Contents

Topic 1
Overview ................................................................. 1
Forcepoint DLP basics ................................................. 2
Forcepoint DLP appliances .......................................... 3
Forcepoint DLP databases .......................................... 3
What can I protect? ..................................................... 4
Data classification .................................................... 5
Managing Forcepoint DLP ............................................ 6
DLP in Forcepoint Web Security and Forcepoint Email Security ........................................ 7

Topic 2
Navigating the System .................................................. 9
Main options ............................................................. 10
Settings options ............................................................ 12
Deploy button ............................................................. 13
Global and status icons ................................................ 14

Topic 3
Initial Setup ................................................................. 17
Entering a subscription key ............................................. 18
Defining general system settings and notifications ................. 19
Configuring system modules ......................................... 19
  Configuring the protector ........................................... 21

Topic 4
Viewing Status ........................................................... 23
Viewing the Dashboard ................................................. 23
Monitoring system health ............................................ 26
Viewing endpoint status .............................................. 29
  Changing table properties ......................................... 31
Viewing mobile device status ....................................... 32
Applying column filters .............................................. 33
Viewing deployment status .......................................... 34

Topic 5
Viewing Incidents and Reports ....................................... 35
The report catalog ....................................................... 36
  Editing a report ....................................................... 37
  Scheduling tasks ..................................................... 57
Viewing the incident list ............................................. 59
  Previewing incidents ............................................... 63
  Managing incident workflow .................................... 66
## Contents

- Remediating incidents ................................................................. 72
- Escalating incidents ................................................................. 74
- Managing incident reports .......................................................... 76
- Tuning policies ........................................................................... 80
- Data Loss Prevention reports ....................................................... 82
  - DLP dashboard .......................................................................... 84
  - Top violated policies ................................................................. 85
  - User risk summary (all incidents) ................................................ 85
  - User risk summary (data theft risk indicators) ............................... 86
  - Incident risk ranking ................................................................. 86
- My cases ....................................................................................... 90
- Violations by severity and action .................................................... 90
- Top sources and destinations .......................................................... 90
- Incident trends ............................................................................. 91
- Incident status ............................................................................. 91
- Incidents by geographical location .................................................. 92
- Mobile devices reports ................................................................. 94
  - Top violated mobile policies ........................................................ 94
  - Top synced messages .................................................................. 95
  - Mobile PII violations .................................................................. 95
  - Mobile credit card violations ....................................................... 95
- Discovery reports ......................................................................... 96
  - Discovery dashboard ................................................................... 98
  - Sensitive data reports ............................................................... 99

### Topic 6  Policies Overview ............................................................. 101

- What’s in a policy? ........................................................................ 103
- Viewing policies .......................................................................... 104
  - Editing a policy ........................................................................ 106
  - Update rules of current policy .................................................. 107
  - Update exceptions of current rule ............................................. 108
  - Update rules of multiple policies .............................................. 108
  - Update exceptions of multiple rules ....................................... 109
- Delete policies ............................................................................. 110
- Policy levels ............................................................................... 111

- Selecting items to include or exclude in a policy................................. 112

### Topic 7  Configuring the Email DLP Policy .................................. 117

- Configuring outbound and inbound email DLP attributes .................. 119
- Defining email DLP policy owners ............................................... 122
- Identifying email DLP trusted domains ......................................... 123

### Topic 8  Configuring the Web DLP Policy .................................... 125

- Configuring web DLP policy attributes ........................................ 126
## Selecting web DLP policy destinations ................................................. 130
## Defining web DLP policy owners ......................................................... 132

### Topic 9

**Configuring the Mobile DLP Policy** ....................................................... 133

- Configuring mobile DLP attributes .................................................. 134
- Mobile DLP attribute properties ...................................................... 135
- Defining policy owners ...................................................................... 137

