Preview, using the buttons at the top of the page.

Chapter 6

Policies Overview

Contents

- [What's in a policy?](#) on page 112
- [Viewing policies](#) on page 113
- [Selecting items to include or exclude in a policy](#) on page 122

After installing Forcepoint DLP software and configuring system settings, the next step is to create a policy.

DLP policies enable monitoring and control of the flow of sensitive data throughout an organization. Depending on the existing Forcepoint DLP configuration, administrators can set up policies to monitor information sent via email and over HTTP and HTTPS channels, and ensure all communications are in line with applicable regulations and compliance laws. It is also possible to monitor email being sent to users' mobile devices.

There are 5 kinds of DLP policies. These include:

- A single **email DLP policy** that contains attributes to monitor in inbound and outbound messages. For each attribute (for example, the appearance of a defined key phrase), define whether to permit or quarantine the message, and whether a notification should be sent.

For more information, see *Configuring the Email DLP Policy*.

- A single **web DLP policy** that contains attributes to monitor in HTTP, HTTPS, and FTP channels, as well as websites to which sensitive data cannot be sent.

For more information, see *Configuring the Web DLP Policy*.

- A single **mobile DLP policy** that contains attributes to monitor in email being sent to users' mobile devices. For each attribute (for example, the appearance of a defined key phrase), define whether to permit or quarantine the message, and whether a notification should be sent.

For more information, see *Configuring the Mobile DLP Policy*.

- A rich set of predefined policies that cover the data requirements for a wide variety of organizations. They include:
 - Acceptable use policies, such as Cyber Bullying, Self Destructive Patterns, and Indecent Images.
 - Content protection policies, such as US PII, Credit Cards, and Financial Information.
 - Data theft indicator policies, such as Suspected Malicious Dissemination and Disgruntled Employee.
 - Regulations, compliance, and standards policies, such as PCI and GDPR-related policies.

For more information, refer to *Using Predefined DLP and Discovery Policies*.

- One or more **custom policies**. After using the regulatory policies for a time and monitoring the results, administrators can create custom policies as needed. For more information, refer to *Creating Custom DLP Policies*.



Note

Administrators cannot delete or rename the email, web, or mobile DLP policy, but can enable or disable their attributes.

Administrators cannot update all rules or exceptions in email or web policies using the batch operations on the Manage Policies screen.

Before getting started with policy management and creation, see *What's in a policy?*

Related concepts

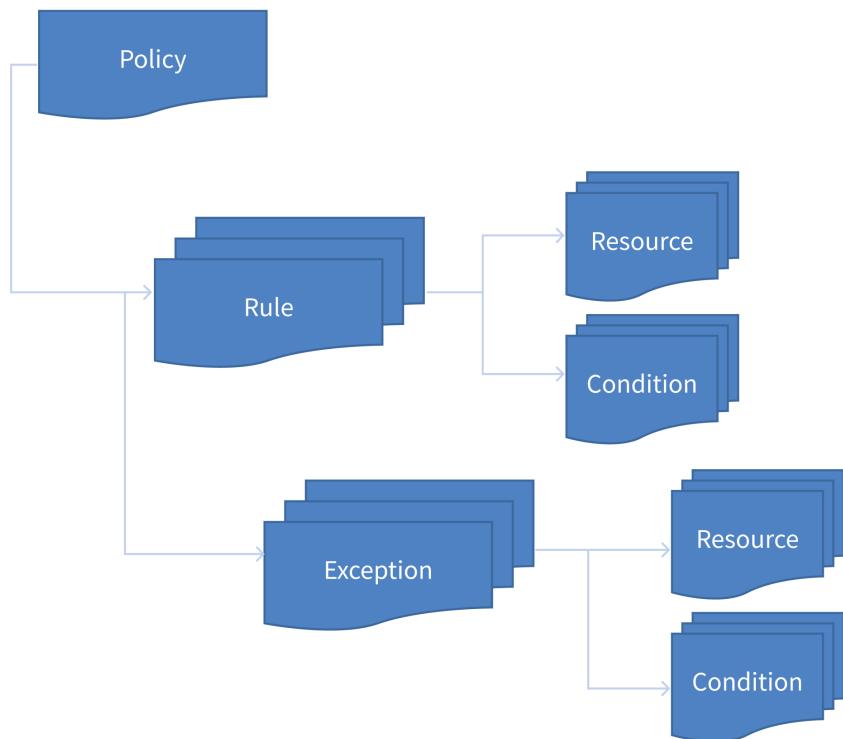
- [Viewing policies on page 113](#)
- [Creating Discovery Policies on page 277](#)
- [Configuring the Web DLP Policy on page 133](#)
- [Configuring the Mobile DLP Policy on page 143](#)
- [Using Predefined DLP and Discovery Policies on page 151](#)
- [What's in a policy? on page 112](#)

Related tasks

- [Creating Custom DLP Policies on page 155](#)
- [Configuring the Email DLP Policy on page 125](#)

What's in a policy?

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



Element	Description
Rules	<p>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?</p> <p>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 <i>drip DLP</i>.</p>
Exceptions	<p>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.</p> <p>You cannot add exceptions to cumulative rules, and exceptions themselves cannot be cumulative.</p>
Content classifiers	<p>Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, scripts, database fingerprints, directory fingerprints, file fingerprints, regex patterns, or by providing positive examples for machine learning.</p>
Resources	<p>Describe the source and destination of the data you want to protect, the endpoint device or application that may be in use, and the remediation or action to take when a violation is discovered (such as block or notify).</p>

These components are the building blocks of a policy. When you create a policy from a policy template, it includes all rules, 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, IBM Domino server, Box directory, database, Exchange server, or Outlook PST files. If you're performing endpoint discovery, it includes the exact computers to scan.

Related concepts

[Managing rules](#) on page 175

[Managing exceptions](#) on page 176

[Classifying Content](#) on page 181

[Defining Resources](#) on page 241

Viewing policies

From the **Main > Policy Management > DLP Policies or Discovery Policies** page, 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.

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

The screenshot shows the 'Manage DLP Policies' window. On the left, the 'Policy Tree' is displayed with several policy nodes expanded, such as 'Email DLP Policy', 'Web DLP Policy', and 'Mobile DLP Policy'. One node, 'Licensing Requirements 13Apr05.doc Rule', is selected and highlighted with a red box. On the right, the 'Details Pane' is shown, also with a red box around its title 'Rule: Licensing Requirements 13Apr05.doc Rule'. The pane contains detailed information about the rule, including its policy ('PreciseID Fingerprinting Files Policy'), severity ('Low'), action ('Audit_Action'), and description ('Rule for matching of the fingerprinted file Licensing Requirements 13Apr05.doc'). It also shows the condition and a preview of the rule's content.

Related concepts

[Policy levels on page 121](#)

The policy toolbar

The policy toolbar provides many functions.

Button	Description
	Create a new policy, rule, or exception.
	Update the selected policy, rule, or exception.
	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.
	Show disabled rules in the policy tree.

Button	Description
	Hide disabled rules so they do not appear in the policy tree.
	<ul style="list-style-type: none"> ■ Use Batch Operations to update or delete multiple items at once. For example: <ul style="list-style-type: none"> ■ Select <i>Update rules of a current policy</i> 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 <i>Update exceptions of current rule</i> to change one or more exceptions in the selected rule at the same time. This overrides the settings in the rule. ■ Select <i>Update rules of multiple policies</i> to make changes to selected rules or all rules across multiple policies. ■ Select <i>Update exceptions of multiple rules</i> to change selected exceptions or all exceptions across multiple rules. ■ Select <i>Delete policies</i> to delete a batch of policies at once: a screen appears so you can choose which policies to delete. ■ Use Rearrange Exceptions to set the order of exceptions under the selected rule. ■ Use Manage Policy Levels to configure policy execution priority order. See <i>Policy levels</i>.
	Exports policy data to a PDF file. You can export the current policy, all policies from this level, or all policies. Policies, rules, and exceptions are exported.
	Refreshes the policy list.

The information icon (“i”), when present, provides additional details about a field.

Related concepts

[Policy levels on page 121](#)

Related tasks

[Update rules of a current policy on page 116](#)
[Update exceptions of current rule on page 117](#)
[Update rules of multiple policies on page 118](#)
[Update exceptions of multiple rules on page 119](#)
[Delete policies on page 120](#)

Editing a policy

Select a name from the policy tree to edit a policy's properties.

Field	Description
Policy name	The name for this policy.
Enabled	Select this box to enable the rule for this policy. If this box is unselected, the rule is present, but disabled.
Policy description	Enter a description for this policy.
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 <i>Selecting items to include or exclude in a policy</i> for instructions. 3) Click OK .

Related concepts

[Selecting items to include or exclude in a policy](#) on page 122

Update rules of a current policy

It is possible 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.

From the **Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies** page:

- 1) Select the policy to modify.
- 2) From the toolbar at the top of the content pane, select **More Actions > Batch Operations > Update rules of current policy**.
- 3) In the Selected Rules box, select the rules that you want to modify.
- 4) In the Fields to Update box, select the fields to update.
- 5) For each field, update the properties in the right pane.

Field	Properties
State	Select whether to enable or disable all the selected rules. This changes their state.

Field	Properties
Severity & Action	<p>Specify the incident severity and action plan to apply to all of the selected rules.</p> <p>If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5), and a Dynamic User Protection Severity value. Click Add to create a new action plan and add it to all risk level action plan lists. You can then select the new action plan for each risk level. See <i>Custom Policy Wizard -Severity and Action</i> for more details.</p>
Source	<p>Select the sources of data to analyze. These sources are applied to all of the selected rules. See <i>Custom Policy Wizard - Source</i>, page for more details. Any changes made here override all other configurations of source in the rule.</p>
Destination	<p>Select the data destinations to analyze. These destinations are applied to all of the selected rules. See <i>Custom Policy Wizard -Destination</i> for more details. Any changes made here override all other configurations of destination in the rule.</p>

- 6) Click **OK**.

Related tasks

[Custom Policy Wizard - Severity and Action](#) on page 161

[Custom Policy Wizard - Source](#) on page 164

Update exceptions of current rule

It is possible 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.

From the **Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies** page:

- 1) Select the rule to modify.
- 2) From the toolbar, select **More Actions > Batch Operations > Update exceptions of current rule**.
- 3) In the Selected Exceptions box, select the exceptions that you want to modify.
- 4) In the Fields to Update box, select the fields to update.
- 5) For each field, update the properties in the right pane.

Field	Properties
State	Select whether you want to enable or disable all the selected exceptions. This changes their state.
Severity & Action	<p>Specify the incident severity and action plan to apply to all of the selected rules.</p> <p>If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5), and a Dynamic User Protection Severity value. Click Add to create a new action plan and add it to all risk level action plan lists. You can then select the new action plan for each risk level. See <i>Custom Policy Wizard - Severity and Action</i> for more details.</p>
Source	Select the sources of data you'd like to analyze. These sources are applied to all of the selected exceptions. See <i>Custom Policy Wizard - Source</i> for more details.
Destination	Select the data destinations that you want to analyze. These destinations are applied to all of the selected exceptions. See <i>Custom Policy Wizard - Destination</i> , for more details.

- 6) Click **OK**.

Related concepts

[Custom Policy Wizard - Destination](#) on page 165

Update rules of multiple policies

It is possible make changes to selected rules or all rules across all policies.

From the **Main > Policy Management > DLP Policies** or **Discovery Policies > Manage Policies** page:

- 1) Select the policy to modify
- 2) From the toolbar, select **More Actions > Batch Operations > Update rules of multiple policies**.
- 3) 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.
- 4) In the Selected Rules box, select the rules that you want to modify. You can see which policies contain the rule.
- 5) In the Fields to Update box, select the fields to update.
- 6) For each field, update the properties in the right pane.

Field	Properties
State	Select whether you want to enable or disable all the rules in the current policy. This changes their state.
Severity & Action	<p>Specify the incident severity and action plan to apply to all of this rule's exceptions.</p> <p>If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5), and a Dynamic User Protection Severity value. Click Add to create a new action plan and add it to all risk level action plan lists. You can then select the new action plan for each risk level. See <i>Custom Policy Wizard - Severity and Action</i> for more details.</p>
Source	Select the sources of data you'd like to analyze. These sources are applied to all of the rules in the policy. See <i>Custom Policy Wizard - Source</i> , 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 <i>Custom Policy Wizard - Destination</i> , page for more details.

- 7) Click **OK**.

Related concepts

[Custom Policy Wizard - Destination](#) on page 165

Related tasks

[Custom Policy Wizard - Severity and Action](#) on page 161

[Custom Policy Wizard - Source](#) on page 164

Update exceptions of multiple rules

It is possible to change selected exceptions or all exceptions across all rules.

From the **Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies** page:

- 1) Select the rule to modify.
- 2) From the toolbar, select **More Actions > Batch Operations > Update exceptions of multiple policies**.
- 3) 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.

- 4) In the Selected Exceptions box, select the exceptions that you want to modify. You can see which rules contain the exception.
- 5) In the Fields to Update box, select the fields to update.
- 6) For each field, update the properties in the right pane.

Field	Properties
State	Select whether you want to enable or disable all the exceptions to the current rule. This changes their state.
Severity & Action	Specify the incident severity and action plan to apply to all of this rule's exceptions. If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5), and a Dynamic User Protection Severity value. Click Add to create a new action plan and add it to all risk level action. See <i>Custom Policy Wizard - Severity and Action</i> for more details.
Source	Select the sources of data you'd like to analyze. These sources are applied to all of this rule's exceptions. See <i>Custom Policy Wizard - Source</i> , for more details.
Destination	Select the data destinations that you want to analyze. These destinations are applied to all of this rule's exceptions. See <i>Custom Policy Wizard - Destination</i> , for more details.

- 7) Click **OK**.

Related concepts

[Custom Policy Wizard - Destination](#) on page 165

Related tasks

[Custom Policy Wizard - Severity and Action](#) on page 161

[Custom Policy Wizard - Source](#) on page 164

Delete policies

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

From the **Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies** page:

- 1) From the toolbar, select **More Actions > Batch Operations > Delete Policies**.

- 2) Select the policy or policies to delete. Click **Select All** to delete all of your policies.
- 3) Click **OK**.
- 4) 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, after installation, Forcepoint DLP has just one priority level.

Related tasks

[Adding or editing policy level](#) on page 121

[Deleting a policy level](#) on page 122

[Rearranging policy levels](#) on page 122

[Rearranging exceptions](#) on page 177

Adding or editing policy level

Use the **Policy level details** page to created or update policy level definitions.

- 1) On the **Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies** page, select **More Actions > Manage Policy Levels**.
The Manage Policy Levels page appears.
- 2) Click **New** in the toolbar at the top of the content pane to add a policy level, or click an existing policy level name in the table to edit the policy level.
- 3) Enter or update the level **Name** and **Description**. 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, Forcepoint DLP stops 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 one or more policy names in the left pane and click **Add>>** to move each to the right pane.
- 6) Click **OK** to confirm the action.

Deleting a policy level

Steps

- 1) On the Manage Policies page, select **More Actions > Manage Policy Levels**.
- 2) Select a level by marking the check box next to it.
- 3) Click **Delete** from the menu bar.
- 4) Click **OK** to confirm the action.

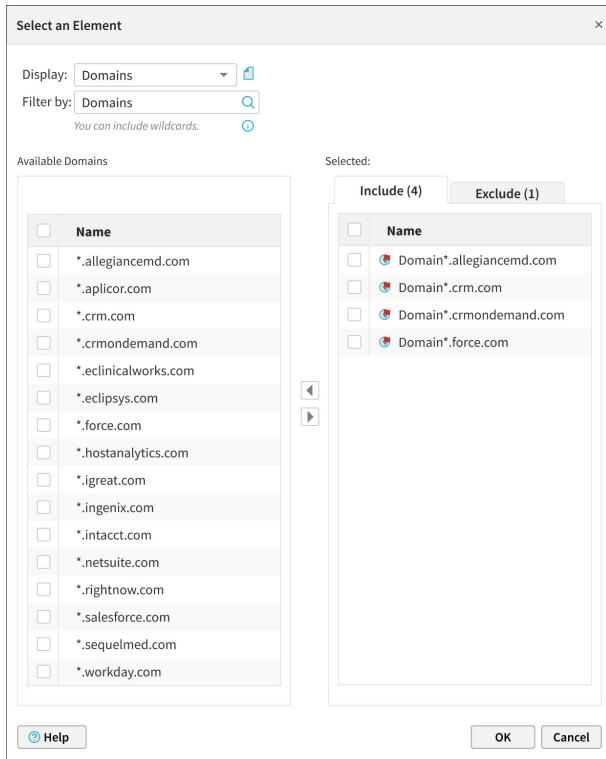
Rearranging policy levels

Steps

- 1) On the Manage Policies page, select **More Actions > Manage Policy Levels**.
- 2) Highlight a level.
- 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

A selector tool is used to select the items to include in a DLP or discovery policy, such as sources, destinations, channels, and actions, among others. For most operations—selecting application names, content classifier names, or files, for example—the selector looks like this:



Use the selector to specify which entities to include in the rule and which to exclude. If, for example, you want users in the Finance group to be able to move, copy, and print corporate financial data in the /finance directory, select the Finance group with the Sources selector and the /finance directory with the Destinations selector.

When there is an exception, add it to the exclusions list. If, for example, user bsmith is a member of the Finance group, but should not have access to the /finance directory, r, you would add user bsmith to the exclusions list.

A rule can have multiple exclusions.

To use the selector, complete the fields as follows:

Field	Description
Display	Select the entity—such as computers or networks if you are selecting a source—to display in the Available List box at the bottom of the page. If you do not see what you want to display, in some cases you can create a new resource by clicking the “new” icon to the right of the field. See <i>Defining Resources</i> , for instructions.
Filter by	Typically, too many entries are available to display on one page. Use the Filter by field to specify criteria for filtering the list. If you enter “jones”, the system searches for any entry that contains the string “jones”. It is equivalent to searching “*jones*”. 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 search icon to filter the data.

Field	Description
Available items	<p>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.</p> <p>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.</p> <p>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.</p>
Selected items	<p>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 Include tab is active, and then click >. If you want to exclude Bob_Computer, make sure the Exclude tab is active when you click >.</p> <p>If you select more than 1500 items, you receive an error message. Consider creating a business unit to add more items to the Selected box.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Tip <p>you can move a group of users, computers, networks, etc. into the Include box, then remove one user, computer, or network by highlighting it on the right and clicking Remove.</p> </div>

Related concepts

[Defining Resources](#) on page 241

Chapter 7

Configuring the Email DLP Policy

Contents

- Configuring outbound and inbound email DLP attributes on page 126
- Defining email DLP policy owners on page 130
- Identifying email DLP trusted domains on page 131

Forcepoint DLP can help administrators control how sensitive data moves through their organization via email using the email DLP quick policy. (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.)

- Depending on the deployment, Forcepoint DLP can protect outbound, inbound, or internal email from data loss, or all three.
- Monitoring email for sensitive data requires either Forcepoint Email Security or the Forcepoint DLP protector.



Tip

To get the full benefit of Forcepoint DLP email capabilities, subscribe to Forcepoint Email Security.

The protector can monitor inbound and outbound email in monitoring mode.

Email Security Cloud protects only outbound email.

Forcepoint Email Security is automatically configured to work with Forcepoint DLP.

- Forcepoint Email Security registers with the management server during installation.
- Forcepoint DLP policies are enabled by default.



Important

Click **Deploy** in the Forcepoint Security Manager to complete the registration process.

To confirm that Forcepoint Email Security has successfully registered with Forcepoint DLP:

- 1) Log on to the Forcepoint Security Manager, hover over the Forcepoint logo at the top of the Forcepoint header and then select **Email** from the drop-down list
- 2) Navigate to the **Settings > General > Data Security** page.
- 3) If the status is “unregistered”, enter the IP address of the management server in the field provided, and click **Register**.
- 4) Hover over the Forcepoint logo at the top of the Forcepoint header and select **Data** from the drop-down list to switch to the Data Security module.
- 5) Navigate to the **Main > Policy Management > DLP Policies > Email DLP Policy** page to configure the quick-start email DLP policy.

- 6) On the **Outbound** tab, select and enable the attributes to monitor in outgoing email messages—for example, attachment type—and configure properties for those attributes. See *Configuring outbound and inbound email DLP attributes*.
- 7) On the **Inbound** tab, select and enable the attributes to monitor inbound email messages—for example, questionable images—and configure properties for those attributes.

**Note**

The email DLP policy can be used to define only inbound and outbound email attributes to monitor.

Monitoring of internal email attributes for network or endpoint email is configured on the Destination tab of the custom policy wizard.

- 8) Identify an owner or owners for the policy. See *Defining email DLP policy owners*.
- 9) Identify trusted domains, if any. See *Identifying email DLP trusted domains*.
- 10) Click **OK**.

**Note**

The email DLP policy cannot be deleted or renamed, but its attributes can be enabled or disabled.

Related tasks

[Configuring outbound and inbound email DLP attributes](#) on page 126

[Defining email DLP policy owners](#) on page 130

[Identifying email DLP trusted domains](#) on page 131

Configuring outbound and inbound email DLP attributes

Use the **Outbound** and **Inbound** tabs of the **Policy Management > Manage DLP Policies > Email DLP Policy** page to select one or more email attributes to include in the policy.

To include an attribute:

- 1) Select the attribute from the Attributes list.
- 2) Mark the **Enabled** check box in the right pane.

Properties that apply to the attribute are listed under the check box.

- 1) Modify the attribute properties as needed, including:
 - The default severity (low, medium, or high)
 - What action to take when a breach is detected (for example, quarantine). Actions are described in *Adding or editing an action plan*.

The available properties for each attribute are described in the table below.

Repeat this procedure for each attribute that you want to include. When the system detects a match for an attribute, it triggers the policy.

To send notifications when there is a violation of a particular attribute setting, mark the **Send the following notification** check box.

- To configure who receives notifications, click the notification name ("Email policy violation"), then 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.

Field	Description
Message size	<p>The size of email messages to monitor. Only messages of the specified size or higher are monitored. The default size is 10 MB.</p> <p>Default severity: low.</p> <p>Available actions: quarantine (default), permit.</p>
Regulatory & compliance	<p>Select the regulatory and compliance rules to enforce. These are applied to all selected regions. (If no regions are selected, an error is displayed. Click Select regions to address the issue.)</p> <ul style="list-style-type: none"> ■ Personally Identifiable Information (PII) ■ Protected Health Information (PHI) ■ Payment Card Industry (PCI DSS) <p>After selecting a law, click its name to view or edit the specific policies to enforce, then select a sensitivity for each policy.</p> <ul style="list-style-type: none"> ■ Wide is highly sensitive and errs on the restrictive side. 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. <p>Default severity: high.</p> <p>Available actions: quarantine (default), permit.</p>

Field	Description
Attachment name	<p>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.</p> <p>For example, after adding a file named confidential.docx, when a user attaches a file with that name to an email message, the system detects it and takes the configured action.</p> <p>Note that only Forcepoint Email Security can drop attachments. If the drop attachments options is selected when the protector or Email Security Cloud is monitoring email, messages are quarantined when a policy is triggered.</p> <p>Default severity: low.</p> <p>Available actions: quarantine, permit, drop attachments (default)</p>
Attachment type	<p>Click Add to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files.</p> <p>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.</p> <p>If the file type does not exist, specify exact files of this type using the Attachment name attribute instead. Default severity: low.</p> <p>Available actions: quarantine, permit, drop attachments (default).</p> <p>Note: Only Forcepoint Email Security can drop attachments. If the drop attachments options is selected when the protector or Email Security Cloud is monitoring email, messages triggering a policy are quarantined.</p>

Field	Description
Patterns & phrases	<p>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.</p> <p>Enter the precise phrase (for example “Internal Only”) or regex pattern (for example ~ m/H.?e/) to include.</p> <p>Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1.</p> <p>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.</p> <p>Default severity: medium.</p> <p>Available actions: quarantine (default), permit.</p> <p>Note: Although you do not define whether to search only for unique strings, the system uses the following defaults:</p> <ul style="list-style-type: none"> ■ Key phrase searches are non-unique. All matches are reported. ■ For regular expression searches, only unique matches are reported as triggered values.
Acceptable use	<p>Select the dictionaries that define unacceptable use in your organization.</p> <p>Forcepoint DLP 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.</p> <p>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.</p> <p>You cannot add or delete terms from predefined dictionaries, but you can exclude terms from detection, if needed. Do this on the Main > Content Classifiers > Patterns & Phrases page. Select the dictionary to edit, then enter the phrases to exclude.</p> <p>By default, the policy is triggered by a single match from the dictionary or dictionaries you select.</p> <p>Default severity: medium.</p> <p>Available actions: quarantine (default), permit.</p>

Field	Description
Questionable images	<p>Select this attribute to prevent pornographic images from entering your organization. Pornographic images pose a legal liability to organizations in many countries.</p> <p>The system judges images based on the amount of flesh tone they contain.</p> <p>Default severity: low.</p> <p>Available actions: quarantine, permit, drop attachments (default).</p>
Number of attachments	<p>Specify the number of attachments to detect. Email messages with this number of attachments (or more) trigger the policy.</p> <p>The default number of attachments is 20. Default severity: low.</p> <p>Available actions: quarantine (default), permit</p>
Number of destination domains	<p>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.</p> <p>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.</p> <p>Also, select which email fields to monitor (To, Cc, Bcc). To and Cc are selected by default.</p> <p>Default severity: low.</p> <p>Available actions: quarantine (default), permit.</p>

Related tasks

[Adding or editing an action plan on page 258](#)

Defining email DLP policy owners

Use the **Policy Owners** tab of the **Policy Management > Manage DLP Policies > Email DLP Policy** page to identify who can view and modify the policy and, if configured, receive notifications of breaches. Notifications are sent only if they are enabled in one or more of the policy's attributes.

To define an owner or owners for the email DLP policy on the Policy Owners tab:

- 1) Click **Edit**.
- 2) Select one or more owners in the Select an Element dialog box. See *Selecting items to include or exclude in a policy* section for instructions.

- 3) Click **OK**.

To send notifications to policy owners:

- 1) Go to the **Main > Policy Management > Resources** page.
- 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* section, for more information.

Related concepts

Selecting items to include or exclude in a [policy](#) on page 122
[Notifications](#) on page 273

Identifying email DLP trusted domains

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



Note

Trusted domain definitions apply to outbound email traffic only.

To define trusted domains:

Steps

- 1) On the Outbound tab, select **Enable trusted domains**.
- 2) Click **Edit**.
- 3) Identify the domain or domains you trust.
- 4) Click **OK**.

Chapter 8

Configuring the Web DLP Policy

Contents

- [Web DLP policy configuration overview](#) on page 134
- [Configuring web DLP policy attributes](#) on page 134
- [Selecting web DLP policy destinations](#) on page 139
- [Defining web DLP policy owners](#) on page 140

Forcepoint DLP lets organizations control how and where users upload or post sensitive data over HTTP or HTTPS connections via the web DLP quick policy. (Note that the web DLP policy applies to network channels only. To monitor HTTP/S on endpoint machines, such as laptops that are off-network, create a custom policy.)

Monitoring HTTP and HTTPS channels for sensitive data requires one of the following:

- Integration with Forcepoint Web Security
- The Web Content Gateway module
- The Forcepoint DLP protector



Tip

To get the full benefit of Forcepoint DLP's web capabilities, subscribe to Forcepoint Web Security. Forcepoint Web Security uses the Forcepoint Master Database to categorize URLs, and includes a built-in policy engine that speeds analysis.

When Forcepoint Web Security is deployed with the DLP Module, the product registers with the management server during installation to connect to Forcepoint DLP.



Important

Click **Deploy** in the Forcepoint Security Manager to complete the registration process.

To confirm that the registration was successful, navigate to the **Settings > Deployment > System Modules** page in the Data Security module of the Security Manager. A module named "Web Content Gateway" should appear.

Related concepts

- [Configuring web DLP policy attributes](#) on page 134
- [Selecting web DLP policy destinations](#) on page 139

Related tasks

- [Defining web DLP policy owners](#) on page 140

Web DLP policy configuration overview

To configure the web DLP quick policy:

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > DLP Policies > Web DLP Policy** page.
- 2) On the Attributes tab, select and enable the attributes to monitor—for example uploaded file type—and configure properties for those attributes. When the configured settings are matched, the policy is triggered. See *Configuring web DLP policy attributes* section.
- 3) Select the Destination tab, then specify the websites to which users should not be allowed to send data. See *Selecting web DLP policy destinations* section.
- 4) Select the Policy Owners tab, then identify an owner for the policy. See *Defining web DLP policy owners* section.
- 5) Click **OK**



Note

The web DLP policy cannot be deleted or renamed, but its attributes can be enabled or disabled.

Related concepts

[Configuring web DLP policy attributes](#) on page 134
[Selecting web DLP policy destinations](#) on page 139

Related tasks

[Defining web DLP policy owners](#) on page 140

Configuring web DLP policy attributes

Use the **Attributes** tab of the **Policy Management > Web DLP Policy** page in the Data Security module of the Forcepoint Security Manager to select one or more web attributes to include in the policy.

To include an attribute:

- 1) Select the attribute from the Attributes list.
- 2) Mark the **Enabled** check box in the right pane.
Properties that apply to the attribute are listed under the check box.
- 3) Modify the attribute properties as needed, including:

- The default severity (low, medium, or high)
- What action to take when a breach is detected (for example, block). Actions are described in *Adding or editing an action plan* section.

The available properties for each attribute are described in the table below.

Repeat this procedure for each attribute that you want to include. When the system detects a match for an attribute, it triggers the policy.

To send notifications when there is a violation related to a specific attribute, mark the **Send the following notification** check box.

- To configure who receives notifications, click the notification name ("Web policy violation"), then 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 DLP Policy* section for more information.

Field	Description
Post size	<p>Disabled by default.</p> <p>Select the minimum size of web posts to monitor. The default is 10 KB (that is, posts 10 KB and above in size are monitored).</p> <p>Default severity: low.</p> <p>Available actions: block (default), permit.</p>

Field	Description
Regulatory & Compliance	<p>Enabled by default.</p> <p>Select the regulatory and compliance rules to enforce. These are applied to all selected regions. (If no regions are selected, an error is displayed. Click Select regions to address the issue.)</p> <ul style="list-style-type: none"> ■ Personally Identifiable Information (PII) ■ Protected Health Information (PHI) ■ Payment Card Industry (PCI DSS) <p>After selecting a category, click its name to view or edit the specific policies to enforce.</p> <p>Applying specific policies improves performance and reduces resource consumption.</p> <p>Select a sensitivity for each policy.</p> <ul style="list-style-type: none"> ■ 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. <p>Default severity: high.</p> <p>Available actions: block (default), permit.</p>

Field	Description
Data theft	<p>Disabled by default.</p> <p>The system protects against content being posted to the Web after your computer is infected. This complements Forcepoint Web Security, which protects against infected content downloaded from the Web.</p> <p>Select the type of data to search for in outbound transactions. When sent outside your network, this data can indicate a serious vulnerability.</p> <ul style="list-style-type: none"> ■ Suspected malware communication identifies transactions that are suspected to be malicious, based on analysis of traffic from known infected machines. This includes phone home and data theft traffic. This feature Forcepoint Web Security with 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. <p>Select a sensitivity for each policy. Sensitivity levels are described in more detail in the Regulatory & Compliance section, above.</p> <p>Note: The selected number of policies and their sensitivity levels affect performance.</p> <p>Default severity: high.</p> <p>Available actions: block (default), permit.</p>

Field	Description
Name of uploaded file	<p>Disabled by default.</p> <p>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 file name and extension. Click Add after each entry.</p> <p>For example, after adding a file named confidential.docx, when a user attempts to post a file with that name, the system detects it and takes the configured action.</p> <p>The system can detect files even when they've been compressed into an archive, such as a .zip file.</p> <p>Default severity: low.</p> <p>Available actions: block (default), permit.</p>
Type of uploaded file	<p>Disabled by default.</p> <p>Click Add to specify the types of files that should be monitored when posted or uploaded to the Web, for example Microsoft Excel files.</p> <p>Next, select the type or types of files to monitor. If there are more file types than can appear on the page, sort the columns or enter search criteria for find file types.</p> <p>If the file type does not exist, specify exact files of this type using the Name of uploaded file attribute instead. Default severity: low.</p> <p>Available actions: block (default), permit.</p>
Patterns & phrases	<p>Enabled by default.</p> <p>Click Add to define key phrases or regular expression (regex) patterns that should be monitored.</p> <p>On the resulting dialog box, enter the precise phrase (for example "Internal Only") or regex pattern (for example ~ m/H.?e/) to include.</p> <p>Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1.</p> <p>Default severity: medium.</p> <p>Available actions: block (default), permit.</p> <p>Note: Although you do not define whether to search only for unique strings, the system uses the following defaults:</p> <ul style="list-style-type: none"> ■ Key phrase searches are non-unique. All matches are reported. ■ For regular expression searches, only unique matches are reported as triggered values.

Related concepts

[Configuring the Web DLP Policy on page 133](#)

Related tasks

[Adding or editing an action plan on page 258](#)

Selecting web DLP policy destinations

Use the **Destinations** tab of the **Policy Management > Web DLP Policy** page in the Data Security module of the Forcepoint Security Manager to select one or more websites to include in the policy. When the system detects that someone is posting sensitive data to those websites, it triggers the policy.

Related concepts

[Configuring the Web DLP Policy on page 133](#)

Related tasks

[Defining web DLP policy owners on page 140](#)

[Business Units on page 251](#)

Selecting destination websites

Under Destination Sites:

- Select **Any website** to prevent sensitive data from being posted or uploaded to any website, without exception.
- Select **Websites that belong to the selected categories** to prevent sensitive data from being posted or uploaded to known or potentially hazardous websites, but not to all websites.

Linking Service must be installed, running, and enabled to monitor selected categories, and the connection to the Linking Service machine must be working. (Enable Linking Service on the **Settings > General > Services** page.)

Expand a category to select or deselect specific site categories.

- Mark **Identified malware sites** to prevent sensitive data from being posted to websites identified as containing malicious software, including Bot Networks, Keyloggers, Phishing and Other Frauds, Spyware, and more.
- Mark **Suspected malware sites** to prevent sensitive data from being posted to websites that contain potentially malicious or undesired content, including Potentially Unwanted Software, Potentially Damaging Content, Suspicious Embedded Link, and more.
- Mark **Data misuse sites** to prevent sensitive data from being posted to websites that are prone to misuse, intentional or not, by users, including Peer- to-Peer File Sharing, Message Boards and Forums, General Email, and more.

Defining trusted domains

To exclude specific domains from policy enforcement:

Steps

- 1) Mark the **Enable trusted domains** check box.
- 2) Click **Edit** to select the trusted domains.
 - Because Forcepoint DLP does not enforce policies for trusted domains, these domains can receive any type of sensitive information via HTTP, HTTPS, or other web channels.
 - Several SaaS domains are excluded from analysis by default.
 - Exclude more domains as needed, or remove existing domains from the exclusion list.

It is also possible to customize the list of resources that are excluded from web policies. For more information, see *Business Units* section.

Defining web DLP policy owners

Use the **Policy Owners** tab of the **Policy Management > Web DLP Policy** page in the Data Security module of the Forcepoint Security Manager to identify who can modify a policy and, if configured, receive notifications of breaches. Notifications are sent only if they are enabled in one or more of the policy's attributes.

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

- 1) Click **Edit**.
- 2) Select one or more owners in the Select an Element dialog box. See *Selecting items to include or exclude in a policy* section for instructions.
- 3) Click **OK**.

To send notifications to policy owners:

- 1) Go to the **Main > Policy Management > Resources** page.
- 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* section, for more information.

Related concepts

- [Configuring the Web DLP Policy on page 133](#)
- [Configuring web DLP policy attributes on page 134](#)
- [Selecting web DLP policy destinations on page 139](#)
- [Selecting items to include or exclude in a policy on page 122](#)
- [Notifications on page 273](#)

Chapter 9

Configuring the Mobile DLP Policy

Contents

- [Mobile DLP policy configuration overview on page 143](#)
- [Configuring mobile DLP attributes on page 144](#)
- [Defining policy owners on page 148](#)

Use the Forcepoint DLP mobile DLP quick policy to define what content can and cannot be sent to mobile devices—such as phones and tablets—from network email systems. This can be used to protect data in case an employee's mobile device 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 mobile DLP policy, it is handled according to the policy, whether the 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, sensitive data can be blocked from being sent to John Doe's mobile devices, but not to a particular device ID.

The mobile DLP policy requires a subscription to Forcepoint DLP Endpoint. Note that the mobile DLP policy applies to mobile email only.

- To monitor network email, configure the email DLP policy.
- To monitor endpoint email, configure a custom policy.

Related concepts

[Mobile DLP attribute properties on page 145](#)

Related tasks

[Configuring mobile DLP attributes on page 144](#)

[Defining policy owners on page 148](#)

[Adding or editing an action plan on page 258](#)

Mobile DLP policy configuration overview

Use the **Main > Policy Management > DLP Policies > Mobile DLP Policy** page in the Data Security module of the Forcepoint Security Manager to configure the mobile DLP policy.

Steps

- 1) On the Attributes tab, specify the attributes to monitor in email synchronized to mobile devices—for example, attachment type—and configure attribute properties. When these settings are matched, the policy is triggered.
See *Configuring mobile DLP attributes* section.
- 2) Identify users that don't need to be monitored (trusted users), if any.
See *Defining mobile DLP trusted users* section.
- 3) Identify one or more owners for the policy.
See *Defining policy owners* section.
- 4) Click **OK**.



Note

The mobile DLP policy cannot be deleted or renamed, but its attributes can be enabled or disabled.

Related tasks

[Configuring mobile DLP attributes](#) on page 144

[Defining policy owners](#) on page 148

[Defining mobile DLP trusted users](#) on page 148

Configuring mobile DLP attributes

Use the **Attributes** tab of the **Policy Management > Mobile DLP Policy** page in the Data Security module of the Forcepoint Security Manager to select one or more email attributes to include in the policy.

To include an attribute:

- 1) Select the attribute from the Attributes list.
- 2) Mark the **Enabled** check box in the right pane.
Properties that apply to the attribute are listed under the check box.
- 3) Modify the attribute properties as needed, including:
 - The default severity (low, medium, or high)
 - What action to take when a breach is detected (for example, quarantine). Actions are described in *Adding or editing an action plan* section.

See *Mobile DLP attribute properties* section, for details about the properties available for each attribute.

Repeat this procedure for each attribute to include.

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

To send notifications when there is a violation of a particular attribute setting, mark the **Send the following notification** check box.

- To configure who receives notifications, click the notification name ("Mobile policy violation"), then define the mail server, email subject, and message body, as well as other required properties.
- By default, policy owners receive notifications.

Mobile DLP attribute properties

The table below lists the mobile DLP attributes and their configurable properties:

Field	Description
Message size	<p>The size of email messages to monitor. Only messages of the specified size or higher are monitored. The default size is 10 MB.</p> <p>Default severity: low.</p> <p>Available actions: quarantine (default), permit.</p>
Regulatory & Compliance	<p>Select the regulatory and compliance rules to enforce. These are applied to all selected regions. (If no regions are selected, an error is displayed. Click Select regions to address the issue.)</p> <ul style="list-style-type: none"> Personally Identifiable Information (PII) Protected Health Information (PHI) Payment Card Industry (PCI DSS) <p>After selecting a law, click its name to view or edit the specific policies to enforce, then select a sensitivity for each policy.</p> <ul style="list-style-type: none"> 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. <p>Default severity: high.</p> <p>Available actions: quarantine (default), permit.</p>

Field	Description
Attachment name	<p>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.</p> <p>For example, after adding a file named confidential.docx, when a user attaches a file with that name to an email message, the system detects it and takes the configured action.</p> <p>Default severity: low.</p> <p>Available actions: quarantine (default), permit</p>
Attachment type	<p>Click Add to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files.</p> <p>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.</p> <p>If the file type does not exist, specify exact files of this type using the Attachment name attribute instead. Default severity: low.</p> <p>Available actions: quarantine (default), permit.</p>

Field	Description
Patterns & phrases	<p>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.</p> <p>On the resulting dialog box, enter the precise phrase (for example “Internal Only”) or regex pattern (for example ~ m/H.?e/) to include.</p> <p>Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1.</p> <p>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.</p> <p>Default severity: medium.</p> <p>Available actions: quarantine (default), permit.</p> <p>Note: Although you do not define whether to search only for unique strings, the system uses the following defaults:</p> <ul style="list-style-type: none"> ■ Key phrase searches are non-unique. All matches are reported. ■ For regular expression searches, only unique matches are reported as triggered values.
Acceptable use	<p>Select the dictionaries that define unacceptable use in your organization.</p> <p>Forcepoint DLP 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.</p> <p>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.</p> <p>You cannot add or delete terms from predefined dictionaries, but you can exclude terms from detection, if needed. Do this on the Main > Content Classifiers > Patterns & Phrases page. Select the dictionary to edit, then enter the phrases to exclude.</p> <p>By default, the policy is triggered by a single match from the dictionary or dictionaries you select.</p> <p>Default severity: medium.</p> <p>Available actions: quarantine (default), permit.</p>

Field	Description
Questionable images	<p>Select this attribute to prevent pornographic images from entering your organization. Pornographic images pose a legal liability to organizations in many countries.</p> <p>The system judges images based on the amount of flesh tone they contain.</p> <p>Default severity: low.</p> <p>Available actions: quarantine (default), permit.</p>

Defining mobile DLP trusted users

Trusted users are those that the organization does not want monitored. Forcepoint DLP does not analyze email sent to mobile devices for trusted users.

If you have users that should not receive mobile DLP policy enforcement:

Steps

- 1) Select **Enable trusted users**.
- 2) Click **Edit**.
- 3) Browse to identify the trusted users, directory entries, and business units.

Defining policy owners

Use the **Policy Owners** tab of the **Policy Management > Mobile DLP Policy** page in the Data Security module of the Forcepoint Security Manager to identify who can view and modify a policy and, if configured, receive notifications of breaches.

Notifications are sent only if they are enabled in one or more of the policy's attributes. To define an owner or owners for this mobile DLP policy:

- 1) Click **Edit**
- 2) Select one or more owners in the Select an Element dialog box.
See *Selecting items to include or exclude in a policy* section for instructions.
- 3) Click **OK**.

To send notifications to policy owners:

- 1) Go to the **Main > Policy Management > Resources** page.
- 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* section for more information.

Related concepts

[Selecting items to include or exclude in a policy](#) on page 122

[Notifications](#) on page 273

Chapter 10

Using Predefined DLP and Discovery Policies

Contents

- Adding a predefined DLP or discovery policy on page 151
- Changing the selected DLP or discovery policies on page 153
- Changing policy industry or region settings on page 154

Forcepoint DLP comes with a rich set of predefined policies that cover the data requirements for a wide variety of organizations. Use the predefined policies as applicable for your industry and region, or refine the policies to meet the organization's needs.

For more information about the predefined policies, see [Predefined Policies and Classifiers](#).



Warning

Once a predefined policy has been customized and saved under a new name, it is no longer maintained automatically by Forcepoint DLP updates. Administrators must manually keep the customized policy up to date.

Adding a predefined DLP or discovery policy

Use the Data Security module of the Forcepoint Security Manager to start using predefined policies:

Steps

- 1) Go to the **Main > Policy Management > DLP Policies or Discovery Policies** page.
- 2) Click **Add predefined policy**.
- 3) For administrators using the policy templates for the first time, a wizard appears. Complete the fields as follows:
 - *Welcome*
 - *Regions*
 - *Industries*
 - *Finish*

Related concepts

[Welcome](#) on page 152

[Regions](#) on page 152

[Industries](#) on page 152

[Finish](#) on page 152

Welcome

The Welcome screen contains introductory information about Forcepoint predefined policies.

Click **Next** to continue.

Regions

On the Regions page, indicate the region or regions for which policies will be created. This helps the policy wizard focus on policies generally relevant to the selected geographical location.

Expand the tree by clicking the plus signs. Click **Next** to continue.

Industries

On the Industries page, select the industry or industries relevant to the policies that will be created. This helps the policy wizard focus on policies generally relevant to an 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.

Click **Next** to continue.

Finish

The Finish page appears, summarizing the selections made in the wizard.

Click **Finish**.

Refer to *Policy list* section, for information about the resulting page.

Related concepts

[Policy list](#) on page 152

Policy list

Use the **Policy Library** page (**Policy Management > DLP Policies or Discovery Policies > Add predefined policy**) to review the available predefined policies.

- Highlight a policy see the policy description in the right pane.
- Use the **View** button in the content pane to specify whether to show all applicable policies or only commonly used policies.

To select and start using the predefined policies:

- 1) Mark the check box next to the name of each policy to apply.
- 2) After selecting policies, click **Use Policies** in the toolbar at the bottom of the page.



Note

The Regions and Industries settings configured in this section are applied to both DLP and discovery policies. They do not need to be selected again. To change them in the future, see *Changing policy industry or region settings* section.

Some organizations deploy only these predefined policies. To determine whether additional policies are needed, start by monitoring incidents from the predefined policies. Based on what monitoring shows, administrators can create custom policies to safeguard additional types of data, as needed: for example, a custom policy could protect proprietary data on file servers and SharePoint.

Custom policies may be created using wizards.

- To create policies for network and endpoint machines, see *Defining Resources* section.
- To create discovery policies, see *Creating Discovery Policies* section.



Warning

Once a predefined policy has been customized and saved under a new name, it is no longer maintained automatically by Forcepoint updates. Be sure to keep the customized policy up to date.

Related concepts

[Defining Resources](#) on page 241

[Creating Discovery Policies](#) on page 277

Related tasks

[Changing policy industry or region settings](#) on page 154

Changing the selected DLP or discovery policies

Use the Data Security module of the Forcepoint Security Manager to update the list of predefined DLP or discovery policies being used:

Steps

- 1) Go to the **Main > Policy Management > DLP Policies** or **Discovery Policies** page.
- 2) Click **Add predefined policies**.

- 3) Select a policy category from the drop-down list, or select **All categories**.
- 4) Click **View**, then choose whether you want to see the most commonly used policies or all policies, then confirm the selection.
- 5) Expand the tree in the left pane to view additional policy categories, as well as policy names.
- 6) Highlight a policy name to view details about the policy in the right pane. The details include a description, as well as a list of the rules and exceptions the policy contains.
- 7) Select one or more policies, then click **Use Policies**.

Changing policy industry or region settings

Use the Data Security module of the Forcepoint Security Manager to change the selected industries and regions for DLP and discovery policies:

Steps

- 1) Go to the **Main > Policy Management > DLP Policies or Discovery Policies** page.
- 2) Click **Add predefined policies**.
- 3) Select a policy category from the drop-down list, or select **All categories**.
- 4) At the top of the screen, locate the following sentence: Displaying policies from n industries in n regions.
- 5) To change industries, click the **industries** link.
- 6) To change regions, click the **regions** link.

Chapter 11

Creating Custom DLP Policies

Contents

- [Custom Policy Wizard - General](#) on page 156
- [Custom Policy Wizard - Condition](#) on page 156
- [Custom Policy Wizard - Severity and Action](#) on page 161
- [Custom Policy Wizard - Source](#) on page 164
- [Custom Policy Wizard - Destination](#) on page 165
- [Rule Wizard - Finish](#) on page 169
- [Selecting a content classifier](#) on page 169
- [Managing rules](#) on page 175
- [Managing exceptions](#) on page 176

DLP policies govern data in motion across the network or on endpoint machines.

To create a custom DLP policy in the Data Security module of the Forcepoint Security Manager:

1) Go to the **Main > Policy Management > DLP Policies** page.

2) Click **Create custom policy**.

The General page of the custom policy wizard opens. See *Custom Policy Wizard - General* section.

3) Complete each page in the wizard, then click **Next**.

For detailed instructions for any page, click **Help > Explain This Page**.

4) After reviewing the information on the final page of the wizard, click **Finish**.

As a best practice:

1) Initially configure policies to apply a permissive action to all sources and destinations of data.

2) After monitoring the results, make updates to permit or block specific sources and destinations and apply more restrictive actions.

Use the **Main > Policy Management > Resources** page to configure source and destination resources for policies.

Related concepts

[Managing rules](#) on page 175

[Managing exceptions](#) on page 176

[Defining Resources](#) on page 241

Related tasks[Custom Policy Wizard - General on page 156](#)

Custom Policy Wizard - General

Use the **General** tab of the custom policy wizard to define a policy name and description, select one or more policy owners, and determine whether to give the rule based on the policy the same name as the policy itself:

Steps

- 1) Enter a unique **Policy name**.
- 2) Indicate whether the rule for this policy is **Enabled**. If this option is not selected, the rule is present, but not used.
- 3) Enter a **Description** of the policy.
- 4) To define one or more owners for this policy:
 - a) Click **Edit**.
 - b) Select one or more owners as described in *Selecting items to include or exclude in a policy* section.
 - c) Click **OK**.
- 5) Every policy has one or more rules. When this policy is created, a rule will automatically be added, based on properties set in the wizard. Indicate how to name the rule associated with this policy:
 - Select **Use the policy name for the rule name** to give the rule for this policy the same name as the policy.
 - Select **Use a custom name for the rule** to define a name for the rule, then enter a name and description for the rule.
- 6) Click **Next**, then continue with *Custom Policy Wizard - Condition* section.

Related concepts[Selecting items to include or exclude in a policy on page 122](#)[Custom Policy Wizard - Condition on page 156](#)

Custom Policy Wizard - Condition

Use the **Condition** tab of the custom policy wizard to define the logic of the rule.

- Select one or more content classifier conditions.

- Generate logic between the conditions using and, or, not, and parentheses. This logic should be based on the organization's business rules. For example:

A bank uses a file fingerprinting classifier to identify a blank application form. Administrators create a custom policy with the following rules:

- Because the blank form is for marketing purposes, and the organization wants people to fill it out to apply for loans, one rule that says if the fingerprinting classifier for the blank form is matched, permit it to be sent from all sources to all destination channels.

- A second rule is constructed so that when the form contains a social security number and the word "income," it is a loan application is permitted to go to one destination: the loan department. It is blocked from all other destinations.

The condition logic states: when the fingerprinting classifier is matched AND a social security number pattern is matched AND the key phrase classifier "income" is matched, it is a standard loan application: 1 AND 2 AND 3.

- A third rule to the policy states that when content contains the social security number and the word "income," as well as 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.

To define the rule logic:

- 1) Use the drop-down box next to **This rule monitors** to select one of the following options:

- To trigger the rule on any content without analysis, select **All activities**. This may lead to large numbers of incidents.
- To monitor one or more specific classifiers, select **Specific data**, then use the **in** drop-down list to indicate when to trigger incidents.
 - Select **all parts of the transaction as a whole** to trigger an incident if the sum of all matches in the transaction exceeds the configured threshold. For example, if the threshold is 3, then a transaction with 2 matches in the message body and one match in the subject line triggers an incident.
 - Select **each part of the transaction separately** to trigger an incident triggered only when the threshold is 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.

- 2) Click **Add**, then use the drop-down list to:

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

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

To edit a condition's threshold (the number of matches that trigger an incident), click a hyperlink in the Properties column. See also, *Viewing or editing conditions and thresholds* section.

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* section for more information.

- 3) Repeat the previous step to add additional content classifiers, as needed.

- 4) If more than one condition is defined, indicate when the rule should be triggered:
- If all of the selected conditions must be matched to trigger the rule, select **All conditions matched**.
 - If only one of the selected conditions must be met, select **At least one of the conditions matched**.
 - To define conditions for the rule, select **Custom**, then:
 - a) Double-click a condition name to add it to the formula box.
 - b) Click the **And**, **Or**, or **Not** button to define a condition.
Optionally add parentheses, as in any mathematical operation. For example:
 $(1 \text{ AND } 2) \text{ OR } (3 \text{ AND } 4) \text{ OR } 5$
Each number corresponds to a condition (1 is the first condition, 2 is the second, and so on).
 - c) Double-click another condition name.
 - d) Continue until the condition is fully defined.

Click the information icon on the right of the box to view a precise description of the condition that has been defined.

Related concepts

- [Classifying Content](#) on page 181
- [Patterns & Phrases](#) on page 170
- [File Properties](#) on page 172
- [Fingerprint](#) on page 173
- [Machine Learning](#) on page 174
- [Transaction Size](#) on page 175
- [Number of Email Attachments](#) on page 175
- [Number of Email Destinations](#) on page 175

Related tasks

- [Custom Policy Wizard - Severity and Action](#) on page 161
- [Viewing or editing conditions and thresholds](#) on page 158
- [Adding a dictionary classifier](#) on page 193

Viewing or editing conditions and thresholds

Click a hyperlink in the **Properties** column on the Condition tab of the custom policy wizard to view and edit the properties of a condition line, including the name, description, and a variety of other details.



Note

See *Fingerprint classifiers* section for information about additional configurable properties that are unique to fingerprint classifiers.

Steps

- 1) A condition's threshold is the number of matches that trigger an incident. Select one of the following:
 - Use **At least** to select the minimum number of matches that must be made. Valid values are 1-999.
 - Use **Between** to select an exact range of matches that must be made. Valid values are 1-999.
 - Use **No match exists** to trigger the rule if there are no matches.

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* section.
- 2) Define how the threshold numbers are calculated:
 - **Count only unique matches** for the transaction. Note that case differences are counted separately for word-related classifiers. For example, word, Word, and WORD would return 3 matches when this option is selected.
 - **Count all matches, even duplicates.**

- 3) Under Analyzed Fields, view and select the fields to search for this content classifier.
- Select **Search all available fields** to search content fields that pose the highest risk of a policy breach. The fields are searched for the specified key phrases, regular expressions, dictionary terms, or fingerprints. This is the default.
 - Select **Search specific fields** to identify one or more fields to search. The fields apply mainly to the email destination channel.

Field	Description
File/attachment	Search files or attachments for each chosen destination channel.
File metadata	Search the metadata of files or attachments.
Subject	Search only the subject line of messages.
Body	Search only the main body of a messages.
From	Search only the From field of a message.
To	Search only the To field of a message (email only).
Cc	Search only the carbon copy field of a message (email only).
Bcc	Search only the blind carbon copy field of a message (email only).
Other header	<p>Search in headers that are not covered by the above options:</p> <ul style="list-style-type: none"> ■ Search in All headers not covered in the above options. Includes all standard headers—Date, Message-ID, or Importance—as well as non-standard headers (x-headers, including x-mailer, x-spam-reason, and x-origin-ip) added during the sending of an email. ■ Search in User-defined header. Some organizations define x-headers to add custom information to the email message header. For example, they might create an x- header such as “X-MyCompany: Copyright 2017 MyCompany”. After selecting this option, enter the header name.

If a selected field is not found in a transaction, it is ignored.

For email messages, only sent email is analyzed. (When users save messages rather than sending them, breaches are not detected.)

Some fields do not apply to all channels, and are ignored for any non-applicable channel.

Related concepts

[Fingerprint classifiers on page 161](#)

Related tasks

[Adding a dictionary classifier on page 193](#)

Fingerprint classifiers

The Properties link for a database classifier opens a page with two tabs: General and Properties. Use the General tab for field selection and the Properties tab to define the threshold and email fields described in above.

For database records classifiers, the page displays table field (or column) names. Select the fields to scan (up to 32 per table).

For endpoints, the number of fields selected for a database fingerprinting classifier can affect accuracy. For the most accurate results, scan 3 or more fields.

- If only one field is being scanned, set a minimum threshold of 5 to reduce the likelihood of unintended matches. (When an administrator attempts to set a lower threshold, the system changes it to 5.)
- If 2 fields are scanned, set the minimum threshold to 3 or more. (Trigger an incident when 3 or more field1/field2 combinations are detected.)

Number of Fields	Minimum Threshold
1	5
2	3
3 or more	1



Note

If a condition applies to 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* section.

Related concepts

[Database fingerprinting](#) on page 217

Custom Policy Wizard - Severity and Action

Use the **Severity & Action** tab of the custom policy wizard to define when to trigger an incident:

- Select **Trigger an incident for every matched condition** to trigger an incident every time a condition in the rule is matched. (For example, if a user sends an email message containing sensitive content, then prints the message, 2 incidents are generated.)
- Select **Accumulate matches before creating an incident** to have the system collect matches for a particular source over time and create incidents when a threshold is met (*drip DLP*). The system remembers user activity and generates incidents for matches that occur within a defined period.

To configure either option, configure the first line in the Severity and Action Plan table:

1) Specify the incident severity:

- **Low** - Incidents that match this rule are of low importance. The policy breach is minor.
- **Medium** - Incidents that match this rule are of medium importance. The policy breach is moderate.

- **High** - Incidents that match this rule are very important and warrant immediate attention. The policy breach is severe.
- 2)** Select an action plan. Action plans are customizable.
- Select **Audit Only** to monitor and record (audit) incidents.
 - Select **Audit and Notify** (default) to monitor and record incidents. In addition, if notifications are configured, generate notifications.
 - Select **Block All** to block and audit incidents. In addition, if notifications are configured, generate notifications.
 - Select **Drop Email Attachments** to remove email attachments that violate policy.
 - Select **Audit Without Forensics** to monitor and record incidents without recording forensic data.
 - Select **Block Without Forensics** to block and audit incidents without recording forensic data.

Define severity and action at a more granular level by selecting the second and third lines of the **Severity and Action Plan** table and selecting a severity and action plan for each line.

For example, when there are at least 10 matches (10 or more), select **Medium** as severity and **Audit & Notify** as action plan. When there are at least 20 matches, select **High** as severity and **Block** as action plan.



Tip

Start with an action plan of audit only. Once policies have been tuned, send notifications or use block actions, as needed.

Click the icon to edit the action plan. Change the action for each channel, as needed. 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* section, for details.

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

- 3)** Under the **Severity and Action** section, select how matches should be calculated:
- Select **greatest number of** matched conditions to have the number of matches compared, and only the greatest number reported. For example, if there are 5 matches for the classifier “Confidential Pattern”, 3 for “SSN Pattern”, and 10 for “My Key Phrases”, the number of matches would be defined as 10.
 - Select **sum of all** matched conditions to have the number of matches added together and the total reported. Given the same example as above, the number of matches would be defined as 18.

Related concepts

[Risk-Adaptive Protection](#) on page 377

[Action Plans](#) on page 257

Related tasks

[Custom Policy Wizard - Source](#) on page 164

[Analytics](#) on page 379

Severity and Action for Risk-Adaptive Protection users

If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5). For each severity level in a rule, you can also configure a Dynamic User Protection Severity value that impacts the risk score calculation for a user in Forcepoint Dynamic User Protection. The following severity levels are available:

- **None (Do not Report)**: DLP incidents are not reported to Forcepoint Dynamic User Protection.
- **None (Report as Informative)**: DLP incidents are reported as informative to Forcepoint Dynamic User Protection.
- **Low**: DLP incidents are of low importance. The policy breach is minor.
- **Medium**: DLP incidents are of medium importance. The policy breach is moderate.
- **High**: DLP incidents are important and should be monitored. The policy breach is significant.
- **Critical**: DLP incidents are very important and warrant immediate attention. The policy breach is severe.

If the severity value does not match the system default for the User-Risk Impact, a notification is displayed.

Dynamic User Protection Severity values can also be batch-configured. See *Updater rules of a current policy* section.

For more information on the Forcepoint Dynamic User Protection treatment of Dynamic User Protection Severity, see the *Dynamic User Protection Help* document on the Forcepoint Support site.

Click the **Add** button () to create a new action plan and add it to all risk-level action-plan lists. You can then select the new action plan for each risk level.

See *Risk-Adaptive Protection* section, and *Analytics* section.



Note

The Risk-Adaptive Protection section only affects users that were defined as risk-adaptive users (see *Custom user directory groups* section and *Custom users* section, on how to define such users.)

When the “Accumulate matches” option is selected, also configure:

1) How to count matches:

- Count incident **transactions** as they accumulate for a given source, even though each incident can have multiple triggers.
- Count **unique matches** to count violation triggers that accumulate for a source, but only triggers that are unique.
If, for example, there is 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.
 - If the user sends 20 email messages with the same credit card number, no triggers are counted, because the numbers were not unique.

Note that case differences are counted separately in word-related classifiers. For example, word, Word, and WORD.

- Count **all matches** (default) 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.

- 2) Select a time period for accumulating matches. The time period is a sliding window. It resets every time a match is detected.
- 3) Use the **Where there are at least** field to define the threshold for triggering an incident. For example, trigger an incident when there are at least 3 matches (3 or more). If the threshold is not met, the match count is 0.
- 4) Use the **The rate of matches should decline...** field to specify how long the system should continue counting matches once the rate begins to decline. As long as the system continues to detect the configured number of matches over the configured period, it continues to accumulate the matches in the same incident.

Related concepts

[Risk-Adaptive Protection](#) on page 377

Related tasks

[Update rules of a current policy](#) on page 116

[Analytics](#) on page 379

[Custom user directory groups](#) on page 246

[Custom users](#) on page 248

Custom Policy Wizard - Source

Use the **Source** tab of the custom policy wizard to identify the sources of data—such as computers, devices, domains, and networks—that apply to this rule. By default, all sources of data are applied.

Steps

- 1) To define specific sources of data, click **Edit**, then see *Selecting items to include or exclude in a policy* section.
- 2) If endpoint machines are a possible source, select the **Machine type**: laptops, static devices (such as desktops), or all machines (default).
- 3) Select the **Network location** of the endpoint machines to analyze: anywhere (default), when connected to the corporate network, or when not connected to the corporate network.

Continue with *Custom Policy Wizard - Destination*.

Related concepts

[Selecting items to include or exclude in a policy](#) on page 122

[Custom Policy Wizard - Destination](#) on page 165

Custom Policy Wizard - Destination

Use the **Destination** page of the custom policy wizard to select possible destinations for data protected by this rule.

The Destination page varies based on subscription. You may see:

- *Standard Forcepoint DLP options*
- *Forcepoint Web Security mode*
- *Forcepoint Email Security mode*

For information on the file sizes that are support for the various destination channels, see the [File Size Limits](#) technical reference.



Tip

For help using the Select Items screen that appears when you edit any policy option, see [Selecting items to include or exclude in a policy](#) section.

Related concepts

[What can I protect?](#) on page 9

[Forcepoint Web Security mode](#) on page 168

[Selecting items to include or exclude in a policy](#) on page 122

Related tasks

[Rule Wizard - Finish](#) on page 169

[Standard Forcepoint DLP options](#) on page 165

[Forcepoint Email Security mode](#) on page 168

Standard Forcepoint DLP options

Steps

- 1) Select **Network Email** to monitor email going through the network or a supported cloud infrastructure such as Microsoft Azure. By default, email is analyzed on all network destinations.
 - Click **Edit** to select the destinations (such as computers, policies, or domains) this policy should analyze.
 - Click **Direction** to select the traffic to monitor: inbound, outbound, internal, or all 3. Forcepoint DLP Email Gateway analyzes traffic in all 3 directions.

Protectors monitor all traffic directed to them. All transactions are regarded as outbound.

Email Security Cloud protects only outbound traffic.

- 2)** Select **Endpoint Email** to monitor email on endpoint machines (requires Forcepoint DLP Endpoint). By default, email is analyzed on all endpoint destinations.

- Click **Edit** to select the domains this policy should analyze.
- If Forcepoint DLP is integrated with Forcepoint Email Security, click **Direction** to select the traffic to monitor: outbound (default) or internal. Inbound email cannot be monitored on endpoints. The selected direction must have been configured under **Settings > General > Endpoint > Email Domains** to analyze endpoint email traffic.

For a complete list of endpoint email applications that Forcepoint DLP supports, see [Forcepoint DLP Endpoint applications](#).

- 3)** Select **DLP Cloud Applications** to analyze files sent to supported cloud applications, such as Office365 or Box.



Important

File analysis occurs only when the following conditions are met:

- Cloud Applications service is activated (**Settings > General > Services**)
- Forcepoint Security Manager is connected to Data Protection Service (**Settings > General > Services**)
- The policy was deployed to this service successfully.

By default, all cloud channels are unselected.

- Select DLP Cloud API, DLP Cloud Proxy, or both.
- If you select DLP Cloud API:
 - By default, all applications are selected for monitoring. Select specific cloud applications to monitor by clicking **Edit** and adding available elements to the Selected Elements list. At least one application must be selected.
If you have an Office 365 cloud application, you can choose to monitor **OneDrive**, **SharePoint**, **Teams**, or **Other**. Select **Other** to monitor Office 365 applications that are not OneDrive, SharePoint, or Teams.
 - Select at least one user operation to monitor (File uploading/attaching, File downloading, External file-sharing, Unrecognized file-sharing).
- If you select DLP Cloud Proxy:
 - By default, all applications are selected for monitoring. Select specific cloud applications to monitor by clicking **Edit** and adding available elements to the Selected Elements list. At least one application must be selected.
If you have an Office 365 cloud application, you can choose to monitor **OneDrive**, **SharePoint**, **Teams**, or **Other**. Select **Other** to monitor Office 365 applications that are not OneDrive, SharePoint, or Teams.
 - Select at least one user operation to monitor (File uploading/attaching, File downloading).

- 4)** Select **Mobile Email** to monitor email sent to users' mobile devices, then select whose devices to monitor. It is possible to 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.

- 5) Select Web** to prevent or monitor users 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 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.
Note that several SaaS domains are excluded from analysis by default. Optionally, exclude more domains or remove domains 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* section.
 - Click **Channels** to select or deselect individual Web channels.
- For a complete list of endpoint browsers supported by Forcepoint DLP, see *Selecting endpoint destination channels to monitor* section.
- 6) Select Endpoint Printing** to analyze files that endpoint users send to printers. (Requires Forcepoint DLP Endpoint.)
To select the printers to analyze click **Edit**.
- 7) Select Endpoint Application** 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**.
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.
- For a list of applications that the system supports out of the box, see [Forcepoint DLP Endpoint Applications](#) section. You can also add custom applications.

**Note**

The list you create here is overridden by trusted application settings you configured under **Resources > Endpoint Applications**. Groups that are trusted on that page are not enforced even if they are included in the policy.

- 8) Select **Endpoint Removable Media** to analyze media such as thumb drives, external hard drives, and other USB devices on endpoint machines. By default, all removable media is included.
 - To select the media to analyze, click **Edit**.
 - For a complete list of supported endpoint removable devices, see *Selecting endpoint destination channels to monitor* section.
 - Linux-based endpoints cannot share removable media devices through NFS.

- 9) Select **Endpoint LAN** 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.
 Endpoint LAN control is applicable to Windows file sharing only.
 To select a network to analyze, click **Edit**.
 - Specify a list of allowed destination IP addresses or hostnames for LAN copy.
 Users may connect to a destination machine using the hostname, IP address, or mapped drive, for example. Forcepoint DLP does not resolve the multiple names for a single destination. To block or allow access to a machine, specify each of the identifiers a user might specify: for example, FQDN, hostname, mapped drive, and so on. Alternatively, always block or allow access using hostname and require users to use hostname.
 - Data from an endpoint client can be intercepted.
 - 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.

Related tasks

[Business Units](#) on page 251

[Selecting endpoint destination channels to monitor](#) on page 456

Forcepoint Web Security mode

By default, web channels are analyzed on all destinations. For Forcepoint Web Security, this includes:

- **FTP** includes FTP-over-HTTP.
- **Web** includes websites, blogs, and forums via HTTP and HTTPS. Click **Edit** to select the destinations to analyze.

Forcepoint Email Security mode

By default, all network email is analyzed in all directions: outbound, inbound, and internal.

- 1) Click **Edit** to select the email destination to analyze.

Rule Wizard - Finish

Steps

- 1) Click **Next** to display a summary of the rule that was just created.
- 2) If adjustments are needed, go back to previous steps to make changes.
- 3) When the rule is correct, click **Finish**.
The new rule is added to the selected policy.

Selecting a content classifier

The Conditions tab of the custom policy wizard is used to add content classifiers or email attributes to the policy.

- Content classifiers are used to identify account numbers, credit card numbers, industry terms, and similar items as sensitive data.
- Attributes are used to identify email components to monitor. The available content classifiers and attributes are:
 - *Patterns & Phrases* classify data by regular expression (regex) patterns, key phrases, dictionaries, and scripts. Regex patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.
 - *File Properties* classify data by file name, type, or size. File name identifies files by their extension. File type identifies files by their “magic number” (an internal identifier).
 - *Fingerprint* files or directories, including SharePoint directories, and database records directly from a database table, Salesforce table, or CSV file.
 - Use *Machine Learning* to provide examples of the data that you want to protect, so the system can learn from them and identify items of a similar nature.
- Set a *Transaction Size* to monitor transactions that exceed a size limit, such as email messages more than 10 MB.
- Set a *Number of Email Attachments* to monitor email messages containing multiple attachments.
- Set a *Number of Email Destinations* to monitor email messages being sent to multiple destination domains.

Related concepts

- [Patterns & Phrases](#) on page 170
- [File Properties](#) on page 172
- [Fingerprint](#) on page 173
- [Machine Learning](#) on page 174
- [Transaction Size](#) on page 175
- [Number of Email Attachments](#) on page 175
- [Number of Email Destinations](#) on page 175

Patterns & Phrases

Patterns & Phrases classify data by regular expression (regex) patterns, key phrases, dictionaries, and scripts. Regex patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.

Related concepts

[General tab](#) on page 170

Related tasks

[Properties tab](#) on page 170

General tab

The General tab of the Select a Content Classifier window lists the available content classifiers. Sort or filter columns to locate specific classifiers.

To search for a classifier, enter a key term (like “credit card”) and click the magnifying glass to search for a pertinent content classifier. Optionally include wildcards, such as “credit*”.

Click **New** to add one or more new content classifiers to the rule. Administrators can add as many as needed. Select from the following classifier types:

- A **Regular Expression** is a string 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.
- A **Key Phrase** is an exact keyword or phrase (such as “top secret” or “confidential”) that might be found in content intended for an external recipient, and possibly indicate that classified information is being distributed. The system can block the distribution of this information.
- A **Dictionary** is a container for words and expressions belonging to the same language. Many dictionaries are built into Forcepoint DLP, including lists for medical conditions, financial terms, legal terms, and credit card terms. You can also create or customize a dictionary list, and then use this it in your policies. Each term in a dictionary can be assigned a weight, so when one term is detected, more points are given towards a threshold than when another term is detected.



Note

While it is possible to select predefined script classifiers, it is not possible to define new scripts on the selection screen. For more information about scripts, how they are used, and how they can be modified, see [Scripts](#) section.

Related concepts

[Scripts](#) on page 198

Properties tab

Define the threshold for matches and the fields to search for the classifier.

Steps

- 1)** Set the **Threshold** that determines the number of matches that trigger an incident:
 - Use **At least** to select the minimum number of matches that must be made (1-999).
 - Use **Between** to select an exact range of matches (1-999).
 - Use **No match exists** to trigger the rule if there are no matches.

- 2)** Define how the threshold numbers are calculated:
 - Count only unique matches. Note that case differences are counted separately for word-related classifiers. For example, word, Word, and WORD would return 3 matches when this option is selected.
 - Count all matches, even duplicates

- 3)** Click **Analyze Fields** to view and select the fields to search for this classifier.
 - Select **Search all available fields** to search content fields that pose the highest risk of a policy breach. The fields are searched for the key phrases, regular expressions, dictionary terms, or fingerprints you specify. This is the default.
 - Select **Search specific fields** to identify one or more fields to search. The fields apply mainly to the email destination channel.

Field	Description
File/attachment	Search files or attachments for each chosen destination channel.
File metadata	Search the metadata of files or attachments.
Subject	Search only the subject line of messages.
Body	Search only the main body of a messages.
From	Search only the From field of a message.
To	Search only the To field of a message (email only).
Cc	Search only the carbon copy field of a message (email only).
Bcc	Search only the blind carbon copy field of a message (email only).
Other header	<p>Search in headers that are not covered by the above options:</p> <ul style="list-style-type: none"> ■ Search in All headers not covered in the above options. Includes all standard headers—Date, Message-ID, or Importance—as well as non-standard headers (x-headers, including x-mailer, x-spam-reason, and x-origin-ip) added during the sending of an email. ■ Search in User-defined header. Some organizations define x-headers to add custom information to the email message header. For example, they might create an x- header such as “X-MyCompany: Copyright 2017 MyCompany”. <p>After selecting this option, enter the header name.</p>

File Properties

File Properties are used to classify the data by file name, type, or size. File name identifies files by their extension. File type identifies files by their “magic number” (an internal identifier)

Related concepts

[General tab](#) on page 172

Related tasks

[Properties tab](#) on page 172

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 (see *File properties* section).
 - File-type classifiers identify a single kind of file (like Microsoft Word File) or a group of similar kinds of files (like Various Archive Formats), based on the file’s magic number (an internal identifier).
 - File-name classifiers identify files by file-name extension (such as *.docx) or the file name itself (such as myfile*.doc).
 - File-size classifiers identify files by their size. Select the classifier to add to the policy’s rule.

Sort or filter columns to help you locate a specific classifier.

Related concepts

[File properties](#) on page 196

Properties tab

Before you begin

Use the Properties tab to configure the threshold for matches.

Steps

- 1) Set the **Threshold** that determines the number of matches that trigger an incident:
 - Use **At least** to select the minimum number of matches that must be made (1-999).
 - Use **Between** to select an exact range of matches (1-999).
 - Use **No match exists** to trigger the rule if there are no matches.

2) Define how the threshold numbers are calculated:

- Count only unique matches. Note that case differences are counted separately for word-related classifiers. For example, word, Word, and WORD would return 3 matches when this option is selected.
- Count all matches, even duplicates

Fingerprint

Fingerprint- files or directories, including SharePoint directories, and database records directly from a database table, Salesforce table, or CSV file.

Related concepts

[General tab](#) on page 173

[Properties tab](#) on page 174

General tab

Two types of fingerprint classifiers can be added: files or database records. The General tab displays all classifiers from both types. Sort or filter columns to locate a specific classifier.

When a database records classifier is highlighted, the bottom of the screen displays the field (or column) names of the selected table. Select the fields to scan (up to 32 per table).

For endpoints, the number of fields selected for a database fingerprinting classifier can affect accuracy. For the most accurate results, scan 3 or more fields.

- If only one field is being scanned, set a minimum threshold of 5 to reduce the likelihood of unintended matches. (When an administrator attempts to set a lower threshold, the system changes it to 5.)
- If you 2 fields are scanned, set the minimum threshold to 3 or more. (Trigger an incident when 3 or more field1/field2 combinations are detected.)

Number of Fields	Minimum Threshold
1	5
2	3
3 or more	1



Note

If a condition applies to 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* section,

Related concepts

[Database fingerprinting](#) on page 217

Properties tab

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

Field	Description
Threshold	A condition's threshold is the number of matches that trigger an incident. Select one of the following: <ul style="list-style-type: none"> ■ 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.
Email Fields	Click Email Fields to view and select the email fields to search for this condition.
Search in all the email fields	Select to search the entire email message for the key phrase, regular expression, or dictionary terms. This is the default.
Search only in these fields	Select to search only specific parts of the email message. Choose one or more of the following: <ul style="list-style-type: none"> ■ 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 any other headers that are not covered by the above options. This includes all x-headers. You can either search in all other headers, or define a specific header that you want to search.

Machine Learning

The page lists all the machine learning classifiers that are ready for use (finished processing). Select a classifier to use in this rule. To find a classifier, use the arrows in the column headers to sort the table by name, description, or accuracy.

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

Transaction Size

Select the size of transactions to monitor. For example:

- For email channels, select 25 MB to detect email messages 25 MB or larger, but ignore messages smaller than 25 MB, even if there is a match.
- For web channels, select 25 MB 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 (20, by default).

For example, select 10 to detect messages with 10 or more attachments, but ignore messages with fewer than 10 attachments, even if there is a match.

Number of Email Destinations

Messages sent to multiple destination domains 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. They can be added to a policy, edited, or deleted from a policy at any time, as well as enabled or disabled.

When a policy is created, a rule is created automatically as content classifiers are configured.

When adding content classifiers to a policy, optionally select **Create Rule from Classifier** to add the rule manually. (See *Creating a rule from a content classifier* section, .)

On the Manage DLP Policies or Manage Discovery Policies page, you can expand a policy in the tree view and click a rule, then select **Edit**, **Add > Rule**, or **Delete** to make changes.

Predefined content classifiers cannot be edited in the rules of the Forcepoint-defined policy templates. The Condition tab for these rules shows the name and type of predefined classifier, but does not allow administrators to view the 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, see *Managing exceptions* section.

Related concepts

[Adding a new exception](#) on page 177

[Managing exceptions](#) on page 176

Related tasks

[Creating a rule from a content classifier](#) on page 239

Managing exceptions

Most rules have exceptions.

In Forcepoint DLP, 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. For example:

- The rule “Pizza” indicates that email messages from John Doe that have the word “pizza” in them should be encrypted.
- An exception to “Pizza” indicates that messages that include 5 instances of “pepperoni” should be quarantined.

As a result, messages from John Doe with both “pizza” and 5 instances of “pepperoni” are quarantined.

Unlike rules, exceptions cannot be cumulative.

Add exceptions on the Manage DLP Policies or Manage Discovery Policies page in the Data Security module of the Forcepoint Security Manager ([Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies](#)).

Select a rule in the tree, then select **Add > Exception** from the toolbar at the top of the content pane.

Like policies, exceptions have levels that define execution priority order. See *Rearranging exceptions* section for information on ordering exceptions.

Related concepts

[Managing rules](#) on page 175

[Adding a new exception](#) on page 177

Related tasks

[Rearranging exceptions](#) on page 177

Rearranging exceptions

Before you begin

Exceptions have execution priority order. The tree structure reflects the current order. When a policy is applied, exception 1 is applied first, then exception 2, and so on. If an exception is triggered, any exceptions below it in the list are not checked.

To manage the order of exceptions:

Steps

- 1) Select **More Actions > Rearrange Exceptions** in the toolbar at the top of the Manage DLP Policies or Manage Discovery Policies page.
- 2) 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

Add exceptions on the Manage DLP Policies or Manage Discovery Policies page in the Data Security module of the Forcepoint Security Manager (**Main > Policy Management > DLP Policies or Discovery Policies > Manage Policies**).

Select a rule in the tree, the select **Add > Exception** from the toolbar at the top of the content pane. (You cannot add an exception to a cumulative rule.)

The exception wizard opens to the first of 4 pages. See *Exception Wizard - General* section.

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

Related concepts

[Exception Wizard - Properties](#) on page 178

Related tasks

[Exception Wizard - General](#) on page 177

[Exception Wizard - Severity & Action](#) on page 178

[Exception Wizard - Finish](#) on page 180

Exception Wizard - General

The General tab of the exception wizard displays the name of the policy and rule affected by the exception being created.

- 1) Enter a unique **Exception name**.
- 2) Indicate whether or not the new exception is **Enabled**.

- 3) Enter a helpful **Description** for the exception.
- 4) Click **Next** to continue to the Properties page of the exception wizard (see *Exception Wizard - Properties* section.)

Related concepts

[Exception Wizard - Properties](#) on page 178

Related tasks

[Custom Policy Wizard - General](#) on page 156

Exception Wizard - Properties

Use the Properties tab of the exception wizard to specify conditions, sources, and destinations that apply to the exception.

To start, highlight a property in the Exception Properties list, then configure the property in the right pane. Mark the check box next to the property name to enable that property.

- Select **Condition** to change the condition parameters established for the rule, such as the content classifier, threshold, or condition relations.
See *Custom Policy Wizard - Condition* section, for explanations of the condition properties.
- Select **Source** to change the source of data defined for the rule.
See *Custom Policy Wizard - Source* section, for explanations of the source properties.
- Select **Destination** to change the destination of data defined for the rule.
See *Custom Policy Wizard - Destination* section, for explanations of the fields on this screen.

When you are finished, click **Next** to continue to the Severity & Action page of the exception wizard (see *Exception Wizard - Severity & Action* section).

Related concepts

[Custom Policy Wizard - Condition](#) on page 156

[Custom Policy Wizard - Destination](#) on page 165

Related tasks

[Custom Policy Wizard - Source](#) on page 164

[Exception Wizard - Severity & Action](#) on page 178

Exception Wizard - Severity & Action

Use the Severity & Action tab of the exception wizard to configure a severity level and an action plan for conditions that match the exception.

- 1) Select severity and action plans according to matches of incidents that match this exception. This overrides the rule's severity and action plan.

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.

Action Plan:

- Select **Block all** to use the strict actions defined under **Main > Policy Management > Resources > Action Plans**.
- Select **Audit & notify manager** (the default) to use the moderate actions defined. These are a compromise between the blocking and auditing plans.
- Select **Audit only** to use audit incidents and not block them.

New and edit icons are displayed to the right of the action plan drop-down list.

- Click the edit icon to 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 new icon to create a new action plan. See *Action Plans* section.

2) 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.

3) If you are using Risk-Adaptive Protection to determine actions according to the source's risk level, select an action plan for each one of the risk levels (1-5), and a Dynamic User Protection Severity value. When the rule is triggered, the action plan that will be executed will be the one that was defined for the risk level of the user as determined by Forcepoint Behavioral Analytics. The following severity levels are available:

- **None (Do not Report)**: DLP incidents are not reported to Forcepoint Dynamic User Protection.
- **None (Report as Informative)**: DLP incidents are reported as informative to Forcepoint Dynamic User Protection.
- **Low**: DLP incidents are of low importance. The policy breach is minor.
- **Medium**: DLP incidents are of medium importance. The policy breach is moderate.
- **High**: DLP incidents are important and should be monitored. The policy breach is significant.
- **Critical**: DLP incidents are very important and warrant immediate attention. The policy breach is severe.

4) If the severity value does not match the system default for the User-Risk Impact, a notification is displayed.

5) Click the Add button () to create a new action plan and add it to all risk-level action-plan lists. You can then select the new action plan for each risk level.



Note

The Risk-Adaptive Protection section only affects users that were defined as risk-adaptive users (see *Custom user directory groups* section and *Custom users* section, on how to define such users.)

6) Click **Next** to continue to the Finish page of the exception wizard. See *Exception Wizard - Finish* section.

Related concepts

[Risk-Adaptive Protection](#) on page 377

[Action Plans](#) on page 257

Related tasks

[Custom Policy Wizard - Severity and Action](#) on page 161

[Analytics](#) on page 379

[Custom user directory groups](#) on page 246

[Custom users](#) on page 248

[Exception Wizard - Finish](#) on page 180

Exception Wizard - Finish

Use the Finish page of the exception wizard to review the exception, make any required updates, and add the exception to the rule.

Steps

- 1) Click **Next** to display a summary of the exception that was just created.
- 2) If adjustments are needed, go back to previous steps to make changes.
- 3) When the exception is correct, click **Finish**. The new exception is added to the selected rule.

Chapter 12

Classifying Content

Contents

- [Content classifier menu bar](#) on page 183
- [Manually deleting fingerprinting classifiers](#) on page 185
- [Details pane](#) on page 186
- [Patterns & Phrases](#) on page 189
- [File Labeling](#) on page 194
- [File properties](#) on page 196
- [Scripts](#) on page 198
- [File fingerprinting](#) on page 200
- [Database fingerprinting](#) on page 217
- [Database Fingerprinting Wizard - Scheduler](#) on page 230
- [Imported fingerprinting](#) on page 233
- [Machine learning](#) on page 235
- [Creating a rule from a content classifier](#) on page 239

Forcepoint DLP policies use content classifiers to describe the data that is being protected. Content can be classified according to file properties, key phrases, scripts, regular expression (regex) patterns, and dictionaries. Forcepoint DLP can also fingerprint data using, or administrators can provide examples of the type of data to protect so the system can learn from it and make decisions.

Use the [Main > Policy Management > Content Classifiers](#) page to start classifying data.

To start, select one of the listed content classifiers.

Classifier	Description
Attributes	
<i>Patterns & Phrases</i>	Classify data using regex patterns, key phrases, dictionaries, and scripts. Regex patterns are used to identify alphanumeric strings of a certain format, such as 123-45-6789.
<i>File Labeling</i>	Classify data by using the labeling system(s).
<i>File properties</i>	Classify data by file name, type, or size. File name identifies files by their extension. File type identifies files by their magic number (an internal identifier).
Fingerprints	
<i>File fingerprinting</i>	Fingerprint files or directories, including Microsoft SharePoint and IBM Domino directories.
<i>Database fingerprinting</i>	Fingerprint database records directly from your database table, Salesforce table, or CSV file.

Classifier	Description
Machine Learning	
<i>Machine learning</i>	Provide examples of the data to protect, so the system can learn from them and identify data of a similar nature.

Forcepoint provides predefined classifiers for the most common use cases. These are described in [Predefined Policies and Classifiers](#).

To classify content, administrators can:

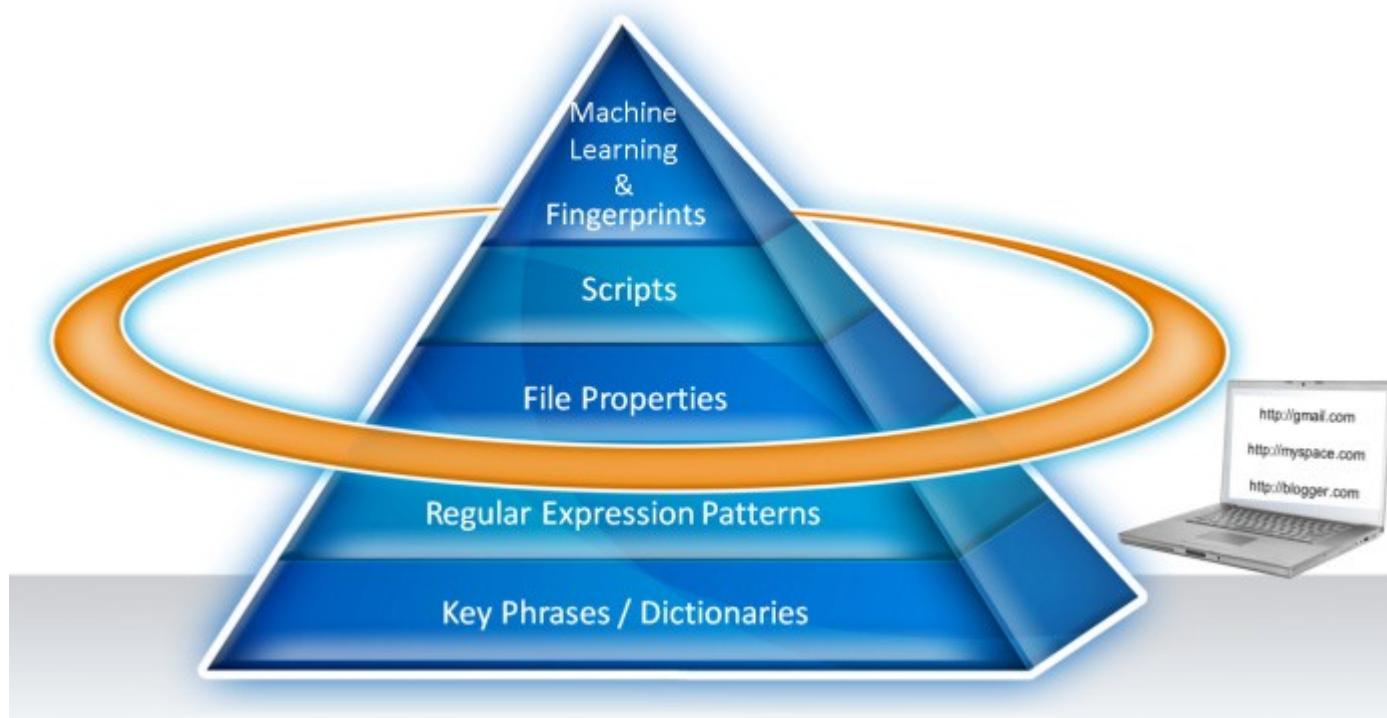
- Select one of the predefined classifiers.
- Customize a classifier as needed.
- Create a new classifier from scratch.



Important

After classifying content, 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.

The diagram below illustrates the granularity of each content classifier.



After classifying data, 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.

Before creating a database fingerprinting classifier, read *Preparing for database fingerprinting* section and *Creating a validation script* section.

Forcepoint DLP automatically runs validation scripts on your new database fingerprinting classifiers if the scripts are set up properly.

Related concepts

- [File properties](#) on page 196
- [Machine learning](#) on page 235
- [Database fingerprinting](#) on page 217
- [File Labeling](#) on page 194
- [File fingerprinting](#) on page 200
- [Preparing for database fingerprinting](#) on page 219

Related tasks

- [Patterns & Phrases](#) on page 189

Content classifier menu bar

When working with most content classifiers, the toolbar at the top of the content pane offers the following options:

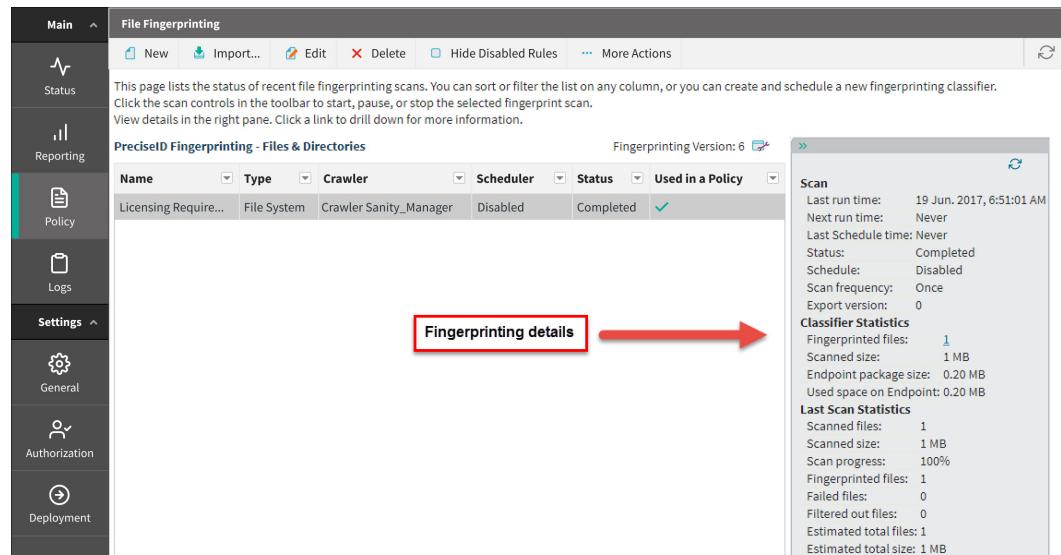
Button	Description
New	Opens a dialog so you can create a new classifier of the selected type.
Delete	Deletes the selected classifier. Be sure to check where the classifier's used before deleting it. (See Where Used , below.) Note: You can delete only one classifier at a time. If you're deleting a fingerprint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

The fingerprinting and machine learning classifiers have additional menu options.

Button	Description
Start	Begins the fingerprinting or machine learning scan. Alerts that the task will be moved into manual mode.
Pause	Fingerprinting only. Pauses the scan.

Button	Description
Stop	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.
More Actions	<p>In addition to Create Rule from Classifier and Where Used, fingerprinting and machine learning classifiers offer a reporting option under More Actions:</p> <p>Download Fingerprinting Report - Database fingerprinting only. Downloads a detailed report on fingerprinting activities.</p> <p>Download Machine Learning Report - Machine learning classifiers only. Downloads a detailed report on machine learning processes.</p> <p>Using this report, you can:</p> <ul style="list-style-type: none"> ■ 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.

In addition, the fingerprinting and machine learning classifiers offer a Details pane on the right to show statistics about the scan and scheduler. See *Details pane* section.



Related concepts

Details pane on page 186

Related tasks

[Manually deleting fingerprinting classifiers on page 185](#)
[Creating a rule from a content classifier on page 239](#)

Manually deleting fingerprinting classifiers

If the crawler is unresponsive for any reason when administrators delete a fingerprinting classifier from the management server, the crawler is not alerted that the classifier has been deleted. When the crawler becomes responsive, it continues to run the fingerprinting scan as scheduled and consume unnecessary resources.

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

The Forcepoint Security Manager displays a warning in this situation, and asks if you want to continue. If so, manually delete the classifier as follows:

1) Identify the ID of the job to delete in one of two ways:

- View the Forcepoint DLP System Log (**Main > Logs > 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 management server, but not from the crawler, Crawler_Name 10.201.33.1.

- Log onto the crawler machine associated with the discovery task.

- a) Switch to the %DSS_HOME%/DiscoveryJobs folder.
 %DSS_HOME% is the Forcepoint DLP installation folder.

- b) 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 the task was named “ora3”, 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.
 %DSS_HOME% is the Forcepoint DLP installation folder.

- b) Run the following command:

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

Here, jobId is the ID number 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. Expand or collapse this pane to show more or less detail. Click the links, if offered, to see additional information on a particular statistic.

For information about the details shown, see *Fingerprinting details* section and *Machine learning details* section.

Related concepts

[Fingerprinting details](#) on page 186

[Machine learning details](#) on page 187

Fingerprinting details

For fingerprinting classifiers, the details pane shows the following Scan details:

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

Statistics are also displayed for fingerprinted and committed data. (After a file is fingerprinted, it is inserted in the fingerprint repository, 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.)

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

In addition, statistics are displayed for the most recently run scan, or the scan in progress (if any).

Statistic	Description
Scanned files	The total number of items detected in the last scan
Scanned size	The size of items detected in the scan, all totaled. (Does not apply to database scans.)
Scan/fingerprinting progress	The progress of the scan, in percentage completed
Fingerprinted files/records	The number of items sent to the policy engine's fingerprint repository
Failed files	The number of 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.
Filtered-out files	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.
Estimated total files/ records	An estimate of the total number of items
Estimated total size	An estimate of the total size of items

Machine learning details

For machine learning classifiers, the Active Classifier section of the details pane shows the following information:

Statistic	Description
Accuracy	Expected rate of unintended and undetected matches (false positives and false negatives).
Last successful scan time	The time and date of the last successful scan
All documents folder	Path to the all documents folder
Positive examples folder	Path to the positive examples folder
Negative examples folder	Path to the negative examples folder

Statistic	Description
Sensitivity	<p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>Click the link to adjust the sensitivity level. Your choice depends on how important it is to prevent sensitive data loss.</p>
Ignore inconsistent examples	<p>Indicates whether to ignore documents that do not appear to belong to the positive examples folder or to use them as positive examples anyway.</p> <p>To view a list of inconsistent example documents, download the Machine Learning report.</p>

To keep the machine learning classifier up to date, periodically rescan the examples folders. The Current Scan Statistics section of the details pane shows information

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.

Statistic	Description
Run time	The time and date that the machine learning process last ran
Status	<p>The status of the current content scan. See <i>Machine learning current scan status options</i> section for an explanation of each status option.</p> <p>The status shown in the details pane may be different from the status shown in the Status column of the table if you click Refresh in one area but not the other.</p>
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
Total scanned files	Total number of documents that were scanned

Statistic	Description
Accuracy	Expected rate of unintended and undetected matches (false positives and false negatives).

Machine learning current scan status options

Possible statuses include:

- **Pre-processing (n files)** - The system is locating and counting all the files in the positive example files, negative example files, and all documents folder.
- **Processing (x%)** - The system is processing files in the sample set. The percentage shows the progress made on the total number of files.
- **Training (x%)** - The system is applying algorithms and learning from your positive, negative, and all-documents sample sets.
- **Reprocessing (x%)** - 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.
- **Retraining (x%)** - The system is applying algorithms to learn from the new or broader scan.
- **Completed** - The current scan succeeded and has become an active classifier that you can use.
- **Completed with warnings** - 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 **More Actions** and download the machine learning report.
- **Failed** - The scan could not be completed and the classifier cannot be used. To view the errors that were encountered, click **More Actions** and download the machine learning report.
- **Paused** - The scan was manually paused using the toolbar button.
- **Stopped** - The scan was manually stopped using the toolbar button.

Patterns & Phrases

Use the **Main > Policy Management > Content Classifiers > Patterns & Phrases** page in the Data Security module of the Forcepoint Security Manager to view or manage a list of script, regular expression, dictionary, and key phrase content classifiers.

- Use the Type column to tell whether a classifier is predefined (built-in) or user-defined. The list can be sorted by this column.
- Refer to [Predefined Classifiers](#) for details about each predefined Patterns & Phrases classifier.

On this page:

- Click **New**, then select the classifier type to add a new regular expression (regex), key phrase, or dictionary.
- Select a classifier, then click **Delete** to remove the selected classifier.
- Refer to the Used in a Policy column to determine whether or not a classifier is used. For classifiers that are in use, click **Where Used** to see which policies use the classifier.

Related concepts

[File properties](#) on page 196

Related tasks[Adding or editing a regular expression classifier](#) on page 191[Adding a key phrase classifier](#) on page 192[Adding a dictionary classifier](#) on page 193

Regular expression patterns

Regex patterns are special text strings for describing search patterns that can be detected within content. (Content includes the body of the content as well as any attachments). You define the patterns to look for in content and you set the action to take when a pattern is found.

For example, the string “a\ld+” 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, Forcepoint DLP

uses regular expressions to find strings in the text that match patterns for confidential information. For example, this is a very basic regular expression for catching Visa credit card numbers:

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

Because a regular expression file contains many internal attributes, if it is improperly written it can create many false-positive incidents, 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, 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” with 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, create each content classifier (a pattern, dictionary or any other), then combine them in a rule condition with an AND operator.

When creating a rule for a policy, specify how many instances (matches) of the pattern must be found before the content is considered suspicious enough for the configured action to be taken (for example, 4 or more Social Security numbers).

For each content transmission, the system tallies the number of instances of the pattern 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.

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.

Pattern to exclude

Administrators can define a list of exceptions to a regular expression, script, or dictionary classifier. This is a list of content that matches the classifier, but should not be considered in the tally of matches. For each content item transmitted, the system tallies the number of instances of the pattern, and subtracts any matches in the Exclude list.

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, 777-88-9999, 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.

List of phrases to exclude

Administrators can add a list of suspicious words to a regular expression, script, or dictionary classifier. For each content item transmitted, the rule applies its action only if the total number of matches is above the threshold, **and** a string from the specified list is found. If the number of matches is reached but no strings from the list are present, no further analysis is performed.

Example:

The pattern is Social Security numbers, the number of matches is 2, and the list of phrases to exclude contains "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

Use the **Patterns & Phrases > Regular Expression Properties** page in the Data Security module of the Forcepoint Security Manager to create a pattern classifier either from scratch, or based on an existing classifier.

To create a pattern from scratch:

- 1) Go to the **Content Classifiers > Patterns & Phrases** page.
- 2) Use the toolbar at the top of the content pane to select **New > Regular Expression**.
- 3) Enter a **Name** for the expression, such as Visa card.
- 4) Enter a **Description** for this pattern, such as Visa credit card patterns.
- 5) Use the **Value** field to enter a regular expression (regex), such as all 3-character strings followed by the sequence "123". The expression should be compatible with Perl syntax.

- The Forcepoint Security Manager does not validate your expression. Click the information icon for a list of valid values.
 - To include Unicode characters in your pattern, use the format \x{hex- number}.
- 6)** Click **Exclude** to exclude certain values from the pattern, 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.
- Define the regex **Pattern to exclude**. Click the information icon for a list of valid values.
 - Define the **List of phrases to exclude**. Enter each phrase one by one, then click **Add** to add it to the list. These phrases, when found in combination with the pattern, affect whether the content is considered suspicious.
- Select a phrase and click **Remove** to remove selected phrases from the list.

- 7)** Click **OK**.

To base a classifier on an existing classifier:

- 1)** Go to the **Patterns & Phrases** page.
- 2)** Click the name of a classifier to use it as the basis for a new classifier.
 - Depending on whether the selected classifier is predefined or user-defined, different classifier properties can be edited.
 - Refer to [Regular Expression Patterns](#) for details about each predefined classifier.
- 3)** Change fields as needed.
If you are starting from a predefined classifier, add or remove exclude values. No other fields can be edited.
- 4)** Click **Save As** at the top of the pane, then save the classifier under a new name.



Warning

Forcepoint regularly updates classifiers with new regulations, but cannot update a classifier that has been saved under a new name. Be sure to keep customized classifiers up to date.

Adding a key phrase classifier

Use the **Patterns & Phrases > Key Phrase Properties** page in the Data Security module of the Forcepoint Security Manager to create or edit 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. Forcepoint DLP makes it possible to block distribution of this information by defining a key phrase classifier. No other protection features, such as fingerprinting, are required.

To access the Key Phrase Properties page:

- To create a new key phrase, **New > Key Phrase** in the toolbar for the Patterns & Phrases page.
- To edit an existing key phrase, click the name of the key phrase in the list on the Patterns & Phrases page.

To define or update the key phrase:

- 1)** Enter a **Name** for the key phrase classifier.

- 2) Enter a **Description** for this key phrase.
- 3) Use the **Phrase to search** field to 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.
- 4) 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

Use the **Patterns & Phrases > Dictionary Properties** page in the Data Security module of the Forcepoint Security Manager to create or edit a dictionary classifier either from scratch.

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

- Many dictionaries are built into Forcepoint DLP. There are lists for medical conditions, financial terms, and more.
- Administrators can also create or customize a dictionary list, then use it in policies, either as a classifier or an exception.

Policies can include a combination of classifier types. For example, a policy might include a regex classifier that identifies alphanumerical sequences found in part numbers, as well as a custom dictionary of part names to further identify risk. This helps to reduce false positives.

To access the Dictionary Properties page:

- To create a dictionary classifier from scratch, select **New > Dictionary** in the toolbar at the top of the Patterns & Phrases page.
- Do edit an existing dictionary classifier, select the classifier name in the Patterns & Phrases list.

To define or update the dictionary:

- 1) Enter a **Name** for this pattern, such as Diseases.
- 2) Enter a **Description** for this dictionary, such as Disease terminology.
- 3) Under List of phrases to include, use the **Phrase** field to enter a word or phrase to include, then 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.
- 4) 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.

- 5) To create a dictionary containing many phrases more quickly, 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. Valid weights are from -999 to 999. If a phrase has no weight, it is assigned the default weight of 1.
- Separate the phrase and weight by a comma. Enclose the phrase in quotes (not required if there is no weight). For example:
"confidential",5
"ProjectX",8
"ProjectY",3
- 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.
- Slashes, tabs, hyphens, underscores, and carriage returns are included in the search.
- Common words are also included, unlike when fingerprint scans are performed.

- 6) Indicate whether or not **The phrases in this dictionary are case-sensitive**.

- 7) If you are editing a predefined dictionary, click **Exclude** to exclude certain values from the classifier, then:

- Define the regex **Pattern to exclude**. Click the "i" icon for a list of valid values.
- 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.

- 8) Click **OK**.

File Labeling

Forcepoint DLP supports file label detection upon the following conditions:

- The file type is included in the list of files supported for metadata extraction. See [Supported File Formats and Size Limits](#) for more information
- The selected labeling system (Microsoft Information Protection or Boldon James) supports the file type.
 - [List of file types supported by Boldon James Classifier](#)
 - [List of file types supported by Microsoft Information Protection](#)

**Note**

Labeling detection for Microsoft Information Protection encrypted files is supported only for the following file types: docx, docm, doc, xlsm, xlsx, xlt, xltx, pptm, pptx, ppsm, ppsx, potm, potx, pdf, dot

Use the **Main > Policy Management > Content Classifiers > File Labeling** page in the Data Security module of the Forcepoint Security Manager to view or edit file labeling classifiers.

On this page:

- Click **New** to add a new file labeling classifier. See *Adding or editing a file label* section.
- Click a file labeling classifier name to view or edit its properties.
- Select a file labeling classifier, then click **Delete** to remove the selected classifier.
- When adding a classifier to a policy, optionally select **Create Rule from Classifier**. See *Creating a rule from a content classifier* section.
- Refer to the **Used** in a Policy column to determine whether or not a classifier is used. For classifiers that are in use, click **Where Used** to view the policies, rules, and exceptions that use the classifier.

If you have not imported labels for Boldon James Classifier or Microsoft Information Protection, a message displays to indicate that you must first import labels before selecting labels for detection. See *Configuring file labeling* section.

**Note**

File labeling classifiers do not work for the print channels (network or endpoint) because file labeling information cannot be extracted from printer drivers. They also do not work for sending email (endpoint).

Related concepts

[Configuring file labeling](#) on page 374

Related tasks

[Adding or editing a file label](#) on page 195
[Creating a rule from a content classifier](#) on page 239

Adding or editing a file label

Use the **Main > Policy Management > Content Classifiers > File Labeling > File Labeling Properties** page in the Data Security module of the Forcepoint Security Manager to view or edit file labeling classifiers.

Use one of the following methods to access the File Labeling Properties page:

- To add a new file labeling classifier, click **New** in the toolbar at the top of the content pane on the File Labeling page.
- To update an existing file labeling classifier, click an existing file labeling classifier name in the list on the File labeling page.

A File Labeling Properties page appears.

To define or edit a file labeling classifier:

- 1) Enter or update the **Name** and **Description** for the classifier.
- 2) Use the **Labeling system** drop-down list to select the labeling system to use:
 - If you select **Microsoft Information Protection** or **Boldon James Classifier**, the File Labels section displays.
Use the arrows to move labels between the All Labels and Detected Labels panes.
In the All Labels list, mark the labels you want to detect and click the **right arrow** to move labels into the Detected Labels list. The classifier is triggered if at least one of the Detected Labels is found on the file.
All Labels tables display the label status in the Label Status column:
 - Active: Indicates the labels can be used for labeling by the labeling system.
 - Deleted: Indicates that labels were removed from the labeling system.
 - Obsolete: Indicates that Forcepoint DLP can apply labels for a legacy system that still uses these labels. (Only for Boldon James Classifier).
 - If you choose **Any Labeling System**, the Detected Labels section is displayed.
 - In the Label field, enter the labels as free text, then click **Add** to add labels to the classifier. You can add multiple labels to the field. The classifier is triggered if at least one of the Detected Labels is found in the file.
Mark the check box **The detected labels are case-sensitive** to indicate that labels are case-sensitive. By default, the labels are case-insensitive.
 - Mark labels and click **Remove** to remove selected labels from the list.
- 3) Click **OK** to save the changes.

File properties

Because classified data is often stored in specific file formats—such as PGP (encrypted) or Excel (xlsx)—Forcepoint DLP can use file-type and file-name classifiers to block the distribution of this information. Data can also be classified by file size.



Tip

For a list of supported file types, see [Supported File Formats](#).

File-type classifiers group like files together (for example, documents or images). You can create a new file type classifier or add files to the existing file type classifiers. (See [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.

Related tasks

- [Adding a file-type classifier](#) on page 197
- [Adding a file-name classifier](#) on page 197
- [Adding a file-size classifier](#) on page 198

Adding a file-type classifier

Use the **File Properties > File Type by Type Properties** page to add file-type classifiers.

To access this page from the **Content Classifiers > File Properties** page, make sure the **By Type** tab is selected, then select **New** from the toolbar at the top of the content pane.

Steps

- 1) Enter a **Name** for this file type, such as “Picture Files.”
- 2) Enter a **Description** for this file type.
- 3) Use the **Filter by** field to enter criteria by which to filter the display, narrowing down the results shown.
Optionally include wildcards.
 - “?” represents any single character, as in the example “file _?.txt”.
 - “*” represents zero or more of any character, such as “*.txt”.
 Click the magnifying glass button to apply the filter.
- 4) Select one or more **Available File Types** in the left pane, then click **>** to add the selection to this content classifier. The additions appear in the right pane. Scroll through the list of supported file types by clicking the video player controls above the list.
- 5) Click **OK**.

Adding a file-name classifier

Use the **Main > Policy Management > Content Classifiers > File Properties > File Type by Name Properties** page to add file-type classifiers.

To access this page from the **Content Classifiers > File Properties** page, make sure the **By Name** tab is selected, then select **New** from the toolbar at the top of the content pane.

Steps

- 1) Enter a **Name** for this group of files, such as “Report Files”.
- 2) Enter a **Description** for these files.
- 3) Use the **File names** field to enter individual file names, then click **Add**. Use the “?” and “*” wildcards as needed. For example: *Report*.*

- 4) To remove a file name from the list, select it and click **Remove**.
- 5) Click **OK**.

Adding a file-size classifier

Use the **Main > Policy Management > Content Classifiers > File Properties > File Type by Name Properties** page to add file-type classifiers.

To access this page from the **Content Classifiers > File Properties** page, make sure the **By Size** tab is selected, then select **New** from the toolbar at the top of the content pane.

Steps

- 1) Enter a **Name** for this group of files, such as “Medium Files” or “Large Files”.
- 2) Enter a **Description** for these files.
- 3) Use the **File size** options to define the size of the files.
 - Select **At least** if the file is always over a certain size, then specify the minimum size in KB.
 - Select **Between** if the file is between 2 sizes, then specify the sizes in KB.
- 4) Click **OK**.



Note

Some Forcepoint 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

Forcepoint DLP provides a list of built-in script classifiers. Many are written in Python, a development language that mimics natural language, and some are written in C++. (See [NLP Scripts](#).)

Script classifiers are most often used to classify numeric data such as credit card numbers and Social Security numbers. Because the scripts are 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 at detecting the exact credit card numbers in your database—for example, your customers’ credit card numbers.

For catching credit card information in general, however, use the script classifier. Scripts detect any valid credit card number.

Fingerprinting and a script classifier may be used in combination 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** in the toolbar at the top of the content pane to delete a selected classifier, or click **Where Used** to see where the classifier is used.

The **Used in a Policy** column in the table indicates whether the classifier is used in a policy at all.

You cannot generate your own scripts, but you can edit an existing script, change its parameters, and save it under a new name.

Click a classifier name to view or edit properties. Add the classifier to a rule to activate it in a policy.

Forcepoint can create custom classifiers for a specific organization on request. Talk to your Sales representative for more details.

Related tasks

[Editing a predefined script](#) on page 199

Editing a predefined script

Use the **Main > Policy Management > Content Classifiers > Patterns & Phrases > Script properties** page to customize a script classifier.

To access this page, click the name of a script on the **Content Classifiers > Patterns & Phrases** page.

Steps

- 1) For user-defined scripts, optionally update the script **Name**.
- 2) For user-defined scripts, optionally update the script **Description**.
- 3) Mark **Edit parameter values** to change the values of the script's parameters.
 - See [NLP Scripts](#) for details about the selected script classifier.
 - Add a new value for each parameter as desired.
- 4) Mark **Exclude** to exclude certain values from the classifier, then select one of the following:
 - Select **Pattern to exclude** to define the regular expression pattern to exclude. Click the “i” icon for a list of valid values.
 - Select **List of phrases to exclude** to enter a comma-separated list of phrases, then click **Add** to add them to the list.

These phrases, when found in combination with the script, affect whether the content is considered suspicious.

Click **Remove** to remove selected strings from the list.

- 5) Click **OK** to save the edited script, or click **Save As** to save the edited classifier under a new name. If you click **Save As**, you are prompted to enter a new classifier name.

File fingerprinting

Forcepoint DLP helps organizations block the distribution of specific information to external recipients by fingerprinting files and directories and scanning data in motion for those fingerprints. Fingerprinting can be used to protect SharePoint directories, as well as any network file system or file shares.



Important

Forcepoint does not save or back up your data in the fingerprinting process. The fingerprint repository only saves partial hashes of fingerprinted data, in order to detect them in future transactions. For your own protection, make sure you have a backup system in place.



Note

The DLP Crawler, when installed on either Windows Server 2012 and above, supports SMBv2 and SMBv3 encryption as a client.

Use the **Main > Policy Management > Policy Management > Content Classifiers > File Fingerprinting** page in the Data Security module of the Forcepoint Security Manager to view or manage a file or directory fingerprinting classifier.

To create a fingerprinting classifier:

- 1) The File Fingerprinting page displays a list of fingerprinting classifiers:
 - a) 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.
 - b) Click the links in the details pane to learn more about the fingerprinted files and folders.
 - c) Start, stop, or pause a fingerprinting task using buttons in the toolbar at the top of the content pane.

- 2) Click **New** in the toolbar at the top of the content pane, then select one of the following to open a fingerprinting wizard:

- File System Fingerprinting (see *File System Fingerprinting Wizard - General* section.)
- SharePoint Fingerprinting (see *SharePoint Fingerprinting Wizard - General* section.)

You can fingerprint data on sites running the following versions of Microsoft SharePoint:

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Domino Fingerprinting (see *Domino Fingerprinting Wizard - General* section.)

**Important**

- Install IBM Notes *before* installing Forcepoint DLP. 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 Forcepoint DLP 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.

- 3) 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* section.

Related concepts

[Classifying Content](#) on page 181

Related tasks

[Managing Forcepoint DLP](#) on page 11

[File System Fingerprinting Wizard - General](#) on page 201

[SharePoint Fingerprinting Wizard - General](#) on page 206

[Domino Fingerprinting Wizard - General](#) on page 211

[Imported fingerprinting](#) on page 233

File System Fingerprinting Wizard - General

Use the General page of the file system fingerprinting wizard to name the classifier and configure its high-level properties:

Steps

- 1) Enter a **Name** for the files you are fingerprinting, such as “finance documents.”
- 2) Enter a **Description** of this set of files.
- 3) Use the **Crawler** drop-down list to elect which crawler to use to perform this fingerprinting.
 - The crawler is the agent that scans documents looking for sensitive data. There may be several in a network if there are many documents to manage.
 - Typically, it is best to select the crawler closest in proximity to the file folder.

- 4) Under Fingerprinting Mode, select which type of fingerprinting to perform:
 - Select **Sensitive content** to identify the content files and documents to fingerprint.
 - Select **Ignored section** 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. It is not necessary to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they're fingerprinted.

 - 5) Under Fingerprinting Method:
 - Select **Content similarity** 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.
 - Select **Exact match** to find only exact matches (the scanned content matches the binary signature for the entire file). This method is quicker, but will not find a match if even 1 character in the file is changed.

For large directory structures with many files, Forcepoint recommends you initially set up an exact match classifier for immediate protection, then go back and change it to content similarity.
-  **Important**

After a fingerprinting method and a fingerprinting mode are saved for a classifier, they cannot be changed.
- 6) Click **Next** to continue. See *File System Fingerprinting Wizard - Root Folder* section.

Related tasks

[File System Fingerprinting Wizard - Root Folder](#) on page 202

File System Fingerprinting Wizard - Root Folder

Use the Root Folder page of the file system fingerprinting wizard to identify the folders to scan:

- 1) Enter the **Root folder** or root directory of the files and folders you want to scan. A root folder is the highest folder in the hierarchy.
For example, to scan \\Server\Public\shared \User1, \\Server\Public\shared \User2, and \\Server\Public\shared \User3, enter:
`\\\Server\Public\shared`
 - The path cannot exceed 256 characters.
 - Select the specific files and folders to scan on the Scanned Files page (the next page in the wizard).

- 2) Enter the **User name** for an account with administrative rights to the shared folder. Read permissions are not sufficient.

- 3) Enter the **Password** for this account.

- 4) Optionally, enter the **Domain** name for the account.

- 5) Click **Next** to continue. See *File System Fingerprinting Wizard - Scanned Files* section.

When you click Next, Forcepoint DLP tries to connect to the root folder using the given credentials. You are alerted if the attempt fails.

Related tasks

[File System Fingerprinting Wizard - Scanned Files](#) on page 203

File System Fingerprinting Wizard - Scanned Files

Use the Scanned Files page of the file system fingerprinting wizard to identify the files to scan.

The files and folders included in the scan are listed in the box at the top of the page. By default, all files and folders in the root folder are included.

- 1) Click **Edit** to modify the list.
- 2) Click the folder icon  to display the directory one level up in the directory tree, or click the breadcrumbs above the list to navigate to another level.

Click **Next** to continue. See *File System Fingerprinting Wizard - Scheduler* section.

Related tasks

[File System Fingerprinting Wizard - Scheduler](#) on page 203

File System Fingerprinting Wizard - Scheduler

Use the Scheduler page of the file system fingerprinting wizard to determine when to start the scan:

Steps

- 1) Mark **Enabled** to enable the fingerprint scan scheduler. If this is not selected, fingerprint scans must be started manually.
- 2) Use the **Run scan** drop-down list to select how often you want to run the scan process: once, daily, weekly, or continuously.

3) Use the options under Properties to configure the scan:

- For daily or weekly scans, specify the hours during which to run the scan. As a best practice, run fingerprint scans outside 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.
- For one-time or continuous scans, to run as soon as possible after a designated time or date, mark **But not before**, then select a date from the drop-down box and a time from the spinner.
- For continuous scans, use **Wait** option to specify the number of minutes to wait between consecutive scans.

4) Click **Next** to continue. See *File System Fingerprinting Wizard - File Filtering* section.

Related tasks

[File System Fingerprinting Wizard - File Filtering](#) on page 204

File System Fingerprinting Wizard - File Filtering

Use the File Filtering page of the file system fingerprinting wizard to use file type, file age, file size, or a combination of properties to determine which files are fingerprinted.

Steps

- 1) To filter based on file type or file name, mark **Filter by Type**, then list the types of files to be fingerprinted, separated by semi-colons.
 - Optionally use the "*" or "?" wildcards. For example, "*.doc; *.xls; *.ppt; *.pdf".
 - Click **File Types** to select the type of files to include in the scan from predefined categories such as Office Documents or Bitmaps.
- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Click **File Types** to select the type of files to exclude in the scan from predefined categories such as Office Documents or Bitmaps.
- 3) To filter based on file modification date, mark **Filter by Age**, then use the radio buttons to select a time period (24 months, by default).

- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
- Mark **Scan only files larger than**, then select a file size from the spinner. By default, all files larger than 1 KB are scanned.
 - Mark **Scan only files smaller than**, then select a file size from the spinner. By default, all files smaller than 100,000 KB are scanned.

**Note**

Files larger than 100 MB are fingerprinted 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.

- 5) Click **Next** to continue.
- If you are creating a new classifier, see *File System Fingerprinting Wizard - Export* section.
 - Otherwise, see *File System Fingerprinting Wizard - Finish* section.

Related concepts

[File System Fingerprinting Wizard - Finish on page 206](#)

Related tasks

[File System Fingerprinting Wizard - Export on page 205](#)

File System Fingerprinting Wizard - Export

When creating a new classifier, use the Export page of the file system fingerprinting wizard to configure settings that allow use of this classifier in policies on a disconnected network.

First, export the classifier to a network location. Later, copy it to the other network and import it via the **Import** option on the File Fingerprinting toolbar. See *Imported fingerprinting* section for details. (The disconnected network must also have a management server.)

Steps

- 1) Mark **Export fingerprints** to export this fingerprint classifier for use in a disconnected network.
 - 2) Enter the **User name** for an account with write access to the export folder.
 - 3) Enter the **Password** for the account.
 - 4) Optionally, enter the **Domain** name for the account.
 - 5) Use the **Export to folder** field to enter the hostname or IP address (in UNC format; for example, \\12.3.45.67) of the destination server, then browse to the folder to use. The folder must already exist.
- 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.

- 6) Click **Next** to continue. See *File System Fingerprinting Wizard - Finish* section.

Related concepts

[File System Fingerprinting Wizard - Finish](#) on page 206

Related tasks

[Imported fingerprinting](#) on page 233

File System Fingerprinting Wizard - Finish

The Finish page of the file system fingerprinting wizard displays a summary of the content classifier. 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
- The scan filters chosen
- 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 fingerprint scan occurs according to its schedule.

SharePoint Fingerprinting Wizard - General

Use the General page of the SharePoint fingerprinting wizard to name the classifier and configure its high-level properties:

Steps

- 1) Enter a **Name** for the files you are fingerprinting, such as “finance documents.”
- 2) Enter a **Description** of this set of documents.
- 3) Use the **Crawler** drop-down list to elect which crawler to use to perform this fingerprinting.
 - The crawler is the agent that scans documents looking for sensitive data. There may be several in a network if there are many documents to manage.
 - Typically, it is best to select the crawler closest in proximity to the file folder.

- 4) Under Fingerprinting Mode, select which type of fingerprinting to perform:
 - Select **Sensitive content** to identify the content files and documents to fingerprint.
 - Select **Ignored section** 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. It is not necessary to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they're fingerprinted.

- 5) Under Fingerprinting Method:
 - Select **Content similarity** 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.
 - Select **Exact match** to find only exact matches (the scanned content matches the binary signature for the entire file). This method is quicker, but will not find a match if even 1 character in the file is changed.

For large directory structures with many files, Forcepoint recommends you initially set up an exact match classifier for immediate protection, then go back and change it to content similarity.
- 6) Click **Next** to continue. See *SharePoint Fingerprinting Wizard - Site Root* section.

Related tasks

[SharePoint Fingerprinting Wizard - Site Root](#) on page 207

SharePoint Fingerprinting Wizard - Site Root

Use the Site Root page of the SharePoint fingerprinting wizard to identify the folders to scan:

Steps

- 1) Enter the SharePoint **Site root hostname** (for example, http://gumby/site_name). (Note that a site is different than a folder in SharePoint. The system supports only site-level URLs for this field.)
 - An IP address may be used, if the SharePoint administrator adds it to an alternate access map. (In SharePoint 2010, this is done under **Central Administration > Alternate Access Mapping > Add Internal URLs**. In SharePoint 2013, go to **Central Administration > Configure Alternate Access Mappings > Add Internal URLs**)
 - The SharePoint fingerprinter connects to site collections—such as <http://intranet/sites/HR:8080>—and not web applications.
- 2) Enter the **User name** for an account with administrative rights to the shared folder. As a best practice, enter the name of the SharePoint site owner with Full Control permissions.
- 3) Enter the **Password** for this account.
- 4) Optionally, enter the **Domain** name for the account.
- 5) Click **Next** to continue. See *SharePoint Fingerprinting Wizard - Scanned Documents* section.

When you click **Next** on this screen, Forcepoint DLP attempts to connect to the root- site using the given credentials. You are alerted if the attempt fails.

Related tasks

[SharePoint Fingerprinting Wizard - Scanned Documents](#) on page 208

SharePoint Fingerprinting Wizard - Scanned Documents

Use the Scanned Documents page of the SharePoint fingerprinting wizard to identify the documents and folders to scan.

By default, no documents or folders are included.

- Click **Edit** to modify the list.
- Only the latest version of each document is scanned, not the entire document history.
- Click the folder icon  to display the directory one level up in the directory tree, or click the breadcrumbs above the list to navigate to another level.

Click **Next** to continue. See *SharePoint Fingerprinting Wizard - Scheduler* section.

Related tasks

[SharePoint Fingerprinting Wizard - Scheduler](#) on page 208

SharePoint Fingerprinting Wizard - Scheduler

Use the Scheduler page of the SharePoint fingerprinting wizard to determine when to start the scan:

Steps

- 1) Mark **Enabled** to enable the fingerprint scan scheduler. If this is not selected, fingerprint scans must be started manually.
- 2) Use the **Run scan** drop-down list to select how often you want to run the scan process: once, daily, weekly, or continuously.
- 3) Use the options under Properties to configure the scan:
 - For daily or weekly scans, specify the hours during which to run the scan. As a best practice, run fingerprint scans outside 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.
 - For one-time or continuous scans, to run as soon as possible after a designated time or date, mark **But not before**, then select a date from the drop-down box and a time from the spinner.
 - For continuous scans, use **Wait** option to specify the number of minutes to wait between consecutive scans.
- 4) Click **Next** to continue. See *SharePoint Fingerprinting Wizard - File Filtering* section.

Related tasks

[SharePoint Fingerprinting Wizard - File Filtering](#) on page 209

SharePoint Fingerprinting Wizard - File Filtering

Use the File Filtering page of the SharePoint fingerprinting wizard to use file type, file age, file size, or a combination of properties to determine which documents are fingerprinted.

Steps

- 1) To filter based on file type or file name, mark **Filter by Type/Document Name**, then list the types of files to be fingerprinted, separated by semi-colons.
 - Optionally use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”.
 - Click **File Types** to select the type of files to include in the scan from predefined categories such as Office Documents or Bitmaps.

- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Click **File Types** to select the type of files to exclude in the scan from predefined categories such as Office Documents or Bitmaps.

- 3) To filter based on file modification date, mark **Filter by Age**, then use the radio buttons to select a time period (24 months, by default).

- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only files larger than**, then select a file size from the spinner. By default, all files larger than 1 KB are scanned.
 - Mark **Scan only files smaller than**, then select a file size from the spinner. By default, all files smaller than 100,000 KB are scanned.


Note

Files larger than 100 MB are fingerprinted 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.

- 5) Click **Next** to continue.
 - If you are creating a new classifier, see *SharePoint Fingerprinting Wizard -Export* section.
 - Otherwise, see *SharePoint Fingerprinting Wizard - Finish* section.

Related concepts

[SharePoint Fingerprinting Wizard - Finish](#) on page 210

Related tasks

[SharePoint Fingerprinting Wizard - Export on page 210](#)

SharePoint Fingerprinting Wizard - Export

When creating a new classifier, use the Export page of the SharePoint fingerprinting wizard to configure settings that allow use of this classifier in policies on a disconnected network.

First, export the classifier to a network location. Later, copy it to the other network and import it via the **Import** option on the File Fingerprinting toolbar. See *Imported fingerprinting* section for details. (The disconnected network must also have a management server.)

Steps

- 1) Mark **Export fingerprints** to export this fingerprint classifier for use in a disconnected network.
- 2) Enter the **User name** for an account with write access to the export folder.
- 3) Enter the **Password** for the account.
- 4) Optionally, enter the **Domain** name for the account.
- 5) Use the **Export to folder** field to enter the hostname or IP address (in UNC format; for example, `\12.3.45.67`) of the destination server, then browse to the folder to use. The folder must already exist. 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.
- 6) Click **Next** to continue. See *SharePoint Fingerprinting Wizard - Finish* section.

Related concepts

[SharePoint Fingerprinting Wizard - Finish on page 210](#)

Related tasks

[Imported fingerprinting on page 233](#)

SharePoint Fingerprinting Wizard - Finish

The Finish page of the SharePoint fingerprinting wizard displays a summary of the content classifier. It lists:

- The name of the classifier
- The crawler being used to perform the fingerprinting
- The type of fingerprinting done
- The SharePoint site root
- Authentication information

- The documents and folders included and excluded
- The scan filters chosen
- 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 fingerprint scan occurs according to its schedule.

Domino Fingerprinting Wizard - General

Forcepoint DLP 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 NSF files on a 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.

Use the General page of the Domino fingerprinting wizard to name the classifier and configure its high-level properties:

Steps

- 1) Enter a **Name** for the files you are fingerprinting, such as "finance documents."
- 2) Enter a **Description** of this set of documents.
- 3) Use the **Crawler** drop-down list to elect which crawler to use to perform this fingerprinting.
 - The crawler is the agent that scans documents looking for sensitive data. There may be several in a network if there are many documents to manage.
 - Typically, it is best to select the crawler closest in proximity to the file folder or Domino server.
- 4) Under Fingerprinting Mode, select which type of fingerprinting to perform:
 - Select **Sensitive content** to identify the content files and documents to fingerprint.
 - Select **Ignored section** 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. It is not necessary to add Ignored Section classifiers to a rule or policy. The classifier filters out files that are being fingerprinted before they're fingerprinted.

5) Under Fingerprinting Method:

- Select **Content similarity** 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.
- Select **Exact match** to find only exact matches (the scanned content matches the binary signature for the entire file). This method is quicker, but will not find a match if even 1 character in the file is changed.

For large directory structures with many files, Forcepoint recommends you initially set up an exact match classifier for immediate protection, then go back and change it to content similarity.

6) Click **Next to continue. See *Domino Fingerprinting Wizard - Server* section.**

Related tasks

[Domino Fingerprinting Wizard - Server](#) on page 212

Domino Fingerprinting Wizard - Server

Use the Server page of the Domino fingerprinting wizard to specify which IBM Domino server to scan.

Steps

- 1) Enter the hostname of the **Domino server to scan**—for example, “gumby”. Do not include the HTTP prefix or leading slashes.**
- 2) Click **Next**.**

The crawler tries to connect to the Domino server using credentials for the account shown. These connection settings were provided when Forcepoint DLP was installed on the Notes machine.



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 Forcepoint DLP installer on the Notes machine, select the **Modify** option, and upload a different user ID file.

See *Domino Fingerprinting Wizard - Scanned Documents* section.

Related tasks

[Domino Fingerprinting Wizard - Scanned Documents](#) on page 212

Domino Fingerprinting Wizard - Scanned Documents

Use the Scanned Documents page of the Domino fingerprinting wizard to define which documents and folders to scan.

Steps

- 1) Enter the name of the field or fields that hold the Domino document names.
If you supply multiple field names, separate them with commas. For example: subject, docname, filename.
By default, the “Subject” field is scanned.

- 2) Under Documents and folders to scan, define the documents and folders included in and excluded from the scan. By default, nothing is included.
Click **Edit** to modify the list.
 - Only the latest version of the documents is scanned, not the entire document history.
 - 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, or use the 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.
 - 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.

- 3) Under Fields to scan, if the document content is stored in more than one field, enter the name of each field, separated by commas. For example, “body, content, main.”
 - In Notes, just as document names are typically stored in the Subject field, document content is typically stored in the Body field.
 - 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.

- 4) Click **Next** to continue. See *Domino Fingerprinting Wizard - Scheduler* section.

Related tasks

[Domino Fingerprinting Wizard - Scheduler](#) on page 213

Domino Fingerprinting Wizard - Scheduler

Use the Scheduler page of the Domino fingerprinting wizard to determine when to start the scan:

Steps

- 1) Mark **Enabled** to enable the fingerprint scan scheduler. If this is not selected, fingerprint scans must be started manually.

- 2) Use the **Run scan** drop-down list to select how often you want to run the scan process: once, daily, weekly, or continuously.

- 3) Use the options under Properties to configure the scan:
 - For daily or weekly scans, specify the hours during which to run the scan. As a best practice, run fingerprint scans outside 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.
 - For one-time or continuous scans, to run as soon as possible after a designated time or date, mark **But not before**, then select a date from the drop-down box and a time from the spinner.
 - For continuous scans, use **Wait** option to specify the number of minutes to wait between consecutive scans.
- 4) Click **Next** to continue. See *Domino Fingerprinting Wizard - Document Filtering* section.

Related tasks

[Domino Fingerprinting Wizard - Document Filtering](#) on page 214

Domino Fingerprinting Wizard - Document Filtering

Use the Document Filtering page of the Domino fingerprinting wizard to use the document name, age, size, or a combination of properties to determine which documents are fingerprinted.

Steps

- 1) To analyze content in document names, mark **Filter by Document Name**. The file names and their paths are fingerprinted.
 - List the exact document names to be fingerprinted, separated by semi-colons.
 - The “*” or “?” wildcards are supported. For example, “top_secret*”.
- 2) Use the **Except** field to list the exact document names to exclude from the scan, separated by semi-colons. The “*” or “?” wildcards are supported.
- 3) To filter based on document modification date, mark **Filter by Age**, then use the radio buttons to select a time period (24 months, by default).
The document age is determined by the most recent date of its body and all attachments.

- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
- Mark **Scan only files larger than**, then select a file size from the spinner. By default, all files larger than 1 KB are scanned.
 - Mark **Scan only files smaller than**, then select a file size from the spinner. By default, all files smaller than 100,000 KB are scanned.

**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.

- 5) Click **Next** to continue. See *Domino Fingerprinting Wizard - Attachment Filtering* section.

Related tasks

[Domino Fingerprinting Wizard - Attachment Filtering](#) on page 215

Domino Fingerprinting Wizard - Attachment Filtering

Use the Attachment Filtering page of the Domino fingerprinting wizard to use the attachment type, size, or both to determine which attachments to scan.

Steps

- 1) To scan for specific attachments, mark **Filter by Type**, then list the types of files to be fingerprinted, separated by semi-colons.
Optionally use the "*" or "?" wildcards. For example, "*.doc; *.xls; *.ppt; *.pdf".
- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
- 3) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only files larger than**, then select a file size from the spinner. By default, all files larger than 1 KB are scanned.
 - Mark **Scan only files smaller than**, then select a file size from the spinner. By default, all files smaller than 100,000 KB are scanned.

**Note**

Files larger than 100 MB are fingerprinted 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.

- 4) Click **Next** to continue.
 - If you are creating a new classifier, see *Domino Fingerprinting Wizard - Export* section.
 - Otherwise, see *Domino Fingerprinting Wizard - Finish* section.

Related concepts

[Domino Fingerprinting Wizard - Finish](#) on page 217

Related tasks

[Domino Fingerprinting Wizard - Export](#) on page 216

Domino Fingerprinting Wizard - Export

When creating a new classifier, use the Export page of the Domino fingerprinting wizard to configure settings that allow use of this classifier in policies on a disconnected network.

First, export the classifier to a network location. Later, copy it to the other network and import it via the **Import** option on the File Fingerprinting toolbar. See *Imported fingerprinting* section for details. (The disconnected network must also have a management server.)

Steps

- 1) Mark **Export fingerprints** to export this fingerprint classifier for use in a disconnected network.
- 2) Enter the **User name** for an account with write access to the export folder.
- 3) Enter the **Password** for the account.
- 4) Optionally, enter the **Domain** name for the account.
- 5) Use the **Export to folder** field to enter the hostname or IP address (in UNC format; for example, \\12.3.45.67) of the destination server, then browse to the folder to use. The folder must already exist.
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.
- 6) Click **Next** to continue. See *Domino Fingerprinting Wizard - Finish* section.

Related concepts

[Domino Fingerprinting Wizard - Finish](#) on page 217

Related tasks

[Imported fingerprinting](#) on page 233

Domino Fingerprinting Wizard - Finish

The Finish page of the Domino fingerprinting wizard displays a summary of the content classifier. It lists:

- The name of the classifier
- The crawler being used to perform the fingerprinting
- The type of fingerprinting done
- The Domino server
- Authentication information
- The documents included and excluded
- The scan filters chosen
- 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 fingerprint scan occurs according to its schedule.

Database fingerprinting

Forcepoint DLP can quickly connect to a database, retrieve records, and fingerprint exact fields from a protected database. For example, it 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.

Forcepoint DLP can also:

- Fingerprint a cloud-hosted salesforce.com database.
- 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. Forcepoint DLP enables you to block the distribution of this information by defining database record fingerprints.

Related concepts

- [Connecting to data sources](#) on page 218
- [Preparing for database fingerprinting](#) on page 219
- [Creating a validation script](#) on page 220
- [Selecting the data to fingerprint](#) on page 223
- [How matches are counted](#) on page 224
- [Data classification](#) on page 10
- [Database Fingerprinting Wizard - Data Source/Site](#) on page 226
- [Database Fingerprinting Wizard - Field Selection](#) on page 228
- [Database Fingerprinting Wizard - Finish](#) on page 232

Related tasks

- [Creating a database fingerprint classifier](#) on page 225
- [Database Fingerprinting Wizard - General](#) on page 226
- [Database Fingerprinting Wizard - Fingerprinting Type](#) on page 231
- [Database Fingerprinting Wizard - Scheduler](#) on page 230

Connecting to data sources

To fingerprint a database, the Forcepoint DLP server must be able to connect to the data source over a supported interface. Forcepoint DLP supports the following database connection interfaces:

- Open Database Connectivity (ODBC)—Forcepoint has certified support for the following ODBC-compliant databases:
 - Oracle 10g (ODBC driver 10.1.0.2.0)
 - Oracle 19.C
 - Oracle Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (32- and 64-bit)
 - Microsoft SQL Server 2000, 2005, 2008, 2012, and 2016
 - Microsoft SQL Server Express (SQL Server Express ODBC driver)
 - IBM DB2 11.5.x (ODBC driver 11.x)
 - 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)

It is possible to define flexible content policies for each data source. In each policy, configure detection rules by combining columns and indicating match thresholds. Be sure to test database connectivity before configuring content policies.

Supported field types

The system scans the following database field types:

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ CHAR ■ WCHAR ■ TINYINT ■ INTEGER ■ DECIMAL ■ REAL ■ DOUBLE | <ul style="list-style-type: none"> ■ VARCHAR ■ WVARCHAR ■ SMALLINT ■ BIGINT ■ NUMERIC ■ FLOAT ■ TIME |
|--|---|

Preparing for database fingerprinting

Before creating a database fingerprinting classifier, there are several preparatory steps to perform to streamline the process and optimize the results. See:

- [Creating a Data Source Name \(DSN\) in Windows](#)
- [Creating a validation script](#)
- [Selecting the data to fingerprint](#)

Related concepts

- [Creating a validation script](#) on page 220
[Selecting the data to fingerprint](#) on page 223

Related tasks

- [Creating a Data Source Name \(DSN\) in Windows](#) on page 219

Creating a Data Source Name (DSN) in Windows



Important

To run fingerprinting or discovery tasks on Oracle, Microsoft SQL Server, or MySQL databases, the password for the account used to access the database cannot include a semi-colon (;).

A DSN is required to create a database table fingerprint or set up database discovery. If the database does not already have a DSN, create one as follows:

Steps

- 1) Go to the crawler machine that is being used for fingerprinting tasks.
- 2) Log in as the Forcepoint DLP administrative user.
- 3) Access the system's ODBC Data Source Administrator.
 - Windows Server 2012: Go to Start > Administrative Tools > ODBC Data Sources (32-bit) or (64-bit).
 - Windows Server 2008: Go to Start > Administrative Tools > Data Sources (ODBC).
- 4) On the User DSN tab, click **Add**.
 User DSNs store information about how to connect to a specific data source. They may be used only by the current user on the current machine.
- 5) Use the Create New Data Source dialog box to select the appropriate database driver.
- 6) When prompted, enter a data source name and description. Some drivers require additional information:
 - For Excel, select a workbook and enter the number of rows to scan.
 - For Access, select the database and the page timeout.

- 7) Click **Advanced** or **Options** as needed to provide details for the database records that will be fingerprinted, then click **OK**.

- 8) If you selected a Sybase or DB2 driver:
 - a) Stop all discovery tasks and fingerprinting jobs running on this machine.
 - b) Open the Windows Services tool (**Start > Administrative > Tools > Services**).
 - c) Right-click **Forcepoint Data Task Scheduler** and select **Restart**.

Creating a validation script

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

Validation script mechanism

Each database fingerprint 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, the configuration file path name, is optional.

The input file 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 from Forcepoint Technical Support.

The output file has the same format as the input file, but instead of using CRLF as the line delimiter, it uses CRCRLF (2 carriage-return characters and one line-feed character). An output sample file is available in the same package as the sample input file.

Validating fingerprinting scans

To validate your fingerprinting scans:

- 1) Optionally, create a copy of the following files in the \ValidationScripts folder where Forcepoint DLP was installed (typically C:\Program Files\WebSense\Data Security\ValidationScripts).
 - default_validation.bat.sample
 - default_validation.ini.sample
 To create your script from scratch, skip this step.

- 2) Name your new validation script using the following convention:

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

Here:

- `<classifier-name>` is the name of the classifier on which the script will be run. Alternatively, use the word "default" for scripts that run 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, name the configuration file using the following convention:

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

Place all files in the \ValidationScripts folder on the server where Forcepoint DLP 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, Forcepoint 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 Forcepoint DLP: 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.
 - The script should read and perform validation on the source file.
 - The 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 Forcepoint DLP.
 - The script should return a return code of 0 if everything succeeded, and non-zero if there was a problem.
- 4) To have the script use a configuration file, place the configuration file 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 the script.
- 5) Create and run the fingerprinting classifier as described in *Creating a database fingerprint classifier* section. Name the classifier with the name given in step 2.

During the scan, if the crawler finds a script with the following name format, it runs that script:

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

If it does not find a script with that naming format, 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.

Related tasks

[Creating a database fingerprint classifier](#) on page 225

Sample validation script

There is a sample validation script in the \Validation Scripts directory where Forcepoint DLP is installed. The script contains the basic abilities required for most customers, such as removing NULL or single-character values from being fingerprinted. You can modify it to suit your needs.

The sample package contains the following files:

- default_validation.bat.sample - Sample validation script
- validation_logic.py - Used by the sample validation script.
- default_validation.ini.sample - 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 Forcepoint DLP installation package.

The sample validation script is a production grade script, which is suitable for many organizations.

Please note that although “default_validation.bat” and “default_validation.ini” files can be renamed according to the conventions mentioned above, do not rename the “validation_logic.py” file. This 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 Forcepoint DLP 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.) Administrators can create UTF-16 files in Windows Notepad by saving the text with “Unicode” encoding.
 - An example of this can be found in the “default_validation.ini.sample” file.
 - A sample dictionary file—“dictionary.txt”—is also provided.
- Regular expressions can be used 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 Forcepoint 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, carefully consider what information to fingerprint.

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

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* section, 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.

Related tasks

[Patterns & Phrases](#) on page 189

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, Forcepoint 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 database policy.

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* section) 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.

Related concepts

[Creating a validation script](#) on page 220

How matches are counted

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

For example, consider the following table:

Column_A	Column_B
1234	AAAA
1234	AAAA
5678	AAAA

And a condition specifying the combination of Column_A and Column_B.

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

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

Creating a database fingerprint classifier

Use the **Main > Policy Management > Content Classifiers > Database Fingerprinting** page to classify your content by fingerprinting database records.



Important

Forcepoint does not save or back up your data in the fingerprinting process. The fingerprint repository only saves partial hashes of fingerprinted data, in order to detect them in future transactions. For your own protection, make sure you have a backup system in place.

To create a new classifier:

- 1) The Database Fingerprinting page displays a fingerprint list appears.
 - a) Expand the right pane to view more details, such as last run time and next run time, or collapse it to show fewer details.
 - b) Click the links in the details pane to learn more about the fingerprinted records.
 - c) Start, stop, or pause a fingerprinting task using buttons in the toolbar at the top of the content pane.
- 2) Click **New** in the toolbar at the top of the content pane, then select **Database Table Fingerprinting**, **Salesforce Fingerprinting**, or **CSV File Fingerprinting**.
A wizard opens. See *Database Fingerprinting Wizard - General* section.



Important

The fingerprinting technology uses data source names (DSNs) to perform database record fingerprinting. Before beginning the wizard, create a DSN for the database records that you intend to fingerprint. See *Preparing for database fingerprinting* section for instructions.

- 3) 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* section, for more information.

Related concepts

[Data classification](#) on page 10

[Database Fingerprinting Wizard - Data Source/Site](#) on page 226

[Database Fingerprinting Wizard - Field Selection](#) on page 228

[Database Fingerprinting Wizard - Finish](#) on page 232

[Preparing for database fingerprinting](#) on page 219

Related tasks

- [Database Fingerprinting Wizard - General on page 226](#)
- [Database Fingerprinting Wizard - Scheduler on page 230](#)
- [Database Fingerprinting Wizard - Fingerprinting Type on page 231](#)
- [Imported fingerprinting on page 233](#)

Database Fingerprinting Wizard - General

Use the General page of the database fingerprinting wizard to name the classifier and configure its high-level properties:

Steps

- 1) Enter a **Name** for the database records you are fingerprinting, such as “finance records.”
- 2) Enter a **Description** of the database.
- 3) Use the **Crawler** drop-down list to elect which crawler to use to perform this fingerprinting.
 - The crawler is the agent that scans records looking for sensitive data.
 - Typically, it is best to select the crawler closest in proximity to the database server.
- 4) Click **Next** to continue. See *Database Fingerprinting Wizard - Data Source/Site* section.

Related concepts

- [Database Fingerprinting Wizard - Data Source/Site on page 226](#)

Database Fingerprinting Wizard - Data Source/Site

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

- *Database table*
- *Salesforce site*
- *CSV file*

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

Continue with *Database Fingerprinting Wizard - Field Selection*.

Related concepts

- [Database Fingerprinting Wizard - Field Selection on page 228](#)

Related tasks

[Database table](#) on page 227

[Salesforce site](#) on page 227

[CSV file](#) on page 228

Database table

Steps

- 1) Select the DSN for the database that you want to fingerprint.
 - If the database does not have a DSN, see *Creating a Data Source Name (DSN) in Windows* section. The DSN must be defined with the same user as the crawler selected on the previous page of the wizard.
 - For a list of supported databases and field types, see *Connecting to data sources* section.
- 2) Select **Use data source credentials** to use the name and password of the Forcepoint DLP service account (the account defined during product installation) to access the database. If you select this option, make sure the crawler is using credentials with permission to access the database.
For Microsoft SQL Server databases that are configured to use SQL Server authentication, select **Use the following credentials** instead, then enter credentials defined in the database itself, such as the sa account. (Do not enter the network credentials.)
 - a) Enter the **User name** for an account with “read” privileges to the database.
 - b) Enter the account **Password**.
 - c) Optionally, enter the **Domain** for the account.

Related concepts

[Connecting to data sources](#) on page 218

Related tasks

[Creating a Data Source Name \(DSN\) in Windows](#) on page 219

Salesforce site

Steps

- 1) Enter the URL of the **Salesforce site** to fingerprint (for example, <https://emea.force.com>).
- 2) Enter the **User name** for an account with access to the Salesforce site.
- 3) Enter the **Password** for the account.

4) Enter the **Salesforce token** for this site.

Applications, including Forcepoint DLP, must provide a security token when connecting to Salesforce via its API.

To receive a security token for your organization, log on to [force.com](#), click **Setup**, and click **Reset your security token**. A token is sent automatically.

CSV file

Steps

- 1) Enter the **User name** for a network account.
- 2) Enter the **Password** for the account.
- 3) Optionally, enter the **Domain** for this account.
- 4) In the **CSV file name** field, enter the UNC path of the server or shared folder where the CSV file resides, then browse to the file itself. For example, \\10.0.0.1\ c\$\MyCSV.

Database Fingerprinting Wizard - Field Selection

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*
- *Salesforce site*

After clicking **Next** on this page, see *Database Fingerprinting Wizard - Scheduler* section.

Related tasks

[Database table or CSV file](#) on page 229

[Salesforce site](#) on page 230

[Database Fingerprinting Wizard - Scheduler](#) on page 230

Database table or CSV file

Steps

- 1) Mark Select up to 32 fields from a table** to select the fields to fingerprint.
 - a)** Use the drop-down list to select a table. CSV files are preselected.
 - b)** Select one or more fields to fingerprint. These correspond to table columns. Select up to 32 fields per table.
 - (*Database tables only*) To change the displayed name for one or more fields, click **Modify Displayed Names**.
 - Review the SQL query that was generated for your selection under Selection as SQL Query.

Click **View Sample Data** to make sure that the correct information is fingerprinted.
- 2) Select Use the following SQL query to select records** to construct a custom SQL query.
 - Enter the query or click **Copy Above Query**, then modify the copied string.
 - 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.
- 3) Click Next** to continue. The system validates the SQL query.



Important

When selecting the fields to fingerprint, be sure to follow the guidelines in *Selecting the data to fingerprint* section. 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. There is a workaround, however.

- a)** Mark **Select up to 32 fields from a table**.
- b)** Select the table and fields.
- c)** Copy the query from the **Selection as SQL query**
- d)** Mark **Use the following SQL query to select records**.
- e)** Paste the query into the box.
- f)** Surround the table name with double quotes. For example:

```
SELECT "name","id","cc","phone" FROM "blade2\informix".custdb.
```

Related concepts

Selecting the data to fingerprint on page 223

Salesforce site

Steps

- 1) Mark **Select up to 32 fields from a table** to select either the fields to fingerprint or a predefined database query.
- 2) Use the drop-down list to select a table from the Salesforce database, 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 up to 32 fields to fingerprint. These correspond to table columns. Forcepoint supplies the 10 most common Salesforce tables. It is possible to any of the tables used by salesforce.com via a public API from Salesforce.
- 3) Under Selection as SOQL Query, review the SOQL query generated for the selection.
- 4) Click **View Sample Data** to make sure that the correct information is fingerprinted.
- 5) Select **Use the following SOQL query to select records** to construct a custom SOQL query.
 - Enter the query or click **Copy Above Query**, then modify the copied string.
 - 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.
- 6) Click **Next** to continue. The system validates your SOQL query.

Database Fingerprinting Wizard - Scheduler

Use the Scheduler page of the database fingerprinting wizard to determine when to start the scan:

Steps

- 1) Mark **Enabled** to enable the fingerprint scan scheduler. If this is not selected, fingerprint scans must be started manually.
- 2) Use the **Run scan** drop-down list to select how often you want to run the scan process: once, daily, weekly, or continuously.

3) Use the options under Properties to configure the scan:

- For daily or weekly scans, specify the hours during which to run the scan. As a best practice, run fingerprint scans outside 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.
- For one-time or continuous scans, to run as soon as possible after a designated time or date, mark **But not before**, then select a date from the drop-down box and a time from the spinner.
- For continuous scans, use **Wait** option to specify the number of minutes to wait between consecutive scans.

4) Click **Next to continue. See *Database Fingerprinting Wizard - Fingerprinting Type* section.**

Related tasks

[Database Fingerprinting Wizard - Fingerprinting Type](#) on page 231

Database Fingerprinting Wizard - Fingerprinting Type

Use the Fingerprinting Type page of the database fingerprinting wizard to determine how scans are performed.

- Select **Full fingerprinting** to perform a full scan every time the data is fingerprinted. (This could be a scheduled or on-demand fingerprinting task.)
 - The entire selected table is fingerprinted.
 - These settings are changed on deploy. Whenever such a setting changes, both the changed repository and the primary repository become un-synchronized.
- Select **Differential fingerprinting** to scan only records that were added incrementally since the last scan. This option is much quicker.
 - 1) Use the **Field by which to compare scans** drop-down list to select the field to use for record comparisons. The crawler retrieves the rows in which the selected field is larger than the previously fingerprinted values. If there are no such rows, the crawler does not initiate a fingerprinting task.
 - 2) Mark **Full scan every...** to periodically run a full scan. Because previously fingerprinted rows can change, it is a best practice to run a full scan periodically.

When you are finished, click **Next** to continue. See:

- (*New classifiers only*) [Database Fingerprinting Wizard - Export](#) section
- [Database Fingerprinting Wizard - Finish](#) section.

Related concepts

[Database Fingerprinting Wizard - Finish](#) on page 232

Related tasks

[Database Fingerprinting Wizard - Export](#) on page 232

Database Fingerprinting Wizard - Export

When creating a new classifier, use the Export page of the database fingerprinting wizard to configure settings that allow use of this classifier in policies on a disconnected network.

First, export the classifier to a network location. Later, copy it to the other network and import it via the **Import** option on the File Fingerprinting toolbar. See *Imported fingerprinting* section for details. (The disconnected network must also have a management server.)

Steps

- 1) Mark **Export fingerprints** to export this fingerprint classifier for use in a disconnected network.
- 2) Enter the **User name** for an account with write access to the export folder.
- 3) Enter the **Password** for the account.
- 4) Optionally, enter the **Domain** name for the account.
- 5) Use the **Export to folder** field to enter the hostname or IP address (in UNC format; for example, `\12.3.45.67`) of the destination server, then browse to the folder to use. The folder must already exist. 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.
- 6) Click **Next** to continue. See *Database Fingerprinting Wizard - Finish* section.

Related concepts

[Database Fingerprinting Wizard - Finish](#) on page 232

Related tasks

[Imported fingerprinting](#) on page 233

Database Fingerprinting Wizard - Finish

The Finish page of the database fingerprinting wizard displays a summary of the content classifier. It lists:

- The name of the data
- The crawler being used to perform the fingerprinting
- The data source type, file name, and credentials
- The SQL or SOQL query
- The fingerprinting type
- 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 fingerprint scan occurs according to its schedule.

Imported fingerprinting

Forcepoint DLP offers the option of importing existing fingerprinting classifiers, created in a separate (disconnected) deployment.

To do this:

- 1) Create a fingerprinting classifier.
- 2) On the Export page of the fingerprinting wizard, export the classifier to a network location.
- 3) Later, manually copy the classifier from the network location to the separate (disconnected) Forcepoint DLP deployment.
- 4) Use the Import option on the File Fingerprinting or Database Fingerprinting toolbar in the second deployment to import the classifier.
 - Re-import 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) Go to the **Main > Policy Management > Content Classifiers** page in the Data Security module of the Forcepoint Security Manager.
- 2) Under Fingerprints, select either **File Fingerprinting** or **Database Fingerprinting**.
- 3) Click **Import** in the toolbar at the top of the content pane.
A wizard opens. See *Import Fingerprint Wizard - Import Source* section.

Related tasks

[Import Fingerprint Wizard - Import Source](#) on page 233

Import Fingerprint Wizard - Import Source

Use the Source page of the import fingerprint wizard to specify the classifier location and select a crawler.

Steps

- 1) Enter the **User name** for an account with access to the network location containing the classifier.
- 2) Enter the **Password** for this account.
- 3) Optionally, enter the account **Domain** name.
- 4) Select which **Crawler** to use to perform this fingerprinting. Typically, this is the crawler closest in proximity to the file or database server.

- 5) Use the **Import from folder** field to enter the hostname or IP address of the server where the classifier is stored, then browse to the folder to use.
- 6) Click **Next** to continue. See *Import Fingerprint Wizard - Properties* section.

Related tasks

[Import Fingerprint Wizard - Properties](#) on page 234

Import Fingerprint Wizard - Properties

Use the Properties page of the import fingerprint wizard to optionally customize the classifier name and description for this deployment. Also review fixed (non-changeable) classifier properties.

Steps

- 1) Enter a **Name** for the new classifier. By default, this is the name of the original classifier.
- 2) Enter a **Description** of this classifier. By default, this is the description of the original classifier.
- 3) Review the following classifier properties. None of these properties can be changed.
 - The name of the classifier that was exported (uneditable)
 - A description of the classifier (uneditable)
 - (Database fingerprinting only) The database table defined in the original classifier
 - (Database fingerprinting only) The database fields to be fingerprinted in the original classifier
- 4) Click **Next** to continue. See *Import Fingerprint Wizard - Scheduler* section.

Related tasks

[Import Fingerprint Wizard - Scheduler](#) on page 234

Import Fingerprint Wizard - Scheduler

Use the Scheduler page of the import fingerprint wizard to determine when to start the scan:

Steps

- 1) Mark **Enabled** to enable the fingerprint scan scheduler. If this is not selected, fingerprint scans must be started manually.
- 2) Use the **Run scan** drop-down list to select how often you want to run the scan process: once, daily, weekly, or continuously.

3) Use the options under Properties to configure the scan:

- For daily or weekly scans, specify the hours during which to run the scan. As a best practice, run fingerprint scans outside 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.
- For one-time or continuous scans, to run as soon as possible after a designated time or date, mark **But not before**, then select a date from the drop-down box and a time from the spinner.
- For continuous scans, use **Wait** option to specify the number of minutes to wait between consecutive scans.

4) Click **Next to continue. See *Import Fingerprint Wizard - Finish* section.**

Related concepts

[Import Fingerprint Wizard - Finish](#) on page 235

Import Fingerprint Wizard - Finish

The Finish page of the database fingerprinting wizard displays a summary of the content classifier. The content of the list varies based on which type of classifier was imported.

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

The fingerprint scan occurs according to its schedule.

Machine learning

Machine learning classifiers are an advanced tool that allows administrators to provide examples of the type of data to protect and not to protect. This allows Forcepoint DLP to learn to identify sensitive data in traffic.

- The examples of what to protect are called positive training sets.
- The examples of what not to protect are called negative training sets. Together, these examples educate the system.

Unlike fingerprinting, the files do not need to contain parts of the actual files to protect, but can instead look similar or cover a similar topic. The system learns and recognizes complex patterns and relationships and makes decisions without the exact include/exclude criteria 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 than fingerprinting classifiers.



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.

After creating a 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, such as non-proprietary marketing plans as a negative example to proprietary marketing plans
- Non-explicit negative examples, such as 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, see *Introduction to Machine Learning for Forcepoint DLP* on the Forcepoint support site.

Creating a machine learning classifier

Create a machine learning classifier on the **Main > Policy Management > Content Classifiers > Machine Learning** page in the Data Security module of the Forcepoint Security Manager.

The Machine Learning page lists the existing machine learning classifiers.

- Expand the right pane to view more details, such as last run time, or collapse it to show fewer.
- Click the links in the details pane to adjust classifier settings or view more details.
- Start, stop, or pause a machine learning process using buttons on the toolbar at the top of the content pane.

To create the classifier, click **New** in the toolbar at the top of the content pane. A wizard opens. See *Machine Learning Wizard - General* section.

Related tasks

[Machine Learning Wizard - General](#) on page 236

Machine Learning Wizard - General

Use the General tab of the machine learning wizard to set a name and description for the classifier.

Steps

- 1) Enter a meaningful **Name** for the machine learning classifier, such as “Engineering source code.”
- 2) Enter a **Description** of this set of classifier.
- 3) Click **Next** to continue. See *Machine Learning Wizard - Credentials* section.

Related tasks

[Machine Learning Wizard - Credentials](#) on page 236

Machine Learning Wizard - Credentials

Use the Credentials tab of the machine learning wizard to identify which crawler to use to scan documents, and where the documents are located.

Steps

- 1) Use the **Crawler** drop-down list to elect which crawler to use to scan the documents.
 - The crawler is the agent that scans documents looking for sensitive data. There may be several in a network if there are many documents to manage.
 - Typically, it is best to select the crawler closest in proximity to the root folder containing the data.
- 2) Enter the **User name** for an account with read permissions for the root folder containing the data.
- 3) Enter the **Password** for this account.
- 4) Optionally, enter the **Domain** name for the account.
- 5) Enter the **Root folder** or root directory containing the files and folders you want to scan. A root folder is the highest folder in the hierarchy.
For example, to scan \\Server\Public\shared \User1, \\Server\Public\shared \User2, and \\Server\Public\shared \User3, enter:
\\Server\Public\shared
 - The path cannot exceed 256 characters.
 - Select the specific files and folders to scan on the Scanned Folders page (the next page in the wizard).
- 6) Click Next to continue. See *Machine Learning Wizard - Scanned Folders* section.

Related tasks

[Machine Learning Wizard - Scanned Folders](#) on page 237

Machine Learning Wizard - Scanned Folders

Use the Scanned Folders page of the machine learning wizard to identify the documents that will be scanned and used for finding similar documents or parts of documents in the future.

Steps

- 1) Under Positive Examples, identify the **Path** 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, 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.

- 2) Use the **Content type** drop-down list to select a type that best describes the content to protect. This must match the type of content in the positive examples folder.

For example, select **Java and C Source code** if the 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 **Other**.

- 3) Under Negative examples, use the check box to indicate whether or not negative examples are available.



Note

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.

If so, identify the **Path** that contains the files. For best results, there should be at least 50 examples in this folder.

The folder:

- Should contain examples of textual data that is similar to but *does not* represent the data you want to protect
- Must be dedicated to negative examples, and it cannot be a subdirectory of the positive examples folder

For example, to protect proprietary source code, the negative examples might reside in 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.

- 4) Under All documents, select the check box if there is not a dedicated negative documents folder. Then identify the **Path** 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 the positive examples to the documents in this folder and decides which files represent negative examples.
 - Select this option *and* provide negative examples to improve the speed and accuracy of the classifier.

- 5) Click **Next** to continue. See *Machine Learning Wizard - Scheduler* section.

Related concepts

[Machine Learning Wizard - Scheduler](#) on page 239

Machine Learning Wizard - Scheduler

By default, the machine learning process runs as soon as you complete this wizard.

Select **But not before** to run the scan later, then specify the earliest time to run the scan.

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.

When you are finished, click **Next** to continue. See *Machine Learning Wizard - Finish* section.

Related concepts

[Machine Learning Wizard - Finish](#) on page 239

Machine Learning Wizard - Finish

A summary of this machine learning classifier appears. It lists the:

- Name of the classifier
- Crawler being used to perform the scan
- Root folder
- Content type
- User logon
- Positive, negative, and all-documents examples provided
- 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

Use the **Create a Rule for the Content Classifier** page to create a rule from a selected classifier.

To access this page:

- 1) Go the Content Classifiers page.
- 2) Select a supported classifier type.
- 3) Select a classifier from the list.
- 4) Click **Create Rule from Classifier** in the toolbar at the top of the content pane.
If this option is not visible, click **More Actions**, then select **Create Rule from Classifier**.

- 5) On the Create a Rule for the Content Classifier page, the name of the selected content classifier and the policy type (Pattern, Key Phrase, etc.) are displayed at the top of the page. This information cannot be edited.

Complete the fields on the page as follows:

- 1) Enter the new **Rule name**.
 - 2) Do one of the following:
 - Select **Add this rule to an existing policy**, then:
 - a) Select the **Policy Type**: data loss prevention or discovery.
 - b) Select the **Policy Name**
 - Select **Add this rule to a new policy**, then:
 - a) Select the **Policy Type** to create: data loss prevention or discovery.
 - b) Enter a new **Policy Name**.
 - c) Enter a new **Policy Description**.
 - d) Select a **Policy level** from the drop-down list to set a priority for the policy. (This option appears only if the system has more than one level defined.)
For more information, see *Policy levels* section.
 - e) Click **Edit** to select one or more **Policy Owners** from a list.
- 3) Click **OK** to save your changes.

Related concepts

[Classifying Content](#) on page 181

[Policy levels](#) on page 121

Chapter 13

Defining Resources

Contents

- General resources on page 242
- Cloud resources on page 242
- Endpoint resources on page 244
- Remediation resources on page 245
- User directory entries on page 245
- Custom user directory groups on page 246
- Custom users on page 248
- Custom computers on page 249
- Networks on page 249
- Domains on page 250
- URL categories on page 251
- Business Units on page 251
- Endpoint Devices on page 252
- Endpoint Applications on page 253
- Endpoint Application Groups on page 254
- Endpoint Printers on page 256
- Remediation on page 257

In a policy, administrators can define:

- Data sources and destinations
- (With some subscriptions) The endpoint device or application that may be used
- The remediation action to take when a violation is discovered (such as block or notify)

In Forcepoint DLP, these are cumulatively known as **resources**.



Important

If no resources are defined, the policies and rules apply to all users, computers, networks, devices, and so on in the deployment.

Select a resource type to define on the **Main > Policy Management > Resources** page in the Data Security module of the Forcepoint Security Manager. Resources are grouped into 4 general areas: General, Cloud, Endpoint, and Remediation.

General resources

There are many possible sources (origins) and destinations of information in an organization. Define the following types of source and destination resources, then specify which to include and exclude in specific policies and rules.

- *User directory entries* are users or groups that may be a source or destination of sensitive data. These entries are imported from your user directory.
- *Custom user directory groups* are derived from custom LDAP queries, and may also send or receive sensitive data.
- *Custom users* are not included in the user directory, but may be a source or destination of sensitive data.
- *Custom computers* are not included in the user directory, but may be a source or destination of sensitive data.
- *Networks* may be a source or destination of sensitive data.
- *Business Units* may be a source or destination of sensitive data.
- *Domains* may be a source or destination of sensitive data.
- *URL categories* may be a source or destination of sensitive data.

Related concepts

[User directory entries](#) on page 245

[URL categories](#) on page 251

Related tasks

[Custom user directory groups](#) on page 246

[Custom users](#) on page 248

[Custom computers](#) on page 249

[Networks](#) on page 249

[Business Units](#) on page 251

[Domains](#) on page 250

Cloud resources

Cloud applications resources are instances of cloud application types (such as Office365) that can be defined as destinations of sensitive data rules. These resources are available only to customers who have Forcepoint DLP version 8.7.1 or later, and a Forcepoint DLP Cloud Applications license.

Use the **Main > Policy Management > Resources > Cloud Applications** page in the Data Security module of the Forcepoint Security Manager to view a list of cloud applications.

Administrators can add and edit cloud applications that support DLP Cloud API and Cloud Data Discovery, but not DLP Cloud Proxy. All cloud applications that support DLP Cloud Proxy are defined in the Forcepoint CASB portal, and are automatically displayed on this page. The page also includes links to the CASB portal, where custom policies can be configured, or applications can be completely removed.

The Show/Hide Columns button enables control of the columns to display, including:

- Application Name
- Application Type

- Description
- DLP Cloud API Status
- DLP Cloud Proxy Status
- Cloud Data Discovery Status

To add a cloud application that supports DLP Cloud API and Cloud Data Discovery:

- 1) Click the **Add** button at the top of the page.

The **Add DLP Cloud Application** window appears, displaying a list of all the available cloud application types defined in the system.



Note

- Pop-up blockers may prevent this page from opening. If this occurs, disable the pop-up blocker and try again.
- It might take a while for the tab to open. Wait for the tab to load, and then complete the steps below. Do not close the page while it is still loading.

- 2) Select an application type, and then click **OK**.

The application is added to the list of application resources.



Note

If you select the Office 365 cloud application type, you can choose to monitor OneDrive, SharePoint, Teams, or Other in **Main > Policy Management > DLP Policies**.

To edit a cloud application:

- 1) Click the name of the application in the **Application Name** column.

The **Cloud Application Properties** window appears in a new browser tab.

For more information on managing these properties, see *Forcepoint CASB Administration Guide*, “Managing Service Assets”.

- 2) Enter a descriptive **Application name** and **Service description** to help administrators manage the service.

- 3) Under Connection, enter the Key and Secret to enable a connection to the selected cloud application, then click **Configure Connection**.

The Cloud Applications service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials.

- 4) Under Service Type, specify whether or not to **Enable activity import** and allow the Cloud Applications service to access and import user activity logs for the selected cloud application.

- 5) Under Mitigation, configure an **Archive folder** within the cloud service for files moved or copied in response to a DLP incident.

- 6) Under Quarantine, optionally configure messages than can be left in place of quarantined files to explain to users that their file has been moved.

Click **Test Connection** to verify that the message file can be copied to the cloud application.

- 7) To save the changes, click **OK**.

- The new application is added to the cloud applications list, which shows the application’s name, type, description, and status.

- The **Edit** link opens the properties window in the CASB portal, which can be used to update configuration for the application.

Repeat these steps as many times as needed to enable the CASB service for each cloud application to which DLP policies will be applied.

Error handling

The following are instructions and recommendations for some of the errors you might encounter:

Error message	Details	Handling
<p><i>No CASB policy is defined, or a CASB policy is configured incorrectly.</i></p> <p><i>Enable the CASB policy and select either Download or Upload user action in the CASB portal.</i></p>	In DLP Cloud Proxy Status column	<p>In the CASB portal do one of the following:</p> <ul style="list-style-type: none"> Create and enable a Forcepoint Data Security DLP Policy, and select a user action (Upload, Download) Create a custom policy with a Forcepoint DLP predicate, and select a user action (Upload, Download) <p>Without one of these configurations, no transaction is sent by DLP to data inspection.</p> <p>For more information, see the Forcepoint CASB documentation.</p>
<p><i>CASB gateway doesn't exist. Contact Forcepoint support.</i></p>	<p>One of the following issues might have occurred:</p> <ul style="list-style-type: none"> No CASB Gateway was installed (needed to support DLP Cloud Proxy) CASB license has expired, and the CASB Gateway was therefore removed. 	Contact Forcepoint Technical Support.

Endpoint resources

These resources are only available to accounts with a Forcepoint DLP Endpoint subscription.

- Endpoint Devices* may be the source or destination of sensitive data.
- Endpoint Applications* may be a source or destination of sensitive data on endpoint machines.
- Endpoint Application Groups* may be a source or destination of sensitive data on endpoint machines.
- Endpoint Printers* may be a source or destination of sensitive data.

**Important**

Note that **Networks** is not an available source for endpoint channels, even if they are defined in the system as a resource. This is not a bug.

Related concepts

[Endpoint Application Groups](#) on page 254

Related tasks

[Endpoint Devices](#) on page 252

[Endpoint Applications](#) on page 253

[Endpoint Printers](#) on page 256

Remediation resources

- *Action Plans* define the action to take when a breach is discovered.
- *Remediation scripts* define the external script to run when a breach is discovered. (Not available with all subscriptions.)
- *Notifications* can be sent to a specific person or email alias when a breach is discovered.

Related concepts

[Action Plans](#) on page 257

[Remediation scripts](#) on page 269

[Notifications](#) on page 273

User directory entries

Use the **Main > Policy Management > Resources > User Directory Entries** page in the Data Security module of the Forcepoint Security Manager to view a list of users, groups, and computers that imported from a user directory such as Microsoft Active Directory or IBM Domino. CSV files are also supported.

**Note**

Because the page shows the results of a user directory import, administrators can view the list but cannot make changes.

These users, groups, and computers are possible sources or destinations of sensitive information within the organization.

Each entry shows 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.)

If there are too many users and groups to display on 1 page, 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 enter an asterisk (*) to 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 page through results.

Click **Settings** in the toolbar at the top of the content pane to add user directory servers, set the server order, or initiate a directory import. If you are using Risk- Adaptive Protection to determine actions permitted according to the user's risk level, you can see the **Risk Level** of each user in the list. A value of 1 to 5 is shown only for users that were assigned to Risk-Adaptive Protection. Level 1 is set for users that are considered less risky for the organization; level 5 is for users that are considered to be most risky. The values are determined by Forcepoint Behavioral Analytics and sent to Forcepoint DLP.

Related concepts

[Remediation on page 257](#)

Related tasks

[Custom user directory groups on page 246](#)

Custom user directory groups

Use the **Main > Policy Management > Resources > Custom User Directory Groups** page in the Data Security module of the Forcepoint Security Manager to add or manage custom 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; 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. If you are using Risk-Adaptive Protection to determine actions permitted according to the user's risk level, you can see the **Risk Level** of each user in the list. A value of 1 to 5 is shown only for users that were assigned to Risk-Adaptive

Protection. Level 1 is set for users that are considered less risky for the organization; level 5 is for users that are considered to be most risky. The values are determined by Forcepoint Behavioral Analytics and sent to Forcepoint DLP.

To add a custom user directory group to a policy, first add it to a business unit. Then,



Tip

Administrators can also create groups of Forcepoint DLP resources. These can contain both user directory entries and non-user directory resources, such as URL categories, geo-locations, custom users, and custom computers. These groups are referred to as business units (see *Business Units* section for more information).

when configuring rules, select the business unit as a source or destination.

The group objects are recalculated every time the user directory is synchronized with the system.

To create a custom user directory group:

Steps

- 1) Click **New**.
- 2) Enter a **Name** for the group.
- 3) Enter a **Description** for the group.
- 4) If you have more than one **User directory** configured, select which one to query.
- 5) Enter an LDAP **Query** to 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"]
    ":" matchingrule ":=" value
present = attr "=*"
substring = attr "=" [initial] any
    [final]
initial = value
any = "*" *(value "*")
final = value Nested operations:
    (|(&(..K1...)(..K2...))(&(..K3...)(..K4...)))
```



Note

Not all user directory entries can be retrieved. Only the following are supported: users, groups, and computers.

Queries are refreshed whenever you re-import user directory.

- 6) Click **View Sample Data** to view examples 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.
- 7) Click **OK**.

Related concepts

[User directory entries](#) on page 245

[Remediation](#) on page 257

[Risk-Adaptive Protection](#) on page 377

Related tasks

[Business Units](#) on page 251

Custom users

Use the **Main > Policy Management > Resources > Custom Users** page in the Data Security module of the Forcepoint Security Manager to add or manage custom users—that is, users that are not part of the user directory.

If you are using Risk-Adaptive Protection to determine actions permitted according to the user's risk level, you can see the **Risk Level** of each user in the list. A value of 1 to 5 is shown only for users that were assigned to Risk-Adaptive Protection. Level 1 is set for users that are considered less risky for the organization; level 5 is for users that are considered to be most risky. The values are determined by Forcepoint Behavioral Analytics and sent to Forcepoint DLP.

To add a custom user, click **New**, then:

Steps

- 1) Enter the **Name** of the custom user.
- 2) Enter the **Email address** for the user.
- 3) Enter a **User name** for the user.
- 4) Optionally, enter the **Windows NT Domain** for the user.
 - Leave this field empty for users who don't belong to a domain and should be considered a match when they log on to a computer using a local account.
 - Set this field to “*” if the user is part of a domain and should be considered a match for all domains.
 - For users who should be considered a match only when they log on to a specific domain, set this field to a precise domain name.
- 5) Optionally enter a **Title** for the person.
- 6) Optionally enter the name of the person's **Manager**.
- 7) Optionally enter the **Department** to which this person belongs.
- 8) Optionally enter the person's **Phone number**.
- 9) Click **OK**.

Custom computers

Use the **Main > Policy Management > Resources > Custom Computers** page in the Data Security module of the Forcepoint Security Manager to view and set up a list of local computers that are possible sources or destinations of information in your organization, in addition from the computers in the user directory.

To add a new computer to the system, click **New**, then:

Steps

- 1) Enter the **IP address or hostname** for the computer.
- 2) Enter a **FQDN** (fully-qualified domain name) for the computer (for example, myhost.example.com).
- 3) Enter a **Description** of this computer.
- 4) Click **OK**.



Note

For custom computers that also have an endpoint profile, include both the FQDN and an IP address.

Networks

Use the **Main > Policy Management > Resources > Networks** page in the Data Security module of the Forcepoint Security Manager to define the networks that are possible sources or destinations of sensitive information in your organization.

To add a network to the system, click **New**, then:

Steps

- 1) Enter a Name for the network you are adding.
- 2) Enter a Description of this network.
- 3) Do one of the following:
 - Select **Network address** 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).
 - Select **IP address range** to enter the IP address range for the network (for example, 192.168.0.0 to 192.168.255.255).
- 4) Click **OK**.

Domains

Use the **Main > Policy Management > Resources > Domains** page in the Data Security module of the Forcepoint Security Manager 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, an organization that has just acquired another company, and has not yet combined user directories, could add the domain of the new company as an authorized destination.

To add a domain, click **New**, then:

- Complete the fields as follows:
- Enter a **Domain** name. Enter either:
 - A concrete domain name that is the name of a specific computer—like www.example.com
 - A name using wildcards to indicate a group of computers—for example, *.example.com, w*.example.com, www-?.example.com.
- Enter a **Description** for this domain.
- Click **OK**.

For expedience, you can also import a list of domains:

- 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:
`myvendor.com, "VendorA, translation vendor for manuals"`
- 2) Click **Import** in the toolbar at the top of the content pane.
- 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 is used.



Note

By default, the system excludes predefined SaaS domains from the destinations list for the Web DLP policy. The domains are part of a business unit called Excluded Resources.

To add domains and other resources to the business unit, or to remove them, click the business unit name to edit it.

See *Business Units* section, for more information.

Related tasks

[Business Units](#) on page 251

URL categories

If you are using Forcepoint Web Security, use the **Main > Policy Management > Resources > URL Categories** page in the Data Security module of the Forcepoint Security Manager to select the URL categories that may be the source or destination of sensitive information.

Use these categories in policies to define rules for web channels. For example, define a rule that credit card numbers cannot be posted to known fraud sites. (The system does not monitor URL categories on endpoint web channels.)

URL categories are imported in one of two ways: Either using Linking Service, from the Forcepoint Master Database, or from Forcepoint Web Security Cloud Portal using an XML file. Categories can, therefore, be viewed but not changed. If you are using Linking Service, periodically click **Update Now** to reconnect with the database and update your category list. If you are importing from Forcepoint Web Security Cloud Portal, you can import multiple XML files.

Getting URL category mapping using either Linking Service or importing Forcepoint DLP supports predefined and custom categories.

Forcepoint Web Security may identify more than one category for a single URL. For example, a blog might have a static category of Blogs and Personal Sites, but also be classified in the Malicious Embedded Link category after having been hacked.

Forcepoint Web Security looks up static URL categories and Content Gateway analyzes dynamic content. Both categories are reflected in your incident reports.



Important

To take advantage of Forcepoint URL categorization, first configure linking. See *Linking Service and mapping URL categories* section.

Related concepts

[Linking Service and mapping URL categories](#) on page 368

Business Units

Use the **Main > Policy Management > Resources > Business Units** page in the Data Security module of the Forcepoint Security Manager 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 Forcepoint DLP resource. These can include both user directory entries, such as users and groups, and non-user directory resources, such as URL categories, geographical locations, custom users, custom computers, networks, domains, and printers.

Create a business unit by adding resources to it. 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, Forcepoint DLP applies the policy only to users in the business unit.

If the analytics engine for incident risk ranking is installed, you can use business units to influence the risk scores shown in reports. First, create a business unit that contains what you consider to be high-risk resources. Then, on the **SettingsGeneral > Analytics** page, indicate which business units to use when calculating risk scores, and specify the level of risk.

To define a business unit, click **New**, then:

- 1) Enter a **Name** for this business unit.
- 2) Enter a **Description** for this business unit.
- 3) Use the **Display** drop-down list to select the item to add to the business unit. Options include:
 - Directory Entries
 - Custom Computers
 - Domains
 - Networks
 - Custom Users
 - Countries (web destinations only; specifies which countries can receive data via web posts)
The selected entry appears in the **Available List** grouping at the bottom of the page.
 - Custom User Directory Groups
- 4) If there are more directory entries than fit on 1 page, use the **Find** field to specify criteria by which to filter the display, then click **Apply**.
 - Use the **from type** drop-down list to select the type of directory entry to search: All, Computer, Group, User, or Organization Unit (OU).
 - Use the **in** drop-down list to indicate whether you want to search all directory servers or the selected directory server.
- 5) Use the **Available Directory entries** list to select the resources to add to the business unit, then click the right arrow (>).
You can add an entire group, then use exclusions to remove people from the business unit.
Selected directory entries appear in the Selected List.

Forcepoint DLP 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.
- 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.

Related tasks

[Custom user directory groups](#) on page 246

Endpoint Devices

Use the **Main > Policy Management > Resources > Endpoint Devices** page in the Data Security module of the Forcepoint Security Manager to define the endpoint devices to specify in policies. If you do not define devices, all devices are covered.

To add a device:

Steps

- 1) Click **New**.
- 2) Enter a **Name** for this device, such as “SanDisk Cruzer Blade on JohnDoe laptop”.
- 3) Enter a **Description** for this device, such as “JohnDoe laptop device”.
- 4) Enter a **Value** for your selection.
For example, “SanDisk Cruzer Blade; 4C530103131102119495” where “4C530103131102119495” is the device serial number.
 - Wildcards are supported. For example, to protect all SanDisk Cruzer Blade devices in the company, use “SanDisk Cruzer Blade*”.
 - Use exact values when wildcards are not used.
 - Include a space after the semicolon when there is more than one value.



Tip

To filter reports by device serial number, use free text under Filter by Destination.

- 5) Click **OK**.

Endpoint Applications

Forcepoint provides a 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 applications, are included in [Endpoint Applications](#).

Use the **Main > Policy Management > Resources > Endpoint Applications** page to review the built-in applications and define custom applications.

To add an application, click **New > Application** or **New > Cloud Application** in the toolbar at the top of the page, then:

- 1) Enter a **Name** for this application, such as Microsoft Word.
- 2) In the **Initiated by** field:
 - For Windows desktop applications, enter the name of the executable file (for example, winword.exe).
 - For Mac or Windows Store apps, enter the app name (for example, Microsoft.SkypeApp* for the Windows Store Camera app).
 - For cloud applications, enter the URL.
- 3) Enter a **Description** for this application.
- 4) To associate the application with an existing application group, mark **Belongs to**, then select the group of interest.
- 5) If enforcement is not needed for an application, mark **Trusted 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.

Specify up to 50 trusted endpoint applications. If necessary, a trusted application can be configured to represent multiple applications. Contact Technical Support for assistance.

There are no trusted cloud applications.

- 6) Under Screen Capture, use the **Action** drop-down list to select the action to take when end users try to capture screens from this application.

Screen captures are not analyzed for content. They are blocked and audited, permitted and audited, or permitted as specified here.



Note

Screen captures cannot be blocked in macOS 11.

- 7) Click **OK**.

The predefined (built-in) applications are identified by the application metadata. This is a very secure method of identifying application usage.

When you add applications, 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.

To add an application so that it is identified according to the application metadata, use an external utility program. For information about the utility and instructions for using it, see [Importing other applications](#).

Endpoint Application Groups

Use the **Main > Policy Management > Resources > Endpoint Application Groups** page to review a list of Forcepoint-defined application groups: categories used to characterize similar applications.

The application groups are listed in a table. Click any column title to sort the table by that column.

The default operations monitored on each application group in Windows environments are shown below. Select other operations as needed.

Type	Copy/Cut	File Access	Paste	Download
Browsers	✓		✓	
CD Burners		✓		
Cloud Storage	✓	✓	✓	
Email			✓	
Encryption Software		✓		
FTP		✓		
IM		✓	✓	
Office Applications	✓			

Type	Copy/Cut	File Access	Paste	Download
Online medical	✓			✓
P2P		✓	✓	
Packaging Software		✓		
Portable Devices		✓		
SaaS (online)	✓			✓

To define your own application group, click **New > Application Group** or **New > Cloud Application Group**, then see *Adding custom application groups* section for instructions.

Related tasks

[Adding custom application groups](#) on page 255

Applying a column filter

On the Endpoint Application Groups page, click the down arrow next to a column heading to apply a column filter in the table. Filters help to narrow down the list of application groups displayed in the table.

When you apply a filter to the Applications column, you're prompted to select one or more applications. If you select more than one (for example, Notepad and Firefox), the system displays groups that have either of the applications. In other words, the OR operation is applied to the filter: if Notepad OR Firefox is in the group, display the group.

The Endpoint Operations filter works the same way. When you apply a filter, you're prompted to select the operations to view. 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 **Policy Management > Resources > Endpoint Application Groups > Application Group** or **Cloud Application Group** page to define application groups that are not in the Forcepoint-defined list. To access this page, click **New** in the toolbar at the top of the content pane on the Endpoint Application Groups page.

- A custom application group can contain predefined and/or custom endpoint applications.
- Applications include locally-installed software packages, like Microsoft Word and Excel, as well as custom applications.
- Cloud applications are those accessed over the web. To configure a custom application group:
 - 1) Enter a **Name** for the application group, such as Desktop Publishing.
 - 2) Enter a **Description** of the application group.

- 3) In the Members box, click **Edit** to select applications to include in this group.
- 4) Under Endpoint Operations, select the operations that should trigger content analysis for the applications in this group.
Because screen captures are not analyzed for content, configure screen capture settings for individual endpoint applications (not application groups).

**Note**

Screen captures cannot be blocked in macOS 11.

- 5) Click **OK**.

Endpoint Printers

Use the **Main > Policy Management > Resources > Endpoint Printers** page to review the endpoint printers monitored by the system. Each printer is associated with

a name, a type (auto-detected or user-defined), and a print server (IP address or hostname).

Initially, only printers detected by the system are shown.

Optionally add printers to the list—local and network printers that may be connected to endpoints.

To add a printer:

- 1) Click **New** in the toolbar.
- 2) Enter a **Name** for the printer or group of printers you're adding. Example: HP- 6050 or All HP printers.
- 3) Enter a **Description** this printer or group of printers.
- 4) Enter a **Value** to specify exactly which printer or printers to include in this setting. Wildcards are supported.
- 5) Indicate whether or not this is a **Trusted endpoint printer**.
When this option is selected, the endpoint printer is not monitored. All print jobs directed to this printer by endpoint users are permitted.
- 6) Click **OK**.

Use policies to 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.

Remediation

After defining which information can go where, identify the remediation steps or actions to perform when a policy breach is discovered.

Related concepts

- [Action Plans on page 257](#)
- [Remediation scripts on page 269](#)
- [Notifications on page 273](#)

Action Plans

Use the **Policy Management > Resources > Action Plans** page in the Data Security module of the Forcepoint Security Manager to define how the system responds when various breaches are discovered.

The following action plans are provided by default.

Name	Description
Audit and Notify	Audit incidents from all channels, and if configured, generate notifications.
Audit Only	(Default) Permit all activity on all channels, and log incidents in the audit log. If configured, it also generates notifications. This action plan is designed for mild breaches.
Audit Without Forensics	Same as Audit Only, but does not store forensic data for the incident.
Block All	Block all incidents on all channels, audit them, and, if configured, generate notifications. This action plan is designed for severe breaches.
Block Without Forensics	Same as Block All, but does not store forensic data for the incident.
Drop Email Attachments	Drop email attachments that breach policy.



Note

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

Select an action plan each time rules or exceptions are added to a policy.

- To create a new action plan, click **New**.
- To edit an action plan, click its name in the Action Plans list. See *Adding or editing an action plan* section.

See *Possible actions for an action plan* section for the actions available for use in an action plan, depending on the channel.

- To delete an action plan, select it and click **Delete**.
- To select an action plan to use by default, select a plan in the list, then click **Set as Default Action Plan**.

Related concepts

[Remediation scripts](#) on page 269

[Notifications](#) on page 273

[Possible actions for an action plan](#) on page 265

Related tasks

[Adding or editing an action plan](#) on page 258

[Adding a new message](#) on page 273

Adding or editing an action plan

Use the **Policy Management > Resources > Action Plans > Action Plan Details** page to create or edit an action plan.

There are several ways to access the Action Plan Details page:

- From the toolbar at the top of the content pane on the Action Plans page, click **New**.
- From the list on the Action Plans page, click the name of an action plan.
- In the Custom Policy wizard, on the Severity & Action tab, click the New or Edit icon next to the name of an Action Plan.

To create or edit an action plan:

- 1) Enter or update the **Name** and **Description** for the action plan.
- 2) The remaining options on the page vary based on subscription. See the appropriate section for your subscription:
 - *Standard Forcepoint DLP options*
 - *Forcepoint Data Discovery options*
 - *Forcepoint Web Security mode*
 - *Forcepoint Email Security mode*

Related concepts

[Standard Forcepoint DLP options](#) on page 259

Related tasks

[Forcepoint Data Discovery options](#) on page 261

[Forcepoint Web Security mode](#) on page 262

[Forcepoint Email Security mode](#) on page 264

Standard Forcepoint DLP options

On the **Data Loss Prevention** tab, complete the fields as follows. See *Possible actions for an action plan* section for a description of each possible action.

1) Under Network Channels:

Action	Description
Email	Select an action to take when a breach is discovered on network email channels.
Mobile email	Select an action to take when a breach is discovered in content being sent to a user's mobile device.
FTP	Select an action to take when a breach is discovered over FTP.
HTTP/HTTPS	Select an action to take when a breach is discovered over HTTP or secure HTTP.
Chat	Select an action to take when a breach is discovered over chat.
Plain text	Select an action to take when a breach is discovered via plain text.

2) Under Endpoint Channels:

Action	Description
Email	Select an action to take when a breach is discovered on endpoint email. You cannot release endpoint email; therefore, you can only block messages, not quarantine them.
Application control	Select an action to take when a breach is discovered on an endpoint application such as Word.
Removable media	Select an action to take when a breach is discovered on an endpoint device such as a thumb drive.
HTTP/HTTPS	Select an action to take when a breach is discovered on an endpoint device over HTTP or secure HTTP.
LAN	Select an action to take when a breach is discovered on an endpoint LAN, such as when a user copies sensitive data from a workstation to a laptop.
Printing	Select an action to take when a breach is discovered on a local or network printer that is connected to an endpoint.

3) Under Cloud Channels, there are two channels: DLP Cloud Proxy and DLP Cloud API.

For DLP Cloud Proxy, select from the drop-down list an action to take when an incident involves files uploaded, attached, or downloaded from a cloud application.

- Select **Permit** to allow files to be uploaded, attached, or downloaded.
- Select **Block** to prevent the user action.

**Note**

When Block is applied, some desktop cloud applications might perform multiple retries to sync with the cloud service, and potentially malfunction. If this happens, multiple incidents might be received by the DLP system.

For DLP Cloud API, select from the drop-down list an action to take when an incident involves files uploaded to, downloaded from, or shared with others.

- Select **Permit** to allow files to be uploaded, synchronized, downloaded, or shared.
- Select **Safe copy** to keep a copy of the file in the cloud archive that is accessible only to administrators.
- Select **Quarantine** to save the file in a quarantine folder defined in the CASB portal.
- Select **Quarantine with note** to quarantine the file and leave a message in place of the original file.
- Select **Unshare external** to remove sharing permissions for any external address.
- Select **Unshare all** to remove all sharing permissions from the file.

- 4) By default, all incidents are audited. Clear the **Audit incident** check box if you do not want to audit incidents.

**Warning**

If you turn off this option, incidents are not logged, so you will not know when a policy is breached.

When Audit incident is selected, select one or more of the following additional options:

- Select **Include forensics** to 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.
- Select **Run remediation script** to have the system run a script when an incident is discovered, then select the script to use from the drop-down list. See *Remediation scripts* section for more information.
- Select **Run endpoint remediation script** to have the system run an endpoint remediation script when an incident is discovered, then select the script to use from the drop-down list.
- Select **Send syslog message** to notify an outside syslog server or ticketing system of the incident.
- Select **Send email notifications** 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* and *Adding a new message* sections 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. Therefore, 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.

- 5) To configure discovery options, continue to the next section. Otherwise, click **OK** to save the changes.

Related concepts

Possible actions for an [action plan](#) on page 265

[Remediation scripts](#) on page 269

[Notifications](#) on page 273

Related tasks

[Adding a new message](#) on page 273

Forcepoint Data Discovery options

Enter the following information in the **Discovery** tab:

Steps

- 1) In the Network Discovery section, select **Run remediation script** when you want the system to run a remediation script for network discovery incidents. Select a script from the associated drop-down list. See [Remediation scripts](#) sections.

- 2) In the Endpoint Discovery section, if file labeling is enabled for deployment, it can be selected from the **Labeling system** drop-down list. Specify up to two Boldon James Classifier labels and up to one Microsoft Information Protection label to apply to the files.
 - If labels are removed from the labeling system, an alert is shown under the removed labels. Select a new label from the drop-down list or clear the check box.
 - If the “No labels were found” message is displayed, import labels as described in [Configuring file labeling](#).
 - Once a label is added, the action plan displays the following information for each label:
 - Labeling system
 - Selected label
 - Label properties (for example, “Marking” or “Protection” for Microsoft Information Protection labels)



Note

Make sure that only one labeling system is selected for an action plan. Forcepoint DLP supports use of only one labeling system at a time: Either Microsoft Information Protection or Boldon James, but not both.

- 3) Select **Run endpoint remediation script** when you want the system to run an endpoint remediation script for endpoint discovery incidents. Select a script from the associated drop-down list.
- Remediation scripts can be added on the **Main > Policy Management > Resources > Remediation Scripts** page. Select **New > Endpoint Script**.

- 4) Under Cloud Discovery, select the Cloud service supported action from the drop-down list:
 - Select **Permit** to allow the transaction.
 - Select **Safe copy** to keep a copy of the file in the cloud archive that is accessible only to administrators.
 - Select **Quarantine** to save the file in a quarantine folder defined in the CASB portal.
 - Select **Quarantine with note** to quarantine the file and leave a message in place of the original file.
 - Select **Unshare external** to remove sharing permissions for any external address.
 - Select **Unshare all** to remove all sharing permissions from the file.

- 5) Click **OK** to save the changes.

Related concepts

[Remediation scripts](#) on page 269

[Configuring file labeling](#) on page 374

Forcepoint Web Security mode

Steps

- 1) Select the Action to take when a user is breaching policy:
 - **Permit** or allow the HTTP, HTTPS, or FTP request to go through.
 - **Block** or deny the request.

- 2) Select **Audit incident** to have Forcepoint DLP to log incidents. When logging is enabled, email notifications are also available.

- 3) Select **Send email notifications** 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* and *Adding a new message* sections 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. Therefore, 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.

Related concepts

[Notifications](#) on page 273

Related tasks

[Adding a new message](#) on page 273

Forcepoint Email Security mode

Steps

- 1) Under Email, select an action to take when a breach is discovered on network email channels.

With Forcepoint Email Security (on-premises), the action option configured here applies to all email directions.

For cloud infrastructure deployments such as Microsoft Azure, this option applies only to outbound email. (Inbound and Internal email is permitted, and an alert is sent to the Forcepoint Email Security administrator.)

- **Permit** the message to go through.
- **Block** or deny the message or post.
- **Quarantine** the message.

Select **Encrypt on release** to have the system encrypt the message before it's released.



Note

Release from quarantine is not supported for messages detected by Forcepoint Email Security Cloud.

- **Drop attachments** that are in breach of policy. Quarantines email messages that:
 - Have a body breach, but not an attachment breach.
 - Have breaches in both the message body and attachment.
 - Are detected by agents other than Forcepoint Email Security, such as the protector.
 - Fail to drop attachments when indicated.



Note

- In a uuencoded attachment, additional content is placed between the attachments, including the attachment name. As a result, if a violation is found in a uuencoded attachment, the attachment is treated as email body and blocked, rather than dropped.
- Note that only Forcepoint Email Security can drop attachments. If the drop attachments options is selected when the protector or Forcepoint Email Security Cloud is monitoring email, messages are quarantined when a policy is triggered.

Select **Encrypt on release** to have quarantined messages 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.

(Incidents are released from quarantine when an administrator selects **Remediate > Release** on the incident details toolbar. Release is not supported for messages detected by Forcepoint Email Security Cloud.)

- **Encrypt** the message.



Tip

Custom actions can also be created in the Email Security module of the Forcepoint Security Manager, specifically for email DLP policies. (Go to the **Policy Management > Actions** page, then click **Add**.)

Custom actions offer more control over what happens to email that leaks sensitive data. For example, Bcc the original unfiltered message, delay message delivery until a certain date, and so on.

Any custom Forcepoint Email Security actions are displayed here, in addition to the default actions.

- 2) Select **Audit incident** to have Forcepoint DLP to log incidents in the incident database. By default, audit is selected irrespective of the action.



Warning

If you turn off this option, incidents are not logged, so you will not know when a policy is breached.

When Audit incident is enabled, several additional actions are available. Select any of these actions to apply.

- 3) If you select **Send email notifications**:

- 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* and *Adding a new message* sections 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. Therefore, 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.

Related concepts

[Notifications on page 273](#)

Related tasks

[Adding a new message on page 273](#)

Possible actions for an action plan

The actions available for use in an action plan depend on the channel being configured.

Possible actions include:

Action	Description
Permit	Allow data to be maneuvered based on your selection—for example, allow it to be printed or posted to a website.
Block	Deny or block data from being printed, posted, or emailed, depending on your selection.
Audit only	Activity is audited and available to review.

Action	Description
Quarantine	<p>Quarantine email messages containing sensitive data. Network email can be encrypted before it's released. Select Encrypt on release to enable this feature (this feature is not supported for Forcepoint Email Security Cloud).</p> <p>Note: 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.</p>
Quarantine with note	Quarantine the message as described above, and provides a note to the user in place of the message.
Safe copy	Keep a copy of the file in the cloud archive that is accessible only to administrators.
Unshare external	Remove sharing permissions for any external addresses.
Unshare all	Remove all sharing permissions from the file.

Action	Description
Drop attachments	<ul style="list-style-type: none"> ■ Drops email attachments that are in breach of policy. <ul style="list-style-type: none"> ■ Applies to messages detected by the Forcepoint Email Security module (except for Forcepoint Email Security Cloud). ■ Applies to rules that monitor data in “each part separately.” ■ Quarantines email messages that: <ul style="list-style-type: none"> ■ Have a body breach, but not an attachment breach. ■ Have breaches in both the message body and attachment. ■ Are detected by agents other than Forcepoint Email Security, such as the protector. ■ Are detected when rules are monitoring data in “the transaction as a whole.” ■ Fail to drop attachments when indicated. <p>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.)</p> <p>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.</p> <p>To release an incident, an administrator selects Remediate > Release on the incident details toolbar.</p>
Encrypt	<p>Encrypt the affected email message.</p> <p>With Forcepoint DLP agents and Forcepoint Email Security, this option applies to all email directions.</p> <p>For cloud infrastructure deployments such as Microsoft Azure, this option applies only to outbound email. (Inbound and Internal email is permitted, and an alert is sent to the Forcepoint Email Security administrator.)</p>
Encrypt with profile key	<p>Removable media only. Encrypts sensitive data for users who will be on authorized, endpoint machines. Passwords are set by administrators and deployed via profiles. Decryption is automatic if the files are accessed on the endpoints.</p>

Action	Description
Encrypt with user password	<p>Windows removable media only. Encrypts sensitive data for users who will be decrypting files from other machines (those without the endpoint agent installed). Passwords are set by endpoint users. Files are decrypted using a special utility.</p> <p>Note that if the user has not yet configured a password when the first breach is detected, the system prompts the user for a password and then blocks the operation. The encryption action is not performed until subsequent transactions.</p> <p>This option is not supported on Mac or Linux endpoints. Removable media transactions are permitted on Mac and Linux when this option is selected.</p>
Confirm	<p>Display a confirmation message, such as the following when a security threat is detected:</p> <p>Forcepoint DLP Endpoint has detected that you're trying to copy sensitive data to a removable drive, which appears to be in violation of corporate policy. Do you want to continue?</p> <p>Users can continue if they enter a business reason for the operation, or</p> <p>they can cancel. If they cancel or wait too long, the default action is taken.</p> <p>To configure the default action, go to the Settings > General > Endpoint page and select Block or Permit on the General tab.</p>
Run remediation script	<p>Run a script that performs specific actions when an incident is detected.</p> <p>Remediation scripts can be run when network discovery, endpoint discovery, or DLP incidents are detected.</p> <p>See <i>Remediation scripts</i> section.</p>
Add classification tag	<p>Add classification tags to files that trigger a discovery incident, following the guidelines established on the Settings > General > Services > Classification Tagging page.</p> <p>Endpoint discovery only.</p> <p>Requires a supported, third-party classification tagging system.</p>

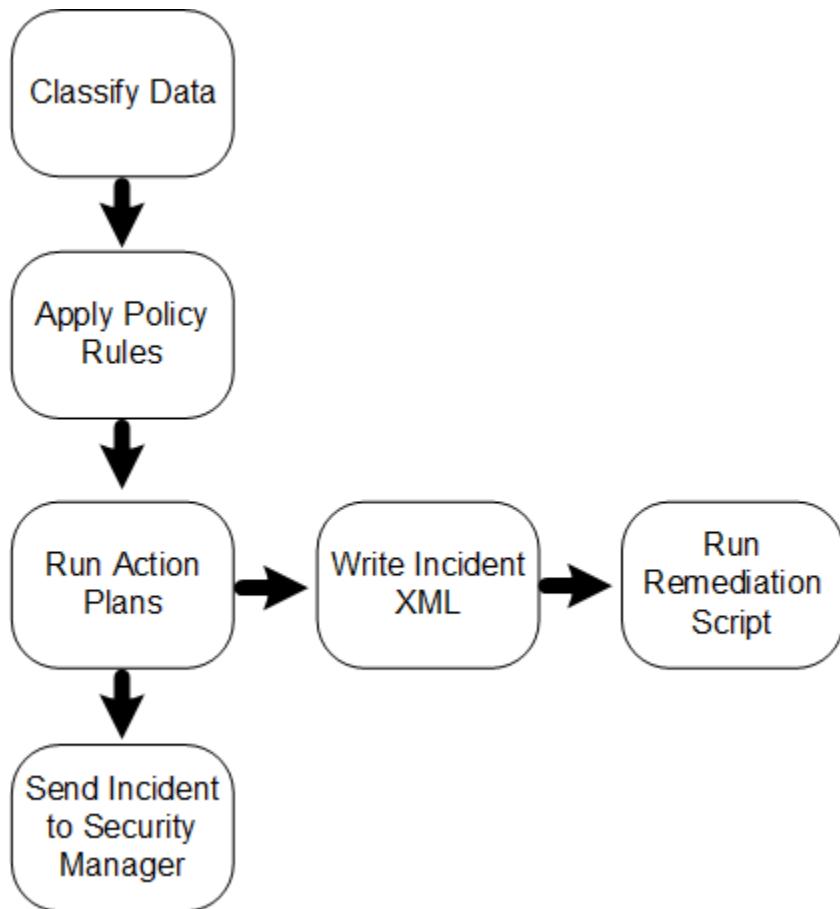
Related concepts

[Remediation scripts](#) on page 269

Remediation scripts

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

A remediation script is an executable run by a policy engine or endpoint agent whenever an incident is triggered.



A remediation script is considered a resource. Configure remediation scripts on the **Resources > Remediation Scripts** page in the Data Security module of the Forcepoint Security Manager. Use this page to identify and manage the external scripts to run when various breaches are discovered.

Related concepts

[Incident XML interface for use in remediation scripts on page 270](#)

Related tasks

[Adding a new remediation script on page 271](#)

Types of remediation scripts

There are 3 types of remediation scripts:

- An **Endpoint Script** runs automatically when endpoint incidents are triggered. Because the script is run on an endpoint device, it should have minimal CPU and disk space requirements. In addition, the script should not assume the endpoint computer is part of the network, and it should be smaller than 5 MB.
- An **Incident Management Script** runs on incidents selected in the Incident Report. To activate this script:

- 1) Open an incident on the **Main > Reporting > Data Loss Prevention > Incidents** page.
- 2) Click **Remediate > Run Remediation Script** in the toolbar at the top of the content pane.
- 3) Select which script to run.

The script can be used to automate tasks such as opening a CRM case. It is not executed automatically.

- A **Policy Script** runs automatically when data loss prevention and discovery incidents are triggered. For example, the script might encrypt data detected in discovery breaches or perform an action in a DRM system. Because the script is associated with the network server, it can be larger and more demanding of CPU resources, and it can make use of other tools in the network.

Note that the Policy Script can only be run by the Policy Engine of the System Module that analyzed the incident.

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* section for details.

For information on writing your own scripts, see *Creating Remediation Scripts* on the Forcepoint support site.

Related concepts

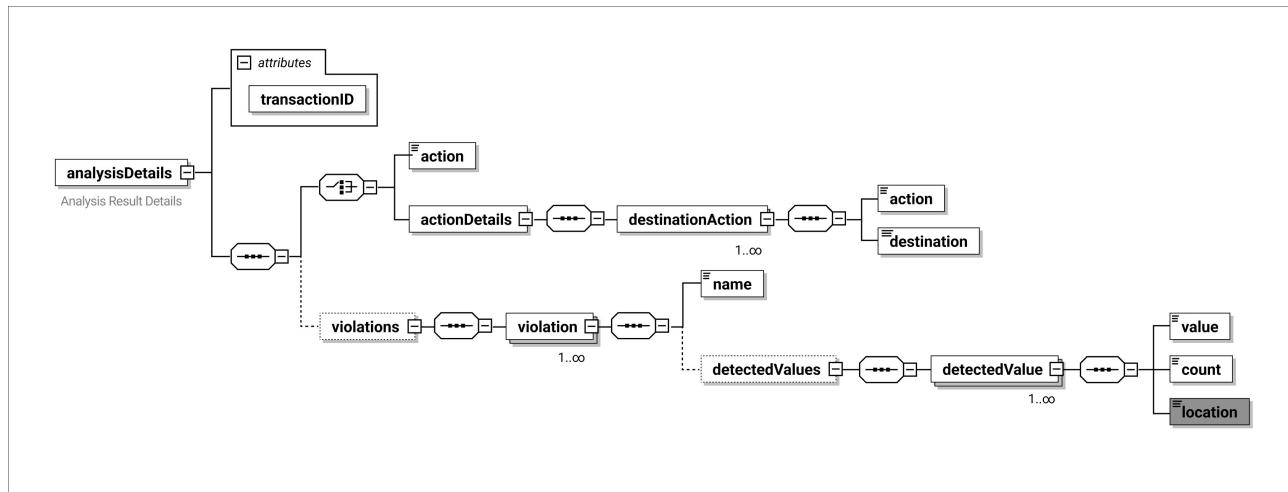
[Copying or moving discovered files](#) on page 288

Incident XML interface for use in remediation scripts

Forcepoint DLP creates an XML file every time an incident is generated. The XML file contains incident details that can be used in remediation scripts, 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:



In this schema:

Element	Description
<code>analysisDetails</code>	Root element.

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

Adding a new remediation script



Warning

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

Use the **Policy Management > Resources > Remediation Scripts > Remediation Script Details** page to define a new endpoint, incident management, or policy script.

- To access this page, click **New** on the **Resources > Remediation Scripts** page, then select the type of script.
- For a description of each type of script, refer to *Remediation scripts* section.

To add a remediation script:

- 1) Enter a **Name** for this remediation script.
- 2) Enter a **Description** for this script.
- 3) The page includes a tab for each operating system supported for the selected script type. There may be up to 3 tabs: Windows, Linux, and Mac.

Define a script for each available operating system. When a breach is discovered on an endpoint, the system knows which version to run.

Complete the fields on each tab as follows:

Field	Description
Executable file	<p>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.</p> <p>Note: If you are using a remediation script that copies files to a \quarantine folder, be sure to exclude this folder from discovery scans.</p> <p>Endpoint scripts must be smaller than 5 MB.</p>

Field	Description
Arguments (optional)	Optionally, enter any arguments you want to include with the command. If the arguments are enclosed in quotation marks, separate arguments by a space. For example: "-e" "-o"
Additional Files	If the script requires additional files, such as a resource file or other scripts that it calls, click Additional Files then browse to a zip file containing the additional file(s) to run. Note: Additional files are placed in the same folder as the script, and they are automatically downloaded by the endpoints.

- 4) 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 management server.
- 3) Click **OK** to continue.
- 4) Browse to the new executable file.
- 5) If necessary, update the additional files in the same way.
- 6) Click **OK**.

For more information about writing a remediation script, see *Creating Remediation Scripts* on the Forcepoint support site. 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

Related concepts

[Remediation scripts](#) on page 269

Notifications

Use the **Main > Policy Management > Resources > Notifications** page in the Data Security module of the Forcepoint Security Manager to define whom to notify when a breach is discovered.

Forcepoint DLP 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.

Related tasks

[Adding a new message](#) on page 273

[Mail servers](#) on page 363

Adding a new message

Use the **Resources > Notifications > Notification Details** page to define notification messages.

To access this page, click **New** in the toolbar at the top of the content pane on the Notifications page.

Steps

- 1) Enter a **Name** for this notification template, such as “Breach notification”.
- 2) Enter a **Description** for the template.

On the General tab

Steps

- 1) Enter the **Sender name** that appears in the email From field when notifications are sent. The maximum length is 1024 characters.
- 2) Enter the **Sender email address**: the email address of the person from whom notifications should be sent. The maximum length is 1024 characters.
 - If you are using Exchange Online, a valid sender email address must be used.
- 3) Information for the currently configured outgoing mail server is displayed. To change the server used, see [Mail servers](#).

- 4) Enter a **Subject** for the notification. This appears in the email Subject: line. The maximum length is 4000 characters.

Click the right arrow to select variables to include in the subject, such as “This is to notify you that your message was %Action% because it breached corporate policy.”

- 5) Define one or more **Recipients** for the notification.

- Click **Edit** to select to select business units or directory entries.
- Select **Additional email addresses**, then click the right arrow to select a dynamic recipient that varies according to the incident. For example, you can choose to send the notification to the policy owners, administrators, source, or source's manager. Select the variable that applies, such as %Policy Owners%. Separate multiple addresses with commas.
- 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.

Related tasks

[Mail servers](#) on page 363

On the Notification Body tab

Steps

- 1) Select a notification **Type**:

- Select **Standard** to include all of the elements shown in the Body Content box. You can enable or disable these elements if you use the standard notification type.
- Select **Custom** to send a custom notification. Edit the default text as needed. The drop-down menu provides variables.

- 2) Select a display format from the **Display as** drop-down list: HTML or plain text.

3) Select from the following display options:

- Select **Logo** to display the Forcepoint logo, date, and time.
- Select **Action** to displays the action taken when the breach was discovered.
- Select **Message to user**, then update the text as needed. The result is displayed in the email body. Click the right-arrow icon to see a list of variables that may be included in the message.
- Select **Incident details** to include incident details in the notification message.
- Select **Violation triggers** to attach a list of rules violated by the breach.
- Select **Include links so that recipients can perform operations on the incident** to include links that administrators can use to perform workflow operations on the incident (like assign, ignore, and escalate) directly from the notification. (See sample links below.)
Administrators can perform only the operations they have permission to perform from their role assignment.

Plain text notifications do not show links.

To support this feature, create an email account for the Forcepoint DLP system in Exchange. To avoid reconfiguration, make sure the credentials assigned to this mailbox do not expire. Once done, navigate to **Settings > General > Mail Servers** and configure the incoming mail server. Use this mailbox for the system email address.

- Select **Allow recipients to release quarantined email from this notification** to give message recipients the ability to release blocked messages by replying to their notification message or by clicking the Release All link within the message.

See *Releasing blocked email in Forcepoint DLP* section on the Forcepoint support site for instructions on setting up the release by reply capability. You must configure options in both Forcepoint DLP and Microsoft Exchange to enable it.



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 *Mail servers* for more information.

4) Select **Attach policy-breach content to include the content that violated policy as an attachment to the message.**

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

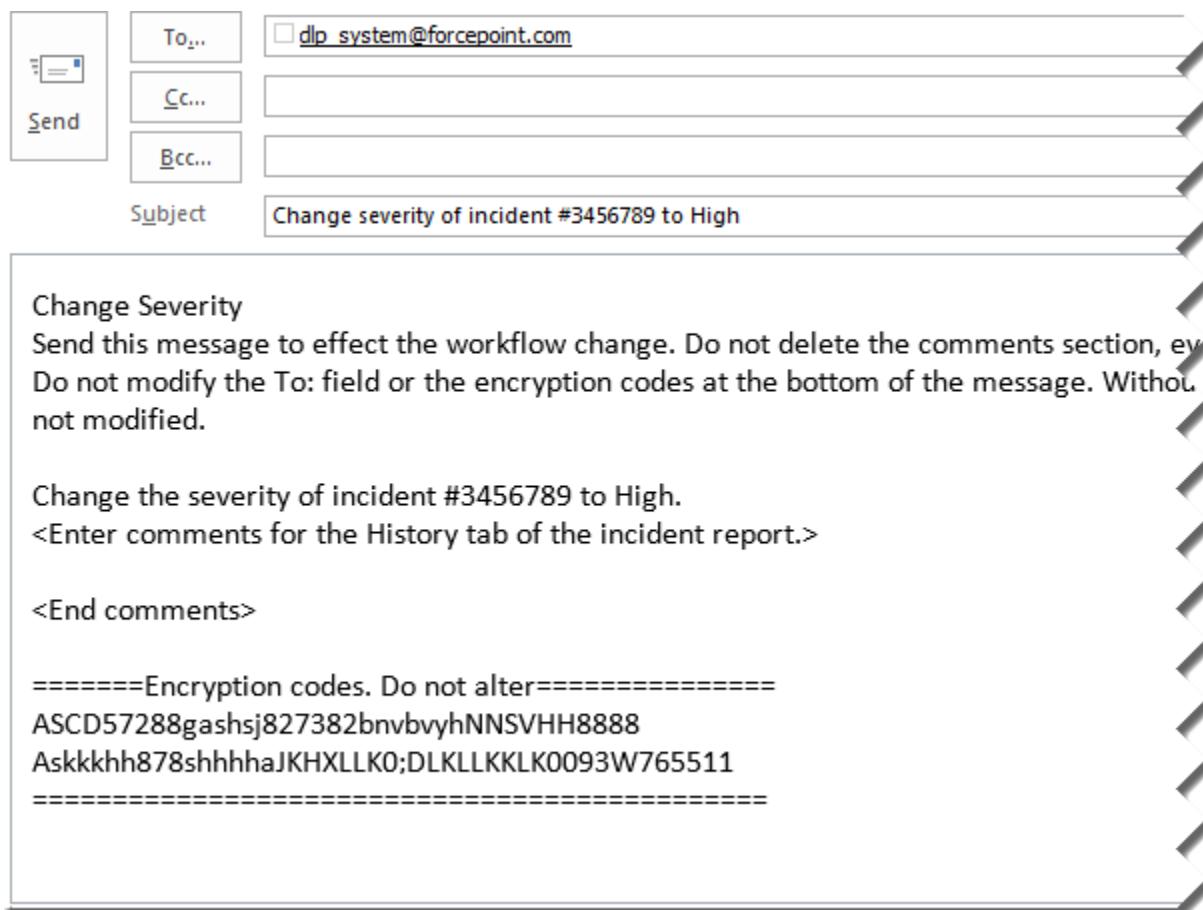
Next steps

The following example shows what recipients see at the bottom of their notification message. Here, they can perform workflow actions on the incident and release the quarantined content.

Actions	
Change severity to:	High Medium Low
Change status to:	New An administrator is reviewing this incident Closed
Escalation:	Escalate to source's manager
More actions:	Assign Ignore Add comments

Each link opens a window used to compose a message to the system's notification server. This is how the workflow operation is communicated to the management server.

For example, if a recipient clicks the link to change the status of an incident to High, an email message opens like this:



A default message is drafted, but the sender can add comments to display on the History tab of the incidents report.

- Do not delete the Comments section, even if there are no added comments.
- If there are custom comments, 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, an error message is sent or the error is saved in the syslog. Syslog errors are logged if the system experiences an internal error.

Related tasks

Mail servers on page 363

Chapter 14

Creating Discovery Policies

Contents

- [Creating a discovery policy](#) on page 278
- [Scheduling the discovery scan](#) on page 280
- [Performing file system discovery](#) on page 281
- [Performing SharePoint discovery](#) on page 282
- [Performing Domino discovery](#) on page 282
- [Performing Box discovery](#) on page 283
- [Performing database discovery](#) on page 284
- [Performing Exchange discovery](#) on page 285
- [Performing Outlook PST discovery](#) on page 285
- [Performing endpoint discovery](#) on page 286
- [Viewing discovery status](#) on page 287
- [Viewing discovery results](#) on page 287
- [Updating discovery](#) on page 288
- [Configuring discovery incidents](#) on page 288
- [Copying or moving discovered files](#) on page 288

Discovery is the act of determining where sensitive content is located in an organization. A discovery policy might, for example:

- Scan all the computers in the network looking for financial documents containing the keyword “Confidential” every Sunday.
- Log what is discovered and send a notification to the Finance manager.

Discovery finds data at rest in the network and identifies the endpoint machines that represent the greatest risk.

To monitor what is done with records found by a discovery policy, or stop them from leaving the building, create a network or endpoint policy.

Performing discovery is comprised of 2 basic steps:

- 1) *Creating a discovery policy***
- 2) *Scheduling Discovery Tasks***

Discovery policies are structurally the same as data loss prevention policies. Both are made up of rules, exceptions, content classifiers, and resources. Rather than specifying destination channels to scan such as FTP, SMTP, and printers, however, discovery tasks describe 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 includes the ability to scan:

- Network file systems to identify data in breach of policies.
- SharePoint directories and identify data in breach of policies.
- Documents in a data management system or IBM Domino server.

Database Discovery scans the organization's database servers and detects confidential information that is defined as policy breaches in tables.

Email Discovery includes the ability to scan:

- The Microsoft Exchange server and identify data in breach of policies.
- Outlook folders to detect confidential information defined as policy breaches in Outlook PST data files.

Endpoint Discovery includes the exact devices to scan.

Discovery policies are different from data loss prevention policies in other subtle ways, as well. For example:

- Content tends to be classified differently in database discovery than on web channels.
- False positives or false negatives in discovery are typically less troubling, because the information is not being sent out of the organization.

Related concepts

[Viewing discovery results](#) on page 287

[Updating discovery](#) on page 288

[Copying or moving discovered files](#) on page 288

[Scheduling Discovery Tasks](#) on page 293

Related tasks

[Configuring discovery incidents](#) on page 288

[Viewing discovery status](#) on page 287

[Creating a discovery policy](#) on page 278

Creating a discovery policy

Create new policies from the **Main > Policy Management > Discovery Policies > Manage Discovery Policies** page in the Data Security module of the Forcepoint Security Manager.

- 1) Click **Add** in the toolbar at the top of the content pane, then select either Predefined Policy or Custom Policy.
- 2) A wizard appears. The options in the wizard are different, based on the policy type that you selected.

Related concepts

[Scheduling Discovery Tasks](#) on page 293

[Managing rules](#) on page 175

[Managing exceptions](#) on page 176

Related tasks

[Creating Custom DLP Policies](#) on page 155

Predefined policies

In the wizard for predefined policies:

Steps

- 1) Click **Next** and select the geographical regions to cover.
- 2) Click **Next** and select the industries to cover.
- 3) The **Finish** screen appears, summarizing your selections. Click **Finish**. The Forcepoint DLP policy database is updated and a confirmation message appears. The policies you selected appear in a list.
- 4) 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, see [Predefined Policies](#).)

Custom policies

In the wizard for custom policies:

Steps

- 1) On the General tab, enter a unique **Policy name** and a **Description** of the policy.
- 2) Mark **Enabled** to activate the policy.
- 3) By default, no **Policy owners** are included in the policy. To define policy owners, click **Edit**, then:
 - a) Select the type of accounts to **Display** (Administrators, by default).
 - b) Select one or more accounts from the list on the left, then click the right arrow to move them to the Selected list. Accounts in this list are considered policy owners, and are notified in the event of a policy breach.
 - c) Click **OK**.
- 4) Indicate whether to **Use the policy name for the rule name** (default) or **Use a custom name for the rule**. If you select the custom name option, enter a custom **Rule name** and, optionally, a **Description**.
- 5) Click **Next**.
- 6) Use the Condition tab, specify whether this rule monitors **specific data** or **all activities**, and whether the data is monitored in **all parts of the transaction as a whole** or **each part of the transaction separately**.

- 7) Click **Add** to add one of the following content classifiers or attributes to the condition you are creating:
 - **Patterns & phrases:** 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 **OK**. See *Patterns & Phrases* section, for details.
 - **File Properties:** Select file properties to add to this policy. Click **OK**. See *File properties* section, for details.
 - **Fingerprint:** Select the fingerprint classifier to use for this policy. Click **OK**. See *Fingerprint* section, for details.

Select a Content Classifier and click **Remove** to not include it in the condition you are defining.
- 8) Select an answer for the question: **When do you want to trigger the rule?**
 - All conditions are matched
 - At least one condition is matched
 - Custom
After selecting custom, use the options on the right to complete the condition description.
- 9) Click **Next** to define the **Severity & Action** for incidents that match this rule and to specify the action plan to be taken. Click **Advanced** to further specify the severity according to the number of matched conditions.
- 10) Click **Next** to complete the wizard.
- 11) Click **Finish** to create the new rule and add it to the policy.

Next steps

The process of adding rules and exceptions to discovery policies is the same as for DLP policies. See *Managing rules* section, and *Managing exceptions* section, for instructions.

Related concepts

- [File properties](#) on page 196
- [Fingerprint](#) on page 173
- [Managing rules](#) on page 175
- [Managing exceptions](#) on page 176

Related tasks

- [Patterns & Phrases](#) on page 189

Scheduling the discovery scan

After creating a discovery policy, schedule the scan on the **Main > Policy Management > Discovery Tasks** page in the Data Security module of the Security Manager. You can schedule network discovery tasks or endpoint discovery tasks.

For more information, see *Scheduling Discovery Tasks*.

Related concepts

[Scheduling Discovery Tasks](#) on page 293

Related tasks

- [Performing file system discovery](#) on page 281
- [Performing SharePoint discovery](#) on page 282
- [Performing database discovery](#) on page 284
- [Performing Exchange discovery](#) on page 285
- [Performing Outlook PST discovery](#) on page 285
- [Performing Domino discovery](#) on page 282
- [Performing endpoint discovery](#) on page 286

Performing file system discovery

To perform discovery on a network file system:

- 1) Prepare your file server.
- 2) Create a discovery policy (see *Creating a discovery policy* section).
- 3) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 4) Under Network Discovery Tasks, select **Add network task > File System Task**.
- 5) Complete the fields on the page, then click **Next** to start the file system discovery task wizard. See *File System tasks* section.
- 6) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

- [Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

- [Creating a discovery policy](#) on page 278
- [File System tasks](#) on page 298

Performing SharePoint discovery

To perform discovery on SharePoint folders:

- 1) Create a discovery policy (see *Creating a discovery policy*).
- 2) Go to the **Main > Policy Management > Discovery Policies** page.
- 3) Under Network Discovery Tasks, select **Add network task > File Discovery > SharePoint Task** on the toolbar.
- 4) Complete the fields on the page, then click **Next** to start the SharePoint discovery task wizard. See *SharePoint tasks* section.
- 5) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

- [Scheduling Discovery Tasks](#) on page 293
- [Scheduling network discovery tasks](#) on page 297
- [Viewing the incident list](#) on page 69

Related tasks

- [Creating a discovery policy](#) on page 278
- [SharePoint tasks](#) on page 303

Performing Domino discovery

To perform discovery on documents on an IBM Domino server:

- 1) Create a discovery policy (see *Creating a discovery policy*).
- 2) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 3) Under Network Discovery Tasks, select **Add network task > File Discovery > Domino Task** on the toolbar.
- 4) Complete the fields on the page, then click **Next** to start the SharePoint discovery task wizard. See *Domino Discovery Task Wizard - General* section.
- 5) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

[Scheduling Discovery Tasks](#) on page 293

[Domino tasks](#) on page 324

[Scheduling network discovery tasks](#) on page 297

[Viewing the incident list](#) on page 69

Related tasks

[Creating a discovery policy](#) on page 278

[Domino Discovery Task Wizard - General](#) on page 325

Performing Box 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, then click **Sites**.
 - c) Enter the web address www.box.com and click **Allow**.
 - d) Click **OK**.
- 2) Create a discovery policy (see *Creating a discovery policy* section).
- 3) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 4) Under Network Discovery Tasks, select **Add network task > File Discovery > Box Task** on the toolbar.
- 5) Complete the fields on the screen and click **Next** to proceed through a wizard. See *Box tasks* section.
- 6) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

[Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

[Creating a discovery policy](#) on page 278
[Box tasks](#) on page 307

Performing database discovery

To perform discovery on a database:

- 1) Create a discovery policy (see *Creating a discovery policy* section).
- 2) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 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. See *Database Discovery Task Wizard - General* section.
- 5) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

[Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

[Creating a discovery policy](#) on page 278
[Database tasks](#) on page 311
[Database Discovery Task Wizard - General](#) on page 312

Performing Exchange discovery

To perform discovery on email on a Microsoft Exchange server:

- 1) Prepare your Exchange server as described in the [Forcepoint DLP Deployment Guide](#).
- 2) Create a discovery policy. (See *Creating a discovery policy* section for instructions.)
- 3) Go to the **Main > Policy Management > Discovery Policies** page.
- 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. See *Exchange tasks* section.
- 6) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

- [Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

- [Creating a discovery policy](#) on page 278
[Exchange tasks](#) on page 316

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* section for instructions).
- 2) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 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. See *Outlook PST tasks* section.
- 5) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

- [Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

- [Creating a discovery policy](#) on page 278
[Outlook PST tasks](#) on page 321

Performing endpoint discovery

To perform discovery on endpoint systems:

- 1) Create a discovery policy. (See *Creating a discovery policy* for instructions.)
- 2) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 3) Under Endpoint Discovery Tasks, select **Add endpoint task**.
- 4) Complete the fields on the screen and click **Next** to proceed through a wizard. See *Scheduling endpoint discovery tasks* section.
- 5) After completing all of the steps in the wizard, to deploy the changes, click **Yes** when prompted.

Discovery will take place at the scheduled time and day. To start discovery immediately, click **Start**. A message indicates when the scan finishes.

To view and respond to discovery results, go to the **Main > Reporting > Discovery** page. See *Viewing the incident list* section.

Related concepts

- [Scheduling Discovery Tasks](#) on page 293
[Scheduling network discovery tasks](#) on page 297
[Viewing the incident list](#) on page 69

Related tasks

[Creating a discovery policy](#) on page 278

Viewing discovery status

To view the status of a discovery task:

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 2) Under Network Discovery Tasks, select **Manage network tasks**.
- 3) View the **Status** column of the task list table.

Next steps

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

You cannot view the status of endpoint discovery.

Viewing discovery results

Use the **Main > Reporting > Discovery** page in the Data Security module of the Security Manager to view and respond to discovery results.

- The report catalog lists reports into the discovery incident database.
- The incident list lists all discovery incidents and their details.

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

High-level discovery information also appears on the Dashboard (**Main > Status > Dashboard**). This includes a summary of discovery incidents, showing the top 5 hosts and top 5 policies per incident. The Dashboard also lists the date and time the last discovery incident was received.

Related concepts

[Viewing the incident list](#) on page 69

Related tasks

[The report catalog](#) on page 40

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

Configure the number of discovery incidents to display in the Data Security module of the Security Manager:

Steps

- 1) Go to the **Settings > General > Reporting** page.
- 2) Select the **Discovery** tab.
- 3) Complete the fields as described in.

Copying or moving discovered files

When Forcepoint DLP discovers sensitive content, it can copy or move sensitive content (files) using the following remediation scripts:

- **CopyFiles** - Copies files that are in breach of corporate policy to another directory.
- **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."

Both the CopyFiles and the MoveFiles scripts can be configured to ignore files that have not been accessed in X number of days.

Note the following:

- These remediation scripts are provided for network file system discovery, discovery on endpoint systems, and SharePoint only.

The scripts cannot be used for Exchange, Outlook PST, or database discoveries, and they cannot be used for local versions of 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 can always access the quarantine folder. If the quarantine folder is outside the network, the operations will not work.

These scripts provide examples of what can be done with remediation scripts. Administrators can create additional scripts to perform an action on discovered incidents, such as encryption or DRM integration.

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

Related concepts

[Preparing and running the remediation scripts](#) on page 289

Preparing and running the remediation scripts

The following steps explain preparing and running the remediation scripts.

STEP 1: Configure CopyFiles and MoveFiles

Steps

- 1) Navigate to the RunCommands subdirectory of the Forcepoint DLP installation directory and open the **CopyFiles.py** script in a text editor (like Notepad).
- 2) Use the **Location** field to define the destination of the *copied* files. This location may be either a network share (UNC path) accessible to all servers and/or endpoints running discovery, or a local path on the server and/or endpoints running discovery. For example:
 - Location = r'\\InfosecServer1\\Quarantine'
 - Location = r'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) Save and close the CopyFiles script.
- 4) In the same directory, open the **MoveFiles.py** script in a text editor.
- 5) Use the **Location** field to define the destination of the moved files. Refer to step 2 for requirements in this field.
 - The DaysKeepActiveFiles parameter defines the number of days to keep files.
 - QuarantineMsg is a stubbed file created by the MoveFiles script.
- 6) Save and close the MoveFiles script.
- 7) In the Data Security module of the Forcepoint Security Manager, go to the **Main > Policy Management > Resources Remediation Scripts** page.
- 8) Select **New > Endpoint Script or Policy Script**.
- 9) Enter a name and description for one of the discovery scripts.

- 10) Browse to the appropriate script: **CopyFiles.py** or **MoveFiles.py**.

It is not necessary to complete the fields on the Linux tab of the Add Policy Remediation Script window.

- 11) Enter a user name and password for an administrator that has all of the following:

- a) Read permissions to the archive folder
- b) Access to all directories in the network
- c) 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.

- 12) Click **OK**.

STEP 2: Add the remediation scripts to an action plan

Steps

- 1) In the Data Security module of the Forcepoint Security Manager, go to the **Main > Policy Management > Resources > Action Plans** page.
- 2) Select an action plan or select **New** from the toolbar.
- 3) On the Discovery tab, do one of the following:
 - Select **Run remediation script**, then select the script.
 - Select **Run endpoint remediation script**, then select the script to run for endpoint discovery.
- 4) Click **OK**.

STEP 3: Add the action plan to a policy

Steps

- 1) In the Data Security module of the Forcepoint Security Manager, go to the **Main > Policy Management > Discovery Policies** page.
- 2) Select the rule of interest and click **Edit**.
- 3) Navigate to the **Severity & Action** page.
- 4) Select the action plan.
- 5) Click **OK**.

STEP 4: Deploy your changes

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



Note

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

Chapter 15

Scheduling Discovery Tasks

Contents

- [Sorting and filtering tasks on page 293](#)
- [Scheduling network discovery tasks on page 297](#)
- [Emailing discovery task status reports on page 330](#)
- [Configuring cloud discovery scans on page 331](#)
- [Adding or editing a cloud discovery scan on page 333](#)
- [Scheduling endpoint discovery tasks on page 333](#)

Use the **Main > Policy Management > Discovery Policies** in the Data Security module of the Forcepoint Security Manager to create or manage discovery policies and tasks.

- Use **Create and Manage Policies** to add both predefined policies and policies with custom policy owners, conditions, severity settings, and action plans.
- Use **Network Discovery Tasks** to set up discovery on network file systems, shared (SharePoint) directories, Domino servers, databases, Outlook PST data files, and Exchange servers.
- Use **Cloud Discovery Scans** to set up discovery on your cloud applications. The feature is available with the Cloud Application license.
- Use **Endpoint Discovery Tasks** to set up discovery on endpoint hosts.

Related concepts

- [Scheduling network discovery tasks on page 297](#)
- [Domino tasks on page 324](#)
- [Configuring cloud discovery scans on page 331](#)

Related tasks

- [File System tasks on page 298](#)
- [SharePoint tasks on page 303](#)
- [Database tasks on page 311](#)
- [Exchange tasks on page 316](#)
- [Outlook PST tasks on page 321](#)
- [Adding or editing a cloud discovery scan on page 333](#)
- [Scheduling endpoint discovery tasks on page 333](#)

Sorting and filtering tasks

Tasks can be sorted, grouped, and filtered column name. Click the down arrow by any column name and choose an option:

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

Buttons and controls

For all discovery tasks:

- Click **New** to create a discovery task.
- Click **Delete** to delete the selected discovery task.

For a network discovery task, click **Edit** to update the active discovery task. If the changes require deployment, the task status changes to “Stopped (deployment needed).” When the task is restarted, it starts from the beginning.

For a cloud discovery scan, clicking **Reset Scan** forces a discovery scan cache reset. All files at rest are queued and processed for scanning with the latest policy configuration, including any files that were previously scanned.



Important

Using the **Reset Scan** button can significantly affect file processing time. Use this action only when significant changes are made to policies or when testing policies with a small data set. Avoid using this button after deployments when possible.



Note

If the crawler is unresponsive for any reason, delete the task manually, as prompted (see *Manually deleting discovery tasks*).

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

Button	Icon	Description
Start	▶	Starts a discovery scan.
Stop	■	Stops a discovery scan. When restarted, task starts from the beginning.
Pause		Pauses a discovery scan. When restarted, task starts from the last point it was paused.

Button	Icon	Description
Download		Downloads a detailed report on discovery scanning activities in CSV format.

Related tasks

[Manually deleting discovery tasks](#) on page 296

Details pane

Network tasks also offer a Details pane to show statistics about the scan and scheduler. Expand or collapse this pane to show more or fewer details.

Scan

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

Task Statistics

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

Last Scan Statistics*

Statistic	Description
Scanned items/tables/files	The total number of items, 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.
Scanned size	The size of items detected in the scan in MB, all totaled. (Does not apply to database scans.)
Scan progress	The progress of the scan, in percentage completed.
Analyzed items/tables/files	The number of items, tables, or files sent to the policy engine's fingerprint repository.

Statistic	Description
Failed items/tables/files	The number of items, tables, or files that failed for various reasons. Click the link to see more details on failed items.
Filtered out items/tables/ files	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.
Scanned mailboxes/ records/computers/shares	The total number of mailboxes, records, computers, or shares that were scanned.
Estimated total items/ tables/files/records	An estimate of the total number of items, tables, files, or records. This is an estimate, because some might be added or removed while the process is running.
Total records/items to scan	The number of items or records you've chosen, out of the total, to scan.
Estimated total size	An estimate of the total size of items in MB.(Does not apply to database scans.)

* 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 a discovery task is deleted from the management server, the crawler is not alerted that the task is deleted. When the

crawler becomes responsive, it continues to run the discovery scan as scheduled and consume unnecessary resources.

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

The Forcepoint Security Manager warns you in this situation, and asks if you want to continue. To delete the task:

- 1) Use either of the methods below to identify the ID of the job to delete:

- Go to the **Main > Logs > System Log** page in the Data Security module of the Security Manager 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 Forcepoint Security Manager, but not from the crawler, Crawler_Name 10.201.33.1.

- Log on to the crawler machine associated with the discovery task, then:
 - a) Go to the %DSS_HOME%/DiscoveryJobs folder.
 - b) To search for the relevant task and ID, open each job, one at a time, and examine the first line of its **definition.xml** file.
For example, the first line of one file might show:

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

This means that task "ora3" has ID 3178b4f9-96fe-4554-ad1d- eaa29fa23374.

2) To delete the job, log on to the crawler machine and go the %DSS_HOME%/ packages/Services folder.

3) Run the following command:

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

Here, jobID is the ID number identified in Step 1.

Scheduling network discovery tasks

Use the **Main > Policy Management > Discovery Policies > Network Discovery Tasks** page in the Data Security module of the Security Manager to configure discovery on your network machines. The page displays all of the network discovery tasks that have been established to date.

Network discovery is performed on:

- A hostname, if it is supplied
- An FQDN, if there is no hostname
- An IP address, if there is no hostname or FQDN The crawler uses the first of these that it finds.

To add a new network task, click **New**, then select the type of task to create from the menu. The types include:

- File Discovery
 - *File System tasks*
 - *SharePoint tasks*
 - *Domino tasks*
- Database Discovery
 - *Database tasks*
- Email Discovery
 - *Exchange tasks*
 - *Outlook PST tasks*

A wizard appears.

**Important**

As a best practice, run discovery tasks only 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.

Related concepts

[Domino tasks on page 324](#)

Related tasks

[File System tasks on page 298](#)
[SharePoint tasks on page 303](#)
[Database tasks on page 311](#)
[Exchange tasks on page 316](#)
[Outlook PST tasks on page 321](#)

File System tasks

Select **New > File Discovery > File System Task** on the **Discovery Policies > Network Discovery Tasks** page in the Data Security module of the Forcepoint Security Manager to launch the wizard for creating file system discovery tasks.

The wizard has 8 pages in total. It opens to the **General** page:

Steps

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for the discovery task.
- 3) Select the **Crawler** to use to perform the scan. Typically, this is the crawler that is located in closest proximity to the network server.
- 4) Click **Next**, then continue with *File System Discovery Task Wizard - Networks*.

Related tasks

[File System Discovery Task Wizard - Networks on page 298](#)

File System Discovery Task Wizard - Networks

Use the **Networks** page of the file system discovery task wizard to define where to run the discovery task.

Steps

- 1) By default, discovery runs on no computers or networks. Click **Edit** to select the computers and networks to scan.



Note

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

- 2) To use a port other than the default Windows port, click **Advanced**, then enter one or more port numbers (use commas to separate multiple values).
Use this option, for example, to run a discovery task on a Linux/UNIX NFS server or a Novell file server.
- 3) Click **Next**, then continue with *File System Discovery Task Wizard - Scanned Folders*.

Related tasks

[File System Discovery Task Wizard - Scanned Folders](#) on page 299

File System Discovery Task Wizard - Scanned Folders

Use the **Scanned Folders** page of the file system discovery task wizard to select folders for scanning.



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.

Steps

- 1) Under Scanned folders:
 - Select **Administrative shares** to scan administrative share drives (sometimes known as hidden shares) such as C\$ and D\$.
 - Select **Shared folders** to scan shared folders such as PublicDocs.
 - Select **Specific folders** to scan one or more specified folders, then enter one or more folder names. Use semicolons to separate multiple entries.

Individual paths cannot exceed 256 characters including hostname or IP.
- 2) Select the port scanning Method to use when scanning network shares:
 - Select **TCP** to scan the share drives using transmission control protocol.
 - Select **ICMP** to scan the share drives using Internet control message protocol.

ICMP is faster than TCP, but may trigger firewall alerts. (Scanning for open shares using ICMP is similar to virus activity.)

To use ICMP, configure your firewall to ignore the specific server running the crawler.

- 3) Enter the **User name** and **Password** for an account with network access to the specified computer or shares. For domain accounts, also enter the **Domain** (optional).



Warning

These credentials aren't verified until the scan starts. Be careful to enter a valid user name and password.

- 4) Click **Next**, then continue with *File System Discovery Task Wizard - Scheduler*.

Related tasks

[File System Discovery Task Wizard - Scheduler](#) on page 300

File System Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the file system discovery task wizard to enable and configure task scheduling.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.
Clear the check box to gain manual control over the task. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.
- 2) Under Run scan, select how often you want to run the scan process: Once, Daily, Weekly, or Continuously. Continuously means that the crawler starts again after every completed scan. (You can set a wait interval between scans.)
 - For Daily or Weekly scans, specify the **Hours to perform the scan** (for example, daily at 2 a.m.). As a best practice, run discovery scans after peak business hours. Select more than one time period to indicate when the scan should continue 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.
 - If Once or Continuously is selected, optionally mark **But not before** to run the scan as soon as possible, but not before a designated time or date. After marking the check box, select a date from the drop-down box and a time from the spinner.
 - If Continuously is selected, select the number of minutes to **Wait...between consecutive scans**. (Each scan starts from the beginning.)
- 3) Click **Next**, then continue with *File System Discovery Task Wizard - Policies*.

Related tasks

[File System Discovery Task Wizard - Policies](#) on page 300

File System Discovery Task Wizard - Policies

Use the **Policies** page of the file system discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *File System Discovery Task Wizard - File Filtering*.

Related tasks

[File System Discovery Task Wizard - File Filtering on page 301](#)

File System Discovery Task Wizard - File Filtering

Use the **File Filtering** page of the file system discovery task wizard to use file type, file age, file size, or a combination of properties to determine which files are scanned.

Steps

- 1) To filter based on file type or file name, mark **Filter by Type**, then list the types of files to be scanned, separated by semicolons.
 - Optionally use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”, or “*temp*.*”
 - To scan all files, set **Include file types** to *.
 - Click **File Types** to select the file types to include by extension. Add or edit file types, as needed.
- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well.
- 3) To filter based on file modification date, mark **Filter by Age**, then use the radio buttons to select a time period:
 - Select **Within** to search only for files modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for files modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From...To** to search for files modified between 2 dates, then specify the dates.
- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only files larger than**, then select a file size from the spinner.
 - Mark **Scan only files smaller than**, then select a file size from the spinner.
- 5) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports on page 330](#)

File System Discovery Task Wizard - Advanced

Use the **Advanced** page of the file system discovery task wizard to configure bandwidth limits, full scan options, and access timestamp behavior.

Steps

1) Select an option for controlling bandwidth used for the discovery process:

- Select **No limit** to avoid limiting the bandwidth used for discovery.
- Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the 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 Forcepoint DLP system.

While planning to use this feature, note that:

- Each file will be downloaded as fast as the operating system will allow.
- Subsequent file operations can be paused to maintain average bandwidth utilization.
- Average bandwidth utilization is maintained across several file operations, not during single file operation.

If the amount of data for discovery is big, consider placing the supplemental server with the crawler and policy engine closer to the 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.

2) Under Full scan schedule, select one of the following to indicate when to perform full discovery scans:

- Select **Only on policy update** to perform full discovery only when a discovery policy changes.
- Select **On policy update or fingerprinting version update** to perform full discovery when a discovery policy or a fingerprinting version changes.
- Select **Always** to perform full discovery at the scheduled time, no matter what has changed. (Forcepoint does not recommend choosing “always,” because this slows the discovery process and taxes the system and file servers.)

3) Under File access timestamp, select **Preserve original access time** to avoid updating the file access timestamp when files are scanned by Forcepoint DLP. When this option is selected, the operating system controls the “Last Accessed” timestamp of scanned files.



Note

To preserve access time, you must give Forcepoint DLP read-write privileges for all hosts where discovery is being performed.

4) Click **Next**, then continue with *File System Discovery Task Wizard - Finish*.

Related concepts

[File System Discovery Task Wizard - Finish](#) on page 303

File System Discovery Task Wizard - Finish

The **Finish** page of the file system discovery wizard displays a summary of the new file system discovery task.

SharePoint tasks

Forcepoint DLP can perform discovery on sites running the following versions of Microsoft SharePoint:

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Microsoft SharePoint 2019
- Microsoft SharePoint Online (Office 365)

The wizard for creating SharePoint discovery tasks has 8 pages. It opens to the

General page:

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for the discovery task.
- 3) Select the **Crawler** to use to perform the scan. Typically, this is the crawler that is located in closest proximity to the SharePoint server.
- 4) Under Data Storage, indicate where your data is located:
 - Select **Local** to perform discovery on a local or network SharePoint server.
 - Select **Online** to perform discovery on data residing in the cloud via SharePoint Online for Office 365.
- 5) Click **Next**, then continue with *SharePoint Discovery Task Wizard - Site Root*.

Related tasks

[SharePoint Discovery Task Wizard - Site Root](#) on page 303

SharePoint Discovery Task Wizard - Site Root

Use the **Site Root** page of the SharePoint discovery task wizard to identify the site to scan.

Steps

- 1) Under Site root hostname:
 - For **Local** SharePoint sites, enter the hostname of the site root, such as `http://gumby:1234/site_name`. (Note that a site is different than a folder in SharePoint. Forcepoint DLP supports only site-level URLs for this field.) It is possible to use an IP address instead of a hostname, but the SharePoint administrator must add the IP address to an alternate access map.
 - For **Online** SharePoint sites, enter the URL of the site root—for example: <http://comp.gumby.com>. The system clock of the Forcepoint DLP server running this task must be synchronized with the Internet time server within 5 minutes for connection to succeed.
- 2) Enter the **User name** and **Password** for an account with access to this site. This must be a user with administrative rights. Read permissions are not sufficient.



Note

SharePoint administrative rights include the following permission levels:

- Browse directories
- View pages
- Open
- Use remote interfaces
- Enumerate permissions
- View items
- View Versions
- Browse user information

Permission names may vary between SharePoint versions.

- 3) Optionally, enter the **Domain** for the administrator account.
- 4) Click **Next**, then continue with *SharePoint Discovery Task Wizard - Scanned Documents*.

Related tasks

[SharePoint Discovery Task Wizard - Scanned Documents](#) on page 304

SharePoint Discovery Task Wizard - Scanned Documents

Use the **Scanned Documents** page of the SharePoint discovery task wizard to determine where discovery runs.

Steps

- 1) By default, discovery runs on no SharePoint sites. Click **Edit** to select the SharePoint sites to scan.
- 2) Click **Next**, then continue with *SharePoint Discovery Task Wizard - Scheduler*.

Related tasks

[SharePoint Discovery Task Wizard - Scheduler](#) on page 305

SharePoint Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the SharePoint discovery task wizard to determine when discovery runs.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.

Clear the check box to gain manual control over the task. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.

- 2) Under Run scan, select how often you want to run the scan process: Once, Daily, Weekly, or Continuously.

Continuously means that the crawler starts again after every completed scan. (You can set a wait interval between scans.)

- For Daily or Weekly scans, specify the **Hours to perform the scan** (for example, daily at 2 a.m.). As a best practice, run discovery scans after peak business hours. Select more than one time period to indicate when the scan should continue 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.
- If Once or Continuously is selected, optionally mark **But not before** to run the scan as soon as possible, but not before a designated time or date. After marking the check box, select a date from the drop-down box and a time from the spinner.
- If Continuously is selected, select the number of minutes to **Wait...between consecutive scans**. (Each scan starts from the beginning.)

- 3) Click **Next**, then continue with *SharePoint Discovery Task Wizard - Policies*.

Related tasks

[SharePoint Discovery Task Wizard - Policies](#) on page 305

SharePoint Discovery Task Wizard - Policies

Use the **Policies** page of the SharePoint discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:

- Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
- Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.

- 2) Click **Next**, then continue with *SharePoint Discovery Task Wizard - File Filtering*.

Related tasks

[SharePoint Discovery Task Wizard - File Filtering](#) on page 306

SharePoint Discovery Task Wizard - File Filtering

Use the **File Filtering** page of the SharePoint discovery task wizard to use file type, file age, file size, or a combination of properties to determine which files are scanned.

**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.

Steps

- 1) To filter based on file type or file name, mark **Filter by Type**, then list the types of files to be scanned, separated by semicolons.
 - Optionally use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”, or “*temp*.*”
 - To scan all files, set **Include file types** to *.
 - Click **File Types** to select the file types to include by extension. Add or edit file types, as needed.
- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well.
- 3) To filter based on file modification date, mark **Filter by Age**, then use the radio buttons to select a time period:
 - Select **Within** to search only for files modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for files modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From...To** to search for files modified between 2 dates, then specify the dates.
- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only files larger than**, then select a file size from the spinner.
 - Mark **Scan only files smaller than**, then select a file size from the spinner.
- 5) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports](#) on page 330

SharePoint Discovery Task Wizard - Advanced

Use the **Advanced** page of the SharePoint discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1)** Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on the SharePoint server, network adapters, and Forcepoint DLP.
- 2)** Under Full scan schedule, select one of the following to indicate when to perform full discovery scans:
 - Select **Only on policy update** to perform full discovery only when a discovery policy changes.
 - Select **On policy update or fingerprinting version update** to perform full discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** to perform full discovery at the scheduled time, no matter what has changed. (Forcepoint does not recommend choosing “always,” because this slows the discovery process and taxes the system and SharePoint servers.)
- 3)** Click **Next**, then continue with *SharePoint Discovery Task Wizard - Finish*.

Related concepts

[SharePoint Discovery Task Wizard - Finish](#) on page 307

SharePoint Discovery Task Wizard - Finish

The **Finish** page of the SharePoint discovery task wizard displays a summary of the new SharePoint discovery task.

Box tasks

Forcepoint DLP can perform discovery on data stored in the Box cloud storage service.

The wizard for creating Box discovery tasks has 8 pages. It opens to the **General** page:

Steps

- 1)** Enter a **Name** for this discovery task.
- 2)** Enter a **Description** for the discovery task.
- 3)** Select the **Crawler** to use to perform the scan. Crawlers that do not support Box discovery (such as older versions) are disabled.
- 4)** Click **Next**, then continue with *Box Discovery Task Wizard - Permissions*.

Related tasks

[Box Discovery Task Wizard - Permissions](#) on page 308

Box Discovery Task Wizard - Permissions

Use the **Permissions** page of the Box discovery task wizard to grant Forcepoint DLP access to the organization's Box account. This requires logging on to Box.

Steps

- 1) If you are using Internet Explorer to configure this task, complete the following steps. This is not required for other browsers.
 - a) Select **Settings > Internet Options**.
 - b) On the Privacy tab, click **Sites**.
 - c) Enter the web address www.box.com, then click **Allow**.
 - d) Click **OK**.
- 2) In the Box discovery task wizard, click **Grant Access**. You're redirected to the Box website.
- 3) Log onto the Box account associated with your organization. Enter the email address (user name) and password of an account administrator, then click **Authorize**.
A Grant Access page appears in the Box interface.
- 4) Click **Grant Access to Box** to give Forcepoint DLP permission to connect with the organization's Box storage. With access, the system can read and write to all files and folders and manage the enterprise. Box issues a security token to the management server and displays connection status.
- 5) On connection, you are returned to the Forcepoint Security Manager to resume task configuration. Click **Next** to continue.
If Box fails to connect, the wizard will not continue to the next page. Try again, or try to log onto Box with different credentials.


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, edit each Box task that uses the token and re-grant access.

- 6) Click **Next**, then continue with *Box Discovery Task Wizard - Scanned Accounts*.

Related tasks

[Box Discovery Task Wizard - Scanned Accounts](#) on page 309

Box Discovery Task Wizard - Scanned Accounts

Use the **Scanned Accounts** page of the Box discovery task wizard to determine what to scan.

Steps

- 1) Select one of the following:
 - Select **All accounts** to scan documents and folders in all user accounts in the Box enterprise.
 - Select **Selected accounts** to specify accounts to scan, then click **Edit** to select the user accounts or folders to scan.
- 2) Click **Next**, then continue with *Box Discovery Task Wizard - Scheduler*.

Related tasks

[Box Discovery Task Wizard - Scheduler](#) on page 309

Box Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Box discovery task wizard to determine when discovery runs.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.
Clear the check box to gain manual control over the task. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.
- 2) Under Run scan, select how often you want to run the scan process: Once, Daily, Weekly, or Continuously.
Continuously means that the crawler starts again after every completed scan. (You can set a wait interval between scans.)
 - For Daily or Weekly scans, specify the **Hours to perform the scan** (for example, daily at 2 a.m.). As a best practice, run discovery scans after peak business hours.
Select more than one time period to indicate when the scan should continue 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.
 - If Once or Continuously is selected, optionally mark **But not before** to run the scan as soon as possible, but not before a designated time or date. After marking the check box, select a date from the drop-down box and a time from the spinner.
 - If Continuously is selected, select the number of minutes to **Wait...between consecutive scans**. (Each scan starts from the beginning.)
- 3) Click **Next**, then continue with *Box Discovery Task Wizard - Policies*.

Related tasks

[Box Discovery Task Wizard - Policies](#) on page 310

Box Discovery Task Wizard - Policies

Use the **Policies** page of the Box discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *Box Discovery Task Wizard - File Filtering*.

Related tasks

[Box Discovery Task Wizard - File Filtering on page 310](#)

Box Discovery Task Wizard - File Filtering

Use the **File Filtering** page of the Box discovery task wizard to use file type, file age, file size, or a combination of properties to determine which files are scanned.



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.

Steps

- 1) To filter based on file type or file name, mark **Filter by Type**, then list the types of files to be scanned, separated by semicolons.
 - Optionally use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”, or “*temp*.*”
 - To scan all files, set **Include file types** to *.
 - Click **File Types** to select the file types to include by extension. Add or edit file types, as needed.
- 2) Use the **Except** field to list the file types to exclude from the scan, separated by semicolons. Wildcards are permitted here as well.
- 3) To filter based on file modification date, mark **Filter by Age**, then use the radio buttons to select a time period:
 - Select **Within** to search only for files modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for files modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From...To** to search for files modified between 2 dates, then specify the dates.

- 4) To filter based on file size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only files larger than**, then select a file size from the spinner.
 - Mark **Scan only files smaller than**, then select a file size from the spinner.

- 5) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports](#) on page 330

Box Discovery Task Wizard - Advanced

Use the **Advanced** page of the Box discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1) Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on network adapters and Forcepoint DLP.

- 2) Under Full scan schedule, select one of the following to indicate when to perform full discovery scans:
 - Select **Only on policy update** to perform full discovery only when a discovery policy changes.
 - Select **On policy update or fingerprinting version update** to perform full discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** to perform full discovery at the scheduled time, no matter what has changed. (Forcepoint does not recommend choosing "always," because this slows the discovery process.)

- 3) Click **Next**, then continue with *Box Discovery Task Wizard - Finish*.

Related concepts

[Box Discovery Task Wizard - Finish](#) on page 311

Box Discovery Task Wizard - Finish

The **Finish** page of the Box discovery wizard displays a summary of the new Box discovery task.

Database tasks

In order to perform discovery on a database, the Forcepoint DLP server must be able to connect to the data source over a supported interface. Forcepoint 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 2000, 2005, 2008, 2012, and 2016
- Microsoft SQL Server Express (SQL Server Express ODBC driver)
- IBM DB2 11.5.x (ODBC driver 11.x)
- 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

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.

Forcepoint DLP scans the following database field types:

<ul style="list-style-type: none"> ■ CHAR ■ NVARCHAR ■ INTEGER ■ NUMERIC ■ DOUBLE 	<ul style="list-style-type: none"> ■ VARCHAR ■ TINYINT ■ BIGINT ■ REAL ■ TIME 	<ul style="list-style-type: none"> ■ WCHAR ■ SMALLINT ■ DECIMAL ■ FLOAT ■ LONGVARCHAR
--	--	--

Performing database discovery

The wizard for creating database discovery tasks has 7 pages. It opens to the **General** page. See *Database Discovery Task Wizard - General*.

Related tasks

[Database Discovery Task Wizard - General](#) on page 312

Database Discovery Task Wizard - General

Use the **General** page of the database discovery task wizard to give the task a name and select a crawler.

Steps

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for the discovery task.
- 3) Select the **Crawler** to use to perform the scan. Typically, this is the crawler in closest proximity to the database server.
- 4) Click **Next**, then continue with *Database Discovery Task Wizard - Data Source Name*.

Related tasks

[Database Discovery Task Wizard - Data Source Name](#) on page 313

Database Discovery Task Wizard - Data Source Name

Use the **Data Source Name** page of the database discovery task wizard to define how Forcepoint DLP connects to the database.

Steps

- 1)** Select the **Data source name** for the database that you want to scan.
 - If the database does not yet have a DSN, create one, or ask the database administrator to do so. See *Creating a Data Source Name (DSN) in Windows*.
 - For a list of supported databases and field types, see *Connecting to data sources*.
 - Click refresh  to refresh the list.

The DSN must be defined with the same user account as the crawler selected on the previous page of the wizard.
- 2)** Under Database Credentials, do one of the following:
 - Select **Use data source credentials** to use the Forcepoint DLP service account to access the database. (This is the local administrator account defined during Forcepoint DLP installation.) Some databases allow NT authentication to verify the login ID, so be sure the crawler's credential has permission to access the database.
Microsoft SQL Server allows you to use NT authentication or SQL Server authentication. For SQL Server authentication, select **Use the following credentials** instead.
 - Select **Use the following credentials** to enter credentials defined in the database itself, such as the sa account. (Do not enter the network credentials.)
 - a)** Enter the **User name** an account with "read" privileges to the database.
 - b)** Enter the **Password** for this account.
 - c)** Optionally, enter the **Domain** for account. If your database is using Windows authentication, include the domain name.
- 3)** Click **Next**, then continue with *Database Discovery Task Wizard - Scheduler*.

Related concepts

[Connecting to data sources](#) on page 218

Related tasks

[Creating a Data Source Name \(DSN\) in Windows](#) on page 219
[Database Discovery Task Wizard - Scheduler](#) on page 313

Database Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the database discovery task wizard to determine when the discovery task runs.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.
Clear the check box to gain manual control over the task. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.
- 2) Under Run scan, select how often you want to run the scan process: Once, Daily, Weekly, or Continuously. Continuously means that the crawler starts again after every completed scan. (You can set a wait interval between scans.)
 - For Daily or Weekly scans, specify the **Hours to perform the scan** (for example, daily at 2 a.m.). As a best practice, run discovery scans after peak business hours. Select more than one time period to indicate when the scan should continue 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.
 - If Once or Continuously is selected, optionally mark **But not before** to run the scan as soon as possible, but not before a designated time or date. After marking the check box, select a date from the drop-down box and a time from the spinner.
 - If Continuously is selected, select the number of minutes to **Wait...between consecutive scans**. (Each scan starts from the beginning.)
- 3) Click **Next**, then continue with *Database Discovery Task Wizard - Policies*.

Related tasks

[Database Discovery Task Wizard - Policies](#) on page 314

Database Discovery Task Wizard - Policies

Use the **Policies** page of the database discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *Database Discovery Task Wizard - Table Filtering*.

Related tasks

[Database Discovery Task Wizard - Table Filtering](#) on page 314

Database Discovery Task Wizard - Table Filtering

Use the **Table Filtering** page of the database discovery wizard to determine which tables to scan.

Steps

- 1) Use **Include tables** to enter the user names, schemas, or table names to scan, separated by semicolons.
 - The discovery filtering mechanism uses a specific full path search pattern. The 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 an 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.

In order for tables to be detected within the full path, use the structure described above.

 - Database discovery analyzes 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.
- 2) Use **Except** to enter the user names, schemas, or table names not to scan.
- 3) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports](#) on page 330

Database Discovery Task Wizard - Advanced

Use the **Advanced** page of the database discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1) Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on database servers, network adapters, and Forcepoint DLP.
- 2) Under Discovery sample, select one of the following options to indicate whether Forcepoint DLP should scan all records of each table, or just a segment.
 - To scan a specific number of records, select **Segment scan to**. The specified number of records from the table (chosen randomly) will be scanned, and not the entire table.
 - Otherwise, select **Scan all records of each table**. This can affect performance.
- 3) Click **Next**, then continue with *Database Discovery Task Wizard - Finish*.

Related concepts

[Database Discovery Task Wizard - Finish](#) on page 316

Database Discovery Task Wizard - Finish

The **Finish** page of the database discovery task wizard displays a summary of the new database discovery task.

Exchange tasks

The wizard for creating Exchange discovery tasks has 8 pages. It opens to the **General** page.

Steps

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for this discovery task.
- 3) Select the **Crawler** to perform the scan. Typically, this is the crawler in closest proximity to the Exchange server.
- 4) Under Data Storage, indicate where your data is located:
 - Select **Local** to perform discovery on a local or network Exchange server.
 - Select **Online** to perform discovery on data residing in the cloud via Exchange Online for Office 365.
- 5) Click **Next** to continue with one of the following:
 - *Exchange Discovery Task Wizard - Exchange Servers (online)*
 - *Exchange Discovery Task Wizard - Exchange Servers (local)*

Related tasks

[Exchange Discovery Task Wizard - Exchange Servers \(online\)](#) on page 316

[Exchange Discovery Task Wizard - Exchange Servers \(local\)](#) on page 317

Exchange Discovery Task Wizard - Exchange Servers (online)

Use the **Exchange Servers (online)** page of the Exchange discovery task wizard to provide connection information.

Before you begin, define a service account for Exchange discovery scanning. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.

- Organization Management
- View Only Organization Management

See [Scanning Microsoft Office 365 documents with Forcepoint Data SecuritySolutions](#) for more information.

- 1) Select an authentication method:
 - **User name and password:** Enter the **Email address** and **Password** used for logging on to the Exchange Online account.
 - **OAuth 2.0:** Enter **Email address**, **Tenant ID**, **Client ID**, and **Client secret**. For more information about getting your Tenant ID, Client ID, and Client secret, see the [Configuring Azure Active Directory to use OAuth2 authentication](#) Knowledge Base article.
- 2) Click **Test Connection** to test the connection to the Exchange server. If the connection fails, verify the credentials entered in Step 1.
- 3) Click **Next** to continue with *Exchange Discovery Task Wizard - Mailboxes*.

Related tasks

[Exchange Discovery Task Wizard - Mailboxes](#) on page 318

Exchange Discovery Task Wizard - Exchange Servers (local)

Use the **Exchange Servers (local)** page of the Exchange discovery task wizard to provide connection information.

Before you begin, define a service account for Exchange discovery scanning. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.

- Exchange Full Administrator
 - Exchange Administrator
 - Exchange View Only Administrator
- 1) Do one of the following:
 - Select **Auto-discovered** to perform discovery on the Exchange servers that were automatically detected by the Forcepoint DLP system. Click **See list** to view the auto-discovered servers.
 - Select **Custom** to explicitly specify Exchange servers to scan.
Use this option if Forcepoint DLP did not find one or more servers when it tried to calculate which Exchange servers host each mailbox and public folders.
 - 2) Enter the **User name** and **Password** for an administrator account with access to the Exchange servers.
 - 3) Optionally, enter the **Domain** for the administrator account.
 - 4) Select **Connect using secure HTTP** to have Forcepoint DLP to connect to the Exchange server using HTTPS and SSL.
Enter the hostname or IP address of each additional server and click **Add**.
- 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.

- 5) Click **Test Connection** to test the connection to the Exchange server. If the test fails, verify the connection credentials. A public folder mailbox and a public folder on the Exchange server are required for the test connection to pass.
- 6) Click **Next** to continue with *Exchange Discovery Task Wizard - Mailboxes*.

Related tasks

[Exchange Discovery Task Wizard - Mailboxes](#) on page 318

Exchange Discovery Task Wizard - Mailboxes

Use the **Mailboxes** page of the Exchange discovery task wizard to select which mailboxes to scan.

Steps

- 1) Under Mailboxes, click **Edit** to select the mailboxes to scan.



Note

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

- 2) Click **Next** to continue with *Exchange Discovery Task Wizard - Scheduler*.

Related tasks

[Exchange Discovery Task Wizard - Scheduler](#) on page 318

Exchange Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Exchange discovery task wizard to determine when the discovery task runs.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.

Clear the check box to gain manual control over the task. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.

- 2) Under Run scan, select how often you want to run the scan process: Once, Daily, Weekly, or Continuously. Continuously means that the crawler starts again after every completed scan. (You can set a wait interval between scans.)
 - For Daily or Weekly scans, specify the **Hours to perform the scan** (for example, daily at 2 a.m.). As a best practice, run discovery scans after peak business hours. Select more than one time period to indicate when the scan should continue 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.
 - If Once or Continuously is selected, optionally mark **But not before** to run the scan as soon as possible, but not before a designated time or date. After marking the check box, select a date from the drop-down box and a time from the spinner.
 - If Continuously is selected, select the number of minutes to **Wait...between consecutive scans**. (Each scan starts from the beginning.)
- 3) Click **Next**, then continue with *Exchange Discovery Task Wizard - Policies*.

Related tasks

[Exchange Discovery Task Wizard - Policies](#) on page 319

Exchange Discovery Task Wizard - Policies

Use the **Policies** page of the Exchange discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *Exchange Discovery Task Wizard - Filtering*.

Related tasks

[Exchange Discovery Task Wizard - Filtering](#) on page 319

Exchange Discovery Task Wizard - Filtering

Use the **Filtering** page of the Exchange discovery task wizard to determine which items to scan.

Steps

- 1) To filter based on mailbox or folder name, mark **Filter by Mailbox or Folder name**, then indicate what names to include and exclude. Wildcards are allowed.
- 2) To filter by the subject line in items like email, calendar items, notes, contacts, and so on, mark **Filter by Subject**, then indicate what subjects to include and exclude.

- 3) To filter based on item modification date, mark **Filter by Age**, then use the radio buttons to select a time period:
 - Select **Within** to search only for items modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for items modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From...To** to search for items modified between 2 dates, then specify the dates.

- 4) To filter based on item size, mark **Filter by Size**, then select one or both of the following options:
 - Mark **Scan only items larger than**, then select a size from the spinner.
 - Mark **Scan only items smaller than**, then select a size from the spinner.

- 5) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports](#) on page 330

Exchange Discovery Task Wizard - Advanced

Use the **Advanced** page of the Exchange discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1) Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on Exchange servers, network adapters, and Forcepoint DLP.

- 2) Under Full Scan, select one of the following options to indicate when to perform full discovery scans:
 - Select **Only on Discovery Policy update** to perform full discovery only when a discovery policy changes.
 - Select **On Discovery policy update or fingerprinting version updates** to perform full discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** 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.)

- 3) Click **Next**, then continue with *Exchange Discovery Task Wizard - Finish*.

Related concepts

[Exchange Discovery Task Wizard - Finish](#) on page 321

Exchange Discovery Task Wizard - Finish

The **Finish** pages of the Exchange discovery task wizard displays a summary of the new discovery task.

Outlook PST tasks

The wizard for creating discovery tasks for Outlook PST files has 7 pages. It opens to the **General** page.

Steps

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for this discovery task.
- 3) Select the **Crawler** to use to perform the scan. Typically, this is the crawler that is in closest proximity to the PST file server.
- 4) Click **Next**, then continue with *Outlook Discovery Task Wizard - Scanned Folder*.

Related tasks

[Outlook Discovery Task Wizard - Scanned Folder](#) on page 321

Outlook Discovery Task Wizard - Scanned Folder

Use the **Scanned Folder** page of the Outlook discovery task wizard to define the folder to scan, and provide access credentials.

Steps

- 1) Under Network Credentials, enter the **User name** and **Password** for an account with access to the network location of the Outlook folder.
- 2) Optionally, enter the Domain for the access account.
- 3) Under Outlook Folder, enter the **Folder name** (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 the PST files are saved in different subdirectories under the same folder, specify the root folder here.
- 4) Mark **Scan subdirectories** if the PST files are saved in different subdirectories under the same root folder. This prompts Forcepoint DLP to scan the subdirectories, as well as the root.



Note

While Forcepoint DLP can scan PST files that are encrypted, it cannot scan files larger than 1 GB.

- 5) Click **Next**, then continue with *Outlook Discovery Task Wizard - Scheduler*.

Related tasks

[Outlook Discovery Task Wizard - Scheduler](#) on page 322

Outlook Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Outlook discovery task wizard to determine when the scan runs.

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.

To retain manual control over the scan, do not select this option. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.

- 2) Under Run scan, select how often you want to run the scan process: once, daily, weekly, or continuously.
 - 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.
- 3) Click **Next**, then continue with *Outlook Task Discovery Wizard - Policies*.

Related tasks

[Outlook Task Discovery Wizard - Policies](#) on page 322

Outlook Task Discovery Wizard - Policies

Use the **Policies** page of the Outlook discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *Outlook Discovery Task Wizard - Filtering*.

Related tasks

[Outlook Discovery Task Wizard - Filtering](#) on page 323

Outlook Discovery Task Wizard - Filtering

Use the **Filtering** page of the Outlook discovery task wizard to filter what information in Microsoft Outlook PST files is scanned by Forcepoint DLP.

PST files contain all the email users get as well as all their contacts, calendar meetings, tasks, and so on. 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, optionally configure Forcepoint DLP to filter by:

- Mailbox or folder (for example, scan only user1\inbox, user2\outbox)
- Email subjects (for example, include all email with the subject “Project Name” or exclude email messages with the subject “Personal”).
- Time period in which the email messages were sent or received (for example, within the last 2 months)
- Size of the email message (for example, larger than 300 KB).

This page configures which folders and mailboxes Forcepoint DLP scans within the PST file, while the Scanned Folder page specifies where to look for the PST file or files.

Steps

- 1) Mark Filter by Mailbox or Folder name** to have Forcepoint DLP scan by mailbox or folder name, then indicate what names to include and exclude. Wildcards are allowed.
 - List the mailboxes or folders to **Include** in the scan, separated by semicolons. To set Forcepoint DLP to scan all mailboxes or folders, set **Include** to *.
 - List the mailboxes or folders to **Exclude** from the scan, separated by semi-colons.
- 2) Mark Filter by Subject** to scan by subject lines (in, for example, email, calendar items, notes, contacts, and so on), then indicate what subjects to include and exclude.
- 3) Mark Filter by Age** to scan by item age, then:
 - Select **Within** to search only for items modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for items that were modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From... To** - to search for items modified between 2 dates, and specify the dates.
- 4) Mark Filter by Size** to scan by item size, then select one or both of the following:
 - Select **Scan only files larger than** to scan only item *larger* than a certain size, then use the spinner to specify the size.
 - Select **Scan only files smaller than** to scan only item *smaller* than a certain size, then use the spinner to specify the size.



Note

Only the latest version of the item is scanned.

- 5) Click Next, then continue with *Emailing discovery task status reports*.**

Related tasks

[Emailing discovery task status reports](#) on page 330

Outlook Discovery Task Wizard - Advanced

Use the **Advanced** page of the Outlook discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1) Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on PST file servers, network adapters, and Forcepoint DLP.
- 2) Under Full scan schedule, select one of the following options to indicate when to perform full discovery scans:
 - Select **Only on policy update** to perform full discovery only when a discovery policy changes.
 - Select **On policy update or fingerprinting classifier update** to perform full discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** 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.)
- 3) Click **Next**, then continue with *Outlook Discovery Task Wizard - Finish*.

Related concepts

[Outlook Discovery Task Wizard - Finish](#) on page 324

Outlook Discovery Task Wizard - Finish

The **Finish** page of the Outlook discovery wizard displays a summary of the new Outlook discovery task.

Domino tasks

With Forcepoint DLP, 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, Forcepoint DLP performs discovery only on documents.

**Important**

To use this feature, you must first:

- Install IBM Notes *before* installing Forcepoint DLP. Notes must be on the same machine as the crawler.
- Provide your Notes user ID file and password when prompted by the Forcepoint DLP 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. It opens to the **General** page (see *Domino Discovery Task Wizard - General*).

Related tasks

[Domino Discovery Task Wizard - General](#) on page 325

Domino Discovery Task Wizard - General

Use the **General** page of the Domino discovery task wizard to give the task a unique name and a description, and to select the crawler to use to perform the scan.

Steps

- 1) Enter a **Name** for this discovery task.
- 2) Enter a **Description** for the discovery task.
- 3) Select the **Crawler** to use to perform the scan. Typically, this is the crawler that is located in closest proximity to the Domino server.
- 4) Click **Next**, then continue with *Domino Discovery Task Wizard - Server*.

Related tasks

[Domino Discovery Task Wizard - Server](#) on page 325

Domino Discovery Task Wizard - Server

Use the Server page of the Domino task wizard to select the Domino server to scan, and to provide connection details.

Steps

- 1) Enter the hostname of the **Domino server to scan**—for example, **gumby**. Do not include the HTTP prefix or leading slashes.

- 2) Enter the **User name** of the Domino account used when Forcepoint DLP was installed on the Notes machine.



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 Forcepoint DLP installer on the Notes machine, select the **Modify** option, and upload a different user ID file.

- 3) Click **Next**. The crawler tries to connect to the Domino server using credentials for the user indicated. When the connection is successful, continue with *Domino Discovery Task Wizard - Scanned Documents*.

Related tasks

[Domino Discovery Task Wizard - Scanned Documents](#) on page 326

Domino Discovery Task Wizard - Scanned Documents

Use the **Scanned Documents** page of the Domino discovery task wizard to determine which documents are scanned during the discovery process.

Steps

- 1) Use **Document names are stored in the following field(s)** to enter the name of the field or fields that hold document names. If there are multiple field names, separate them with commas. For example: subject, docname, filename.
By default, the “Subject” field is scanned.
- 2) Under Documents and folders to scan, identify the documents and folders included in and excluded from the scan. 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.
 - 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. Alternatively, 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.
- 3) Under Fields to scan, indicate whether to scan the document body, attachments, or all fields except a selected list.
 - Use **Scan document body** to enter the name of the field or fields that hold documents' body text. By default, it is “Body.” If there are multiple field names, separate them with commas. For example: body, content, main.
 - When **Scan all other fields** is selected, all fields *except* body, subject, and attachment are scanned.

- 4) Click **Next**, then continue with *Domino Discovery Task Wizard - Scheduler*.

Related tasks

[Domino Discovery Task Wizard - Scheduler](#) on page 327

Domino Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Domino discovery task wizard to specify when the scan is run:

Steps

- 1) Mark **Enabled** to enable the scheduler for the current task.

To keep manual control of the task, clear the check box. When the scheduler is disabled, start and stop tasks using the scan controls on the toolbar.

- 2) Under Run scan, select how often to run the scan process: once, daily, weekly, or continuously. Continuously means that the crawler restarts after every scan, operating continuously.

- If you choose Daily or Weekly, specify when to run the scan (for example, daily at 2 a.m.). As a best practice 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.
- If you select Once or Continuously, optionally select **But not before** 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.
- If you select Continuously, use the **Wait...minutes between consecutive scans** to select the number of minutes to pause between scans. (Each scan starts from the beginning.)

- 3) Click **Next**, then continue with *Domino Discovery Task Wizard - Policies*.

Related tasks

[Domino Discovery Task Wizard - Policies](#) on page 327

Domino Discovery Task Wizard - Policies

Use the **Policies** page of the Domino discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:

- Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
- Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.

- 2) Click **Next**, then continue with *Domino Discovery Task Wizard - Document Filtering*.

Related tasks

[Domino Discovery Task Wizard - Document Filtering](#) on page 328

Domino Discovery Task Wizard - Document Filtering

Use the **Document Filtering** tab of the Domino discovery task wizard to determine which documents are scanned.

Steps

- 1) Select **Filter by Document Name** to prompt the crawler to look for specific document names.
 - List the exact document names for which to search, separated by semicolons. You can use the "*" or "?" wildcards. For example, "top_secret*".
The crawler searches for file names and their complete paths.
 - Under Except, list the exact document names to exclude from the scan, separated by semicolons. Wildcards are permitted.

- 2) To only scan documents modified within a specified period, mark **Filter by Age**, then select the option that best describes the time period (within 24 months, by default).
The age of a document is the latest date of its body and all attachments.

- 3) Mark **Filter by Size** to use size as a determining factor in what to scan, then select one or more of the following:
 - Select **Scan only files larger than**, then select a minimum size from the spinner. By default, all files larger than 1 KB are scanned.
 - Select **Scan only items smaller than**, then select a maximum size. 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.

- 4) Click **Next**, then continue with *Domino Discovery Task Wizard - Attachment Filtering*.

Related tasks

[Domino Discovery Task Wizard - Attachment Filtering](#) on page 328

Domino Discovery Task Wizard - Attachment Filtering

Use the **Attachment Filtering** page of the Domino discovery task wizard to determine which attachments are scanned.

Steps

- 1) Under Filter by Type, specify which types of attached files to include in the scan or exclude from scanning.
 - Select **Include file types** to look for specific attachments, then list the types of files to be fingerprinted, separated by semicolons.
The “*” and “?” wildcards are supported. For example, “*.doc; *.xls; *.ppt; *.pdf”.
 - Select **Except** to list the file types to exclude from the scan, separated by semicolons. Wildcards are permitted.

- 2) Use the Filter by Size to determine whether or not attachment files are scanned based on their size.
 - Mark **Scan only files larger than**, then select a minimum file size from the spinner. By default, all files larger than 1 KB are scanned.
 - Mark **Scan only files smaller than**, then select a maximum 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.

- 3) Click **Next**, then continue with *Emailing discovery task status reports*.

Related tasks

[Emailing discovery task status reports](#) on page 330

Domino Discovery Task Wizard - Advanced

Use the **Advanced** page of the Domino discovery task wizard to configure bandwidth limits and full scan options.

Steps

- 1) Select an option for controlling bandwidth used for the discovery process:
 - Select **No limit** to avoid limiting the bandwidth used for discovery.
 - Select **An average of** to limit the bandwidth used for discovery, then select the average (1-9999 Mbps) to set as the limit.

This reduces strain on Domino servers, network adapters, and Forcepoint DLP.

- 2) Under Full scan schedule, select one of the following options to indicate when to perform full discovery scans:
 - Select **Only on policy update** to perform full discovery only when a discovery policy changes.
 - Select **On policy update or fingerprinting classifier update** to perform full discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** 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.)

- 3) Click **Next**, then continue with *Domino Discovery Task Wizard - Finish*.

Related concepts

[Domino Discovery Task Wizard - Finish](#) on page 330

Domino Discovery Task Wizard - Finish

The **Finish** page of the Domino discovery task wizard displays a summary of the new Domino discovery task.

Emailing discovery task status reports

Use the Email Report page of the discovery task wizard to have a status report on the scanned files sent to an administrator or group alias via email when the discovery task is completed.

Steps

- 1) Select **Email discovery report** to enable the email option.
- 2) Enter a **Sender name** for the report. This is the name that appears in the “From” field of the email message.
- 3) Enter a **Sender email address**.
- 4) Verify the IP address and port of the outgoing mail server, or see the indication that Exchange Online is selected.
These settings are configured on the Settings > General > Mail Servers page, under Outgoing Mail Server.
- 5) Enter a **Subject** for the email message. Click the arrow next to the Subject field to include supported variables (like %Task Name%) in the email subject.
- 6) Edit the **Message body**. Default text is provided.
Click the arrow next to the Message body field to include supported variables (like %Task End Time%) in the email message body.
- 7) In the Recipients field, click **Edit** to select one or more recipients for the emailed report.
Use the selection window to identify Administrators, Directory entries, or Custom users as message recipients, then click **OK**.
- 8) To manually enter the email addresses of additional recipients, select **Additional email addresses**, then use the field provided to enter addresses in a comma- separated list.

- 9) Click **Next**, then continue to the Advanced page of the task wizard:

- [File System Discovery Task Wizard - Advanced](#)
- [SharePoint Discovery Task Wizard - Advanced](#)
- [Box Discovery Task Wizard - Advanced](#)
- [Database Discovery Task Wizard - Advanced](#)
- [Exchange Discovery Task Wizard - Advanced](#)
- [Outlook Discovery Task Wizard - Advanced](#)
- [Domino Discovery Task Wizard - Advanced](#)
- [Endpoint Discovery Task Wizard - Advanced](#)

Related tasks

- [File System Discovery Task Wizard - Advanced](#) on page 302
- [SharePoint Discovery Task Wizard - Advanced](#) on page 307
- [Box Discovery Task Wizard - Advanced](#) on page 311
- [Database Discovery Task Wizard - Advanced](#) on page 315
- [Exchange Discovery Task Wizard - Advanced](#) on page 320
- [Outlook Discovery Task Wizard - Advanced](#) on page 324
- [Domino Discovery Task Wizard - Advanced](#) on page 329
- [Endpoint Discovery Task Wizard - Advanced](#) on page 336

Configuring cloud discovery scans

Use the **Main > Policy Management > Discovery Policies > Cloud Discovery Scans** page in the Data Security module of the Security Manager to discover and remediate sensitive data at rest stored in authorized cloud applications.

Initially, the Cloud Discovery Scans page does not list any scans.

To create a new scan, click **New** in the toolbar at the top of the content page. A Cloud Discovery Scan Properties page opens. See *Adding or editing a cloud discovery scan* for information on how to add a new scan or to edit the existing scan.

If you receive an error message, go to the **Settings > General > Services > Cloud Applications** page in the Data Security module of the Security Manager to verify one of the following:

- DLP Cloud Applications is connected. See *Configuring DLP Cloud Applications*.
- Cloud applications are defined. See the *Forcepoint CASB Administration Guide*, available on the Forcepoint CASB management portal.
- At least one discovery policy is defined and enabled. See *Creating a discovery policy*.

After a new scan is created and saved, it appears in the list of cloud discovery scans. The Cloud Discovery Scans list displays the following properties:

- Scan Name - A name that you entered when the scan was created.
- Description - A description that you entered when the scan was created or modified.
- Cloud Application - The cloud application with which this scan is associated. Each cloud application can be assigned to only one scan. A Cloud Application name can be edited by a CASB administrator.

**Note**

A **cloud application** in Forcepoint DLP is referred to as **asset** in Forcepoint CASB.

If a cloud application that is used in a scan was deleted in the CASB portal, the application name and type are **N/A** and the scan status becomes **Inactive**.

- Type - A cloud application name (e.g., Office 365). The type cannot be changed. The “Office 365” type may include several Office 365 cloud applications, each with its own name and configuration.
- Enabled - Indicates whether the scan is enabled or disabled. Enable or disable the scan from the Cloud Discovery Scan Properties page.
- Scan Status - The status of the scan in Forcepoint DLP:
 - Active - Indicates that the scan is running
 - Inactive - Indicates one of the following:
 - The scan was deleted in the CASB portal.
 - The Data at Rest option is not selected in the CASB portal.
 - The default DLP policy was removed.
 - Deployment needed - Indicates that not all changes were deployed. Click **Deploy** to deploy scan changes.
- Enforced Policies - All discovery policies to be enforced on the files stored in the cloud applications or selected policies
-

To reset the discovery scan cache, click **Reset Scan**.

**Important**

You need to deploy all changes you made in the system before you can run a scan, even if the changes are not related to a selected scan.

Clicking **Reset Scan** forces a discovery scan cache reset. All files at rest are queued and processed for scanning with the latest policy configuration, including any files that were previously scanned.

Using the **Reset Scan** button can significantly affect file processing time. **Use this action only when significant changes are made to policies or when testing policies with a small data set.** Avoid using this button after deployments when possible.

To delete a scan, select the desired scan and click **Delete**.

Use the **Main > Logs > Audit Log** page in the Data Security module of the Security Manager to see administrator actions related to cloud discovery scans that were performed in the system.

Use the **Main > Logs > System Log** page in the Data Security module of the Security Manager to see system alerts, warnings, errors, or information that relate to a CASB connection or to cloud discovery scans.

Related tasks

[Adding or editing a cloud discovery scan](#) on page 333

[Configuring DLP Cloud Applications](#) on page 371

[Creating a discovery policy](#) on page 278

Adding or editing a cloud discovery scan

Use the **Main > Policy Management > Discovery Policies > Cloud Discovery Scans > Cloud Discovery Scan Properties** page in the Data Security module of the Forcepoint Security Manager to create or edit a cloud discovery scan.

To access the Cloud Discovery Scan Properties page, do one of the following:

- Click **New** in the toolbar at the top of the content pane on the Cloud Discovery Scans page to add a new scan.
- Click an existing scan name in the table on the Cloud Discovery Scans page to update an existing scan.

A Cloud Discovery Scan Properties page appears. To create or edit a scan:

- 1) Enter or update a **Scan name** and **Description** for the scan.
- 2) Mark **Enable scan** to enable the cloud discovery scan.
- 3) Choose a cloud application from the drop-down list for the new scan.

The Cloud Application field lists all unassigned cloud applications created from the Cloud Applications page (for example, Dropbox-Test Instance).

Only applications that support data at rest are shown in the drop-down list. **Data at rest** is enabled for all supported assets in the CASB portal. To disable **Data at rest**, go to the CASB portal and modify the relevant asset. Each cloud application can be assigned to only one scan.

Note that you cannot change the Cloud application name when you edit the scan.



Note

A **cloud application** in Forcepoint DLP is referred to as **asset** in Forcepoint CASB.

- 4) Use the **Discovery Policies** section to determine which policies to apply during the scan.
Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 5) To save the changes and return to the Cloud Discovery Scans page, click **OK**.
- 6) To deploy all the configured changes, click **Deploy**.

Scheduling endpoint discovery tasks

Use the **Main > Policy Management > Discovery Policies > Endpoint Discovery Tasks** page in the Data Security module of the Security Manager to configure discovery on endpoint machines. The page displays all existing endpoint discovery tasks.

To create a new endpoint task, click **New**. A wizard appears.

The wizard for creating endpoint discovery tasks has 7 pages. It opens to the **General** page.

On this page:

Steps

- 1) Enter a **Name** for this endpoint discovery task.
- 2) Mark **Enabled** to enable the endpoint discovery task.
- 3) Enter a **Description** for the task.
- 4) Click **Next**, then continue with *Endpoint Discovery Task Wizard - Endpoints*.

Related tasks

[Endpoint Discovery Task Wizard - Endpoints](#) on page 334

Endpoint Discovery Task Wizard - Endpoints

Steps

- 1) By default, discovery will run on all endpoint machines. Click **Edit** to select the endpoint to scan.
 - Linux network mounts, files symbolic links, folders symbolic links, classifiers, and filters are not scanned.
 - 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.
- 2) Click **Next**, then continue with *Endpoint Discovery Task Wizard - Scheduler*.

Related tasks

[Endpoint Discovery Task Wizard - Scheduler](#) on page 334

Endpoint Discovery Task Wizard - Scheduler

Use the Scheduler page of the endpoint discovery task wizard to determine how often the discovery task is run.

Steps

- 1) Use the **Run scan** option to select how often you want to run the scan process: daily or weekly.
- 2) Specify the hours in which you want to run the scan (for example, daily at 2 a.m.). As a best practice, run discovery scans 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.

- 3) Select **Scan only while computer is idle** 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.
- 4) Select **Pause scanning while computer is running on batteries** to avoid running discovery if the endpoint machine switches to battery mode.
- 5) Click **Next**, then continue with *Endpoint Discovery Task Wizard - Policies*.

Related tasks

[Endpoint Discovery Task Wizard - Policies](#) on page 335

Endpoint Discovery Task Wizard - Policies

Use the **Policies** page of the endpoint discovery task wizard to determine which policies to apply during the scan.

Steps

- 1) Do one of the following:
 - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
 - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.
- 2) Click **Next**, then continue with *Endpoint Discovery Task Wizard - File Filtering*.

Related tasks

[Endpoint Discovery Task Wizard - File Filtering](#) on page 335

Endpoint Discovery Task Wizard - File Filtering

Use the File Filtering page of the endpoint discovery task wizard to specify which files to include in the scan.

Steps

- 1) Mark **Filter by Type** to filter the files to scan by file type.
- 2) Use **Include file types** to list the types of files to be scanned, separated by semi- colons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”
 - Click **File Types** to select the file types to include by extension. You can add or edit file types in the resulting box if necessary.
 - To set Forcepoint DLP to scan all files, set this option to *.

- 3) Use **Except** to list the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted.
- 4) Mark **Filter by Age** to filter the files to scan by file age.
- 5) Under Scan only files that were modified:
 - Select **Within** to search only for files that were modified within a certain period, then indicate the period (in months) using the spinner.
 - Select **More than** to search only for files that were modified more than a certain number of months ago, then specify the number using the spinner.
 - Select **From...To** to search for files modified between 2 dates, and specify the dates.
- 6) Mark **Filter by Size** to filter the files to scan by file size, then select one or both of the following:
 - Select **Scan only files larger than** to set a minimum file size, then use the spinner to specify the size.
 - Select **Scan only files smaller than** to set a maximum file size, then use the spinner to specify the size.
- 7) Click **Next**, then continue with *Endpoint Discovery Task Wizard - Advanced*.

Related tasks

[Endpoint Discovery Task Wizard - Advanced](#) on page 336

Endpoint Discovery Task Wizard - Advanced

Use the Advanced page of the endpoint discovery task wizard to set a schedule for running full scans, and to specify whether or not the discovery process alters file timestamps.

Steps

- 1) Under Full Scan Schedule, select one of the following options to indicate when to perform full discovery scans:
 - Select **Only on policy update** to perform discovery only when a discovery policy changes.
 - Select **On policy update or fingerprinting classifier update** to perform discovery when a discovery policy or a fingerprinting version changes.
 - Select **Always** to perform discovery on the scheduled time no matter what has changed.
- 2) Under File Access Timestamp, select **Preserve original access time** to avoid having file access timestamps updated when files are scanned by Forcepoint DLP.

Then this option is selected, the operating system controls the “Last Accessed” timestamp of scanned files.



Note

To preserve access time, Forcepoint DLP must have read- write privileges for all hosts where discovery is being performed.

- 3) Click **Next**, then continue with *Endpoint Discovery Task Wizard - Finish*.

Related concepts

[Endpoint Discovery Task Wizard - Finish](#) on page 337

Endpoint Discovery Task Wizard - Finish

The Finish page of the endpoint discovery task wizard displays a summary of the new endpoint discovery task.

Chapter 16

Viewing Forcepoint DLP Logs

Contents

- [Filtering log data](#) on page 339
- [Printing and exporting logs](#) on page 340
- [The Forcepoint DLP traffic log](#) on page 340
- [The Forcepoint DLP system log](#) on page 343
- [The Forcepoint DLP audit log](#) on page 343

Forcepoint DLP traffic and events are recorded in a number of logs that can be viewed from the Data Security module of the Forcepoint Security Manager. Use the logs to assess system performance, track events, and audit administrator actions in the Security Manager.

To access the logs, go to **Main > Logs**, then select an entry in the menu:

- [*The Forcepoint DLP traffic log*](#)
- [*The Forcepoint DLP system log*](#)
- [*The Forcepoint DLP audit log*](#)

Related concepts

- [The Forcepoint DLP traffic log](#) on page 340
- [The Forcepoint DLP system log](#) on page 343
- [The Forcepoint DLP audit log](#) on page 343

Filtering log data

Filter log data to see only entries that meet specific criteria. For example, filter the audit log to review the actions of a particular administrator on a certain date.

Data on the log pages can be sorted, grouped, and filtered by column name. For example, the traffic log can be sorted by incidents, action taken, or event time.

To sort or filter the table items on a status or log screen, click the down arrow by any column name and choose an option:

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

Field	Description
Clear filter	Select this option to clear the filter and display all tasks.

To view the current filters in use, click the information ("i") icon next to **Column Filtering Activated**.

When a filter is applied to a column, a funnel icon  appears next to the column name.

To clear the filter from a column, click the down arrow by any column name and select **Clear filter**. The toolbar at the top of the content pane also offers a **Filter** button that can be used to clear a single filter or all filters.

If there are too many items to fit on the screen, use the Next, Previous, First, and Last buttons to browse the list.

Printing and exporting logs

Each log offers one or more options for printing or exporting the log data. The icons used to print or export the data appear on the right-hand side of the toolbar at the top of the content pane. Which option or options appear depends on which log is selected.

Mouse over the icons to see a tool tip explaining its function. To print logs, click **Print Preview**.

To export logs to a PDF or CSV file, click **Export to PDF** or **Export to CSV**. The CSV contains all the rows in the main table, without paging. If the list is filtered, only the filtered records are exported.

The Forcepoint DLP traffic log

Use the **Main > Logs > Traffic Log** page in the Data Security module of the Security Manager to see details of the traffic monitored over specific periods, as well as the action taken.

For the endpoint channel, the log displays only traffic that breaches policy. The list includes:

- Event ID
- Event Time
- Channel
- Action Taken

To customize the information shown in each column, click **Table Properties** () just above the right edge of the table. See *Changing table properties* section, for more information.

The **Updated to** field shows when the traffic log was last updated. To see the latest data, click **Update Now** in the toolbar at the top of the content pane.

If one or more modules fails to provide updated traffic information, an **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, as well as reasons for the update failure.

Related concepts

[Changing table properties](#) on page 341

Changing table properties

After clicking Table Properties, select the properties to display in the table and specify the column width for each property.

Column	Description
Action Taken	The online action that was performed (allow or block).
Analysis Canceled	Displays whether analysis was canceled.
Analysis Failed	Displays whether analysis failure occurred.
Analyzed By	Displays the name of the policy engine that analyzed the event.
Channel	Channel on which the event was intercepted, for example SMTP, HTTP, or FTP.
Classifier Time	Time spent analyzing all classifiers, in milliseconds. Includes the time spent processing dictionaries, scripts, key phrases, patterns, and fingerprints.
Database Fingerprint Latency	Time in milliseconds that the transaction spent in the policy engine waiting for structured fingerprint analysis.
Database Fingerprint Search Time	Time in milliseconds spent on searching for structured fingerprint data in this transaction's content.
Destination	The destination of the event, for example an IP address or an email address.
Details	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.
Detected By	Displays the protector or agent that caught the event.
Dictionary Latency	Time in milliseconds that the event spent in the policy engine waiting for dictionary analysis.
Dictionary Search Time	Time in milliseconds spent on searching for dictionary phrases in this event's content.
Event ID	Unique traffic log event number.
Event Time	Date and time the event was detected.
Extraction Time	Time spent extracting text from the event, in milliseconds.
File Fingerprint Latency	Time in milliseconds that the event spent in the policy engine waiting for unstructured fingerprint analysis.
File Fingerprint Search Time	Time in milliseconds spent on searching for unstructured fingerprint data in this event's content.

Column	Description
Host Name Resolution Time	Time in milliseconds spent on performing external resolution from IP to hostname on this event's source or destination.
Incident	Displays a check mark if the event was determined to be an incident (a policy violation).
Incident Creation Time	Time spent creating an incident when a breach is detected, in milliseconds. If no incident was created, this field is "0".
Key Phrase Latency	Time in milliseconds that the event spent in the policy engine waiting for key phrase analysis.
Key Phrase Search Time	Time in milliseconds spent on searching for key phrases in this event's content.
Latency	Time the event spent in the policy engine waiting for analysis, in milliseconds—in other words, Processing Time + Incident Creation Time + Queue Time.
Regular Expression Latency	Time in milliseconds that the event spent in the policy engine waiting for regular expression analysis.
Regular Expression Processing Time	Time in milliseconds spent on all regular expression calculations performed on this event's content.
Resolution Time	Time spent resolving user names for all sources and destinations in the event, in milliseconds.
Script Search Time	Time in milliseconds spent on all script classifications performed on this event's content.
Search Time	Time it took to search the event for breaches, in milliseconds—in other words, Classifier Time + Extraction Time + Resolution Time.
Size	The size of the event content, for example a file or an email message.
Source	The source from which the event originated. This could be an email address or IP address or other source.
Text Extraction Latency	Time in milliseconds that the event spent in the policy engine waiting for text extraction.
Timeout	Displays whether analysis was stopped due to a timeout restriction.
Total Queue Time	Total amount of idle time, in milliseconds, that the event spent in internal queues.
URL Categorization Time	Time in milliseconds spent on categorizing the destination URL of this event.
User Name Resolution Time	Time in milliseconds spent on performing external resolution from IP to user name on this event's source.
User Resolution Latency	Time in milliseconds that the event spent in the policy engine waiting for user name resolution.

The Forcepoint DLP system log

Use the **Main > Logs > System Log** page in the Data Security module of the Security Manager to see system actions sent from different Forcepoint components, such as Forcepoint DLP servers, protectors, gateways, and policy engines. Examine the details of each action, including the date and time it occurred and the component that reported the action.

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.

System log records are kept for 60 days.

Column	Description
Type	Defines whether the action is an error, or is reported for informational purposes.
Status	Displays either New or Confirmed. Once you view a new action, you can mark it as confirmed to show you've reviewed it. To mark a new action as confirmed, select the action and click Mark as Confirmed . To revert a confirmed action to new, select the event and click Mark as New .
Message	This column may contain variables that are filled by the system, for example a full folder path or a component name. If there are multiple identical messages in a short time interval, a combined message is displayed. The Forcepoint 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.)."
Date & Time	Date and time the action occurred.
Local Date & Time	Date and time on the component where the action occurred.
Topic	<ul style="list-style-type: none"> ■ 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 Forcepoint DLP Server - USA.
Component	Displays the internal component name, for example Policy Engine or Endpoint Server.

The Forcepoint DLP audit log

Use the **Main > Logs > Audit Log** page in the Data Security module of the Security Manager to review actions performed by administrators in the system. For example, the audit log 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 (Configure auditing for viewing incident details on the **Settings > Authorization > Administrators** page. Select **Audit incident detail views**)

The audit log can be used to investigate unauthorized or irregular changes to the system that might jeopardize employee privacy or breach an IT security compliance policy.

By default, the displayed actions are sorted by date and time. If a filter is used, the number of displayed actions is shown at the top of the list.

Column	Description
Action ID	ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the Find Action ID field and clicking Find .
Date & Time	Date and time the action occurred.
Administrator	Name and user name of the administrator that initiated the action in the Forcepoint Security Manager.
Access Role	Role of the administrator.

Column	Description
Topic	<p>You can filter the Audit Log by topic types.</p> <ul style="list-style-type: none"> ■ Administration - 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. ■ Log on/Log out - Displays log on and log out actions so you know which administrators were active during the designated period. ■ Status - Displays actions performed on status reports and logs, such as deleting an entry or creating an audit record. ■ Policy management - Displays actions performed on policies, such as updating predefined policies, editing quick policies, or creating a new policy. ■ Reporting - Displays actions performed on reports during the designated period, such as editing or creating a new report. ■ Incident management - Displays actions performed on incidents, such as deleting incidents. ■ Archiving - Displays actions performed on incident archives, such as deleting or restoring an archive. ■ System modules - Displays actions performed on system modules, such as editing a configuration or adding a module.

Column	Description
Action Performed	Description of the action performed by the administrator—for example, “exported DLP incident to PDF file”.
Details	Additional information about the action. For example, for an action such as adding a policy, rule, or exception, this shows the policy, rule, or exception name. For actions such as previewing or exporting a report, it includes the report name.
Modified Item	Identifies the object that was changed, added, or deleted. For actions performed on incidents (e.g., viewing incident details), it includes the incident ID. For report generation, it includes a task number. Click the link to view additional details.

Retention of audit logs

Audit log records are kept indefinitely by default. However, an automatic service can be configured in the SQL Server database to delete old audit log records. When enabled, cleanup occurs daily at 6:00am in which logs older than a configured number of days are deleted.

Use the following steps to configure automatic cleanup in the SQL Server database.

1)

```
INSERT INTO PA_CONFIG_PROPERTIES (ID, NAME, GROUP_NAME, VALUE, GROUP_ORDER, OPTLOCK)
SELECT TOP 1 dbo.PA_CONFIG_PROPERTIES_NEXVAL(), 'DELETE_AUDIT_RECORDS_OLDER_THAN_DAYS',
'AUDIT_CONFIGURATION', 0, 0, 0 FROM sys.objects T1 WHERE NOT EXISTS (SELECT 1 FROM
PA_CONFIG_PROPERTIES WHERE (NAME = 'DELETE_AUDIT_RECORDS_OLDER_THAN_DAYS'));
```

2)

```
Update PA_CONFIG_PROPERTIES set value = <number of days> where NAME =
'DELETE_AUDIT_RECORDS_OLDER_THAN_DAYS';
```

Replace **<number of days>** with the age, in days, after which old audit log records should be deleted. Cleanup does not occur if this property is missing or its value is less than one.

3) Restart the “Websense Data Security Manager” service on the management server.

Chapter 17

General System Settings

Contents

- Setting reporting preferences on page 348
- Backing up the system on page 351
- Exporting incidents to a file on page 354
- Configuring endpoint settings on page 357
- Remediation on page 361
- Mail servers on page 363
- Alerts on page 365
- Archive storage on page 366
- Services on page 368
- Analytics on page 379
- User directory settings on page 380
- Archiving incident partitions on page 387
- Updating predefined policies and classifiers on page 392
- Entering subscription settings on page 395

Configure Forcepoint DLP systems settings on the **Settings > General** pages in the Data Security module of the Forcepoint Security Manager.

- Set preferences for reports (see *Setting reporting preferences* section).
- Back up and restore the Forcepoint DLP (see *Backing up the system* section).
- Define parameters for exporting incidents to a file (see *Exporting incidents to a file* section).*
- Configure endpoint hosts (see *Configuring endpoint settings* section).*
- Configure mobile email devices (included with Forcepoint Email Security). See *Remediation* section.
- Configure remediation (see *Remediation* section).*
- Configure incoming and outgoing mail servers (see *Mail servers* section).
- Set up alerting (see *Alerts* section).
- Configure archive storage (see *Archive storage* section).
- Configure Data Protection Service, Cloud Applications, URL Categories, Linking service, MIP Decryption, File Labeling, and Risk-Adaptive Protection (see *Services* section).
- Configure high-risk resources for incident risk ranking (see *Analytics* section).
- Configure user directory settings (see *User directory settings* section).
- Archive incident partitions (see *Archiving incident partitions* section).
- Update predefined policies and classifiers (see *Updating predefined policies and classifiers* section).
- Enter subscription settings (*Entering subscription settings* section).

*These options are not included in the Forcepoint Web Security or Forcepoint Email Security DLP Module.

Related concepts

[Setting reporting preferences](#) on page 348
[Backing up the system](#) on page 351
[Services](#) on page 368
[User directory settings](#) on page 380
[Archiving incident partitions](#) on page 387
[Updating predefined policies and classifiers](#) on page 392
[Archive storage](#) on page 366

Related tasks

[Exporting incidents to a file](#) on page 354
[Configuring endpoint settings](#) on page 357
[Remediation](#) on page 361
[Mail servers](#) on page 363
[Alerts](#) on page 365
[Analytics](#) on page 379

Related reference

[Entering subscription settings](#) on page 395

Setting reporting preferences

Use the **Settings > General > Reporting** page in the Data Security module of the Forcepoint Security Manager to configure preferences for Forcepoint DLP reports. For example:

- For data loss prevention incidents, define attachment size and forensics settings.
- Define general settings, like filtering and printing, that apply to all types of incidents.

To set preferences for incidents and reports, complete the fields on each tab of the Reporting page. See:

- [*Setting general reporting preferences*](#)
- [*Setting preferences for data loss prevention reports*](#)
- [*Setting preferences for Incident Risk Ranking reports*](#)
- [*Setting preferences for mobile incident reports*](#)

Related concepts

[Viewing Incidents and Reports](#) on page 39

Related tasks

[Setting general reporting preferences](#) on page 349
[Setting preferences for data loss prevention reports](#) on page 350
[Setting preferences for mobile incident reports](#) on page 350
[Setting preferences for Incident Risk Ranking reports](#) on page 350

Setting general reporting preferences

Use the **General** tab of the **Settings > General > Reporting** page in the Data Security module of the Security Manager to define general settings for security incidents and reports:

Steps

- 1) Under Attachments, select a **Maximum number of attachments per message** (1-40) to set the highest number of reports that can be appended to an email notification message (40, by default).
- 2) Set the **Maximum size of attachments** (1-20 MB) included with an email notification message (5 MB, by default).
- 3) Mark **Zip incident and discovery reports** to have reports compressed in a zip archive to reduce the size of the notification message.
- 4) Under Printing and Exporting Incidents, set the maximum **Number of incidents** (50-500) to include when the Print Preview or Export to PDF option is selected (400, by default).
If a list of Forcepoint DLP incidents or reports is very long, this allows it to be broken into manageable groups.
 - When the total number of items to export is larger than the number set here, administrators can select from a range of pages. For example, if the number of incidents to include is set to 200, and there are 700 incidents, administrators are asked whether to export 1-200, 201-400, 401-600, or 601-700 incidents.
 - To export all incidents, enter an email address to which to send a PDF file.

- 5) Select one of the following options to determine whether a custom logo is displayed in reports:
 - Mark **No custom logo** to display only the Forcepoint DLP logo on the first page of the report.
 - To add a custom logo to the top of the first page in the report, mark **Add the following logo**, 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.

As a best practice, upload an image that is 200x50 pixels. The system reduces larger images to this size, so the resolution may be affected.

The custom logo appears on the top right of the report, while the Forcepoint DLP logo appears on the top left.

- 6) Select one of the following options to determine whether to add a disclaimer to the bottom few the report:
 - Select **No disclaimer** (default) to show no disclaimer at the bottom of the report.
 - To include a disclaimer, select **Add the following disclaimer**, 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.
- 7) Under Forensics, select **Secure forensics with plain text** to have forensics data appear in the report in plain text, rather than potentially malicious HTML.
- 8) Select **Delete forensics for closed incidents** to have forensics data deleted when an incident's status is changed to "Closed." This reduces the size of your forensics repository.
Forensics data is not deleted for incidents closed before this option is selected.

- 9) Click **OK** to save the changes.

Setting preferences for data loss prevention reports

Use the **Data Loss Prevention** tab of the **Settings > General > Reporting** page in the Data Security module of the Forcepoint Security Manager to define settings for reviewing data loss prevention incidents:

Steps

- 1) Select the **Arrange the following fields...** option to specify optional fields to display on reporting pages. Type field names, separated by commas, in the order you want to view them. For example:
`to, subject, body`
- 2) To include non-formatted data on the reporting page, mark **View non-formatted data**. Examples include: to, subject, subj, body, msgbody, plainmsg, cc, bcc, from, login.
- 3) Click **OK** to save the changes.

Setting preferences for Incident Risk Ranking reports

Use the **Incident Risk Ranking** tab of the **Settings > General > Reporting** page in the Data Security module of the Forcepoint Security Manager to define settings for Incident Risk Ranking reports:

Steps

- 1) Under Risk Threshold, select a range of risk levels to display by default on the Dashboard and in the Incident Risk Ranking report.
For example, to see only the most severe risks, select 8.0-10. Cases assigned a risk score in this range will be shown. To show all risk cases, select 0-10. This is the default.
- 2) Under Work Week, indicate whether the organization's normal work week is Monday - Friday (default) or Sunday - Thursday.
This shows on the Incident Risk Ranking report date filter.
- 3) Click **OK** to save the changes.

Setting preferences for mobile incident reports

Use the **Mobile** tab of the **Settings > General > Reporting** page in the Data Security module of the Forcepoint Security Manager to define settings for mobile incidents:

Steps

- 1) Use the **Keep mobile incidents...** field to set the number of days to keep incidents pertaining to mobile devices.
 - Set a number of days from 1-999.
 - The default is 90 days.

Incidents older than this number are deleted from the incident database and no longer available for reporting.
- 2) Click **OK** to save the changes.

Backing up the system

Use the **Settings > General > Reporting** page in the Data Security module of the Forcepoint Security Manager to configure Forcepoint DLP system backups.

Be sure to back up your Forcepoint DLP system periodically to safeguard your policies, forensics, configuration data, fingerprints, encryption keys, and more. (See *Backup folder contents*, for a complete list of the data that is saved.)

To configure backup settings:

- 1) Enter a **Path** for storing the backup files.
 - If you enter a local path, it is local to the 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.
- 2) If the Forcepoint DLP administrator account doesn't have write privileges for the specified path, provide credentials for an account that does have the appropriate permissions.

Field	Description
Domain	Enter the domain for the account.
User name	Enter the user name for an administrator account with access to this path.
Password	Enter the account password. It must: <ul style="list-style-type: none"> ■ Be at least 8 characters ■ Contain upper case characters ■ Contain lower case characters ■ Contain numbers ■ Contain non-alphanumeric characters
Confirm password	Type the password a second time.

- 3) Specify how many backup files to keep (5, by default).
 - Every time you backup the system, the system uses another backup folder.
 - You can have between 1 and 60 backup folders.

- When the maximum is reached, the system overwrites the oldest folder with the new data.
- 4) Indicate whether or not to **Include forensics** (from the incident database) in the backup.
The incident database can be quite large, and backing it up requires additional disk space.
- 5) Click **OK** to save the settings.
To run the backup task, use Windows Task Scheduler as described in *Scheduling backups*.
If a backup fails, refer to the **CPSBackup.log** file in the Forcepoint DLP 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.

Related concepts

[Monitoring backups on page 353](#)

[Backup folder contents on page 353](#)

Related tasks

[Scheduling backups on page 352](#)

Scheduling backups

To schedule a Forcepoint DLP backup:

- 1) On the Forcepoint management server, open the Windows Task Scheduler (**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 an administrator password for the 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. As a best practice, however, 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 Forcepoint DLP machines.

Monitoring backups

Every backup operation writes start and completion entries in the system log screen (**Main > Logs > System Log**) in the Data Security module of the Forcepoint Security Manager.

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 subfolders—each is a backup of a different component in the system:

Subfolder	Contents
PreciseID_DB	The fingerprint repository
MngDB	The Forcepoint DLP reporting database (containing policies, incidents and configuration)
Forensics_repository	Encrypted forensic incidents information
Crawlers	Information on the discovery and fingerprinting crawlers
Certs	Certificate files used for communication between the Forcepoint Security Manager and Forcepoint DLP 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

Use the Forcepoint DLP “Modify” wizard on the management server to initiate the restore operation.



Important

Do not restore the backup on 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:

Steps

- 1) Make sure all Forcepoint DLP modules—servers, agents, protectors—are registered with the management server and the system is operating normally.
- 2) On the management server, open the Windows Control Panel and select Programs > Uninstall a program.
- 3) Select Forcepoint DLP, then click **Uninstall/Change**.
- 4) When asked if you want to add, remove, or modify Forcepoint DLP, 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).
- 11) Log onto the Forcepoint 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

Use the **Settings > General > Incident Export** page in the Data Security module of the Forcepoint Security Manager to configure how incidents are exported to a log file for analysis.

Steps

- 1) To enable incident export, select **Export incidents to a file**.

- 2) Enter a **Path** to define the storage location for the incident report (C:/Program Files (x87)/Websense/Data Security/incidents-export, by default).
- 3) Enter a **File name** for the export file.
 - The name must be fewer than 180 characters.
 - File names cannot include the following characters:
/:*?"\\<|>;,&%@#!^&\$%()+'=~`{}
- 4) Set the **Maximum number of files**, from 1 to 20, to keep (5, by default).
- 5) Under New File Creation, indicate whether to base new file creation on file size (default) or time.
 - To create a new file when the file reaches a specified size, select **When file size reaches**, then set a size from 1-5MB.
 - To create a new file daily at 12:00 a.m., select **At the start of a new day**.

- 6) Click **OK** to save your changes.

The following fields are exported:

Field	Description
Incident ID	External incident ID.
Insert date	The incident insert date.
Source hostname	The incident source hostname.
Source IP	The incident source IP.
Source full name	The incident source full name.
Source email	The incident source email.
Source DN	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.
Destinations list	A list of the incidents destinations, in the format of dest1;dest2;dest3...
Channel name	The channel name.
Max action taken	A readable action taken (e.g.: Blocked, Audited).
Urgency	Incident's urgency, sometimes called sensitivity (e.g.: Moderate).
Policy category	A policy category for the current line (an incident can generate multiple lines).
Filenames	The filename or filenames related to the current incident policy, up to 1024 characters. In the format of [fn1;fn2;...;fnX].
Filenames trimmed	True if the actual value for the filenames filed is greater than 1024 characters. Please notice that in few cases you do not get the actual file name. For example, for some SMTP incidents you might see the filename as MESSAGE-BODY.
Breached contents	The breach content of the incident for the current policy, up to 1024 characters, in the format of [content1;content2;...;contentX].
Breached content trimmed	True if the actual size of the previous filed is more than 1024 characters.

Configuring endpoint settings

Use the tabs of the **Settings > General > Endpoint** page in the Data Security module of the Forcepoint Security Manager to configure parameters for endpoint software, such as how often to test connectivity and check for updates.

The page opens with the **General** tab displayed. Configure the options on the General tab as follows:

- 1)** Under Connectivity, use the **Test connectivity every** field to specify how often, in minutes (between 1 and 60), endpoint clients test connectivity (5 minutes, by default).
- 2)** Use the **Check for updates every** drop-down list to select how often (between 30 seconds and 24 hours) endpoint clients check for configuration updates (1 hour, by default).
- 3)** Use the **An endpoint is disconnected...** field to determine after how long (between 1 and 60 hours) an endpoint client is determined to be disconnected (48 hours, by default).
- 4)** Under Administration, set which **Action** (Permit or Block) is taken when users do not respond to a request for confirmation after attempting to perform an operation that breached policy (Block, by default).
- 5)** If you do not want endpoint users to be able to un-install the endpoint client software or disable blocking or anti-tampering, select **Enable endpoint administrator password**, then enter and confirm the password. It must meet all of the following conditions:
 - Be at least 8 characters
 - Contain upper case characters
 - Contain lower case characters
 - Contain numbers
 - Contain non-alphanumeric characters

A password is not required to administer endpoint clients.

- 6)** Click **Save**.

For the next step in configuring endpoint settings, continue with *Endpoint settings: the Email Domains tab*.

Related concepts

[Endpoint Application Groups](#) on page 254

Related tasks

[Configuring Endpoint Deployment](#) on page 445

[Endpoint Devices](#) on page 252

[Endpoint Applications](#) on page 253

[Endpoint settings: the Email Domains tab](#) on page 357

Endpoint settings: the Email Domains tab

Use the **Email Domains** tab of the **Settings > General > Endpoint** page to configure email monitoring.

This includes defining 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.

To configure email monitoring:

Steps

- 1) Under Internal email domains, use the **Domain** field to enter each internal domain used by the organization. These are domains from which users in the organization 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 list blank. When there are no entries in the list, endpoint email is not analyzed.

- 2) Select **Outbound** to monitor traffic between a source domain defined in the Internal email domains list and any destination domain that is not in the list.
- 3) Select **Internal** to monitor email traffic between source and destination domains that are both in the Internal email domains list.
- 4) Click **Save**.

Next steps

For the next step in configuring endpoint settings, continue with *Endpoint settings: the Detection tab*.

Related concepts

[Endpoint settings: the Detection tab](#) on page 358

Endpoint settings: the Detection tab

Use the **Detection** tab of the **Settings > General > Endpoint** page:

- To select URLs to be analyzed using the Endpoint Online Applications feature
- To permit Windows users to burn data to CD/DVD using third-party applications

Improved Detection for Web File Uploads

The Improved Detection for Web File Uploads feature enhances the detection of sensitive data being uploaded to cloud storage solutions through supported web browsers. Incidents can be generated and activities that put sensitive data at risk can be audited or blocked.

This option applies only to websites and cloud applications that bypass browser extensions. Only URLs accessed from Google Chrome, Microsoft Edge Chromium, and Mozilla Firefox are analyzed.

By default, this setting is disabled.

To enable the feature, select **Enable web file uploads analysis**.

By default, the following list of URLs is supported: mail.google.com, drive.google.com, *.dropbox.com, *.amazon.com/clouddrive, *.box.com, *.icloud.com, mail.yahoo.com. To add a URL to the list:

- 1) Enter the URL name into the URL field. Wildcards are supported:
 - A question mark (?) to represent a single character, as in the following example: "exa?ple.com"
 - An asterisk (*) to represent zero or more characters, as in the following example: "*example.com", where "*example.com" matches [www.example.com](#), [www.mail.example.com](#), and example.com

- 2) Click **Add** to add a new URL.

To remove URLs from the list:

- 1) Mark the desired boxes from the list to select URLs.

- 2) Click **Remove**.

To view incidents related to web file uploads, navigate to **Main > Reporting > DLP > Incidents** page. The Forensics tab shows when the detected breach was a URL-protected file.

Optical Media

Under Optical Media, specify whether or not to **Permit third-party CD/DVD burning on Windows**.

- The system monitors non-native Windows CD/DVD burner applications, blocking or permitting operations without performing content classification.
- 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.

Click **Cancel** to discard all changes you made on the Detection page. Click **Save** to save all changes on the Detection page.

To deploy all of the configured changes on the Detection page, click **Deploy** in the Security Manager toolbar.

For the next step in configuring endpoint settings, continue with *Endpoint settings: the Disk Space tab*.

Related tasks

[Endpoint settings: the Disk Space tab](#) on page 359

Endpoint settings: the Disk Space tab

Use the **Disk Space** tab of the **Settings > General > Endpoint** page to configure the maximum storage size for logs, incidents, and other data.

Near the top of the tab, the amount of space reserved for system file storage is displayed. This number cannot be changed.

Steps

- 1) Set the **Maximum log file size** (16-100 MB) to limit the size of the endpoint client's log file (16-100 MB; default is 16MB).
- 2) Specify the **Incident storage size** (10-2000 MB) to allocate for disconnected endpoints (100 MB, by default).
- 3) Specify the **File fingerprint storage size** (1-1000 MB) to allocate for storage of directory and SharePoint fingerprints (50 MB, by default).
- 4) Specify the **Database fingerprint storage size** (1-1000 MB) to allocate for storage of database fingerprints (250 MB, by default).
- 5) Specify the **Contained file storage size** to allocate for storage of contained files (500 MB, by default). Contained files are those that are held in temporary storage on an endpoint. Files are contained when policies 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 Solutions End User's Guide](#) for more information.
- 6) Review the **Total allocated disk space** summary to see how much total storage space is being allocated for Forcepoint DLP functions on each endpoint machine, and make adjustments to the various disk space settings as needed.
- 7) Click **Save**.

Next steps

For the final step in configuring endpoint settings, continue with *Endpoint settings: the Advanced tab*.

Related tasks

[Endpoint settings: the Advanced tab](#) on page 360

Endpoint settings: the Advanced tab

Use the **Advanced** tab of the **Settings > General > Endpoint** page to configure applications or folders to decouple from Forcepoint DLP Endpoint drivers. These are typically applications that experience compatibility problems with the endpoint software.

- 1) Under Excluded Applications, use the **Application/Folder** field to enter the name of an application or folder to exclude.
 - For Windows endpoints, enter an executable filename in the form **winword.exe** (for Microsoft Word), or a folder name in the form **\office15** (for the entire Microsoft Office 2013 suite).
Do not include the drive letter.
 - For macOS endpoints, enter a case-sensitive application name like **TextEdit** or a case-sensitive full path such as:
`/Applications/TextEdit.app/Contents/MacOS/TextEdit`

Mac endpoints do not support relative folders.

 - Filenames cannot include spaces.

- File and folder names must be in ASCII characters.
 - Do not use wildcards.
- 2) Select the operating system on which the application runs.
- 3) Click **Add** to add the application to the Excluded Applications list.
- 4) Repeat steps 1-3 for each application that you want to exclude.
- 5) Click **Save**.

Up to 30 applications and folders can be entered.

File access is monitored for the listed applications, but there is no monitoring or enforcement for other operations, like copy/cut/paste and printing.

After the updated profile is deployed to an endpoint machine, the machine must be rebooted for this setting to take effect.

Remediation

Use the **Settings > General > Remediation** page in the Data Security module of the Forcepoint Security Manager to define the location of the syslog server and mail release gateway used for remediation.

- 1) Under Syslog Settings, enter the **IP address or hostname** of the syslog server, and the logging **Port**.
- 2) To set the origin of syslog messages, select **Use syslog facility for these messages**, then use the drop-down menu to select the type of message to appear in the syslog:
- **User-level Messages (#1)** logs generic user-level messages, such as “username/password expired”.
 - **Security/Authorization Messages (#4)** logs authentication- and authorization-related commands, such as “authentication failed for admin user”.
 - **Security/Authorization Messages (#10)** logs non-system authorization messages inside a protected file (for information of a sensitive nature, such as passwords).
 - **Local use 0-7 (#16-23)** specifies unreserved facilities available for any local use. Processes and daemons that have not been explicitly assigned a facility can use any of the “local use” facilities. Configuration is done in the syslog.conf file.

To send incident data to the syslog, select **Audit Incident > Send Syslog Message** in the action plan for the policy.

- 3) Click **Test Connection** to send the syslog server a verification test message.
- 4) Under Release Quarantined Emails, specify which gateway to use when releasing a quarantined email message.
- The default is **Use the gateway that detected the incident**. This gateway could be Forcepoint Email Security or the protector MTA, depending on your subscription.
 - To define a specific gateway, select **Use the following gateway**, then enter the gateway **IP address or hostname** and **Port**.

- 5) If only recipients of a message should be able to release it from quarantine, select **Validate user before releasing message**.

The system then ensures that the person attempting to release a message is a recipient of the message, and therefore authorized. Unauthorized users receive an email notification that they are not allowed release the message.

- 6) Click **OK** to save your changes.

Syslog messages can be sent to an SIEM tool if desired. They are compatible with both ArcSight Common Event Format (CEF) and Audit Quality SIEM format.

The ArcSight CEF message includes the following information for each incident:

```
CEF:0|Forcepoint|Forcepoint DLP|8.3|{id}|DLP Syslog|{severity}| act={action}
duser={destinations} fname={attachments} msg={details} suser={source} cat={policyCategories}
sourceServiceName={channel}analyzedBy={policyEngineName} loginName={name}sourceIp={ip}
```

Here:

- 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

The ArcSight Audit Quality SIEM message adds additional information for each incident:

```
severityType=MEDIUM sourceHost=MNG_ENDPOINT_1 productVersion=8.3 maxMatches=6 timeStamp=2015-03-11
16:33:48.333 destinationHosts=ACCOUNTS.GOOGLE.COM,10.0.0.17.2 apVersion=8.3
```

Here:

- severityType = incident severity (low, medium, high)
- sourceHost = hostname or IP address of incident source
- productVersion = version number of Forcepoint DLP product (e.g., 8.3)
- maxMatches = maximum number of violations triggered by any given rule in the incident.
- timeStamp = date and time of incident (e.g., 2015-04-30 16:33:48.333)
- destinationHosts = hostnames, IP addresses, or URLs of incident destinations
- apVersion = Forcepoint version number

Related concepts

[Remediation on page 257](#)

Incident risk ranking cases

When incident risk ranking cases are sent to syslog, the message includes case information. For example:

```
CEF:0|Forcepoint|Forcepoint DLP|8.3.0.1184836|983645|DLP Syslog|1| riskScore=1.4 caseDescription=High-severity breach content and a suspected false-positive event caseDateAndTime=07 Jul. 2016, 9:33:18 AM caseClassification=Unknown caseSummary=Low risk content;Number of files in case (46);Destination is unusual;PII breach (1 match);Possible false positive (23%) numberOfIncidents=2 eventIDs=14359168827488891711,3765310750806591754
```

Here:

- riskScore = risk score assigned to the case
- caseDescription = case description
- caseDateAndTime = date and time case was created
- caseClassification = case classification: suspected data theft or uncategorized/ unknown
- caseSummary = case summary
- numberOfIncidents = number of incidents in the case. Cases can contain several incidents, so this number varies from the number of eventIDs.
- eventIDs = IDs for up to 20 incidents in the case or 1024 characters. If there are more incidents in the case, it is indicated by an ellipsis.

Mail servers

When Forcepoint DLP is configured to send incident notifications to administrators, the notifications can include links that permit the administrators to perform workflow operations on the incident. For example, they can click a link to change the incident's 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 Forcepoint DLP that a workflow operation has been requested.

Use the **Settings > General > Mail Servers** page in the Data Security module of the Forcepoint Security Manager to set up the mail server that receives email requests for workflow updates—the incoming mail server—as well as the mail server sends 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) Under Incoming Mail Server, select **Mail server type** from the drop-down. This is the email server address that collects and stores incoming email from administrator notifications. These are the email messages that are sent to the system when administrators try to update workflow operations from inside a notification email. If you select **Other mail server**, do the following:
 - a) Select the protocol to use for email retrieval: **POP3** or **IMAP**. Most mail servers support both.
 - b) Specify whether or not to **Use secure connection (SSL)** to connect to the incoming mail server. This protects the content of the email from users outside of your network.
- 2) Enter a dedicated **System email address** to which workflow email requests are sent. For example: **DLPsystem@mycompany.com**.

- Set up an email account on your mail server for this purpose. Use a dedicated account, because the system deletes its contents regularly. Any email in this folder is lost.
 - If you are using Exchange Online, a valid email address must be used.
 - This email address automatically appears in the To: field of the email message when administrators click a workflow operation link.
The exception 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.
- 3) Enter the following information depending on the mail server type you selected.
- If you selected **Exchange Online**, enter the **Tenant ID**, **Client ID**, and **Client secret**.
For more information about getting your Tenant ID, Client ID, and Client secret, see the [Configuring Azure Active Directory to use OAuth2 authentication](#) Knowledge Base article.
 - If you selected **Other server type**:
 - a) Enter the **IP address or hostname** and **Port** for the mail server that can open the specified email address.
 - b) Enter the **User name** and **Password** for a network account (not a Security Manager account) with access to both the incoming mail server and system email address. The system needs to connect to this server to retrieve the workflow updates.
- 4) Click **Test Connection** to test the incoming mail server settings. The system tries to connect to the server and returns a success or failure message. This can take several minutes.
- 5) Under Outgoing Mail Server, select a **Mail server type** from the drop-down.
This is the email server address that waits and listens for outgoing notifications and alerts.
If you change the outgoing mail server here, the mail server for scheduled tasks, notifications, alerts and discovery task email reports are affected. Make sure that you use or update a new valid sender email address in these components, otherwise, information will not be sent via email for these components.
- If you selected **Exchange Online**, do one of the following:
 - Select **Same as Incoming Mail Server**.
 - Enter applicable **Tenant ID**, **Client ID**, and **Client secret**, if different than the incoming mail server. For more information about getting your Tenant ID, Client ID, and Client secret, see the [Configuring Azure Active Directory to use OAuth2 authentication](#) Knowledge Base article.
 - If you selected **Other mail server**:
 - Enter the **IP address or hostname** and **Port** for your outgoing mail server.
- 6) Click **Test Connection** to test the outgoing mail server settings. 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.
- If using Exchange Online, the sender email address must be valid or the connection test will fail.
- 7) Click **OK** to save your changes.

Alerts

Use the **Settings > General > Alerts** page in the Data Security module of the Security Manager to define which conditions trigger alerts and whether the alerts should be sent to the syslog or emailed to an administrator. For emailed alerts, define the sender, recipients, subject, and mail server.

When you navigate to the Alerts page, the **General** tab is displayed first.

Steps

- 1) 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:
 - SSL certificate is about to expire
 - Your subscription is about to expire
 - Policy updates fail during upgrade
 - 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
- 2) Click **OK** to save your changes.

Next steps

To finish configuring alerts, continue with *Setting up email properties*.

Related tasks

[Setting up email properties](#) on page 365

Setting up email properties

Use the **Email Properties** tab of the **Settings > General > Alerts** page to define properties for alerts that are sent by email:

Steps

- 1) Enter the **Sender name** for alert notifications sent to administrators.
- 2) Enter the **Sender email address** for the account from which notifications are sent.
 - If you are using Exchange Online, a valid sender email address must be used.

3) Review the Outgoing mail server information:

- For a local server, the IP address or hostname and port are displayed.
- For an online server, the server name (Exchange Online) is displayed.

This is the email server address that waits and listens for outgoing notifications and alerts

Change the outgoing mail server on the **Settings > General > Mail Servers** page, or by clicking **Mail Server Settings** in the toolbar at the top of the content pane. The outgoing mail server settings affect scheduled tasks, notifications, and email workflow.

4) Enter the Subject line for scheduled alert notifications.

5) To update the email alert Recipients, click Edit.

The Directory Entries window opens with searchable and selectable recipients. After making selections, click **OK** to save your changes.

To add one or more further recipients, select **Additional email addresses**, then enter the addresses of the recipients. Use commas to separate multiple email addresses.

6) Click OK to save your changes.

Archive storage

The incident database is partitioned quarterly. Archiving partitions optimizes performance. Use the **Settings > General > Archive Storage** page to specify where to store the incident archives and how much disk space to allow.

(Archive partitions on the **Settings > General > Archive Partitions** page.) To begin, select whether to use local or remote storage.

- If you select **Store archive locally**, archive files are stored in the location configured during installation (displayed in the Archive Folder field).

The Maximum Archive Disk Space value is also displayed. This value cannot be changed.

- If you select **Store archive remotely**, define a location for the archive files as follows:

Field	Description
Use existing storage location	Use the drop-down menu to select a previously configured storage location. Click Delete to remove unneeded locations.
Name new storage location	Select this option to define a new storage location. Enter a name for the new location.
IP address or hostname	Enter an IP address or hostname for the machine on which the storage will be located.
Domain	Enter the domain name for the account used to access the location.
User name	Enter the user name for the account.
Password	Enter the password for the account.

Field	Description
Archive folder	Type a folder name for the new archive. For example: Forcepoint\DLP\archive. Do not include preceding or trailing backslashes. The folder is relative to the IP address or hostname provided.
Test Connection	Click Test Connection to make sure the Forcepoint DLP server can access the storage location. This ensures the path is valid (hostname and folder) and also checks the access credentials.
Description	Optionally, enter a description for the archive location.
Maximum archive disk space	Select a limit on the storage drive for disk space used by the archive. Find guidelines for estimating the required disk space below.

When you are finished, click **OK** to save your changes.

Related concepts

[Forcepoint DLP databases](#) on page 8

Disk space calculation

The amount of disk space needed 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:

(number of incidents per quarter) * (average transaction size) * 12

The product is multiplied 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 Dashboard (**Main > Status > Dashboard**).
- The size of the metadata for the incidents

The metadata size can vary depending on the number of policies used and on incident complexity. 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: (number of incidents per quarter) * 20 bytes * 12

The total disk space required 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.

Services

Use the **Settings > General > Services** page in the Data Security module of the Forcepoint Security Manager to configure the following local and external services that interact with Forcepoint DLP:

- When Forcepoint DLP integrates with Forcepoint Web Security, Linking Service provides IP address to user name resolution for HTTP incidents. This allows Forcepoint DLP to display user names in incident reports, rather than IP addresses.
See *Linking Service and mapping URL categories*.
- Forcepoint DLP can decrypt and analyze Microsoft Office files that were encrypted by Microsoft Information Protection.
See *Configuring MIP for endpoint decryption*.
- With a Forcepoint DLP Cloud Applications subscription, the Cloud service can be used to apply DLP policies to files uploaded to, downloaded from, or shared within a variety of cloud applications.
See *Configuring DLP Cloud Applications*.
- Data Protection Service gives you the option to enforce DLP rules that protect cloud applications through integration with Forcepoint CASB or Forcepoint Email Security Cloud. It also protects data that is uploaded to web applications through integration with Forcepoint Web Security Cloud.
See *Configuring Data Protection Service*.
- Organizations that use a supported, third-party classification system to label files used in the network can enable Forcepoint DLP to integrate with the existing system.
See *Configuring file labeling*.
- Forcepoint DLP Risk-Adaptive protection allows administrators to define dynamic DLP Policy Rules that perform different actions based on the current end-user risk level. The Forcepoint DLP Endpoint can receive the current end-user risk level by integration with Forcepoint Behavioral Analytics technology, or alternatively, by installing Forcepoint Dynamic User Protection on the same endpoint system.
See *Analytics*.

Related concepts

[Linking Service and mapping URL categories](#) on page 368

[Configuring file labeling](#) on page 374

Related tasks

[Configuring MIP for endpoint decryption](#) on page 370

[Configuring DLP Cloud Applications](#) on page 371

[Configuring Data Protection Service](#) on page 372

[Analytics](#) on page 379

Linking Service and mapping URL categories

The **URL Categories** tab of the **Settings > General > Services** includes two main functions: Getting URL category mapping using either Linking Service or importing from Forcepoint Web Security Cloud Portal, and using Linking Service to provide IP- address to user-name resolution for HTTP incidents.

- *Using Linking Service*
- *Importing URL categories from Forcepoint Web Security*

Related tasks[Mail servers on page 363](#)[Importing URL categories from Forcepoint Web Security on page 370](#)

Using Linking Service

In addition to providing IP-address to user-name resolution for HTTP incidents, Linking Service allows Forcepoint DLP to import Forcepoint Web Security predefined and custom URL categories. These categories can then be added as resources in DLP policies so that you can map URLs to categories and view them in incident reports.

Steps

- 1) Note the IP address and port of the Linking Service machine. This is added automatically during installation.
- 2) Make sure that **Enabled** is selected.
- 3) Click **Test Connection** to test the linking connection. A confirmation message is returned.
If connection fails, enter the **IP address or hostname** of the Linking Service machine, and the connection **Port** (56992, by default), then test the connection again.



Note

If the IP or port are invalid and the import fails, any currently existing categories already mapped are deleted. To correct this situation:

- a) Enter a valid IP and port, and then click **OK**.
- b) Click **Deploy**
- c) Go to **Resources > URL Categories**, and click **Upload** to get the most updated URL category list.

Next steps

Dynamic user name resolution and category mapping are enabled by default when you install Forcepoint DLP. If you are experiencing significant latency during content analysis, edit the service **Properties** to limit the use of Linking Service to the most important functions. Only change these settings if the connection between your data and web solutions is poor.

- 1) Under Incident Reports, mark **Show user names in incident reports** to have user names to display in incident reports rather than IP addresses. This may make it easier to determine who is moving sensitive data.
- 2) Mark **Show URL categories in incident reports** to display URL categories rather than URLs in reports. For example, instead of <http://www.cnn.com>, reports might display News and Media.
- 3) Under Content Analysis, mark **Resolve user names when analyzing content** to have the system resolve IP addresses to user names when it is analyzing transactions.
Use this option if there are rules that include or exclude user names as a source. For example, block John Doe from posting the document MyDoc.doc to the Web.

If there is a match, the rule is triggered.

- 4) **Mark Map URL categories when analyzing content** to have the system to map URLs to categories when it is analyzing transactions.
Use this option if there are rules that include or exclude URL categories as a destination. For example, block John Doe from posting the document MyDoc.doc to News and Media sites.
- 5) Click **OK** to save your settings.

Importing URL categories from Forcepoint Web Security

To use this method, you need an XML file with a list of categories from the Forcepoint Web Security Cloud Portal. This option is only available with a subscription to Forcepoint Web Security Cloud. See the **Subscription** page (**Settings > General > Subscription**) to see your subscriptions.

Steps

- 1) Click **Choose File**, and browse to the location of the XML file with the URL categories.
- 2) Select the file, and then click **OK**. The file is uploaded to the server.
- 3) Repeat as many times as needed (multiple files can be uploaded, one by one).



Important

- If you previously worked with Linking Service, and thus already have URL categories in your rules, and now want to import URL categories using an XML file, note that categories imported via XML from the Forcepoint Cloud Security Gateway will override the existing rules. This can cause missing categories or conflicts, and it is highly recommended that you review your rules after importing new URL categories and make sure they are using valid categories.
- If any of the following properties are missing for a URL category in the XML file, the DLP manager ignores the category, and it is not added to the database nor is it listed in the Security Manager:
 - Name
 - Predefined/Custom
 - Parent (note that “root” is a valid value)
- If a URL category is corrupted (for example, is missing an ID number), it is recommended that you remove it from the XML file before uploading.

Configuring MIP for endpoint decryption

Forcepoint DLP integrates with Microsoft Information Protection (MIP) to apply DLP policies to MIP-encrypted files on Windows endpoints. This feature enables enterprises to maintain sensitive data visibility and control for files protected using MIP. Forcepoint DLP interacts directly with MIP, enabling MIP to work both on and off the network. It can also be used to better understand how MIP is being used by employees to protect sensitive data.

Use the **MIP Decryption** tab of the **Settings > General > Services** page to configure Forcepoint DLP to decrypt and analyze Microsoft Office files that were encrypted by Microsoft Information Protection on Windows endpoints. This includes files found on Windows endpoints (discovery) or sent via any endpoint channel.

By default, this setting is disabled.

To enable MIP decryption, select **Enable MIP decryption**, then click **OK**.



Note

The MIP decryption feature relies on the Microsoft RDS SDK. Therefore, for MIP decryption to work, Microsoft Remote Desktop Services must be running on the endpoints.

Office files that are protected by Microsoft Information Protection include Office File Formats based on OCP (Office 2010 and later), legacy Office File Formats (Office 2007), PDF files, Generic PFILE support, and files that support Adobe XMP.

The system uses logged-in user credentials to access the MIP server. Because the system runs under the security context of the logged-in user, it uses the same permission as the user and, therefore, can read everything the user can read. For example, when a user creates a document, the user has permission to read the document and so does the system. When the user has read permissions to the document, explicitly or as part of an Active Directory group, so does the system. In case of errors, the transaction is permitted without analysis and the error is recorded in a log file.

The Microsoft Information Protection file detection feature has the following prerequisites:

- 1) The endpoint machine must be in your organization's domain.
- 2) Forcepoint DLP Endpoint version 19.xx or higher must be installed.
- 3) Azure Active Directory/Office 365 single sign-on (SSO) between the local active directory and the Azure active directory must be configured and working. Users must be able to MIP-decrypt a document without a login request.

To view MIP-related incidents in the Data Security module of the Security Manager, navigate to the page > **Main > Reporting > DLP > Incidents - Last 3 days**.

See Microsoft documentation for more information on MIP:

- [Microsoft Information Protection Overview](#)
- [DLP & MIP Deployment Acceleration Guide_Updated.zip](#) (download)
- [Azure Information Protection](#)



Note

Please note that the following are not supported:

- Decryption of MIP-encrypted file can only be done for single logged-in user. Multiple users logged into the same machine is not supported.
- RPMSG message (RMS protected mail message) are not supported.

Configuring DLP Cloud Applications

Use the **DLP Cloud Applications** tab of the **Settings > General > Services** page to activate or deactivate DLP Cloud Applications.

With a Forcepoint DLP Cloud Applications subscription, DLP Cloud Applications:

- Provides content inspection for files used in cloud collaboration applications, including downloaded, uploaded, shared, and stored files
- Applies DLP policies to sensitive data

First, DLP Cloud Applications must be activated:

- 1) Click **Activate**.
The DLP Cloud Service Activation dialog box is displayed.
- 2) Enter the following information from the DLP Cloud Applications fulfillment letter:
 - a) The **Access key ID**
 - b) The **Access key secret** for the account
 - c) The **Service URL**
- 3) Click **OK**.
The connection process is initiated. This may take some time to complete.

When the DLP Cloud Applications service is successfully activated, the tab is updated with a list of supported modules according to the existing license, and with a link that enables you to recheck the license. It also displays a Module Connection Status section, with an indication of the current connection status of the CASB Portal module, and a link to recheck connection status.

Configuring Data Protection Service

Use the **Data Protection Service** tab of the **Settings > General > Services** page to connect to Data Protection Service. Uploading tenant information is part of the connection process.

Data Protection Service:

- Enables enforcement of DLP rules that protect cloud applications through integration with Forcepoint CASB, for the DLP Cloud Proxy, DLP Cloud API, and Cloud Data Discovery channels.



Note

To support these channels, DLP Cloud Applications must be activated. For more information, see *Configuring DLP Cloud Applications*.

- Protects data over web traffic through integration with Forcepoint Web Security Cloud.



Note

As part of the integration with the Forcepoint Web Security Cloud, URL categories can now be imported from the Forcepoint Web Security Cloud Portal. See *Linking Service and mapping URL categories* for more information.

- Enables enforcement of DLP rules for the Network Email channel through integration with Forcepoint Email Security Cloud. For more information, see the [Forcepoint Email Security Cloud and Forcepoint DLP Integration Guide](#).

First, Data Protection Service must be connected. This is done by uploading tenant information from a JSON file received by email as part of the onboarding process. Note that each time a file is uploaded, the system resets as if this is the first connection:

- 1) Click **Select File**, and in the dialog box that appears, click **Choose File**. Browse to the JSON file you received from Forcepoint, and then click **OK**.
The file is uploaded to the server, and the information begins to appear in the Connection area of the Data Protection Service tab.
- 2) Click **Connect** to establish the connection with Data Protection Service:
- 3) Click **Deploy** to begin enforcing policies in cloud channels.
- 4) Click **OK** at the bottom of the screen to complete the process.

When the connection is active, the **Connect** button turns into a **Disconnect** button, enabling disconnection of Data Protection Service from Forcepoint DLP.

In the Data Protection Service Status area, upon successful connection, the status is marked as **Connected successfully**, the time and date of the connection is displayed, and the **Recheck connection** link is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as **Failed to connect**.

Related concepts

[Linking Service and mapping URL categories](#) on page 368

Related tasks

[Configuring DLP Cloud Applications](#) on page 371

Error handling

- If Data Protection Service shows the status “Failed to connect”, the module is temporarily unavailable. Click **Connect** or **Recheck Connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is “Never connected”. This is because the Forcepoint Security Manager has never successfully connected to the Cloud Policy Engine. In this case, it is probable that a Cloud Policy Engine was not created. Contact Forcepoint Technical Support for assistance
- If you receive the following message in the Data Protection Service Status area:

This service is not connected to Forcepoint CASB. Incident reporting and policy enforcement will be affected for cloud channels. See “Explain this page” for more information.

This means that there is a connection issue, and DLP Cloud API and Cloud Data Discovery channels will not enforce DLP policies, and the DLP Cloud Proxy channel might not report incidents to the Forcepoint Security Manager. See [Viewing deployment status](#) for more information.

Related concepts

[Viewing deployment status](#) on page 37

Configuring file labeling

Forcepoint DLP can integrate with third-party file labeling systems.

Use the **File Labeling** tab of the **Settings > General > Services** page to select a file labeling system and to view file labeling system usage, label import status, and the last successful import.

The File Labeling page includes supported labeling system names.



Note

Version 8.7 and up support two file labeling systems: Boldon James Classifier and Microsoft Information Protection. Only one labeling system can be used at a time.

Click the desired labeling system name to open the labeling system property page.

- If you select Boldon James Classifier, see *Configuring Boldon James classifier*.
- If you select Microsoft Information Protection, see *Configuring Microsoft Information Protection*.

Related tasks

[Configuring Boldon James classifier](#) on page 374

[Configuring Microsoft Information Protection](#) on page 375

Configuring Boldon James classifier

Use the **Boldon James Classifier Properties** page to enable and configure file labeling using the Boldon James Classifier system. This feature allows Forcepoint DLP to add labels to files and modify labels based on discovery policies and to import labels for detection (for more information about creating file labeling classifiers for detection, see *File Labeling*).

To open the Boldon James Classifier Properties page, go to **Settings > General > Services > File Labeling** tab and click on the **Boldon James Classifier** link. The Boldon James Classifier Properties page opens.



Note

To enable and use this feature, a supported labeling system must already be in use on the network.

To enable and configure the File Labeling system:

- 1) Under Imported Labels, click **Import Labels**. The Import Labels dialog box opens.
- 2) From the Import Labels dialog box, select **Choose File**. Browse to the Boldon James configuration file to import. This file is usually called spif.xml. If unable to find the file, contact technical support for the Boldon James system.
- 3) Click **OK** to start the import process.
- 4) After a successful import, the **Last import** field lists the date and time of the import, along with the number of imported labels.
- 5) If any action plans have labels that no longer exist in the labeling system, a warning is displayed with **Show details** as a link.

- 6) Click the link to view which action plans have labels that no longer exist in the labeling system. It is recommended that these action plans be updated. See *Forcepoint Data Discovery options*.
- 7) Mark the **Apply file labels** check box.
 - When you enable the check box, you can define DLP action plans that use Boldon James Classifier file labels.
 - When the check box is not marked, Boldon James Classifier file labels are used only for detection.
- 8) Under Guidelines, mark one or more check boxes to specify when Forcepoint DLP should add or modify a label:
 - When the file has a lower priority label (upgrade the classification)
 - When the file has a higher priority label (downgrade the classification)
 - When the file has a tag whose priority cannot be compared to the new label
 - When the file is not already labeled

In cases where a file does not meet a selected condition, its labeling remains unchanged. This may mean that the file remains unlabeled, or that the original label or labels added by the third-party system remain in place.

In incident reports, the incident details provide information about whether labels were found on a file, and whether labels were changed.
- 9) Click **OK** to save the changes.

The audit log (**Main > Logs > Audit Log**) is updated when the administrator imports classification labels and when the file labeling system or the guidelines are enabled or disabled. Click the **Guidelines updates** link for more information on updates.

After the **Apply file labels** check box has been marked, administrators can configure the specific labels to use on the Discovery tab of each action plan. See *Action Plans*.

Related concepts

- [File Labeling on page 194](#)
- [Action Plans on page 257](#)

Related tasks

- [Forcepoint Data Discovery options on page 261](#)

Configuring Microsoft Information Protection

Use the **Microsoft Information Protection Properties** page to use imported Microsoft Information Protection labels for detection (for more information about creating file labeling classifiers for detection, see *File Labeling* section) and for labeling (for more information about configuring labels in an action plan, see *Forcepoint Data Discovery options* section).

To open the Microsoft Information Protection Properties page, go to **Settings > General > Services > File Labeling** tab and click the **Microsoft Information Protection** link. The Microsoft Information Protection Properties page opens.

**Important**

- Before you import Microsoft Information Protection labels for the first time, you must obtain permission for the Forcepoint application to import the labels.
Log into the Microsoft 365 [Admin Consent page](#), authenticate using your Microsoft 365 admin credentials, and accept the permissions statement.
- Forcepoint Security Manager enables import of sensitivity labels from the Microsoft 365 Security and Compliance Center. If you want to import Azure Information Protection labels, you must migrate them to Microsoft 365, as described on [Microsoft's Azure Information Protection site](#).
- Files that are protected by Microsoft Information Protection can be decrypted automatically during DLP analysis (see *Configuring MIP for endpoint decryption* section).

To import labels:

- 1) Enter your **Microsoft Office 365 admin** credentials and click **Import Labels**.
We recommend that you enter credentials for an administrator who has visibility to all Microsoft Information Protection labels used in the organization.
User credentials are not stored on Forcepoint servers. However, you should ensure that your web browser does not store this information.
- 2) Click **OK** to start the import process.
If “admin consent” has not already been established, this step generates an error message and the import does not occur. Complete the Microsoft admin consent process and try again.
- 3) After a successful import, the Last Import Details section is updated with the imported labels and a message. The message lists date, time and number of imported labels.
- 4) To apply labels, mark the **Apply file labels** check box.
 - When you enable the check box, you can define DLP action plans that use Microsoft Information Protection file labels.
 - When the check box is not marked, Microsoft Information Protection file labels are used only for detection.

**Note**

The system applies Microsoft Information Protection labels to a file only if the label is a higher priority than the existing label.

- 5) Click **OK** to save the changes.

The audit log (**Main > Logs > Audit Log**) is updated when the administrator imports classification labels and when **Apply file labels** is either checked or unchecked.

After the **Apply file labels** check box has been marked, administrators can configure the specific labels to use on the Discovery tab of each action plan. See *Action Plans* section.

If any action plans include labels that no longer exist in the labeling system, a warning is displayed, with a **Show details** link, leading to a list of action plans with labels that are no longer in the labeling system. Forcepoint recommends updating these action plans. See *Forcepoint Data Discovery options* section.

Related concepts

[File Labeling](#) on page 194
[Action Plans](#) on page 257

Related tasks

[Forcepoint Data Discovery options](#) on page 261

[Configuring MIP for endpoint decryption](#) on page 370

Risk-Adaptive Protection

Risk-Adaptive Protection combines the power of the Forcepoint DLP and Forcepoint Behavioral Analytics capabilities, performing modeling and analytics to determine a user profile risk. Then, based on the user risk level, actions are executed when Forcepoint DLP policies are triggered.

Forcepoint provides two solutions that perform user activities modeling and determine the user profile risk:

- Forcepoint Behavioral Analytics
- Forcepoint Dynamic User Protection

Risk-Adaptive Protection with Forcepoint Behavioral Analytics

Forcepoint Behavioral Analytics is an on-premises solution that runs a set of dedicated servers that ingest DLP events and incidents data into the Forcepoint Behavioral Analytics platform, and performs modeling and analytics to determine a user risk profile. The calculated user risk level is sent to the Forcepoint Security

Manager and pushed to the Forcepoint DLP Endpoints. Then, when Forcepoint DLP policies are triggered, different reactions can take place based on the current user risk level.

Forcepoint Behavioral Analytics requires that the endpoint to be connected to the corporate network in order for the endpoints to send the DLP events and incidents data to the Forcepoint Behavioral Analytics servers.

To enable Risk-Adaptive Protection with Forcepoint Behavioral Analytics:

Steps

- 1) Deploy a Forcepoint Behavioral Analytics instance. See the [Forcepoint Behavioral Analytics Administration and Troubleshooting manual](#).
- 2) Enable Risk-Adaptive Protection in Forcepoint DLP. See *Analytics* section.
- 3) Configure relevant policies and rules so that actions are risk-level dependent. See *Custom Policy Wizard - Severity and Action* section.
- 4) Enable/Disable Risk-Adaptive Protection for specific users/groups. Use the RAP UserManager.exe. See the [Dynamic Data Protection Getting Started Guide](#) for more information.
- 5) Users can be either custom or based on a user directory. Users are assigned risk level 1 as a default risk-level value.
- 6) Sync the modified list of Risk-Adaptive Protection users in the Forcepoint Behavioral Analytics system. See [Forcepoint Behavioral Analytics Administration and Troubleshooting manual](#).

- 7) Check DLP incidents. See *Managing incident reports* section.
- 8) Investigate users. See [Forcepoint Behavioral Analytics Administration and Troubleshooting manual](#).

Related concepts

[Adding a high-risk resource](#) on page 379
[Managing incident reports](#) on page 86

Related tasks

[Analytics](#) on page 379

Configuring Risk-Adaptive Protection to use Forcepoint Behavioral Analytics

To use Risk-Adaptive Protection with Forcepoint Behavioral Analytics, go to the **Settings > General > Services** page. Select the **Risk-Adaptive Protection** tab, and then:

Steps

- 1) Mark the **Enable Risk-Adaptive Protection** check box.
- 2) Enter the following settings:
 - The Forcepoint Behavioral Analytics hostname or IP address.
 - The **Port** number. The default port number is 9093.
- 3) Click **Test Connection** to test the Forcepoint Behavioral Analytics connection to Forcepoint DLP. A confirmation message returns.
 If connection fails, enter again the Forcepoint Behavioral Analytics hostname or IP address and the port number; then test again.
- 4) Click **OK** to save the changes.
- 5) Click **Deploy**.



Note

If you already defined Forcepoint DLP rules to determine actions by user risk level, disabling this option (by clearing the Enable Risk-Adaptive Protection check box) disconnects Forcepoint Behavioral Analytics from Forcepoint DLP and actions are determined only by DLP matches.

Risk-Adaptive DLP with Forcepoint Dynamic User Protection

Forcepoint Dynamic User Protection is an endpoint blade that can be installed with the Forcepoint DLP Endpoint on the same machine. It performs modeling and analytics to determine a user profile risk on the endpoint itself, even when the endpoint is disconnected from the corporate network, or the user is working off-site.

Forcepoint DLP Endpoint passes all events and incidents to the Forcepoint Dynamic User Protection blade, which then calculates the current user's risk level locally on the endpoint. Then, when Forcepoint DLP policies are triggered, the action called for is based on the particular user's risk level.

If Forcepoint Security Manager is connected to Data Protection Service (see *Configuring Data Protection Service* section for more information) and if transactions are being sent to Data Protection Service for DLP analysis from one of DLP integrated cloud products such as Forcepoint CASB, Forcepoint Web Security Cloud or Forcepoint Email Security Cloud agents (see [Cloud Security Gateway Integration Guide \(Web Security Cloud, CASB, and DLP\)](#) and [Forcepoint Email Security Cloud and Forcepoint DLP Integration Guide](#), for more information), then Data Protection Service will enforce the Forcepoint DLP policies based on the particular user's risk level and report to the DLP incidents reports.

To enable Risk-Adaptive DLP with Forcepoint Dynamic User Protection, do one of the following:

- Build a unified Forcepoint F1E installer to install Forcepoint DLP and the Dynamic User Protection blade.
- Download Forcepoint Dynamic Endpoint Protection as a separate installer directly from the Forcepoint Dynamic User Protection cloud console, and distribute it to endpoint systems that are running Forcepoint DLP.

For more information, see the [Forcepoint Behavioral Analytics Administration and Troubleshooting manual](#).

Related tasks

[Configuring Data Protection Service](#) on page 372

Analytics

Use the **Settings > General > Analytics** page in the Data Security module of the Forcepoint Security Manager to configure high-risk business units for incident risk ranking. (Create business units containing high-risk resources on the **Main > Policy Management > Resources > Business Units** page.)

The settings on the Analytics page affect how the analytics engine calculates risk scores for the Incident Risk Ranking report. They can only be edited by administrators with permission to configure analytics.

Steps

- 1) Select **Use high-risk resources for risk scoring** to enable use of the business units.
- 2) Click **Add** to add one or more resource groups to use when formulating risk scores for Incident Risk Ranking reports. See [Adding a high-risk resource](#) section.
Note that only user resources can be added as high-risk resources. Other resources types, like computers and networks, are not added.
To remove a resource, select its check box, then click **Remove**.
- 3) Click **OK**.

Adding a high-risk resource

Clicking Add on the **Settings > General > Analytics** page opens a list of all the business units in the system. Select a business unit to add its users to the high-risk resource group and configure its properties.

**Important**

When you add a business unit to the high-risk resource group, only the user resources in the business unit are added. Other resource types, like domains, computers, and networks, are not used.

Field	Description
Filter by	If there is a large number of business units listed, use the filter to narrow down the list.
Type	Select the type of resources in the business unit (high-risk source or privileged account). You can add only one business unit of each type: that is, one high-risk source and one privileged account.
Level	Select the risk level for this business unit. The High-risk source options are: <ul style="list-style-type: none">■ Risk■ High risk■ Very high risk The Privileged account options are: <ul style="list-style-type: none">■ Privileged■ High privileged■ Most highly privileged

User directory settings

Use the **Settings > General > User Directories** page in the Data Security module of the Forcepoint Security Manager to define the user directory to use for Forcepoint DLP end users and other policy resources (such as devices and networks).

(The LDAP directory or directories used for adding and authenticating Forcepoint administrators with network accounts is defined on the Security Manager **Global Settings > User Directories** page.)

Configure Forcepoint DLP to connect to supported directories (such as Microsoft Active Directory or IBM Domino) to ensure that the most current end user and resource information is available.

Use the User Directories page to:

- Add a directory server. Click **New** in the toolbar at the top of the content pane, then see *Adding or editing user directory server information* section.
- Update the configuration of an existing directory server. Select an entry in the list, then see *Adding or editing user directory server information* section.
- Delete an existing directory server.
- Import user information (see *Importing users* section and *Importing user entries from a CSV file* section).

Note that user names with a “/” character cause an import failure from Domino user directories. Please contact Forcepoint Technical Support if your user names contain these characters.

- Define the ranking order of your directory servers. Click **Rearrange Servers** in the toolbar at the top of the content pane, then see *Rearranging user directory servers* section.

Related tasks

[Adding or editing user directory server information](#) on page 381

[Importing users](#) on page 383

[Importing user entries from a CSV file](#) on page 384

[Rearranging user directory servers](#) on page 383

Adding or editing user directory server information

On the **Settings > General > User Directories > Add/Edit directory server** page in the Data Security module of the Forcepoint Security Manager:

Steps

- 1) Mark the **Enabled** check box to import user information from this directory server.
- 2) Enter or update the **Name** for the user directory server.
- 3) Select the **Type** of directory from the drop-down menu: Active Directory, Domino, or Comma Separated Value (CSV) file.
 - If you select Active Directory or Domino, see *Using Active Directory or Domino* section.
 - If you select Comma Separated Value (CSV) file, see *Using a CSV file* section.

Related tasks

[Using Active Directory or Domino](#) on page 382

[Using a CSV file](#) on page 381

Using a CSV file

If you selected Comma Separated Value (CSV) file, under Connection Settings:

Steps

- 1) Enter the **Path** to the CSV file containing the user directory entries in UNC format. For example, <\SharedServer\Shared\Groups\Network>.
- 2) Enter the **User name** and **Password** for an account with access to the path.
- 3) Click **Test Connection** to verify that Forcepoint DLP can access the path.

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



Important

CSV files must use a specific format. Refer to *Importing user entries from a CSV file* section for details.

Related tasks

[Importing user entries from a CSV file](#) on page 384

Using Active Directory or Domino

If you selected Active Directory or Domino:

Steps

- 1) Under Connection Settings, enter the **IP address or hostname** and **Port** to use to connect to the user directory server.



Note

The default port is 3268, which is the Global Catalog (GC). The GC has only a partial copy of the user attributes, which can result in failure to receive all the attributes requested during the testing or LDAP import processes.

To connect directly to the Domain Controller and receive all of the requested attributes, use port 389. Alternatively, the Global Catalog can be configured to include additional attributes.

[Learn more about the Global Catalog on the Microsoft website.](#)

- 2) Enter the **User distinguished name** and **Password** for an account with access to the directory server.
 - For Active Directory, the format “domain\username” is supported.
 - For Domino, use the format “CN=User, OU=Department, DC=DomainComponent, DC=com”.
- 3) Optionally, enter the **Root naming context** that Forcepoint DLP should use to search for user information.
 - When entering a value, ensure that it is a valid context in the domain.
 - If the field is left blank, the system begins searching at the top level of the directory service.
- 4) Mark **Use SSL encryption** to connect to the directory server using Secure Sockets Layer (SSL) encryption.



Important

If your Active Directory is configured for LDAP channel binding and LDAP signing communication, you *must* mark **Use SSL encryption**, otherwise the user directory import will fail and communication between the DLP manager and the LDAP server will fail.

- 5) Mark **Follow referrals** to have Forcepoint DLP follow server referrals, should they exist. Referrals are an LDAP feature that provide 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.
- 6) Click **Test Connection** verify that Forcepoint DLP can connect to the directory server.

- 7) Under Directory Usage, mark **Get user attributes** to retrieve user attributes from the directory server, then:
 - a) Enter the user **Attributes to retrieve** for all users (comma separated).
 - b) If the directory includes photo attributes, use the **User's photo attribute** to enter them in a comma-separated list. The default is thumbnailPhoto.
 - 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.
 - c) Under Test Attributes, in the **Sample email address** field, enter a valid email address that can be used to test whether Forcepoint DLP can retrieve the configured attributes from the user directory server.
 - d) Click **Test Attributes** to retrieve user information.
- 8) Click **OK** to save your changes.



Note

If you change user directory settings at a later date, existing accounts 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 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.

Define the ranking your user directory servers on the **Settings > General > User Directories > Rearrange User Directory Servers** page in the Forcepoint Security Manager:

Steps

- 1) In the User Directory Servers list, click individual server names and use the up/ down arrows to promote or demote the servers to the desired order.
- 2) Click **OK** to save your changes.

Importing users

Use the **Settings > General > User Directories** page in the Forcepoint Security Manager to import user data. Either import user data immediately from a directory or schedule the import. Only users with email addresses are imported.

To define when to import user directory information, do one of the following:

- Click **Import Now** in the toolbar at the top of the page to immediately import user information in the server list order. (It can take some time to perform this action. A confirmation screen appears.)
Use this option to import user directory data from CSV files. Imports from CSV cannot be scheduled.

- Click the **Import...** link on the left, above the table, to determine how often (daily or weekly) and at what time the import occurs. In the dialog box that opens:
 - 1) Select **Enabled** to enable the scheduler.
If this box is *not* selected, the user directory remains static until you manually update it via the **Import Now** button.
 - 2) Indicate whether to update user directory information **Daily** or **Weekly**.
 - 3) Specify a time of day for the import. If you have selected a weekly import, also select a day of the week. Many administrators choose to synchronize the directories during off- business hours.
 - 4) Click **OK**.



Note

During the import process, custom resources that you add (groups, users, computers) may not be activated even after they have been deployed. Wait until the system log shows that the Resource Repository synchronization has succeeded to begin working on custom resources.

Importing user entries from a CSV file

User directories information can be imported via CSV files. To do this, generate a set of files in a specific structure, as follows:

Steps

- 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 toolbar at the top of the **Settings > General > User Directories**
- 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 the **Settings > General > User Directories** page and click **Import Now** in the toolbar at the top of the page.

Related concepts

[CSV file formatting](#) on page 385

CSV file formatting

When creating user directory files in CSV format, 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:
 - 1) Enclose fields that contain a special character (semicolon, new line, or double quote) in double quotes.
 - 2) 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:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier
Group name	String	No	Name of user directory group
Description	String	Yes	Description
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)

For example:

```
08b3b46b-3631-46cb-adc7-176c2871e94c,Marketing - EMEA, Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05
```

```
40632a33-db39-4f93-bd80-093e0b3230ca,Marketing - APAC, Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05
```

```
7c9d4db6-1737-4b80-9e6e-42f415300a05,Marketing all,All Marketing departments
```

Users file format

Each row in the **users.csv** file should contain:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier
Username	String	No	Login or user ID

Name	Data Type	Optional	Description
Email	String	Yes	Email address (primary)
Description	String	Yes	Description
UUID	String	Yes	UUID of the current user's manager
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)
Zero or more “additional attributes” fields	String	Yes	See “Additional Attributes” below

User records can also have additional attributes in the form of name value pairs. Some of these attributes have predefined names (see below). A file containing an additional attribute should be defined as a regular expression of the following format:

[aA][tT][tT][rR]:(.+)/=(.+)

Any name can be used for custom attributes. The attributes are stored as an associated array on the user object, and are used only for display. Examples include:

- wbsn_proxy_address - secondary (alternative) email address
 - wbsn_nt_domain\wbsn_login_name - the user login name (principal name on Windows-based systems)
 - wbsn_full_name - the user's display name
 - wbsn_department - department
 - wbsn_telephone_number - the user's telephone number
 - wbsn_title - the user's title
 - wbsn_mailbox_store - the server on which the user's Exchange mailbox is stored
- The table below illustrates some attributes:

String	Name	Value
attr:wbsn_title=/Manager	wbsn_title	Manager
aTTr:my amazing attr=/the value	my amazing attr	the value
“ATTR:name=/value1,value2”	name	value1,value2

For example:

6278ab76-2ce2-4f16-8e49-aa5104da7d0b, jdoe-mgr, jdoe.manager@example.com,CEO,7c9d4db6-1737-4b80-9e6e-42f415300a05,attr:room=/201,attr:parkingSpace=/1

ff255105-4e43-4e9a-b2bd-e366872cd212, jdoe, jdoe@example.com, administrator, 6278ab76-2ce2-4f16-8e49-aa5104da7d0b,"08b3b46b-3631-46cb-adc7-176c2871e94c;7c9d4db6-1737-4b80-9e6e-42f415300a05",attr:room=/101

Computers file format

Each row in **computers.csv** should contain:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier

Name	Data Type	Optional	Description
Name	String	No	Computer name (hostname)
FQDN	String	Yes	DNS fully qualified domain name

Name	Data Type	Optional	Description
Description	String	Yes	Description
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)

For example:

```
379a287f-0a5c-40ff-85fd-fae3da462d03, gumby, gumby.example.com, print server, "7c9d4db6-1737-4b80-9e6e-42f415300a05"
```

Archiving incident partitions

The incident database is partitioned every 90 days. To optimize performance, archive partitions periodically.

The Forcepoint DLP keeps a dynamic tally of incidents, which are automatically saved in the *Online-Active* partition. When a partition is full, it becomes inactive, and a new, active partition is created to store incident data.

Use the **Settings > General > Archive Partitions** page in the Data Security module of the Forcepoint Security Manager to view a list of current partitions and their status. You can archive, restore, or delete a partition, and set storage limits.

The bolded first line of the Archive Partitions page lists 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 of time and hundreds of thousands of incidents.

When the reporting database is hosted on Microsoft SQL Server Standard or Enterprise, it can have a maximum of 8 online partitions (approximately 2 years). Refer to *Remote SQL Server machines* section, for special instructions.

SQL Server Express, on the other hand, 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 (3 years of records).

The columns in the archive list are sortable.

Column	Description
ID	An internal identification number for the partition, beginning with the year. Click incident partitions to select them for archiving.

Column	Description
Status	<p>The current status:</p> <ul style="list-style-type: none"> ■ Online-Active marks the partition into which local incidents are dynamically stored. ■ Online indicates a former (now full) Online-Active partition. This partition is no longer active, but it has not been archived or deleted. ■ Archive marks partitions that have been archived in an offline location. ■ Deleted marks partitions that have been permanently deleted. ■ Restored marks partitions that were restored to Online status after having been archived.
From	The date of the first event logged in the archive.
To	The date of 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	Optional, administrator-added comments about the archive.
Show deleted partitions	When selected, deleted partitions are displayed in the Archiving list.

Use the buttons in the toolbar at the top of the content pane to archive, restore, or delete selected partitions.

Button	Description
Archive	Send a selected archive to offline storage. See <i>Archiving a partition</i> section.
Restore	Restore a selected archived partition. See <i>Restoring a partition</i> section.
Delete	Permanently delete a selected partition. See <i>Deleting a partition</i> section.
Settings	Open a settings paged used to define the archive size and storage location. See <i>Archive storage</i> section.

Related concepts

[Viewing Incidents and Reports](#) on page 39

[Archive storage](#) on page 366

Related tasks

[Archiving a partition](#) on page 390

[Restoring a partition](#) on page 390

[Deleting a partition](#) on page 391

[Remote SQL Server machines](#) on page 389

Remote SQL Server machines

The choice of whether to use a local or remote Microsoft SQL Server database is made during installation, when Forcepoint DLP components are installed on the management server machine.

If a remote database is selected, administrators have the option to enable Forcepoint DLP archiving. (Archiving is automatically enabled when a local database is used.)

When incidents are archived, they are initially stored in a temporary folder. For a remote SQL Server database, this folder is defined during Forcepoint DLP installation. Both the database and the management server must have access to the temporary folder.

If the temporary folder is not defined during Forcepoint DLP installation, it is not possible to archive incidents. Attempts to manually archive partitions cause the Forcepoint Security Manager to display a warning that archive settings have not been fully configured, so archiving won't work. Automatic archiving fails and sends a message to syslog.

If you receive an archiving warning or error message, modify your installation as follows to enable archiving:

Steps

- 1) Launch the Forcepoint Security Installer on the management server.
- 2) Next to Forcepoint DLP, select **Modify**.
- 3) Click **Next** until you reach the Temporary File Location page.
- 4) Select Enable incident archiving and backup.
- 5) Enter the local or network path to the temporary folder to use during incident archiving.
 - The folder must already exist.
 - Both SQL Server and the management server must be able 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 with read/write permissions to the temporary folder.
- 8) Complete the installation wizard.
- 9) Open the Data Security module of the Security Manager and click **Deploy**.

Next steps

Note that you only configure the temporary archive folder in the installer. To configure the final location of the archive, use the **Settings > General > Archive Storage** page in the Data Security module of the Security Manager.

Archiving a partition

Incident partitions fill automatically, but you can only keep either 4 partitions (SQL Server Express) or 8 partitions (Microsoft SQL Server Standard or Enterprise) online. To save older partitions, archive them offline. The maximum local offline storage allowed is 12 partitions (approximately 3 years of records). To archive a partition:

Steps

- 1) Go to the **Settings > General > Archive Storage** page in the Data Security module of the Forcepoint Security Manager.
- 2) Select one or more incident partitions.
- 3) Click **Archive** in the toolbar.
- 4) Review the list of partitions to be archived, adding comments, if needed.
For an explanation of the information shown for each partition, see *Archiving incident partitions* section.
- 5) Click **OK** to continue.

Next steps

The number of partition archives you can create depends on the size of the partition location.

Related concepts

[Archiving incident partitions](#) on page 387

Restoring a partition

Archived partitions can be restored to online status. This may be helpful, for example, to allow comparison between older and newer incident patterns. Up to 4 partitions (approximately 1 year of records) can be restored.

To restore incident partitions from their archives:

Steps

- 1) Go to the **Settings > General > Archive Storage** page in the Data Security module of the Forcepoint Security Manager.
- 2) Use the check boxes to select one or more partitions.

- 3) Click **Restore** in the toolbar at the top of the content pane.
A “Selected archive partitions were successfully restored” confirmation message is displayed.
- 4) Click **OK**.
The Status line for the restored partitions indicates that they are now online.



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, it cannot be performed.

After restoring a partition, delete the archived records from the archive folder.

Deleting a partition

To delete partitions:

Steps

- 1) Go to the **Settings > General > Archive Storage** page in the Data Security module of the Forcepoint Security Manager.
- 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.

Next steps

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

Warning messages are displayed both 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 Forcepoint Technical Support to retrieve the archive.

Updating predefined policies and classifiers

For your convenience, Forcepoint DLP includes many predefined policies, content classifiers, and file types. Forcepoint research teams stay abreast of regulations across many industries and keep the policies and classifiers up-to-date.

When these elements are updated between product release cycles, administrators can update them via the **Settings > General > Policy Updates** page in the Data Security module of the Forcepoint Security Manager.

See the related topics list above for a complete list of the policies, classifiers, and file types provided at the time of this product's release.

Related concepts

[Viewing your update history](#) on page 392

Related tasks

[Installing policy updates](#) on page 393

[Restoring policies to a previous version](#) on page 394

Determining the policy version you have

When you are upgrading or restoring policy versions, it is helpful to know what version you currently have.

This information is displayed on the **Settings > General > Policy Updates** page. Check the **To Version** column for the entry with the latest date.

Viewing your update history

Use the **Settings > General > Policy Updates** page in the Data Security module of the Forcepoint Security Manager to view a policy update history (including when updates were performed, what they contained, and more).

This page lists any updates, along with the original policy version and new version.

Column	Description
Date	The date the update occurred.
Administrator	The administrator who performed the update.
Type	The type of policy that was updated. Standard Policies are those predefined by Forcepoint and available to all customers. Custom policies are those that have been built just for a specific organization.
From Version	The version of policies, classifiers, and file types installed prior to the update.

Column	Description
To Version	The version of policies, classifiers, and file types installed during the update.
Details	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.
File name	The name of the update file used to perform the update.

Use the buttons in the toolbar at the top of the content pane to install updates or restore policies to a previous version:

Button	Description
Install Updates	Install the latest policy updates, content classifiers, and file types on your system. A wizard is launched. (See <i>Installing policy updates</i> section, for instructions on using the wizard.)
Restore	Restore your policies, content classifiers, and file types to the selected version. (See <i>Restoring policies to a previous version</i> section, for instructions.)

Related tasks

[Installing policy updates](#) on page 393

[Restoring policies to a previous version](#) on page 394

Installing policy updates

Forcepoint researchers update the predefined policies (adding policies or changing existing ones) on a regular basis. Forcepoint researchers also update the predefined content classifiers and file types.

To install the most recent updates:

- 1) Download a file containing the latest updates from [support.forcepoint.com](#).
 - a) Click **My Account** at the top of the page and enter your login information.
 - b) Click the **Downloads** link in the navigation bar at the top of the page.
If the Data Security downloads are not listed automatically, click the **All Downloads** button under “My Downloads.”
 - c) Under Forcepoint DLP, select the software version.
Find version information on the **Help > About** page in the Forcepoint Security Manager.

- d) If an update exists, it is listed in the **Hotfix** section. Click the title to open the Hotfix & Patch download page, then click the **Download** link to download the .zip file. Do not unzip the file.
- 2) In the Data Security module of the Security Manager, go to the **Settings > General > Policy Updates** page.
 - 3) Click **Install Updates** in the toolbar at the top of the content pane. (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, then click **Next**.
The version of your current policies and the new policies is displayed. To see what's new in the update, click the link that's provided at the top of the page.
 - 5) Click **Next** to install the updated policies and content classifiers. Once started, the update cannot be canceled (though you can later restore an older version).
 - 6) The Update Process page shows the progress of the update: what's being added, deleted, and updated.
 - 7) When the updates have installed successfully, click **Next** to apply them.
 - 8) A message confirms the update has completed successfully. Click the link to view a summary of the update, then click **Finish**.
The summary screen appears with the details of this update listed in the table. See *Viewing your update history* section, for a description of this page.

Related concepts

[Viewing your update history](#) on page 392

Related tasks

[Restoring policies to a previous version](#) on page 394

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 Forcepoint, 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.

Restore policies to a previous version on the **Settings > General > Policy Updates** page in the Data Security module of the Forcepoint Security Manager:

- 1) In the table, select the **From Version** to which you want to revert.
- 2) Click **Restore** in the toolbar at the top of the content pane.
- 3) Click **OK** to confirm the selection.
The system restores policies and classifiers to the selected version and date. Progress indicators show whether components were restored successfully.
- 4) Click **Close**. The summary screen shows the date the policies were restored, the version you moved from, and the version you moved to. See *Viewing your update history* section for a description of this page.

Related concepts

[Viewing your update history](#) on page 392

Related tasks

[Installing policy updates](#) on page 393

Entering subscription settings

Reference topic:

- [Subscription alerts](#) section.

Related concepts

[Subscription alerts](#) on page 398

Forcepoint DLP license types

Starting in version 8.5.1, two core license types are available for Forcepoint DLP: IP Protection and Compliance. The table below maps out the functional differences between the two license types and which legacy licenses are covered by each type.

License Type Name	Current Products Covered	Legacy Products Covered	Use Case	Feature Differences
IP Protection	DLP Suite (IP Protection) DLP Cloud Applications (IP Protection) DLP Endpoint (IP Protection) DLP Network (IP Protection) DLP Discover (IP Protection) DLP Suite (IP Protection Upgrade) DLP Cloud Applications (IP Protection Upgrade) DLP Endpoint (IP Protection Upgrade) DLP Network (IP Protection Upgrade) DLP Discover (IP Protection Upgrade)	TRITON AP-DATA Gateway TRITON AP-DATA Discover TRITON AP-DATA Cloud App Security TRITON AP- Endpoint DLP Data Security Suite TRITON Enterprise TRITON Security Gateway Websense Data Endpoint Websense Data Gateway Websense Data Discover	Enterprises looking to address both IP Protection and regulatory compliance use cases with advanced content detection capabilities and integrated DLP analytics.	Features included: <ul style="list-style-type: none"> ■ Structured and unstructured data fingerprinting ■ Machine learning classifiers ■ Incident Risk Ranking, including DLP Analytics Engine (software and virtual appliance)
Compliance	DLP Suite (IP Protection) DLP Cloud Applications (Compliance) DLP Endpoint (Compliance) DLP Network (Compliance) DLP Discover (Compliance)	None	Enterprises looking to address only regulatory compliance and data privacy use cases using pre-defined and custom policies.	Features not included: <ul style="list-style-type: none"> ■ Structured and unstructured data finger- printing ■ Machine learning classifiers ■ Incident Risk Ranking, including DLP Analytics Engine (software and virtual appliance)

Forcepoint DLP license types (IP Protection and Compliance) cannot be mixed within the same Forcepoint DLP Deployment. All product licenses must be IP Protection or Compliance types. The only exception is for the DLP modules within Forcepoint Email Security and Forcepoint Web Security. In Forcepoint DLP v8.5.1 and later, these modules unlock the full IP Protection feature set.

Licensing options available as of version 8.6 support the following Forcepoint DLP components:

- Forcepoint DLP Cloud Applications (license has start and termination dates)
- Perpetual Forcepoint DLP Suite subscription combined with Forcepoint DLP Cloud Applications (license has start and termination dates for cloud applications)

Licensing options available as of version 8.8 support the following Forcepoint DLP components:

- Forcepoint Web Security Cloud (license has start and termination dates, and must be IP Protection or Compliance type)

Licensing options available as of version 8.9 support the following Forcepoint DLP components:

- Forcepoint Email Security Cloud (license has start and termination dates, and must be IP Protection or Compliance type). For more information about the Data Protection for Email license, see the [Forcepoint Email Security Cloud and Forcepoint DLP Integration Guide](#).

The **Settings > General > Subscription** page of the Forcepoint Security Manager shows the terms of your subscription. See *Entering a subscription key* section.

You can upgrade from a DLP Compliance product license type to an IP Protection license type, which will make available the additional IP Protection features by purchasing the relevant “IP Protection Upgrade” licenses. Please contact your Forcepoint reseller or Forcepoint sales account team to discuss an upgrade.

Related tasks

[Entering a subscription key](#) on page 397

Entering a subscription key

Data loss prevention over web or email channels is automatically included with the DLP Module for Forcepoint Web Security or Forcepoint Email Security. In these integrated deployments, the subscription key is entered in the Web Security or Email Security module of the Forcepoint Security Manager, and not the Data Security module.

Providing web and email DLP through other means—such as the Forcepoint DLP protector—requires a Forcepoint DLP subscription. A Forcepoint DLP subscription is also needed to analyze images or protect DLP channels as well as web and email.

To enter the Forcepoint DLP subscription key:

- 1) Log on to the Security Manager.

If you have installed an add-on DLP component—such as Image Analysis or the endpoint agent—you are prompted to enter the subscription key.

- 2) Browse to the subscription file, then click **Submit**.

Your subscription terms are displayed, including the start and expiration dates (or “n/a” if you have a perpetual subscription), the number of subscribed users, and the modules and services to which you subscribe. You are automatically logged out of the Forcepoint DLP application and must log in again.



Note

The subscription dates apply only to the modules in the section and not to the CASB license. CASB dates are determined by the CASB license.

When you purchase an upgrade or change subscription type, update the Forcepoint DLP subscription file. If you do not, an error message displays when you try to use Forcepoint DLP.

To update your Forcepoint DLP subscription:

- 1) In the Security Manager, go to the **Settings > General > Subscription** page. Your current subscription terms are displayed.
- 2) Click **Update** in the toolbar at the top of the content pane.

- 3) Browse to the new subscription file, then click **OK**.

You are automatically logged out of the Forcepoint DLP application and must log in again.

Subscription alerts

The health alert summary on the Forcepoint DLP Dashboard shows an alert when the 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 policy violations 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 Forcepoint DLP sales representative.

Chapter 18

Configuring Authorization

Contents

- [Defining administrators on page 399](#)
- [Working with roles on page 404](#)
- [Customizing your own administrator account settings on page 408](#)

Use the **Settings > Authorization** menu to configure authorization options for the Data Security module of the Forcepoint Security Manager. Authorization options are used to:

- View and edit administrator permissions.
 - Administrators are the people who manage the Forcepoint DLP system.
 - Administrator accounts must first be defined under **Global Settings > General > Administrators** before they appear in the Data Security module of the Security Manager.
- See [Defining administrators](#).
- Set up roles, such as the Super Administrator, Basic, and Auditor, to define groups of administrators with similar permissions. Each role has its own set of permissions.
See [Working with roles](#).
- Configure personal settings for your own administrator account.
See [Customizing your own administrator account settings](#).

Related concepts

[Defining administrators on page 399](#)

Related tasks

[Working with roles on page 404](#)

[Customizing your own administrator account settings on page 408](#)

Defining administrators

Forcepoint DLP administrators configure security policies, view incidents, fine-tune system performance, and more. An organization might have one Super Administrator or multiple administrators with different responsibilities.

Administrator accounts for all Forcepoint Security Manager modules are added and deleted on the **Global Settings > General > Administrators** page (accessed via the Global Settings button in the Security Manager toolbar). When creating an administrator account, define whether it has access to the Data Security module.

Once the account has been defined, use the Data Security module of Security Manager to configure its Forcepoint DLP-specific permissions.

There are 2 types of Forcepoint DLP administrators:

- The User type is used for all administrator accounts that have access to the Data Security module of the Security Manager.
- The Application type is used to access REST API services in the Data Security module of the Security Manager. The Application type provides permissions to perform API requests to query incidents and perform operations on incidents. When the Application type is selected, only permission for the Data module are granted. All permissions for other modules are disabled.

There are 3 types of Forcepoint DLP accounts:

- Local administrator accounts are defined via Global Settings and granted Forcepoint DLP permissions. The administrator's role is assigned in the Data Security module of the Security Manager.
- Network administrator accounts are defined in an LDAP user directory, added via Global Settings, and granted Forcepoint DLP permissions. The administrator's role is defined in the Data Security module of the Security Manager.
- Network group administrator accounts belong to a user directory group added via Global Settings and granted Forcepoint DLP permissions. Each member of this group can log on to the Security Manager and work with the Data Security module. The group's role is assigned in the Data Security module of the Security Manager.

Group members can belong to more than one 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 Security Manager 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.

- Network group administrators cannot be assigned incidents or release incidents.
- Audit log records reflect the administrator who is currently logged on, not the administrator's group.
- On the Administrators page, local administrators, network administrators, and user directory groups are listed. Administrators within the network group are not displayed.
- Local and network administrators can be policy owners, as can network groups (provided they have a valid email address). Individuals within the network group cannot own policies.
- Local and network administrators can receive notifications, as can network groups (provided they have a valid email address). Individual within the network group cannot receive notifications.
- Report ownership is given to individual administrators and not to directory groups. This ownership is given according to the administrator who is currently logged on, so group members can own reports.
- Data Security module configurations are saved per administrator, rather than per group.
- Several reports in the Security Manager show top values per administrator. In such reports, only individual administrators are displayed, and not groups.

Related tasks

[Viewing administrators on page 400](#)

[Editing administrators on page 401](#)

[Working with roles on page 404](#)

[Adding a new role on page 405](#)

Viewing administrators

Use the **Settings > Authorization > Administrators** page in the Data Security module of the Forcepoint Security Manager to view a list of administrators with access to the Data Security module.

The page lists all the administrators that have been defined, along with their user names, user information source, roles, and permissions.

- 1) To view details about all Forcepoint DLP administrators, click the **Export to PDF** button.
 - Choose **Summary** to export basic information about the modules, policies, and business units each administrator can access.
 - Choose **Details** to export detailed information, including Forcepoint DLP permissions.

Save or print the report as needed.

- 2) Select a name to view or edit an administrator profile.
 - When administrators are first added to the system, click the account name and assign it a role.
 - Administrators with Forcepoint DLP access permissions are assigned initially to the default role, which provides only reporting and Dashboard access.
 - Global Security Administrators are assigned the Super Administrator role in Forcepoint DLP.
 - If you select an administrator with the Application type, then the information is view only. You cannot edit the information for an Application.

See *Editing administrators* section, for more information.

Related concepts

[Defining administrators on page 399](#)

Related tasks

[Editing administrators on page 401](#)

[Working with roles on page 404](#)

[Adding a new role on page 405](#)

Editing administrators

Administrator user names and email addresses are defined under Global Settings, and cannot be changed in the Data Security module of the Security Manager.

Administrator roles and access permissions, however, are configured in the Data Security module.

To edit administrator permissions:

Steps

- 1) Go to the **Settings > Authorization > Administrators** page in the Data Security module of the Security Manager.

 - 2) Select the name for the administrator whose profile you want to edit. Note that changes to administrator profiles are recorded in the audit log.

 - 3) If the administrator type is User, select a role for this administrator from the drop-down list (see *Working with roles* section), or click **New** to create a new role.
- Click **View Permissions** to view the permission settings for the selected role.



Note

You cannot configure a role if the Administrator type is Application.

- 4) Under Incident Management, indicate which incidents this administrator should 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:
- [Select Incidents](#)
 - [Select Policies](#)
 - [Select Business Units](#)
- 5) To add a record to the audit log each time this administrator views incident details in the Incidents report, select **Audit incident detail views**.
- The audit log (**Main > Logs > Audit Log**) is updated when the administrator clicks (and highlights) an incident in the report, and 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 when the administrator 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.



Note

If local administrators are also defined as members of a user directory group, the permissions you assign here supersede those of the group.

- 6) Click **OK**.

Related concepts

[Defining administrators on page 399](#)

Related tasks

[Select Incidents on page 403](#)
[Select Policies on page 403](#)
[Select Business Units on page 404](#)
[Working with roles on page 404](#)
[Adding a new role on page 405](#)

Select Incidents

Steps

- 1) When editing an administrator's profile (see *Editing administrators* section), optionally select which incidents this administrator can manage. The administrator can access the incident reports and remediate the incidents that you select.
 - Select **All incidents** to enable the administrator to manage all incidents from the selected policies and business units.
 - Select **Only incidents assigned to this administrator** to allow 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.

Related tasks

[Editing administrators](#) on page 401

Select Policies

Steps

- 1) When editing an administrator's profile (see *Editing administrators* section), optionally select which policies the administrator can manage. This affects which incidents the administrator can manage, as well. The administrator can access all DLP and discovery incidents for these policies.
 - Select **All** to enable this administrator to manage all policies. This includes both current and future policies (and their incidents).
 - Select **Selected** to identify specific policies the administrator can access. The **Select All** option selects all the items listed in the current window, but future policies are not selected.

- 2) Click **OK**.

The administrator must have a role that permits policy management. If he or she does not, these settings have no effect.

Related tasks

[Editing administrators](#) on page 401

Select Business Units

Steps

- 1) When editing an administrator's profile (see *Editing administrators* section), optionally select the business units for which this administrator can access incidents. For example, configure the 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** to enable this administrator to access DLP incidents from all business units, current and future.
 - Select **Selected** to identify specific business units the administrator can access. The **Select All** option selects all the items listed in the current window, but future business units are not selected.
- 2) Click **OK** to save your changes.

Related tasks

[Editing administrators](#) on page 401

Working with roles

When an administrator account is defined on the **Global Settings > General > Administrators** page, it can either be assigned access to specific Security Manager modules, or be granted Global Security Administrator access to all modules.

In the Data Security module, fine-tune permissions by assigning administrators roles: specific sets of permissions.

For example, one administrator may be responsible for installing and deploying system components. Another may configure and fine-tune security policies. 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.

By default, the following roles are defined:

- **Super Administrator** can access all configuration and management screens in the Data Security module with read and write privileges. This is different from Global Security Administrators who have Super Administrator privileges to all Security Manager 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, as well as 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** can access only reports and the Dashboard. This role is assigned to new administrator accounts when they are granted Data Security module access on the **Global Settings > General > Administrators** page.
- **Multiple Combined** has privileges from several roles. This applies only to network administrators who belong to multiple user directory groups. When such administrators log on to the Security Manager, the system automatically generates a custom role that unifies the roles of all their groups. Because they are system-generated, these combined roles are not listed on the roles screen. Administrators with this role see this role name in the toolbar when they log on.

Optionally edit access privileges for the default roles or add new roles.

Steps

- 1) Go to the **Settings > Authorization > Roles** page.
The page lists all the roles that have been defined, along with the permissions set for the roles and descriptions.
- 2) Click a name to edit a role, or click **New** to define a new role.
- 3) To delete a role, select it, then click **Delete**.
Changes to roles are recorded in the audit log.

Adding a new role

To define a new role:

- 1) Go to the **Settings > Authorization > Roles** page in the Data Security module of the Security Manager.
- 2) Click **New** in the toolbar at the top of the content pane.
- 3) Enter a Name for the new role.
- 4) Enter a Description for the role.
- 5) Under Permissions, select one of the following:
 - Select **Full Control** to give this role complete access to system functions, then click **OK** to create the role.
 - Select **Customized** to define the reach of this role, then continue with *Customized role permissions*.

Related tasks

[Viewing administrators on page 400](#)

Customized role permissions

Configure customized permissions for the role as follows:

Steps

- 1) Under Status, select the status reports to which this role should have access:
 - The **Dashboard** shows system alerts, statistics, and an incident summary over the last 24 hours.
 - The **System Health** screen enables you to monitor the performance of Forcepoint DLP servers and protectors.
 - The **Endpoint Status** screen summarizes the results of endpoint connectivity tests. (Not included in Forcepoint Web Security or Forcepoint Email Security.)
 - The **Mobile Status** contains details of the traffic being monitored by Forcepoint DLP over specific periods, such as data that has breached policies and the actions taken.

 - 2) Under Reporting, select the Data Loss Prevention & Mobile incident and reporting functions that this role should be able to access.
 - Select **Summary reports** to give administrators with this role access to data loss prevention summary reports.
 - Select **Detail reports** to give administrators with this role access to data loss prevention incident detail reports. When this option is selected, several more are made available:
 - Select **View violation triggers** to allow administrators to view the values that trigger violations.
 - Select **View forensics** to allow administrators 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.)
 - Select **Perform operations on incidents** to allow administrators with this role to be able to perform all escalation, remediation, and workflow operations on data loss prevention or mobile incidents.
 - Select **Export incidents to a PDF or CSV file** to allow administrators with this role to bulk export DLP or mobile incidents from an incident report to a PDF or CSV file. Exports include all data in the current report.
 - Select **Incident Risk Ranking reports** to allow administrators with this role to access Incident Risk Ranking and My Case reports.
 - Select **Hide source** or select **Destination** to prevent administrators with this role from seeing source or destination information like user names and IP addresses. Instead, reports will show sources and destinations as unique IDs generated by the system.
- These permissions do not affect the source and destination fields in the syslog. Syslog always displays names.
- In addition, these permissions do not affect the source and destination fields in:
- **Incident Export** - in order to prevent the administrators from viewing the source and destination, make sure the 'All other general settings' option is disabled.
 - **Traffic Log** - in order to prevent the administrators from viewing the information, make sure the 'Traffic log' option is disabled.

- 3) Select the Discovery incident and reporting functions for this role. Discovery functions are not included in Forcepoint Web Security or Forcepoint Email Security.
 - **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.
 - **Export incidents to a PDF or CSV file** - Select this option if you want to allow administrators with this role to bulk export discovery incidents from an incident report to a PDF or CSV file. Exports include all data in the current report.
- 4) Mark **Send email notifications** if administrators with this role should be notified when an incident is assigned to them.
- 5) Under 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* section 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 clear this box, this option is grayed out for administrators with this role.
- 6) Under Logs, select the logs to which this role should have access.
 - The **Traffic log** contains details of the traffic being monitored by Forcepoint DLP over specific periods, such as data that has breached policies and the actions taken.
 - The **System log** displays system events sent from different Forcepoint components, for example Forcepoint DLP servers, protectors, or policy engines.
 - The **Audit log** displays actions performed by administrators in the system.
- 7) Under Settings, select which General settings options administrators with this role should be able to access.
 - **Services** - Administrators can configure local and external services like Linking Service and Microsoft RMS.
 - **Archive Partitions** - Administrators can select incident partitions, then archive, restore or delete them.
 - **Policy Updates** - Administrators can update predefined policies to the latest version. All other general settings
 - **Analytics** - Administrators can configure settings used to calculate risk scores in the Incident Risk Ranking report.
 - **All other general settings** - Administrators can configure all other settings in the **Settings > General** menu.

- 8) Indicate whether administrators in this role can configure Data Security module **Authorization** settings.
- 9) Under Deployment, select which functions administrators with this role should be able to perform.
 - **Manage system modules** - Give this role the ability to register modules with the management server.
 - **Manage endpoint profiles** - Give this role the ability to view and edit endpoint profiles. Administrators can add new endpoint profiles, delete profiles, and rearrange their order. (Not included in Forcepoint Web Security or Forcepoint Email Security.)
 - **Deploy settings** - Give this role the ability to deploy configuration settings to all system modules.
- 10) Click **OK** to save your changes.

Related concepts

[Database Fingerprinting Wizard - Field Selection](#) on page 228

Customizing your own administrator account settings

The Security Manager may prompt you to perform certain activities, or ask if you're sure you want to perform a task. In most cases, it is possible to dismiss the prompt and select an option to not show it again.

Use the **Settings > Authorization > My Settings** page to configure the system to show previously dismissed prompts.

- 1) Under Restore Reminders, select **Show all reminders** to display prompts for which the “do not show again” option was previously selected.
- 2) Click **OK** to save your changes.

Related concepts

[Deploy button](#) on page 17

[My cases](#) on page 100

Chapter 19

Managing Forcepoint DLP System Modules

Contents

- Adding Forcepoint DLP system modules on page 410
- Configuring protector services on page 432
- Removing Forcepoint DLP modules on page 441
- Balancing the load on page 441

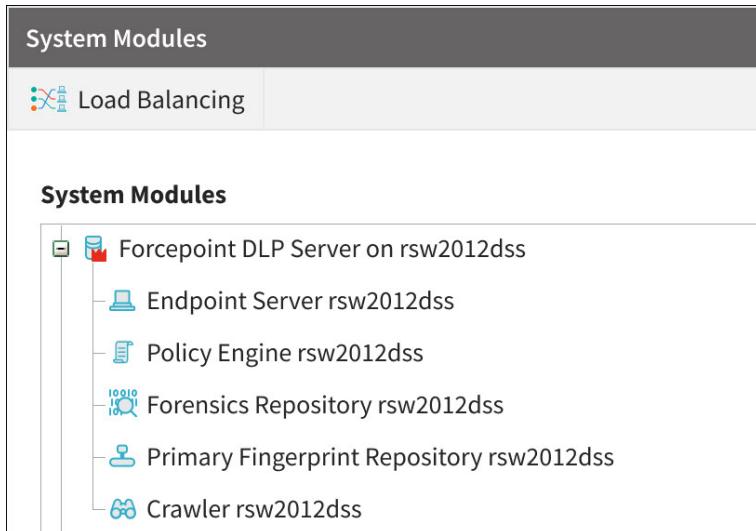
Use the **Settings > Deployment > System Modules** page in the Data Security module of the Forcepoint Security Manager to configure all the components in the Forcepoint DLP network and distribute the load between them evenly.

The nodes that appear in the System Modules tree depend on the options selected during installation.

- In Forcepoint Web Security deployments, nodes include the management server, Web Content Gateway, and supplemental Forcepoint DLP servers, if any.
- In Forcepoint Email Security deployments, nodes include the management server, Forcepoint Email Security, and supplemental Forcepoint DLP servers, if any.
- In a full Forcepoint DLP deployment, nodes may include:
 - The management server and any supplemental Forcepoint DLP servers
 - The protector
 - Web Content Gateway
 - Forcepoint DLP Email Gateway
 - Standalone agents
 - Data Protection Service (shown only after the JSON file upload in the Data Protection Service tab; see *Configuring Data Protection Service*)

Forcepoint DLP servers and management servers include several components, such as the fingerprint repository, crawler, and policy engine.

Each module and component is represented by an icon. Next to each module is a version number, to make it evident at a glance whether a particular module has been upgraded.



As shown in the on-screen legend, icons are shown in gray when a component is disabled, and are marked with a red exclamation point when the component has not yet been registered. If changes have been made to a module, but the changes have not yet been deployed, the icon appears with a pencil next to it.

If there is more than one Forcepoint DLP server, a **Load Balancing** button appears on the toolbar. Use the button to balance the load between policy engines to optimize performance. See *Balancing the load*.

Related concepts

[Removing Forcepoint DLP modules](#) on page 441

Related tasks

[Adding Forcepoint DLP system modules](#) on page 410
[Configuring Forcepoint DLP system modules](#) on page 411
[Balancing the load](#) on page 441

Adding Forcepoint DLP system modules

To add a new module to an existing Forcepoint DLP deployment, run the Forcepoint Security Installer on a supported machine. (See the [Forcepoint DLP Installation Guide](#) for instructions.)

The installation wizard prompts for the FQDN or IP address of the management server and the credentials for a Forcepoint DLP administrator with system modules permissions. This information allows the module to register with the management server automatically.

- To accept the default configuration, log on to the Forcepoint Security Manager after the installation is complete, then click **Deploy** in the Data Security module.
- To create a custom configuration, log on to the Forcepoint Security Manager and navigate to the **Data > Settings > Deployment > System Modules** pages, then click the module to edit. Follow the instructions in [Configuring Forcepoint DLP system modules](#).
 This requires system modules permissions. (See [Adding a new role](#) for information on permissions.)

When 2 standalone agents are installed on the same machine, the system registers each one independently, and they appear in the System Modules tree as 2 separate nodes.

If the IP address or hostname (FQDN) of a module changes after registration, it must be re-registered to notify the management server of the change.

If both the IP address *and* the hostname of a module change, re-register it twice, once after each change. If you wait until both changes have been made before re-registering, the management server thinks the module is brand new, and does not retain the module's configuration information (minimum/maximum transaction size, monitoring mode, and so on).

Related tasks

[Configuring Forcepoint DLP system modules](#) on page 411

[Adding a new role](#) on page 405

Configuring Forcepoint DLP system modules

Although configuration settings may be customized at any time, the default module configuration may be sufficient:

- Typically, in Forcepoint Web Security deployments, no additional configuration is needed.
- In full Forcepoint DLP deployments, in most cases, the only module that *must* be configured after installation is the protector. This is covered in *Configuring the protector*.

To configure a Forcepoint DLP system module:

Steps

- 1 Go to the **Settings > Deployment > System Modules** page in the Data Security module of the Forcepoint Security Manager.
- 2 Click a module.

- 3) Complete the fields as shown in the appropriate section below. Note that not all modules are available for all deployments.
- [Configuring the Forcepoint DLP management server](#)
 - [Configuring a supplemental Forcepoint DLP server](#)
 - [Configuring the fingerprint repository](#)
 - [Configuring the endpoint server](#)
 - [Configuring the crawler](#)
 - [Configuring the forensics repository](#)
 - [Configuring the policy engine](#)
 - [Configuring the OCR server](#)
 - [Configuring the protector](#)
 - [Configuring ICAP](#)
 - [Configuring the Web Content Gateway module](#)
 - [Configuring the Forcepoint Email Security module](#)
 - [Configuring Forcepoint DLP Email Gateway](#)
 - [Configuring the integration agent](#)
 - [Configuring protector services](#)
 - [Configuring the analytics engine](#)

Related concepts

- [Configuring ICAP on page 427](#)
[Configuring the Web Content Gateway module on page 428](#)
[Configuring the Forcepoint Email Security module on page 430](#)
[Configuring Forcepoint DLP Email Gateway on page 431](#)
[Configuring the integration agent on page 431](#)
[Configuring the analytics engine on page 432](#)

Related tasks

- [Adding Forcepoint DLP system modules on page 410](#)
[Configuring the protector on page 24](#)
[Configuring the Forcepoint DLP management server on page 413](#)
[Configuring a supplemental Forcepoint DLP server on page 414](#)
[Configuring the fingerprint repository on page 414](#)
[Configuring the endpoint server on page 416](#)
[Configuring the crawler on page 417](#)
[Configuring the forensics repository on page 417](#)
[Configuring the policy engine on page 418](#)
[Configuring the OCR server on page 419](#)
[Configuring protector services on page 432](#)

Configuring the Forcepoint DLP management server

When you install Forcepoint DLP, the Forcepoint DLP management server is installed on the Windows server that hosts all Forcepoint management components.

The Forcepoint DLP management server is the heart of the system. It provides the core data loss technology, analyzing traffic on your network and applying policies to incidents. All other modules register and synchronize with the management server.

- If the management server FQDN must change, run the Modify action on the installer, then re-register all agents.
- The management server cannot be deleted, but its name and description can be changed.

To edit the Forcepoint DLP management server module () , click its entry on the System Modules page.

The following information is displayed, but cannot be changed:

- The Type of module.
- The FQDN (fully qualified domain name) given to the module when it was installed.
- The module Version.

To update the module, optionally edit the following fields:

- 1) Enter a new **Name** for the management server if desired (up to 128 characters).
- 2) Enter a new **Description** for the management server (up to 4000 characters).
- 3) Click **OK** to save your changes and return to the System Modules page.

The management server includes many other components: a primary fingerprint repository, endpoint server, crawler, forensics repository, and policy engine. To configure any of these components, expand the management server node on the System Modules screen and click a component.

For configuration instructions for these components, see:

- [Configuring the fingerprint repository](#)
- [Configuring the endpoint server](#)
- [Configuring the crawler](#)
- [Configuring the forensics repository](#)
- [Configuring the policy engine](#)

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Configuring the endpoint server](#) on page 416

[Configuring the crawler](#) on page 417

[Configuring the policy engine](#) on page 418

[Configuring the forensics repository](#) on page 417

Configuring a supplemental Forcepoint DLP server

Supplemental Forcepoint DLP servers include a secondary fingerprint repository, endpoint server, crawler, policy engine, and OCR server.

The following information is displayed, but cannot be changed:

- The Type of module.
- The FQDN (fully qualified domain name) given to the module when it was installed.
- The module Version.

To update the module, optionally edit the following fields:

- 1) Enter a new **Name** for the Forcepoint DLP server if desired (up to 128 characters).
- 2) Enter a new **Description** for the Forcepoint DLP server (up to 4000 characters).
- 3) Click **OK** to save your changes and return to the System Modules page.

To configure components on a supplemental server, expand the supplemental server node and click the component of interest. See:

- *Configuring the fingerprint repository*
- *Configuring the endpoint server*
- *Configuring the crawler*
- *Configuring the policy engine*
- *Configuring the OCR server*

Although you cannot delete the management server, you can delete a supplemental Forcepoint DLP server.

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Configuring the endpoint server](#) on page 416

[Configuring the crawler](#) on page 417

[Configuring the policy engine](#) on page 418

[Configuring the OCR server](#) on page 419

Configuring the fingerprint repository

The primary Forcepoint DLP fingerprint repository is stored on the management server. The primary repository creates secondary repositories on protector, Content Gateway, and Forcepoint DLP server instances, and on any other module with a policy engine. These contain structured (database) fingerprints and are updated frequently to remain current. File fingerprints are not stored in the secondary repository, because they are transmitted in real time.

**Important**

Forcepoint does not save or back up your data in the fingerprinting process. The primary fingerprint repository only saves partial hashes of fingerprinted data, in order to detect them in future transactions. For your own protection, make sure you have a backup system in place.

To configure the selected repository:

Steps

- 1) Enter the **Name** of the module.
- 2) Enter a **Description** of the module (up to 4000 characters).
- 3) Continue with one of the following:
 - *Primary Fingerprint Repository*
 - *Secondary Fingerprint Repository*

Related tasks

[Primary Fingerprint Repository](#) on page 415

[Secondary Fingerprint Repository](#) on page 415

Primary Fingerprint Repository

Under Tuning Performance:

Steps

- 1) Select the **Maximum disk space** allocated for use by the fingerprint repository, in megabytes (50,000 MB, by default).
- 2) Select the **Maximum cache size** for the fingerprint repository to use to cache fingerprints in memory, in megabytes (512 MB, by default).
- 3) Click **OK** to save your changes and return to the System Modules page.

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.

Steps

- 1) In the Repository Selection section, use the options under Detect fingerprints from to indicate where fingerprint detection should be performed:
 - Select **the repository installed on** to perform detection on a remote repository, then select the server where the repository resides. This is typically the primary repository on the management server, but it can be any repository. Forcepoint recommends selecting a repository in the same LAN as this one. When the primary repository is selected, administrators never have to perform synchronization. The primary repository is always up to date with the most recent fingerprints.
 - Select **this local repository** to have detection performed locally. When this option is selected, performance tuning options are enabled. Synchronization occurs only when this repository does not have the most up-to-date fingerprints.

- 2) If the local repository is selected, under Tuning Performance, select the **Maximum cache size** (maximum amount of memory) allocated for the fingerprint repository, in megabytes.

- 3) Indicate whether there are periods when the secondary repository should not be updated.
 - By default, secondary repositories check for updates from the primary **Continuously** (every 30 seconds). This ensures the secondary repository machine always has the latest fingerprints.
 - To exclude a certain time period from this I/O activity, select **Continuously except between** and specify the blackout time period—for example: peak business hours.

During this period, the secondary repository will *not* check with the primary for updates. (Times are assumed to be in the database repository zone.)

Limiting I/O can improve fingerprinting performance, but accuracy can be affected, because the latest fingerprints may not be used.

- 4) Click **OK** to save your changes and return to the System Modules page.

Configuring the endpoint server

The endpoint server is the server component of Forcepoint DLP Endpoint. Endpoint servers receive incidents from, and send configuration settings to, endpoint clients.

To configure the endpoint server, select it on the System Modules page and complete the fields as follows:

- 1) Select or clear the **Enabled** option to enable or disable the module.

- 2) Optionally enter a new, descriptive **Name** for the module (up to 128 characters).

- 3) Optionally enter a helpful **Description** of the module (up to 4000 characters).

- 4) Enter the **FQDN** of the module. This is required when the module is deployed outside of the company network.

- 5) Click **OK** to save your changes and return to the System Modules page.

The page also displays the module type and hostname, which cannot be changed.

Related tasks

- [Adding an endpoint profile](#) on page 447
- [Configuring endpoint settings](#) on page 357

Configuring the crawler

The crawler is the agent that performs fingerprint and discovery scans. There can be multiple crawlers in a Forcepoint DLP deployment.

To configure a crawler, select it on the System Modules screen and complete the fields as follows:

- 1) Enter the **Name** of the module (up to 128 characters).
- 2) Enter a **Description** of the module (up to 4000 characters).
- 3) Click **OK** to save your changes and return to the System Modules page. The page also displays the module type and FQDN, which cannot be changed.

Related concepts

- [File fingerprinting](#) on page 200
- [Database fingerprinting](#) on page 217
- [Scheduling network discovery tasks](#) on page 297

Related tasks

- [Scheduling endpoint discovery tasks](#) on page 333

Configuring the forensics repository

The forensics repository contains complete information about transactions monitored by Forcepoint DLP. For SMTP transactions, for instance, the repository stores the original email message. For other channels, the system translates transactions into EML.

The forensics repository is different from the incident database, in that the former contains raw transactions, while the latter 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:

- 1) Enter the **Name** of the module (up to 128 characters).
- 2) Enter a **Description** of the module (up to 4000 characters).
- 3) Use the **Forensics path** field to enter the complete path to use for hosting the forensics repository. By default, it's stored in the \Forensics subdirectory under the Forcepoint DLP installation path.
- 4) Under Log on as, specify how the system connects to the forensics path:
 - Select **Local account** to log on as a local user (primarily used when the path is local).

- Select **This account** to log on with specific user credentials, then enter the user name and password to use. Domain is optional.
- 5) Set the maximum disk space to use for **Network forensics** (100 MB minimum; 50000 MB, by default). When the maximum is reached, the oldest records are moved to the archive folder to free space.
 - 6) Select the maximum disk space to use for **Mobile forensics** (100 MB minimum; 20000 MB, by default). When the maximum is reached, the oldest records are deleted to free space.
 - 7) Click **OK** to save your changes and return to the System Modules page.

The page also displays the module type and FQDN, which cannot be changed, as well as a sum of the total disk space allocated for the forensics repository.

Related concepts

[Forcepoint DLP databases](#) on page 8

Related tasks

[Setting preferences for data loss prevention reports](#) on page 350

Configuring the policy engine

The policy engine is responsible for parsing data and using analytics to compare it to the rules in Forcepoint DLP policies. There can be multiple policy engines in a deployment to manage high transaction volumes.



Tip

To balance the load between policy engines, click Load Balancing in the System Modules toolbar. Refer to *Balancing the load* for more information.

Policy engines reside on the:

- Management server
- Supplemental Forcepoint DLP servers
- Protectors
- Content Gateway machines
- Forcepoint Email Security machines

To configure a policy engine instances, select it on the System Modules screen, then use the edit page to update the following fields:

- 1) Select or clear **Enabled** to enable or disable the module in your deployment.
- 2) Enter a **Description** of the module (up to 4000 characters).
- 3) Supplemental Forcepoint DLP servers include an OCR server capable of intercepting textual images in many languages.
Select **Enable OCR by** to enable optical character recognition, then select an OCR server from the drop-down list.

- OCR is disabled by default.
- For best performance, select the OCR server that is in closest proximity to the policy engine.
- If the server is not installed, this option is not configurable. See *Configuring the OCR server* for more information.

4) Click **OK** to save your changes and return to the System Modules page.

The page also displays the module type, name, and FQDN, which cannot be changed.

Related tasks

[Balancing the load](#) on page 441

[Configuring the OCR server](#) on page 419

Configuring the OCR server

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 policy attribute to configure for optical character recognition (OCR). If sensitive text is found, the image is blocked or permitted according to the active policies.

The server can also be used to locate sensitive text in images during network discovery.

This feature does not support either handwriting or images containing text that is skewed more than 10 degrees.

To use OCR, install a supplemental Forcepoint DLP server; the OCR server is automatically included in supplemental Forcepoint DLP server installations.

To enable OCR analysis in your network:

- 1)** Navigate to the **Settings > Deployment > System Modules** page in the Data Security module of the Security Manager and edit the policy engine on each server or agent that will receive traffic that you want analyzed.
- 2)** In each Edit window, select **Enable OCR by** and indicate which OCR server (supplemental Forcepoint DLP server) to use to extract text from images.

When OCR is enabled, images of the following types are sent to that OCR server for text extraction:

- JPEG_2000_JP2_File - JPEG-2000 JP2 File Format Syntax (ISO/IEC 15444-1) (.jp2, .j2k, .pgx)
- 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 Forcepoint DLP extractor, not the OCR server. Should the system fail to extract text from a PDF, it is forwarded to the OCR server.



Tip

To specify a PDF type that should always be routed to the OCR server, edit the **extractor.config.xml** file as described in this [knowledge base article](#).

Images embedded in Microsoft Office documents are sent to the OCR server for text extraction.

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)

Use the System Modules page to configure the languages to analyze and to fine-tune the module's accuracy profile to optimize performance.

View OCR server status on the **Main > Status > System Health** page.

Related concepts

[Monitoring system health](#) on page 30

Related tasks

[Adding or editing an OCR server](#) on page 420

Adding or editing an OCR server

To add or edit an OCR server:

- 1) Enter a **Description** of the module (up to 4000 characters).
- 2) Under Accuracy, indicate your tolerance for speed versus accuracy.
 - Select **Fast** if you have a high volume of images (the load level on your OCR server will be large), and 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 may sacrifice accuracy.
 - Select **Accurate** if you have a small number of images (the load level on your OCR server will be small). 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.
 - Select **Balanced** (default) for a balance between accuracy and speed.
- 3) Some languages are included with Forcepoint DLP (see *Languages included with Forcepoint DLP (no language pack required)*)
 - Image analysis can be time consuming. Select fewer languages to optimize performance.
 - False positives (unintended matches) are more likely to occur when multiple languages are selected. For this reason, exercise caution when selecting the languages to enforce.
 - Click **OK** to save your changes and return to the System Modules page.

The page also displays the module type, name, and FQDN, which cannot be changed.

Related concepts

[Languages included with Forcepoint DLP \(no language pack required\) on page 422](#)

Languages included with Forcepoint DLP (no language pack required)

Afrikaans	Albanian	Arabic
Aymara	Basque	Bemba
Blackfoot	Brazilian	Breton
Bugotu	Bulgarian	Byelorussian
Catalan	Chamorro	Chechen
Chinese (Simplified)	Chinese (Traditional)	Corsican
Croatian	Crow	Czech
Danish	Dutch	English
Eskimo	Esperanto	Estonian
Faroese	Fijian	Finnish
French	Frisian	Friulian
Gaelic (Irish)	Gaelic (Scottish)	Galician
Ganda (Luganda)	German	Greek
Guarani	Hani	Hawaiian
Hebrew	Hungarian	Icelandic
Ido	Indonesian	Interlingua
Italian	Japanese	Kabardian
Kasub	Kawa	Kikuyu
Kongo	Korean	Kpelle
Kurdish	Latin	Latvian
Lithuanian	Luba	Luxembourgish
Macedonian	Malagasy	Malay
Malinke	Maltese	Maori
Mayan	Miao	Minangkabau
Mohawk	Moldavian	Nahuatl
Norwegian	Nyanja	Occidental
Ojibway	Papiamento	Pidgin English
Polish	Portuguese	Provencal
Quechua	Rhaetic	Romanian
Romany	Rundi	Russian
Rwanda	Sami	Sami (Lule)
Sami (Northern)	Sami (Southern)	Samoan
Sardinian	Serbian	Serbian (Latin)
Shona	Sioux	Slovak
Slovenian	Somali	Sorbian (Wend)
Sotho	Spanish	Sundanese
Swahili	Swazi	Swedish
Tagalog	Tahitian	Thai
Tinpo	Tongan	Tswana (Chuana)

- Tun
- Vietnamese
- Wolof
- Zulu

- Turkish
- Visayan
- Xhosa

- Ukrainian
- Welsh
- Zapotec

Configuring the protector

Forcepoint DLP provides several options for email DLP:

- The protector can act as an MTA to prevent data loss over email.
- The protector MTA can be combined with Forcepoint DLP Email Gateway to offer a combination of on-premises and cloud-based data protection.
- Forcepoint Email Security can act as an MTA, instead of the protector. Enforcement over the web channel (Web DLP) also has several options:
 - The protector can monitor and report on web traffic.
 - Use the Web Content Gateway appliance included with Forcepoint DLP Network.
 - Use Forcepoint Web Security, instead of the protector
 - Provide web DLP via a third-party proxy via ICAP.

In deployments that use the protector for email DLP, web DLP, or both, configure the protector via the **Settings > Deployment > System Modules** page in the Data Security module of the Security Manager.

Select a protector node in the list to open the Edit Protector page, which includes 4 tabs:

- *Edit Protector: General tab*
- *Edit Protector: Networking tab*
- *Edit Protector: Local Networks tab*
- *Edit Protector: Services tab*



Tip

The protector can also be configured via its command-line interface (CLI). See the Deployment & Installation Center for details.

Protectors include an ICAP server, policy engine, and secondary fingerprint repository. To configure these components on the protector, expand the protector node on the System Modules page and click the component. See:

- *Configuring the fingerprint repository*
- *Configuring the policy engine*
- *Configuring ICAP*

Related concepts

[Edit Protector: Services tab on page 426](#)

[Configuring ICAP on page 427](#)

Related tasks

- [Edit Protector: General tab](#) on page 424
- [Edit Protector: Networking tab](#) on page 424
- [Edit Protector: Local Networks tab](#) on page 426
- [Configuring the fingerprint repository](#) on page 414
- [Configuring the policy engine](#) on page 418

Edit Protector: General tab

The most common protector topologies are as follows:

- HTTP and SMTP in monitoring mode
- SMTP in MTA mode

Regardless of topology, use the General tab to make sure that the protector is enabled and that **Collect protector statistics** is selected.

- 1) Select or clear the **Enabled** option to enable or disable this protector.
- 2) Optionally update the **Name** of the protector.
- 3) Enter a **Description** for the protector.

The page also displays the following information, which cannot be changed:

- The hostname of the machine hosting the protector
- The IP address of the machine hosting the protector
- The version of this module

Edit Protector: Networking tab

Use the Networking tab to set protector networking properties:

Steps

- 1) Enter the IP address for the **Default gateway**, in the format 123.45.67.8. The default gateway's IP address should be from the same subnet as eth0.
- 2) Select an **Interface** to which packets for this route will be sent.
- 3) To add a DNS server to the **DNS servers** list, enter its IP address and click **Add**.
- 4) (Optional) To add a suffix to the **DNS suffixes** list, enter the suffix and click **Add**. The domain suffix is used by the resolver to help resolve names that are not fully qualified.
- 5) Review the **Connection mode**.

In SPAN/Mirror Port, the protector can only monitor the traffic and cannot interfere with it. In this mode, the protector connects to a switch/TAP port that relays all traffic traversing the network to the protector for analysis.

- 6) The protector can use 3 types of network interfaces: Management, Monitoring, and Network. To configure the protector's interfaces, click the name of the interface, then see *Interface configuration in SPAN/Mirror Port mode*.
- 7) Select **Enable VLAN support** if the monitored traffic contains VLAN tagging.

Next steps

If you are using HTTP in monitoring mode, make the following selections:

- 1) Set **Default Gateway** to the outbound gateway.
- 2) Edit the network interface **br0** as follows:
 - a) Set the Link Speed to one of the following: **10Mb/s**, **100 Mb/s**, **1000Mb/s**, or Auto.
 - b) Set the Duplex Mode to one of the following: **Half**, **Full**, or **Auto**.

The name of the bridge is shown, but cannot be edited.

Related tasks

[Interface configuration in SPAN/Mirror Port mode on page 425](#)

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.

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.

Steps

- 1) Select the **Interface name**.
- 2) Set the interface operation Mode to either **Network** or **Monitoring**.
- 3) Enter the **Interface IP address**.
If Monitoring mode is selected this is not displayed; there is no need for an IP address for eth1 in Monitoring mode.
- 4) Set the interface Status to **Up** or **Down**. The status is learned from the protector but can be forced manually via this option.
- 5) Enter the **Subnet mask** for the interface.
- 6) Set the Link speed to: **10Mb/s**, **100 Mb/s**, **1000Mb/s**, or **Automatic**.
- 7) Set the Duplex mode to: **Half**, **Full**, or **Automatic**.

Edit Protector: Local Networks tab

Specify the traffic the protector will monitor on 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, regardless of whether a specific direction (inbound or outbound) is configured elsewhere. This may drastically increase the load on the system and the system may collect unnecessary traffic.

- **Include specific networks** (default). After selecting this option:

- 1) Click **Add** to define the networks.
- 2) Enter the network address and subnet mask.

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: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

- When using this option, be sure that all of 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” when considering inbound/ outbound/internal directives for the different channels.

If you are using HTTP and SMTP in monitoring mode or SMTP in MTA mode, be sure to select **Include specific networks**.

- Add all the internal networks for all sites.
- Consider the mail servers and mail relays part of the internal network; this list is used to identify the direction of the traffic.

Click **OK** to apply the settings.

Edit Protector: Services tab

Use the Services tab to set protector services properties.

All services that have been configured for the protector are listed. The page shows whether each is enabled or disabled, its ports, a direction (inbound, outbound, or internal), and a description.

Click any service name to modify its settings. Click **New** to add a service.

Each protector can have only one service per port. One service can be removed from a port and a different one can be added, but no 2 services can run on the same port.

When the protector works in blocking mode, setting the direction is very important—in SMTP 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* for details on configuring protector services. The channels that can be configured are:

- *Protector: Configuring SMTP*
- *Protector: Configuring HTTP*
- *Protector: Configuring FTP*

- [Protector: Configuring plain text](#)

Related tasks

- [Configuring protector services](#) on page 432
[Protector: Configuring SMTP](#) on page 433
[Protector: Configuring HTTP](#) on page 436
[Protector: Configuring FTP](#) on page 438
[Protector: Configuring plain text](#) on page 439

Configuring ICAP

The protector supports Internet Content Adaptation Protocol (ICAP), and can be integration points for third-party solutions that support ICAP, such as some web proxies.

To configure an ICAP server for the protector, select the ICAP server on the System Modules screen. The Edit ICAP window is displayed.

There are 3 tabs in the Edit ICAP window:

- [Edit ICAP: General tab](#)
- [Edit ICAP: HTTP tab](#)
- [Edit ICAP: FTP tab](#)

Related tasks

- [Edit ICAP: General tab](#) on page 427
[Edit ICAP: HTTP tab](#) on page 428
[Edit ICAP: FTP tab](#) on page 428

Edit ICAP: General tab

Use the General tab of the Edit ICAP page to configure the module name, description, and basic behavior.

Steps

- 1) Select or clear **Enabled** to enable or disable this module.
- 2) Enter the module **Name**.
- 3) Enter a **Description** of the module.
- 4) 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 (for example, 1333,1334).

- 5) Under Allow connection to this ICAP Server from the following IP addresses, select whether this ICAP server should allow connections from **All IP addresses** or **Selected IP addresses**.

For the selected IP addresses option, enter an IP address to allow, then click **Add**. Repeat this process to allow additional IP addresses.

The page also displays the module type, which cannot be changed.

Edit ICAP: HTTP tab

Use the HTTP tab of the Edit ICAP page to review how HTTP traffic is handled:

Steps

- 1) Review the module's deployment Mode.

Monitoring mode monitors HTTP traffic, but does not block it.

- 2) Under When an unspecified error occurs, review the action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed.

Permit traffic allows HTTP traffic to continue unprotected.

- 3) Select the **Minimum transaction size** to monitor, in bytes.

Edit ICAP: FTP tab

Use the FTP tab of the Edit ICAP page to review how FTP traffic is handled:

Steps

- 1) Review the module's deployment Mode.

Monitoring mode monitors FTP traffic, but does not block it.

- 2) Under When an unspecified error occurs, review the action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed.

Permit traffic allows FTP traffic to continue unprotected.

- 3) Select the **Minimum transaction size** to monitor, in bytes.

Configuring the Web Content Gateway module

There are two Web Content Gateway module options available for Forcepoint DLP.

- The one included with Forcepoint DLP Network provides DLP over the web channel including encrypted SSL content. This core Forcepoint DLP component permits the use of custom policies, fingerprinting, and more.
- The one included in Forcepoint Web Security provides SSL decryption, URL categorization, content security, web policy enforcement, and more. In this deployment mode, the gateway is limited to the web DLP quick policies.

When either Web Content Gateway option registers with the management server, the Web Content Gateway module appears on the **Settings > Deployment > System Modules** page.

To configure the Web Content Gateway module, select it on the System Modules page. The Edit Content Gateway page opens with the General tab selected. See *Edit Content Gateway: General tab*.

Note that Web Content Gateway modules include a policy engine and secondary fingerprint repository. To configure these components for a Web Content Gateway module, expand the module on the System Modules screen and click the component. See:

- *Configuring the fingerprint repository*
- *Configuring the policy engine*

Related concepts

[Edit Content Gateway: General tab](#) on page 429

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Configuring the policy engine](#) on page 418

Edit Content Gateway: General tab

Use the General tab of the Edit Content Gateway page to update the module **Description** (up to 4000 characters), as needed.

The tab also displays the following information, which cannot be changed:

- The module Type
- The module Name
- The FQDN (fully-qualified domain name) of the machine on which the module was installed
- The module Version

Continue with *Edit Content Gateway: HTTP/HTTPS tab*.

Related tasks

[Edit Content Gateway: HTTP/HTTPS tab](#) on page 429

Edit Content Gateway: HTTP/HTTPS tab

Use the HTTP/HTTPS tab of the Edit Content Gateway page to configure HTTP and HTTPS monitoring and blocking behavior for the module.

- 1) Select the deployment Mode for the module:
 - Select **Monitoring** to monitor HTTP and HTTPS traffic but not block it.
 - Select **Blocking** to deny HTTP and HTTPS actions that breach policy.
- 2) Select the action to take **When an unspecified error occurs** during data analysis and traffic cannot be analyzed:
 - Select **Permit traffic** to allow HTTP and HTTPS traffic routed through the Content Gateway to continue unprotected.
 - Select **Block traffic** to stop all HTTP and HTTPS traffic through the gateway until the problem is resolved.

- 3) Set the **Minimum transaction size** for the system to monitor, in bytes.
- 4) Select **Display default violation message** to show a default message in the user's browser whenever a URL violation is detected.
Click the link to view the message.
- 5) Use the **Redirect to URL** field to specify the URL to which to redirect users when they try to access a website that violates policy.

Continue with *Edit Content Gateway: FTP tab*.

Related tasks

[Edit Content Gateway: FTP tab](#) on page 430

Edit Content Gateway: FTP tab

Use the FTP tab of the Edit Content Gateway page to configure FTP monitoring and blocking behavior for the module.

Steps

- 1) Select the deployment Mode for the module:
 - Select **Monitoring** to monitor FTP traffic but not block it.
 - Select **Blocking** to deny FTP actions that breach policy.
- 2) Select the action to take **When an unspecified error occurs** during data analysis and traffic cannot be analyzed:
 - Select **Permit traffic** to allow FTP traffic routed through the Content Gateway to continue unprotected.
 - Select **Block traffic** to stop all FTP traffic through the gateway until the problem is resolved.
- 3) Set the **Minimum transaction size** for the system to monitor, in bytes.

Configuring the Forcepoint Email Security module

The Forcepoint Email Security module resides on a V Series appliance. It filters inbound, outbound, and internal email messages for spam and viruses, and uses Forcepoint DLP to analyze content.

Forcepoint Email Security is automatically registered with the management server when you enter its subscription key in the Forcepoint Security Manager. Registration

occurs when you enter this key for your first Forcepoint Email Security appliance. The key is propagated for all subsequent Forcepoint Email Security appliances.



Important

To complete the registration, be sure to click **Deploy** in the Data Security module of the Security Manager.

When registration is successful, you can see an Email Security module on the **Settings > Deployment > System Modules** page in the Data Security module of the Security Manager. Select the module to configure its description.

The configuration page also shows the following information, which cannot be changed:

- The module Type
- The module Name
- The FQDN (fully-qualified domain name) of the machine on which the module was installed
- The module Version

Email Security modules include a policy engine and secondary fingerprint repository. To configure these components, expand the Email Security module on the System Modules page and click the component. See:

- *Configuring the fingerprint repository*
- *Configuring the policy engine*

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Configuring the policy engine](#) on page 418

Configuring Forcepoint DLP Email Gateway

Forcepoint DLP Email Gateway is a virtual appliance for the Microsoft Azure cloud infrastructure that allows an organization to protect data being sent through Exchange Online email. Like other modules, it includes a policy engine and fingerprint repository.

For information on installing and deploying Forcepoint DLP Email Gateway, refer to [Installing Forcepoint Email Security in Microsoft Azure](#).

To configure the module, click the module node on the **Settings > Deployment > System Modules** page in the Data Security module of the Forcepoint Security Manager.

The only field that can be updated is the module description.

The configuration page also shows the following information, which cannot be changed:

- The module Type
- The module Name
- The module Deployment location (Cloud)
- The FQDN (fully-qualified domain name) of the machine on which the module was installed
- The module Version

Configuring the integration agent

The integration agent allows third-party products to send data to Forcepoint DLP for analysis. It is embedded in third-party installers and communicates with Forcepoint DLP via a C-based API. (The Integration agent does not support discovery transactions.)

To change the module name and description, select the module node on the **Settings > Deployment > System Modules** page in the Data Security module of the Forcepoint Security Manager.

The configuration page also shows the following information, which cannot be changed:

- The module Type
- The FQDN (fully-qualified domain name) of the machine on which the module was installed
- The module Version
- *Configuring the fingerprint repository*
- *Configuring the policy engine*

Related tasks

[Configuring the fingerprint repository](#) on page 414

[Configuring the policy engine](#) on page 418

Configuring the analytics engine

An analytics engine is used to calculate incident risk, rank it with similar activity, and assign it a risk score. To use this feature, you must first install the analytics engine on a 64-bit Linux machine. (See the [Forcepoint DLP Installation Guide](#) for instructions.)

To configure the agent, select its node on the **Settings > Deployment > System Modules** page in the Data Security module of the Security Manager.

Optionally update the module Name and Description.

The configuration page also shows the following information, which cannot be changed:

- The module Type
- The FQDN (fully-qualified domain name) of the machine on which the module was installed
- The module Version

Configuring protector services

There are several services that the protector can monitor. To configure the services:

- 1) Go to the **Settings > Deployment > System Modules** page in the Data Security module of the Forcepoint Security Manager.
- 2) Select the protector.
- 3) On the Protector Details page, select the **Services** tab.
- 4) Click the service you want to configure:
 - SMTP (see *Protector: Configuring SMTP*)
 - HTTP (see *Protector: Configuring HTTP*)
 - FTP (see *Protector: Configuring FTP*)
 - Plain text (see *Protector: Configuring plain text*)

Related tasks

- [Configuring the policy engine](#) on page 418
[Protector: Configuring SMTP](#) on page 433
[Protector: Configuring HTTP](#) on page 436
[Protector: Configuring FTP](#) on page 438
[Protector: Configuring plain text](#) on page 439

Protector: Configuring SMTP

Selecting SMTP on the Protector Details page opens the Protector Service Details window, which may include up to 5 tabs, depending on the protector mode (monitoring or MTA).

The Details window opens to the General tab, which displays the service type at the top of the pane.

Steps

- 1) Select or clear **Enabled** to enable or disable the SMTP service.
- 2) Enter or update the service **Name** and **Description**.
- 3) Enter the **Ports** to monitor, separated with commas (for example, 25, 1333).
- 4) Select **Intelligent protocol discovery** to have the system match data from unknown ports to this SMTP service. If enabled, the protector tries to parse the transaction regardless of the port number. (This has an effect on protector performance.)
- 5) Select a protector Mode:
 - In **Monitoring** mode, Forcepoint DLP monitors and analyzes a copy of all traffic but does not enable policies to block transactions.
 - In **Mail Transfer Agent (MTA)** mode, the protector acts as an MTA. Configure mail servers and clients to forward mail to the protector.

When the protector functions as an MTA, be sure to limit the networks it monitors in order to prevent the protector from becoming an open relay.

Continue with *Protector SMTP service: Traffic Filter tab*.

Related tasks

- [Protector SMTP service: Traffic Filter tab](#) on page 433

Protector SMTP service: Traffic Filter tab

Use the Traffic Filter tab to configure protector SMTP monitoring:

Steps

- 1) Under Transaction Size, select the **Minimum transaction size** to monitor, in bytes.

2) Under Direction:

- Select **Inbound** to monitor incoming email traffic.
- Select **Outbound** to monitor outgoing email traffic.



Important

If you are using HTTP in active bridge mode or monitoring mode, be sure to set the Direction mode as **Outbound only**.

- Select **Internal** to monitor internal email traffic.

3) Under Source's Network, select **Enable filter to enable the source's network filter.** This tells Forcepoint DLP to watch for messages sent from specific networks and not analyze those messages.

Enter the network IP address and subnet mask that should not be analyzed, then click **Add**. Repeat this process for each network address to skip.

Continue with *Protector SMTP service: SMTP Filter tab*.

Related tasks

[Protector SMTP service: SMTP Filter tab](#) on page 434

Protector SMTP service: SMTP Filter tab

Use the SMTP filter tab to configure SMTP monitoring by domain, direction, and source email address.

Steps

1) Under Direction, select **Enable filter to enable the SMTP filter.**

2) Under Internal email domains, enter the name of an internal domain to monitor, then click **Add.**
Do this for each internal email domain that you want to monitor.

3) Under Direction:

- Select **Inbound** to monitor incoming email traffic.
- Select **Outbound** to monitor outgoing email traffic.
- Select **Internal** to monitor internal email traffic.



Important

If you do not select a direction, only rules governing outbound traffic are applied.

4) Under Source's Email Address, select **Enable filter 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 **Add**. Repeat this process for each email address you want to skip.

5) Do one of the following:

- If you selected monitoring mode on the General tab, click **OK** to save your changes and return to the Protector Details page.
- If you selected MTA mode, continue with *Protector SMTP service: Mail Transfer Agent (MTA) tab*.

Related tasks

[Protector SMTP service: Mail Transfer Agent \(MTA\) tab](#) on page 435

Protector SMTP service: Mail Transfer Agent (MTA) tab

Use the Mail Transfer Agent (MTA) tab to configure MTA settings for the protector.

Steps

1) Under Operation Mode, select one of the following:

- Select **Monitoring** to monitor SMTP traffic only.
- Select **Blocking** to block SMTP traffic that breaches policy.

2) Select the option to take when an unspecified error occurs:

- Select **Permit traffic** to allow all SMTP traffic to go through if an unspecified error occurs during data analysis, and traffic cannot be analyzed.
- Select **Block traffic** to block all SMTP traffic in the event of an unknown error.

3) Under SMTP Settings, specify an **SMTP HELO name** (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.

4) Select **Set next hop MTA** (also known as the Smart Host) to provide the IP address or hostname and port of the mail server or gateway to which the protector should forward traffic after analysis.

5) Set the **Maximum message size** for email (33 MB, by default).

6) Specify the **Network address** and **Subnet mask** for each network that has permission to send email via the protector's SMTP service, then click **Add**.

This is necessary to prevent the protector from being used as a mail relay.

7) Under Email Settings, select **Add the following footer...**, then enter footer text to append to all email messages processed by the protector.

8) Select **Send notifications...** to send notifications when there is a problem with email, then enter the email addresses to which the notifications should be sent.

Continue with *Protector SMTP service: Encryption & Bypass tab*.

Related tasks

[Protector SMTP service: Encryption & Bypass tab](#) on page 436

Protector SMTP service: Encryption & Bypass tab

Use the Encryption & Bypass tab to configure how the protector handles encrypted messages and messages flagged for bypass.

Steps

- 1) Select **Enable redirection gateway** to have encrypted or flagged email bypass content analysis, then enter the IP address and port number of the redirection gateway to which those messages should be sent.
- 2) Under Encryption, select **Verify that at least one of the following conditions is met** to have the protector verify that a condition before sending email to the redirection gateway, then:
 - Select '**Subject**' contains **Encryption Flag** to prompt the protector to look for a specific string, or flag, in the Subject field of the message, then enter the string.
In the event that a policy specifies that certain content should be encrypted, this flag is automatically added to the Subject field.
 - Select **X-header Field Name** to prompt the protector to look for a specific x- header field, then enter the field string.
If a user clicks **Encrypt** in Outlook or similar applications, an x-header is added to the message.
- 3) Under Bypass, select **Verify that at least one of the following conditions is met** to prompt the protector to verify condition before sending email to the redirection gateway, then:
 - Select '**Subject**' contains **Bypass Flag** to prompt the protector to look for a specific string, or flag, in the Subject field of the message, then enter the string.
 - Select **X-header Field Name** to prompt the protector to look for a specific x- header field, then enter the field string.
- 4) Click **OK** to save your changes and return to the Protector Details page.

Protector: Configuring HTTP

To configure the protector's HTTP service, click **HTTP** on the Services tab of the Protector Details page. The Protector Service Details window opens to the General tab, which displays the service type at the top of the pane.

Steps

- 1) Select or clear **Enabled** to enable or disable the HTTP service.
- 2) Enter or update the service **Name** and **Description**.
- 3) Enter the **Ports** to monitor, separated with commas (for example, 80,8080).

- 4) Select **Intelligent protocol discovery** to have the system 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.)

Continue with *Protector HTTP service: Traffic Filter tab*.

Related tasks

[Protector HTTP service: Traffic Filter tab on page 437](#)

Protector HTTP service: Traffic Filter tab

Use the Traffic Filter tab to configure protector HTTP monitoring.

If you are using HTTP and SMTP in active bridge mode or monitoring mode, be sure to set the Direction mode to outgoing *only*!

Steps

- 1) Under Transaction Size, select the **Minimum transaction size** to monitor, in bytes.
- 2) Under Direction:
- 3) Under Source's Network, select **Enable filter** to enable the source's network filter. This tells the system to watch for transactions sent from specific networks and not analyze those transactions.
 - Select **Inbound** to monitor incoming HTTP traffic.
 - Select **Outbound** to monitor outgoing HTTP traffic.
 - Select **Internal** to monitor internal HTTP traffic.

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.

Continue with *Protector HTTP service: HTTP Filter tab*.

Related tasks

[Protector HTTP service: HTTP Filter tab on page 437](#)

Protector HTTP service: HTTP Filter tab

Use the HTTP Filter tab to specify domains that should be excluded from analysis.

Steps

- 1) Select **Exclude destination domains** to exclude certain domains from analysis.
- 2) Enter each domain to exclude, then click **Add**.

To remove a domain from the exclusion list, select the domain and click **Remove**.

3) Do one of the following:

- If you have configured all of the tabs available in the Protector Service Details window, click **OK** to save your changes and return to the Protector Details page.
- If the Advanced tab is displayed, continue with *Protector HTTP service: Advanced tab*.

Related tasks

[Protector HTTP service: Advanced tab](#) on page 438

Protector HTTP service: Advanced tab

Steps

- 1)** Under Operation mode, select the mode to use for HTTP traffic:
 - Select **Monitoring** to monitor HTTP traffic only.
 - Select **Blocking** to block HTTP traffic that breaches policy.
- 2)** Under Policy violation, select **Display default message** to show a 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.
- 3)** Select **Redirect to URL** to send the browser to an alternate URL when a URL is blocked due to a policy violation, then enter the URL to which to redirect traffic.
- 4)** Select which option to use when an unspecified error occurs:
 - Select **Permit traffic** to allow HTTP traffic to continue unprotected when an unspecified error occurs during data analysis and traffic cannot be analyzed.
 - Select **Block traffic** to stop all HTTP traffic when an unspecified error occurs until the problem is resolved.
- 5)** Select **Display default message** to show a 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.
- 6)** Select **Redirect to URL** to send the browser to an alternate URL when a URL is blocked due to an unspecified error, then enter the URL to which to redirect traffic.
- 7)** Click **OK** to save your changes and return to the Protector Details page.

Protector: Configuring FTP

Selecting FTP on the Protector Details page opens the Protector Service Details window. The window opens to the General tab, which displays the service type at the top of the pane.

Steps

- 1)** Select or clear **Enabled** to enable or disable the FTP service.

- 2) Enter or update the service **Name** and **Description**.
- 3) Enter the **Ports** ports to monitor, separated with commas (for example, 20,2121).
- 4) Select **Intelligent protocol discovery** to have the system 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.)

Next steps

Continue with *Protector FTP service: Traffic Filter tab*.

Related tasks

[Protector FTP service: Traffic Filter tab](#) on page 439

Protector FTP service: Traffic Filter tab

Use the Traffic Filter tab to configure FTP monitoring.

Steps

- 1) Under Transaction Size, select the **Minimum transaction size** to monitor, in bytes.
- 2) Under Direction:
 - Select **Inbound** to monitor incoming FTP traffic.
 - Select **Outbound** to monitor outgoing FTP traffic.
 - Select **Internal** to monitor internal FTP traffic.
- 3) Under Source's Network, select **Enable filter** 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.
- 4) Click **OK** to save your changes and return to the Protector Details page.

Protector: Configuring plain text

Selecting Plain text on the Protector Details page opens the Protector Service Details window. The window opens to the General tab, which displays the service type at the top of the pane.

Steps

- 1) Select or clear Enabled to enable or disable the plain text service.
- 2) Enter or update the service Name and Description.

- 3) Enter the Ports to monitor, separated with commas (for example, 22, 5222). Continue with *Protector plain text service: Traffic Filter tab*.

Related tasks

[Protector plain text service: Traffic Filter tab](#) on page 440

Protector plain text service: Traffic Filter tab

Use the Traffic Filter tab to configure telnet monitoring.

Steps

- 1) Under Transaction Size, enter the **Minimum transaction size** to monitor, in bytes.
- 2) Under Direction:
 - Select **Inbound** to monitor incoming telnet traffic.
 - Select **Outbound** to monitor outgoing telnet traffic.
 - Select **Internal** to monitor internal telnet traffic.
- 3) Under Source's Network, select **Enable filter** 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.
- 4) If the Protector Service Details window includes the Advanced tab, continue with *Protector plain text service: Advanced tab*.
Otherwise, click **OK** to save your changes and return to the Protector Details page.

Related tasks

[Protector plain text service: Advanced tab](#) on page 440

Protector plain text service: Advanced tab

Use the Advanced tab to configure characteristics of the data being processed.

Steps

- 1) Select **Stop processing connection if...** to stop processing the connection if the binary data that is detected reaches a certain size threshold, then select the **Binary character threshold**.
The threshold is the maximum size, in characters, of binary data to process. If the data detected exceeds this threshold, the connection is no longer processed.
- 2) Select a **Text delimiter** from the drop-down list: tab, space, semicolon, or other. If you select other, enter the character in the box provided.

- 3) Use the **Buffer interval** field to select the maximum amount of time to wait before forwarding content to the Forcepoint DLP server, in milliseconds.
- 4) Click **OK** to save your changes and return to the Protector Details page.

Removing Forcepoint DLP modules

To remove a Forcepoint DLP module permanently, open the module node on the Settings > Deployment > System Modules page in the Data Security module of the Forcepoint Security Manager and click **Remove**. Typically, modules only need to be removed if their host system has changed both IP address and hostname.

When a module IP address or hostname changes:

- In Forcepoint Web Security deployments, re-register the module in the Content Gateway manager.
- In Forcepoint Email Security deployments, re-register the module in the Email Security module in the Security Manager.
- For supplemental Forcepoint DLP servers, run the Forcepoint Security Installer in Modify mode to provide the new IP address and re-register the server.

See [Changing the management server IP address or name](#) for steps.

Do not use the Remove option to take modules out of service temporarily (for maintenance, for example). Instead, be sure to reroute traffic from those servers before taking them offline. Since the modules aren't sending transactions, they can remain registered.

Alternatively, a protector can be temporarily disabled to remove it from service. After re-enabling the protector or agent, click **Deploy** to return it to active service.

Balancing the load

A Forcepoint DLP deployment may include several policy engines. There is one on each Forcepoint DLP server, one on the protector, and one on the Content Gateway host (if applicable).

Policy engines are responsible for analyzing the data flowing through the network, comparing it to policies, and performing the remediation action, if any.

At times, a policy engine can become overloaded. The System Health page in the Data Security module of the Forcepoint Security Manager can provide information about the impact that traffic is having on performance.

Steps

- 1) Go to the **Main > Status > System Health** page.
- 2) Expand the relevant system module and select its policy engine.
- 3) Review the number of transactions being analyzed and the policy engine latency see *Monitoring system health*.

Next steps

To distribute the processing load between more evenly:

- 1) Go to the **Settings > Deployment > System Modules** page.
- 2) Click **Load Balancing** in the toolbar at the top of the content pane. 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.
- 3) To change the configuration, placing the load on different policy engines, click one or more of the services. See *Defining load balancing distribution*.



Note

As a best practice, do not distribute the load to the management server.

Related concepts

[Monitoring system health](#) on page 30

Related tasks

[Defining load balancing distribution](#) on page 442

Defining load balancing distribution

Double-click a service to configure which policy engine should analyze it.

The page shows:

- The name of the service
- The host responsible for the service:
 - Forcepoint DLP Server
 - Protector
 - Crawler
 - ICAP Server
 - Content Gateway
 - Cloud Email
 - Integration agent

To make configuration changes:

- 1) Under Analyzed by:
 - Select **All available policy engines** to open analysis for the selected service to all available policy engines. The policy engine on the protector is available for the protector only.
 - Select **Selected policy engines** to specify one or more policy engine instances to perform analysis for this service.

**Note**

You cannot balance the load with the management server.

- 2) Select **Apply these settings to all of this agent's services** to apply these settings to all of the selected agent's services without having to configure each manually.

Chapter 20

Configuring Endpoint Deployment

Contents

- Viewing and managing endpoint profiles on page 446
- Configuring encryption for removable media on page 453
- Selecting endpoint destination channels to monitor on page 456
- Bypassing endpoint clients on page 458
- Rearranging and deploying endpoint profiles on page 459
- Using the endpoint client software on page 460

Deploying endpoint client software for Forcepoint DLP requires a subscription to Forcepoint DLP Endpoint.

- Endpoint client software resides on an endpoint machine (such as a laptop or workstation). It monitors real-time traffic and applies security policies to applications and storage media, as well as data at rest. The client software allows administrators to analyze content on endpoint machines and block or monitor policy breaches (defined in endpoint profiles). Administrators can create policies that allow full content visibility without restricting device usage. When endpoint client software is installed, it attempts to connect to a Forcepoint DLP server to retrieve policies and profiles. As soon as its settings are deployed, the endpoint client starts running according to its profile settings.
- The endpoint server component is installed automatically on the management server and supplemental Forcepoint DLP servers. Endpoint servers receive incidents from, and send configuration settings to, endpoint clients.

The endpoint software deployment process includes the following basic steps:

- 1) Install the Forcepoint DLP management server.
- 2) Build a package for the endpoint client and deploy it on users' computers (desktop and laptop machines), as described in the endpoint documentation.
- 3) Add an endpoint profile in the Data Security module of the Forcepoint Security Manager, or use the default profile installed with the client package. See *Adding an endpoint profile* section and *Rearranging and deploying endpoint profiles* section.
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 to protect sensitive data. Each profile is deployed to selected endpoint clients.
- 4) Configure endpoint settings. See *Configuring endpoint settings* section.
- 5) Create endpoint resources. See *Endpoint Devices*, *Endpoint Applications* and *Endpoint Application Groups* sections.
- 6) Create or modify a rule for endpoint channels. See *Selecting endpoint destination channels to monitor* section.
- 7) Define the type of endpoint machines to monitor, and configure on- and off- network behavior. See *Custom Policy Wizard - Source* section.

8) Deploy endpoint configuration settings.

Once endpoint client software has been deployed and configuration and profile creation is complete, administrators can:

- Review the status of endpoint systems. See *Viewing endpoint status* section.
- Review incidents detected by endpoint software, and take action on them, such as editing the incident details, changing the severity of the incident, or escalating the incident to a manager. See *Viewing the incident list* section.

In special circumstances, monitoring and protection can be bypassed for an endpoint client. See *Bypassing endpoint clients* section, for more information on this capability.

For information on what end users see on their machine when endpoint software is installed, see the [Endpoint Solutions End User's Guide](#) on the Forcepoint Documentation page. This document can be distributed to end users, as needed.

Related concepts

[Endpoint Application Groups](#) on page 254

[Viewing the incident list](#) on page 69

Related tasks

[Adding an endpoint profile](#) on page 447

[Rearranging and deploying endpoint profiles](#) on page 459

[Configuring endpoint settings](#) on page 357

[Endpoint Devices](#) on page 252

[Endpoint Applications](#) on page 253

[Selecting endpoint destination channels to monitor](#) on page 456

[Custom Policy Wizard - Source](#) on page 164

[Viewing endpoint status](#) on page 33

[Bypassing endpoint clients](#) on page 458

Viewing and managing endpoint profiles

A default endpoint profile is automatically installed on the endpoint client. Additional profiles can be added, as needed.

To view a list of existing endpoint profiles, go to the **Settings > Deployment > Endpoint Profiles** page in the Data Security module of the Forcepoint Security Manager.

Use this page to:

- Add a new profile (see *Adding an endpoint profile* section).
- Delete an existing profile.
- Rearrange existing profiles (see *Rearranging and deploying endpoint profiles* section).
- Back up and restore encryption keys (see *Backing up encryption keys* section and *Restoring encryption keys* section).

Select a profile from the list to view or edit its properties.

Related tasks

- [Adding an endpoint profile](#) on page 447
- [Rearranging and deploying endpoint profiles](#) on page 459
- [Backing up encryption keys](#) on page 454
- [Restoring encryption keys](#) on page 454

Adding an endpoint profile

A default endpoint profile is automatically installed on the endpoint client. It is applied to all endpoint clients that have not been assigned another profile. The default profile cannot be deleted, but parts of it can be edited.

Define additional profiles, as needed.

- To create a new profile, click **New** in the toolbar at the top of the Endpoint page.
- To edit an existing profile, click a profile **Name** in the Endpoint Profile List.

The endpoint profile wizard opens to its General tab.

- 1) Enter a **Name** and **Description** for the profile.
- 2) Select or clear **Enabled** to enable or disable the profile in the endpoint profile list. If the profile is disabled, it is not deployed to any endpoint hosts.
- 3) By default, the profile is applied to all endpoints. To include or exclude specific endpoints in the profile, click **Edit**.
- 4) Select an endpoint category from the **Display** drop-down list. The Available List updates to show available endpoints in that category.

**Note**

When Directory Entries are selected, the Available List changes to show the default user directory location and the endpoints within it. With Active Directory, the Filter by field changes to a Find field.

- 5) To filter the available endpoints, enter text in the **Filter by** or **Find** field.
 - Click the Apply filter (funnel) icon to enable the filter.
 - Click the Clear filter (X) icon to remove the current filter.
 Wildcards are supported: 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, browse the list using the Next, Previous, First, and Last buttons.
- 6) To include a specific endpoint in this profile:
 - a) In the Selected List, select the **Include** tab.
 - b) In the Available List, select the endpoint.

**Tip**

Use the Shift or Ctrl key to select multiple endpoint hosts.

A maximum of 1500 elements (Include and Exclude) can be added. Use AD Groups or business units to add more endpoints to the profile.

- c) Click > to move the endpoint into the Selected List.

- 7) Click **OK**.

- 8) 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.

- 9) Click **OK**.

Related tasks

[Rearranging and deploying endpoint profiles on page 459](#)

Endpoint profile: Servers tab

The Servers tab of the endpoint profile wizard lists the endpoint servers installed in the system. Each Forcepoint DLP server includes an endpoint server.

Incidents are sent to servers defined as Primary. If multiple servers are defined as Primary, the system round robin endpoint traffic (clients send and receive data to and from all available servers in their list). If all primary servers fail, 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**

Endpoint profiles cannot be deployed if there are no active endpoint servers.

Also use the Servers tab to define the connection protocol between the endpoints and the endpoint servers.

Steps

- 1) 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.

- 2) Select a connection type from the drop-down list. The default type is **HTTPS**.

- 3) To use a proxy server for the connection, check the box and enter the proxy's IP address and port number.

Next steps

Continue with *Endpoint profile: Properties tab* section.

Related tasks

[Endpoint profile: Properties tab](#) on page 449

Endpoint profile: Properties tab

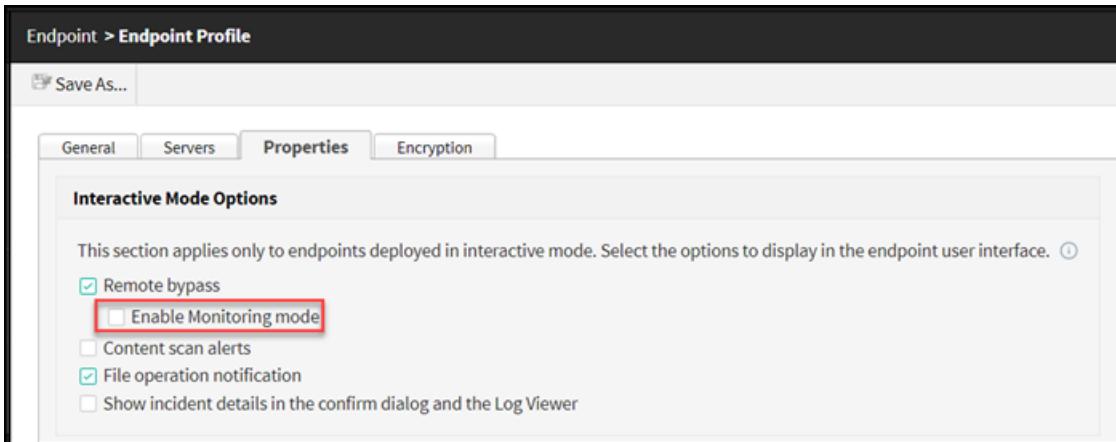
Use the Properties tab to enable user notifications, define message templates, and configure policy override settings.

Under Interactive Mode Options:

- Enable **Remote bypass** to allow end users that belong to this profile to disable the Forcepoint DLP Endpoint software on their machines.
This action requires a bypass code from the administrator. (See *Bypassing endpoint clients* section for additional information.)

- **Enable Monitoring mode** allows the endpoint to report incidents to the Forcepoint Security Manager (FSM) even when the endpoint is operating in bypass mode. This feature enables the security administrators to track the user activities when the endpoints are operating in bypass mode.

To enable monitoring in bypass mode, go to **Deployment > Endpoint > Profiles > Properties** tab, then select **Enable Monitoring mode** check box.



- Enable **Content scan alerts** to inform endpoint users when a violation is found during scanning. When this option is enabled, a popup message appears on the bottom of users' screens.



Note

Content scan alerts are not displayed when data is copied to removable media using a non-desktop environment, such as an SSH terminal connection.

- Enable **File operation notifications** to notify endpoint users when a violation is found during file operations. Depending on the application, file operations can include cut/copy, paste, file access, printing, LAN, encryption, and copying to removable media.
- Enable **Show incident details in the confirm dialog and the Log Viewer** to provide additional incident details to the endpoint user in the confirmation dialog message and the Log Viewer, allowing better investigation of sensitive data stored in a file. Details include policy name and number of matches.

Under Endpoint Message Template:

- Enable **Set message template** to change the default endpoint message template. Then select the template from the drop-down list.
 - Message templates are used for messages sent to the endpoint client, such as status details and alert messages. The templates are XML files, and are available in the endpoint profile in multiple languages.
 - Templates are stored in the `\custom\endpoint\msgFiles` subdirectory of the Forcepoint DLP installation directory. Modify them as required. Each message can include up to 256 characters. Any additional characters are truncated.

Template files can be cloned, renamed, and modified. When a new file is added to the `\msgFiles` folder, it appears as a template option in the Security Manager. See [Customizing Forcepoint DLP Endpoint client messages](#).

■ Set Regional location support:

- If regional location support is not enabled (check box is unselected), all endpoints in the profile receive the message template set as the default template.
- If regional location support is enabled (check box is selected) all endpoints in the selected profile display message template content in the operating system's language.

This is applicable only to the supported languages, which are: Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Simplified Chinese, and Traditional Chinese.

This also applies to custom templates stored in the `\custom\endpoint\msgFiles` subdirectory. Note that custom templates must follow a strict naming convention of `<language>-custom.xml`.

**Note**

The regional location support applies to Forcepoint F1E versions 21.07 and above. For previous endpoint versions, only the default language is displayed to the endpoint user, regardless of the endpoint operating system language setting.

Under Forcepoint Browser Extension:

- Set the mode of the endpoint extension of the supported browser. This applies to all endpoints that belong to the profile.
 - Select one of the following options from the Chrome extension mode drop-down list:
 - **Enabled:** Endpoint blocking alert will be shown and incidents will be created in the Security Manager.
 - **Monitoring only:** Endpoint blocking alert will not be shown. Transactions will be permitted, but incidents will be created in the Security Manager.
 - **Disabled:** The extension is inactive. Endpoint blocking alert will not be shown and incidents will not be created in the Security Manager.

Under Data Loss Prevention (DLP) Policy Settings:

- Enable **Disable blocking and encryption capabilities when policy violations are detected** to disable blocking and encryption of endpoint traffic. If a policy is specifically set up to block or encrypt content, the endpoint client overrides this setting and allows traffic.
Use this option, for example, if a policy is preventing a user from doing his job; the block can be overridden for a specific endpoint client.

Continue with *Endpoint profile: Encryption tab*.

Related tasks

[Bypassing endpoint clients](#) on page 458

[Endpoint profile: Encryption tab](#) on page 451

Endpoint profile: Encryption tab

Encryption allows trusted 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**

Encrypt with user password allows users to decrypt files from other machines (without the endpoint agent installed). See *Configuring encryption for removable media* section.

The strength of the encryption lies with the encryption algorithm and key length used by the algorithm. Forcepoint DLP 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 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.

Define an encryption key for each endpoint profile. Forcepoint DLP includes one default encryption key. Note that each endpoint client might have a different encryption key, based on its profile.

**Note**

The default profile contains a default key based on the password of the administrator that installed the Security Manager.

To create an encryption key:

- 1) Click **New**.
- 2) Enter a password and confirm it.

**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

- 3) Click **OK**.

- 4) Enter a description (for example “Encryption key for March”).

A code is generated based on the password, and the key appears on the Encryption tab with Pending status. The status is Pending until settings are deployed to the endpoint servers. While a key is awaiting deployment, additional keys cannot be generated.

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.

The following additional actions can be performed on this tab:

- To disable a decryption-only key, select the key and click **Disable**. Only decryption-only keys can be disabled. The change takes place only after all of the following:
 - 1) Settings are deployed.
 - 2) The endpoint receives the change.
 - 3) 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**. Only pending keys can be deleted.

Forcepoint recommends backing up the encryption keys every time you modify them. See *Backing up encryption keys* section.

Related tasks

- [Backing up encryption keys](#) on page 454
- [Restoring encryption keys](#) on page 454
- [Configuring encryption for removable media](#) on page 453

Configuring encryption for removable media

Forcepoint DLP Endpoint provides 2 methods for encrypting sensitive data that is being copied on removable media devices:

- **Encrypt with profile key** encrypts data 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 this option when configuring action plans for endpoint removable media. The action defaults to permitted on macOS endpoints, regardless of your action plan setting.
- **Encrypt with user password** encrypts data 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 this option when configuring action plans for endpoint removable media. The action defaults to permitted on macOS endpoints, regardless of your action plan setting.

Encrypt with profile key is the most secure method of protecting data on USB devices.

- The encryption key is provided when administrators create endpoint profiles for each user or group of users (see *Endpoint profile: Encryption tab* section).
- The endpoint client automatically decrypts files for users whose profiles have the relevant key. Users do not need to supply a password.
- Administrators can back up and restore encryption keys (see *Backing up encryption keys* section and *Restoring encryption keys* section).

Encrypt with user password allows 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 macOS machine.
- Users must run a Forcepoint 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 [Forcepoint DLP Endpoint User Guide](#) for more information.

**Note**

For CD/DVD media, Forcepoint DLP automatically promotes the “encrypt” action to “block files being transferred” if the destination is a CD writer.

Related tasks

- [Endpoint profile: Encryption tab](#) on page 451
- [Backing up encryption keys](#) on page 454
- [Restoring encryption keys](#) on page 454

Backing up encryption keys

When Forcepoint DLP is installed, it includes one default encryption key for use with endpoint profiles. Back up this key, and any subsequent keys that you create, to an external file. In the case of a system crash, this ensures that any files that were encrypted on endpoints using these keys can still be decrypted.

To back up encryption keys:

- 1) Go to the **Settings > Deployment > Endpoint Profiles** page in the Data Security module of the Security Manager.
- 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 that will host the backup file.
- 5) Click **Save**.
- 6) Click **Close**.

The file is saved in a proprietary format, which cannot be edited.

Related tasks

- [Endpoint profile: Encryption tab](#) on page 451
[Restoring encryption keys](#) on page 454

Restoring encryption keys

When encryption keys are restored from an external file, the keys are added to all endpoint profiles as disabled keys. For more information on managing keys in

endpoint profiles, see *Endpoint profile: Encryption tab* section. To restore encryption keys:

- 1) Go to the **Settings > Deployment > Endpoint Profiles** page in the Data Security module of the Security Manager.
- 2) Click the down arrow next to Encryption Keys, then click **Restore**.
- 3) Click **Browse** and navigate to the backup file location.
- 4) Click **Open**.
- 5) Click **OK**.

After restoring encryption keys:

- 1) Generate a new active key for each profile.
- 2) Enable the restored keys.

For example, profile A has key A1 and profile B has key B1. Then:

- 1) Back up the keys.
- 2) Restore the keys.
Both profiles now have 2 disabled keys (A1 and B1).
- 3) Create a new active key for each profile (for example, A2 and B2).
- 4) Enable the old (restored) keys for decryption only, to ensure that files that were encrypted before the restore process can still be decrypted. The result looks like this:

Profile A:

- Key A1 - Decrypt only
- Key B1 - Disabled
- Key A2 - Active
- Key A1 - Disabled
- Key B1 - Decrypt only
- Key B2 - 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) Repeat steps 1 and 2 for each endpoint profile.
- 4) Click **Deploy**.

Related tasks

- [Endpoint profile: Encryption tab on page 451](#)
- [Backing up encryption keys on page 454](#)

Selecting endpoint destination channels to monitor

Endpoint data sent to destination channels like removable media (including USB drives, CD/DVD, and other external drives), the Web, printers, and software applications can be monitored and analyzed.

To target a specific device, first add the device to the resources list:

- 1) Go to the **Main > Policy Management > Resources** page in the Data Security module of the Security Manager.
- 2) Click **Endpoint Devices**, then click **New** (see *Defining Resources* section).

To select endpoint destinations for monitoring in a policy:

- 1) Go to the **Main > Policy Management > DLP Policies** page in the Data Security module of the Security Manager.
- 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 from the following:
 - Select **Endpoint Email** to monitor outbound or internal email messages sent to specified destinations. By default, this option covers all endpoint destinations. To select destinations, click **Edit**.
The system analyzes all email messages sent from endpoint users, even if they send them to external webmail services such as Yahoo.



Important

For endpoint email to be analyzed, one or more internal email domains must be specified on the Email Domains tab of the **Settings > General > Endpoint** page.

For Windows, Forcepoint DLP can analyze endpoint email generated by Microsoft Outlook and IBM Notes. (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 2010, 2013, and 2016 but not the Windows 8 touch version. Forcepoint DLP supports IBM Notes versions 8.5.1, 8.5.2 FP4, 8.5.3, and 9.

For macOS, the system can analyze endpoint email generated by Outlook 2011, Outlook 2016, and Apple Mail.

Forcepoint DLP can detect incidents in S/MIME encrypted messages sent from Outlook 2013 (Windows), Outlook 2016 (Windows), and Outlook 2016 (Mac).

- 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. This traffic can be monitored when endpoint machines are outside the network.

The endpoint software intercepts HTTP(S) posts as they are being uploaded within the browser. (It does not monitor download requests.)

For a list of supported browser versions, see the [Certified Product Matrix](#).

Note that this destination is different from the 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 Google Chrome, Microsoft Edge, Firefox, Safari, and Opera.

If Linking Service is active, URL category information is included in the incident (see *Linking Service and mapping URL categories* section).

- Select **Endpoint printing** 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. The system cannot detect metadata in any document sent to a printing channel.
- Select **Endpoint application** to 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.

To prevent performance degradation when all activities on a rule's condition page are analyzed:

- 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 Google Chrome, Microsoft Edge, 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 article [Forcepoint DLP Endpoint Applications](#). Custom applications can also be defined.

- Select **Endpoint removable media** to 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.

Non-native CD/DVD blocking applies to CD, DVD, and Blue-ray read-write devices on Windows 8, Windows 10, Windows Server 2008 R2, and Windows Server 2012 endpoints.

On Windows, the system can also monitor unencrypted data being copied to Android devices through the Windows Portable Devices (WPD) protocol.

- Select **Endpoint LAN** to monitor or prevent sensitive data from being transferred via a LAN connection to a network drive or share on another computer. Forcepoint DLP administrators can:
 - Specify a list of IP addresses, hostnames, or networks that are allowed as a source or destination for LAN copy.
 - Intercept data copied from an endpoint client to a network share.
 - 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.

Destination channels are supported as follows:

- On Windows endpoints, all destination channels are supported.
The cut, copy, paste, file access, and download operations are not supported for cloud apps on Windows endpoints, however, when they are used through a Windows Store browser.
- On Mac endpoints, all destination channels except the clipboard channel are supported, with one exception: cloud apps are not supported.

Destination Channel	Windows	Mac
Web HTTP/HTTPS	✓	✓
Printing	✓	✓
Email	✓	✓
Removable media	✓	✓
LAN	✓	✓
Applications	✓	✓

For more information on monitoring destinations and protecting data on endpoints, see *Custom Policy Wizard - Destination* section.

Related concepts

[Defining Resources](#) on page 241

[Custom Policy Wizard - Destination](#) on page 165

[Linking Service and mapping URL categories](#) on page 368

Bypassing endpoint clients

It is possible to temporarily disable the endpoint client software on a user's computer. Disabling the endpoint software means that no content traffic on that endpoint is analyzed, and if there is a policy breach, content is not blocked.

To disable the endpoint client software:

Steps

- 1) Instruct the user on the endpoint to open the Forcepoint DLP Endpoint application and click **Disable**.
- 2) Have the user provide the bypass ID that appears in a dialog box.
- 3) In the Data Security module of the Security Manager, go to the **Main > Status > Endpoint Status** page.

- 4) Select the endpoint client to disable.
- 5) Click **Bypass Endpoint**.
- 6) In the Bypass Endpoint window, enter the bypass ID supplied by the end user.
- 7) Use the Activate bypass options to:
 - Select a specific amount of time, in minutes (5, 15, or 30) or hours (1, 2, 5, 10, or 24)
 - Set a specific end date and time for the bypass period
This option also allows administrators to specify a time zone.
- 8) Click **Generate Code**. A bypass code is displayed.
- 9) Send the bypass code to the user. It is applicable only to his or her endpoint client instance.
- 10) Tell the user to type the code into the dialog box from step 2 and click **Enter**.

Next steps

If the user is in stealth mode, this entire procedure can be done via the command line.

It is possible to customize or choose another language for the bypass message that appears on the client. See [Customizing Forcepoint DLP Endpoint client messages](#) for more details.

Rearranging and deploying 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.



Note

The default profile always appears at the bottom of the profile list. Its placement cannot be changed.

To rearrange profiles:

- 1) Go to the **Settings > Deployment > Endpoint Profiles** page in the Data Security module of the Security Manager.
- 2) Click **Rearrange Profiles** in the toolbar at the top of the content pane.
- 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 specified order.

After defining all of the settings for an endpoint profile and ensuring that the profiles are in the correct order, deploy the profile to the endpoint server and clients. To do this, click **Deploy** in the Data Security toolbar, then click **Yes** to confirm the deployment.

Related tasks

[Adding an endpoint profile](#) on page 447

Using the endpoint client software

Forcepoint DLP Endpoint client software is installed on users machines according to settings in the Forcepoint Endpoint Package Builder.

If the software was installed in interactive mode, an icon  appears on the endpoint machine's task bar.

For end-user instructions on using the endpoint client software, see the [Endpoint Solutions End User Guide](#).

Updating the endpoint client

Endpoint clients check for updates to policies and profile settings at specified intervals (see *Configuring endpoint settings* section).

End users can start an update check at any time by clicking **Update** on the Forcepoint DLP Endpoint screen.

Related tasks

[Configuring endpoint settings](#) on page 357

Chapter 21

Troubleshooting

Contents

- [Discovery](#) on page 461
- [Endpoint](#) on page 462
- [Fingerprinting](#) on page 463
- [Incidents](#) on page 465
- [Miscellaneous](#) on page 467
- [Performance](#) on page 469
- [Linking Service](#) on page 469
- [Online Help](#) on page 471
- [Technical Support](#) on page 471

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. Forcepoint engineers go to great pains—including continuing product refinement—to ensure easy software installation and maintenance, but problems can arise.

The topics in this chapter discuss the conditions, circumstances and resolution of issues that might occur in the use of Forcepoint DLP products, and includes contact information for Forcepoint Technical Support.

See the Related Topics box to choose a specific area to investigate.

Related concepts

- [Endpoint](#) on page 462
- [Fingerprinting](#) on page 463
- [Incidents](#) on page 465
- [Miscellaneous](#) on page 467
- [Performance](#) on page 469
- [Linking Service](#) on page 469

Related tasks

- [Discovery](#) on page 461

Discovery

If discovery is configured to discover sensitive files but the files are not found, the Forcepoint DLP server may not be on the domain, and may therefore not have rights to shares on other machines on the domain.

To alleviate this, do one of the following:

- Launch the Forcepoint Security Manager from a machine on the domain, logged in with an account that has rights to view shares.
- Add the Forcepoint DLP server to the domain.

Endpoint

This section lists problems related to endpoint deployments and their solutions. See the list below to choose a specific area of concern.

- *Endpoint Status page does not show user name*
- *Endpoint system icon does not display on the client computer*
- *Failed to deploy endpoint configuration*

Related concepts

[Failed to deploy endpoint configuration](#) on page 463

Related tasks

[Endpoint Status page does not show user name](#) on page 462

[Endpoint system icon does not display on the client computer](#) on page 463

Endpoint Status page does not show user name

The Forcepoint DLP Endpoint requires the Terminal Services service to be enabled and set to **Manual** to report user names back to the endpoint agent service.

- 1) On the endpoint machine for the missing user, open Windows Control Panel and select **Administrative Tools** > **Services**.
- 2) Locate the Terminal Services service. Double-click it.
- 3) Change the service's Startup type from **Disabled** or **Automatic** to **Manual**.
- 4) Click **OK**.
- 5) Reboot the computer.

The user name should properly be displayed in the list on the **Status** > **Endpoint Status** page once the endpoint has rebooted.

Endpoint system icon does not display on the client computer

The Forcepoint DLP Endpoint requires the Terminal Services service to be enabled and set to **Manual** to display its icon in the system tray.

- 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 Forcepoint DLP 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* section for instructions on how to perform these actions.

Related tasks

[Restoring encryption keys](#) on page 454

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 Forcepoint 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

More detailed error messages appear in the log files: `PAFastKeyPhrases.log` and `fprep.log`.

Related concepts

[Validation script timeout](#) on page 464

Related tasks

[File has no fingerprint](#) on page 464

[No connectivity to fingerprint database](#) on page 465

[Other fingerprinting errors](#) on page 465

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 module of the Forcepoint Security Manager.

Steps

- 1) Go to the **Main > Policy Management > Content Classifiers > File Fingerprinting** page
- 2) Select the classifier configured for the file, then click **Edit**.
- 3) Under Classifier Properties in the wizard's navigation pane, select **File Filtering**.
- 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* section for more information on validation scripts.

Related concepts

[Creating a validation script](#) on page 220

No connectivity to fingerprint database

Connectivity to a fingerprint repository has been lost. Fingerprint repositories are located on all Forcepoint DLP servers and protectors. Additional repositories can be located on network servers.

Steps

- 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 management server.
- 3) Check that credentials were supplied correctly.

Other fingerprinting errors

Steps

- 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 MB)
 - 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 list below to choose a specific area of concern.

- *Cannot clear ignored incidents from the Discovery Dashboard*
- *Traffic log shows audited events, but no incident is created*
- *Incident export lacks Discovery incidents*
- *NLP policy isn't being triggered, and events are undetected*

Related concepts

Traffic log shows audited events, but no incident is created on page 466

Incident export lacks Discovery incidents on page 467

NLP policy isn't being triggered, and events are undetected on page 467

Related tasks

[Cannot clear ignored incidents from the Discovery Dashboard](#) on page 466

Cannot clear ignored incidents from the Discovery Dashboard

Try deleting the incidents rather than ignoring them:

- 1) Go to the **Main > Reporting > Discovery > Incidents** page.
- 2) Locate the incident or incidents in question.
For multiple incidents, it may be helpful to use the display and column filters to show only the incidents that will be deleted.
- 3) Use the check boxes in the left-most column to select the incidents to delete.
- 4) In the toolbar at the top of the page, click **Workflow**, then select **Delete > Selected Incidents**.

This clears the incidents from the dashboard summary.

Traffic log shows audited events, but no incident is created

If there are any off-box components in the Forcepoint DLP installation and the Forcepoint DLP servers are not on the domain, then all passwords and user names must match for the service accounts being used for Forcepoint DLP.

For example, if the account Forcepoint with a password of “Pa55word123” is being used as the service account on the Forcepoint Security Manager, then the service account in use for any off-box Forcepoint DLP-installed components must also be Forcepoint 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 management server, which will prevent incidents from being recorded to the archive folder on the 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. Forcepoint 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 list below to choose a specific area of concern.

- [Failed user directory import](#)
- [Wrong default email address displays](#)
- [Error 400, bad request](#)
- [Invalid Monitoring Policy XML File](#)

Related concepts

[Error 400, bad request](#) on page 468

[Invalid Monitoring Policy XML File](#) on page 468

Related tasks

[Failed user directory import](#) on page 467

[Wrong default email address displays](#) on page 468

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. Take these steps in the Forcepoint Security Manager:

Steps

- 1) Go to the [Settings > General > User Directories](#) page.
- 2) Select the user directory and double-check its IP address and port settings.
Access problems typically occur when the IP address or port for the user directory server is incorrect.

- 3) If the problem is an incorrect CSV file structure, follow the instructions in *Importing user entries from a CSV file* section.

Related tasks

[Importing user entries from a CSV file](#) on page 384

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:

Steps

- 1) In the Forcepoint Data Security module of the Forcepoint Security Manager, select **Settings > Authorization > Administrators**.
- 2) Select the account 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.

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

If discovery and fingerprinting scans are slow, and third-party antivirus software is being used, configure the antivirus software to exclude the following directories from scanning on all Forcepoint DLP servers and management servers:

- `:\Program Files (x87)\Websense*.*`
- `:\Program Files\Microsoft SQL Server*.*`
- `:\Inetpub\mailroot*.*`
- `:\Inetpub\wwwroot*.*`
- `%TEMP%*.*`
- `%WINDIR%\Temp*.*`

See the antivirus software documentation for instructions. On non-management servers, such as Forcepoint DLP 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 antivirus software is not being used, contact Forcepoint Technical Support (see *Technical Support* section) for help on improving performance.

Related concepts

[Technical Support](#) on page 471

Linking Service

This section lists problems related to linking and the Linking Service and their solutions. See the list below to choose a specific area of concern.

- *Linking Service stops responding*
- *System alerts that Linking Service is not accessible*
- *Buttons in Forcepoint Security Manager tray return error*

Related concepts

[System alerts that Linking Service is not accessible](#) on page 470

[Buttons in Forcepoint Security Manager tray return error](#) on page 470

Related tasks

[Linking Service stops responding](#) on page 470

Linking Service stops responding

In the Forcepoint Data Security module of the Forcepoint Security Manager, take these steps:

Steps

- 1) Choose **Settings > General > Services Linking Service**.
- 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 Forcepoint software subscription includes both Forcepoint Web Security and Forcepoint DLP modules, the 2 security solutions are integrated. A system alert appears on the Dashboard in the Forcepoint Security Manager when the Linking Service is not accessible or has been disabled.

When the Linking Service is working:

- Forcepoint DLP software gains access to user data gathered by Forcepoint Web Security components.
- Forcepoint DLP software can access Master Database categorization information.

To configure the Linking Service, go to the **Settings > General > Services > Linking Service** page in the Forcepoint Data Security module of the Security Manager.

Buttons in Forcepoint Security Manager tray return error

If an error appears when clicking a module tab (Web, Data, Email, or Mobile) in the Forcepoint Security Manager, the administrator account used to log on may not have been granted permission to access the selected module.

To be able to access multiple Security Manager modules, an administrator must:

- Be added to the **Global Settings > General > Administrators** page
- Be given access to each module

The default administrator account, **admin**, has access to all modules.

Global Security Administrators can configure each administrator's level of access to the Security Manager.

Online Help

Click the Help icon in the Security Manager toolbar, then select **Explain This Page** 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, click **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 Forcepoint software and services is available 24 hours a day at www.forcepoint.com/support/. This includes:

- The latest release information
- The searchable Forcepoint 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 Help icon in the Security Manager toolbar, then select **Support Portal**.

Appendix A

Appendix A: How Do I

Contents

- [Archive my incident data?](#) on page 474
- [Configure a DLP policy?](#) on page 474
- [Define an exception?](#) on page 476
- [Filter incidents?](#) on page 476
- [Fingerprint data?](#) on page 477
- [Ignore sections of my document when fingerprinting?](#) on page 478
- [Fingerprint specific field combinations in a database table?](#) on page 480
- [Mitigate false positives in pattern or dictionary phrases?](#) on page 481
- [Move from monitor to protect?](#) on page 481

Use this selection of quick tips to get started with some of the most common Forcepoint DLP tasks and procedures.

- *Archive my incident data?*
- *Configure a DLP policy?*
- *Define an exception?*
- *Filter incidents?*
- *Fingerprint data?*
- *Ignore sections of my document when fingerprinting?*
- *Fingerprint specific field combinations in a database table?*
- *Mitigate false positives in pattern or dictionary phrases?*
- *Move from monitor to protect?*

Related concepts

[Configure a DLP policy?](#) on page 474

[Filter incidents?](#) on page 476

[Ignore sections of my document when fingerprinting?](#) on page 478

[Mitigate false positives in pattern or dictionary phrases?](#) on page 481

Related tasks

[Archive my incident data?](#) on page 474

[Define an exception?](#) on page 476

[Fingerprint data?](#) on page 477

[Fingerprint specific field combinations in a database table?](#) on page 480

[Move from monitor to protect?](#) on page 481

Archive my incident data?

To save older incident database partitions, archive them offline as follows:

- 1) In the Data Security module of the Forcepoint Security Manager, go to the **Settings > General > Archive Partitions** page.
- 2) Select one or more incident partitions.
- 3) Click **Archive** in the toolbar at the top of the content pane.
- 4) Review the list of partitions to be archived, adding comments as needed.
- 5) Click **OK** to continue.

For a deeper understanding of the archiving process (including restoring and deleting archives), see *Archiving incident partitions* section.

Related concepts

[Archiving incident partitions](#) on page 387

Configure a DLP policy?

The following sections explain on how to configure a DLP policy.

To add a predefined policy

Forcepoint DLP comes with a rich set of predefined policies that cover the requirements for a variety of regions and industries.

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > DLP Policies** page.
- 2) Under Custom Policies, select **Add predefined policy**.
- 3) Complete the Predefined Policy Wizard that appears. (See *Adding a predefined DLP or discovery policy* section.)
- 4) Click **Deploy**.

Related tasks

[Adding a predefined DLP or discovery policy](#) on page 151

To create a quick policy

If you are interested in web, email, or mobile DLP alone, configure a “quick policy.” This is the easiest way to get started with DLP for a single channel.

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > DLP Policies** page.
- 2) Under Quick Policies, select **Email DLP Policy**, **Web DLP Policy**, or **Mobile DLP Policy**.
- 3) Configure one or more attributes to identify the data to monitor and protect, then click **OK**. For instructions, see:
 - *Configuring the Email DLP Policy*
 - *Configuring the Web DLP Policy*
 - *Configuring the Mobile DLP Policy*
- 4) Click **Deploy**.

Related concepts

[Configuring the Web DLP Policy on page 133](#)

[Configuring the Mobile DLP Policy on page 143](#)

Related tasks

[Configuring the Email DLP Policy on page 125](#)

To create a custom policy

Administrators can create custom policies for multiple channels. Custom policies can include advanced conditions, and use complex features such as fingerprinting and machine learning.

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > DLP Policies** page.
- 2) Under Custom Policies, select **Add custom policy**.
- 3) Complete the wizard as described in *Creating Custom DLP Policies* section.
- 4) Click **Deploy**.

Related tasks

[Creating Custom DLP Policies on page 155](#)

Define an exception?

Most rules have exceptions. To add an exception to a rule:

Steps

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > DLP Policies** or **Discovery Policies > Manage Policies** page.
- 2) Expand a policy's tree view, so that its rules are displayed.
- 3) Do one of the following:
 - 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.
- 4) The exception begins empty—select the fields to edit. Unedited fields retain the same data as the rule.

Next steps

To review the process for using the exception wizard and obtain more information on adding (and rearranging) exceptions, see *Adding a new exception* section.

Related concepts

[Adding a new exception](#) on page 177

Filter incidents?

To filter incidents in a report, edit the report filters or apply column filters.

Editing report filters

To change the filters that are applied to a report:

Steps

- 1) Open the report.
- 2) Select **Manage Report > Edit Filter** in the report toolbar.
- 3) Select a filter from the Filter by list, then select **Enable filter**.

- 4) Configure the filter properties, if any.
For example, for the Action filter, indicate which actions to include in the report.
- 5) Repeat steps 3 and 4 for each filter that you want to apply.
- 6) Click **Run**.
- 7) To save the report for later use, select **Manage Report > Save As**.

Applying column filters

The incidents list is a table displaying all data loss prevention or discovery incidents. By default, incidents are sorted by time, but the table can be sorted by any of its columns (ascending or descending). You can also group by and filter by columns.

To filter incidents by columns in the incident list:

Steps

- 1) Click the down arrow button in a column header to see the sort and filter options available. These vary based on the column contents.
- 2) Select **Filter by this Column** to open a dialog box with options for filtering the column. For example:
 - To filter the Source column, select one or more users, computers, or domains to include or exclude.
 - To filter the Channel column, select one or more channels
- 3) Click **OK** to apply the filter.
 - The incident table is updated to show only rows that match the selected filter.
 - An icon appears next to the column header to show that a filter has been applied to that column.

Next steps

To clear a column filter, click the filter icon in the column header and select **Clear Column's Filter**.

Fingerprint data?

To fingerprint files and directories:

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Content Classifiers** page.
- 2) Select **File Fingerprinting**.
- 3) Click **New** in the toolbar at the top of the content pane, then select one of the following:
 - File System Fingerprinting
 - SharePoint Fingerprinting

- Domino Fingerprinting
- 4) The fingerprinting wizard opens and guides you through the process. For more information, see *File fingerprinting* section.
- 5) After completing the wizard, click **Run** to perform the scan.
- 6) Add the fingerprint classifier to a rule/policy when prompted.

To fingerprint a database, Salesforce site, or CSV file:

- 1) Go to the **Main > Policy Management > Content Classifiers** page.
- 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) The fingerprinting wizard opens and guides you through the process.
For more information and best practices, see *Database fingerprinting* section.
- 5) After completing the wizard, click **Run** to perform the scan.
- 6) Add the fingerprint classifier to a rule/policy when prompted.

Related concepts

[File fingerprinting](#) on page 200

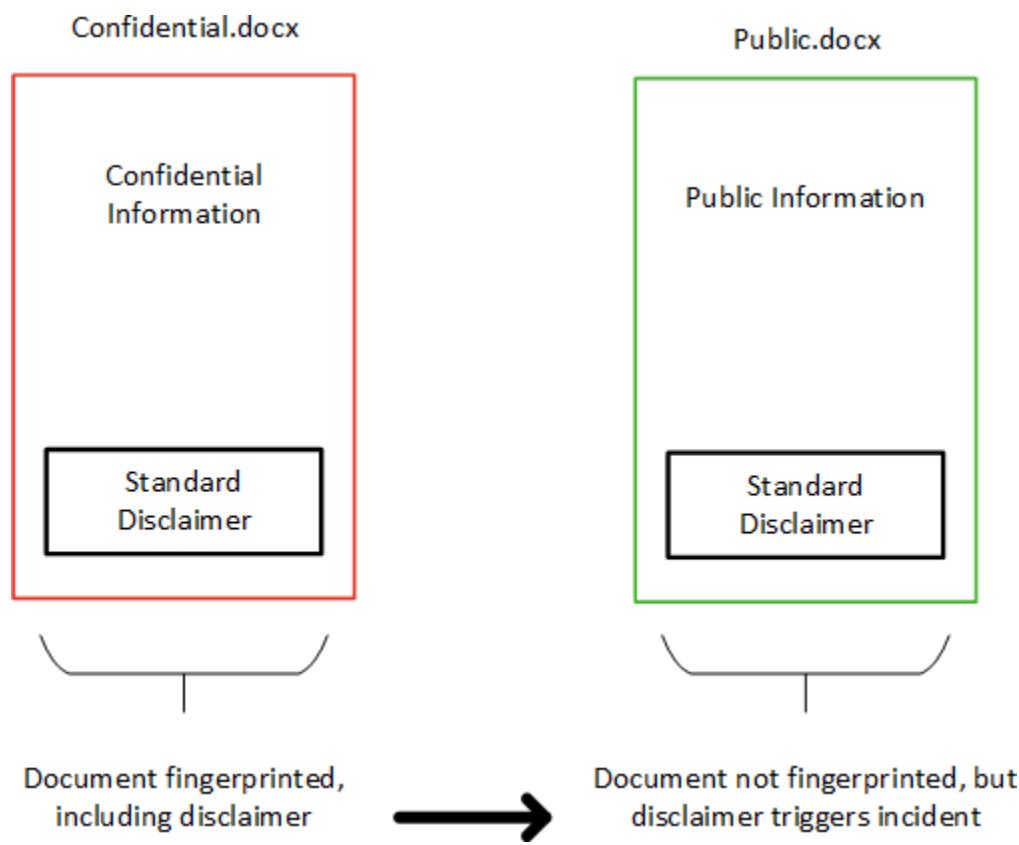
[Database fingerprinting](#) on page 217

Ignore sections of my document when fingerprinting?

File fingerprinting can identify both confidential or sensitive information to protect, and information to ignore.

For example, if all documents, both confidential and public, contain a standard copyright statement or disclaimer, the standard text can be identified as an “ignored section.”

- Text in an ignored section does not trigger policy violations.
- Ignored sections apply to all policies.



Without the ignored section, if a confidential document containing a disclaimer is fingerprinted, any documents that contain the disclaimer could result in an incident, creating many unintended matches.

- 1) Create a file containing only the text that fingerprinting should treat as an ignored section.
- 2) In the Data Security module of the Security Manager, go to the **Main > Content Classifiers > File Fingerprinting** page.
- 3) Click **New**, then choose the type of fingerprint to create: file system, SharePoint, or Domino.
- 4) On the General tab of the wizard, select **Ignored Section** for the Fingerprinting Mode.
- 5) On the **Scanned Files** or **Scanned Documents** page, click **Edit**.
- 6) In the left pane of the selector, highlight the file containing the text to ignore.
- 7) Click the right arrow to move the file into the Include list.
- 8) Click **OK**.
- 9) Continue through the wizard, and click **Finish** when done.
- 10) Run the fingerprint scan.

Fingerprint specific field combinations in a database table?

To fingerprint specific field combinations, first create a fingerprint classifier for the database table:

- 1) In the Data Security module of the Security Manager, go to the **Main > Policy Management > Content Classifiers** page.
- 2) Select **Database Fingerprinting**.
- 3) Click **New** in the toolbar at the top of the content pane, then select **Database Table Fingerprinting**.
- 4) Work through the wizard as described in *Creating a database fingerprint classifier* section. On the Field Selection page, select **Select up to 32 fields from a table**, then select the table name and the field combination to fingerprint.
- 5) Continue through the wizard, and click **Finish** when done.
- 6) Run the fingerprint scan.

Next, add the new fingerprint classifier to a rule. The same classifier can be added more than once, selecting a different combination of fields and different thresholds to match against.

- 1) Go to the **Main > Policy Management > DLP Policies > Manage Policies** page.
- 2) Select a rule, then click **Edit**.
- 3) Select **Condition** from the rule properties.
- 4) Click **Add**, then select **Fingerprint** from the drop-down list.
- 5) Select the content classifier to add, then define the field combination and threshold to use.
- 6) Click **OK**.
- 7) To add the same classifier again with a different field combination and threshold, repeat steps 4 - 6.
- 8) Set up condition relations for the classifiers using the **And**, **Or**, and **Customized** options. For more information on setting up conditions, see *Custom Policy Wizard Condition* section.

Related concepts

[Custom Policy Wizard - Condition](#) on page 156

Related tasks

[Creating a database fingerprint classifier](#) on page 225

Mitigate false positives in pattern or dictionary phrases?

One way to protect against false positives in a pattern or dictionary phrase is to exclude certain values that falsely match it. When creating the classifier, define a *Pattern to exclude* that lists 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?

Forcepoint recommends that administrators start by setting policies to apply to all sources and destinations of data with a permissive action. After monitoring the results, they can start to apply more restrictive actions.

To block SMTP traffic with the protector (explicit MTA):

- 1) In the Data Security module of the Security Manager, go to the **Settings > Deployment > System Modules** page and select the protector.
- 2) In the Edit Protector window, select the **Services** tab, then click the SMTP service.
- 3) In the Edit SMTP Service window, under the General tab, select **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) Adjust the configuration as needed, then click **OK**.
- 6) Click **Deploy**.

The protector must be integrated with a third-party proxy to enforce DLP policy on HTTP traffic.

Alternately, use the Web Content Gateway appliance with Forcepoint DLP Network Gateway or Forcepoint Web Security to block HTTP traffic.

Action plans

Action plans can also be configured to block incidents that contravene policy. In the Data Security module of the Security Manager, go to the **Main > Policy Management > Resources > Action Plans** page to configure action plans.

- Click an action plan in the list to update it. The action for each channel can be changed, if needed (quarantine for SMTP, block for HTTP via Web Content Gateway).

- Click **New** in the toolbar at the top of the page to create a new action plan. See *Action Plans* section, for more information.

Related concepts

[Action Plans on page 257](#)