### Topic 10

**Using Predefined DLP and Discovery Policies** ........................................ 139

- Adding a predefined DLP or discovery policy ....................................... 139
  - Welcome ......................................................................................... 140
  - Regions ......................................................................................... 140
  - Industries ....................................................................................... 140
  - Finish ............................................................................................ 140
  - Policy list ....................................................................................... 140
- Changing the selected DLP or discovery policies ..................................... 141
- Changing policy industry or region settings .......................................... 142

### Topic 11

**Creating Custom DLP Policies** ............................................................ 143

- Custom Policy Wizard - General ......................................................... 144
- Custom Policy Wizard - Condition ...................................................... 144
  - Viewing or editing conditions and thresholds .................................... 146
- Custom Policy Wizard - Severity and Action .......................................... 149
- Custom Policy Wizard - Source .......................................................... 152
- Custom Policy Wizard - Destination .................................................... 152
- Rule Wizard - Finish .......................................................................... 156
- Selecting a content classifier ............................................................... 156
  - Patterns & Phrases ........................................................................ 157
  - File Properties .............................................................................. 159
  - Fingerprint ..................................................................................... 160
  - Machine Learning ......................................................................... 161
  - Transaction Size ........................................................................... 161
  - Number of Email Attachments ......................................................... 162
  - Number of Email Destinations ......................................................... 162
- Managing rules ................................................................................... 162
- Managing exceptions ........................................................................... 163
  - Rearranging exceptions ................................................................ 164
  - Adding a new exception ................................................................ 164

### Topic 12

**Classifying Content** ........................................................................... 169

- Manually deleting fingerprinting classifiers .......................................... 172
- Details pane ....................................................................................... 173
  - Machine learning details .............................................................. 175
- Patterns & Phrases ............................................................................ 177
Contents

Adding or editing a regular expression classifier ......................... 179
Adding a key phrase classifier ........................................... 180
Adding a dictionary classifier ............................................ 181
File properties ..................................................................... 183
  Adding a file-type classifier ............................................. 183
  Adding a file-name classifier ........................................... 184
  Adding a file-size classifier ............................................. 184
Scripts ................................................................................. 185
  Editing a predefined script .............................................. 186
File fingerprinting ............................................................... 187
  File System Fingerprinting Wizard - General .................... 188
  File System Fingerprinting Wizard - Root Folder ............. 189
  File System Fingerprinting Wizard - Scanned Files .......... 190
  File System Fingerprinting Wizard - Scheduler ............... 190
  File System Fingerprinting Wizard - File Filtering .......... 190
  File System Fingerprinting Wizard - Export ................... 191
  File System Fingerprinting Wizard - Finish .................... 192
  SharePoint Fingerprinting Wizard - General .................... 192
  SharePoint Fingerprinting Wizard - Site Root .................. 193
  SharePoint Fingerprinting Wizard - Scanned Documents ..... 194
  SharePoint Fingerprinting Wizard - Scheduler ................ 194
  SharePoint Fingerprinting Wizard - File Filtering .......... 195
  SharePoint Fingerprinting Wizard - Export .................... 196
  SharePoint Fingerprinting Wizard - Finish .................... 196
  Domino Fingerprinting Wizard - General ....................... 197
  Domino Fingerprinting Wizard - Server ......................... 198
  Domino Fingerprinting Wizard - Scanned Documents ........ 198
  Domino Fingerprinting Wizard - Scheduler .................... 199
  Domino Fingerprinting Wizard - Document Filtering ........ 200
  Domino Fingerprinting Wizard - Attachment Filtering ..... 200
  Domino Fingerprinting Wizard - Export ......................... 201
  Domino Fingerprinting Wizard - Finish ......................... 202
Database fingerprinting ...................................................... 203
  Connecting to data sources ............................................ 204
  Preparing for database fingerprinting ......................... 205
  How matches are counted .............................................. 211
  Creating a database fingerprint classifier ....................... 212
  Database Fingerprinting Wizard - General .................... 213
  Database Fingerprinting Wizard - Data Source/Site .......... 213
  Database Fingerprinting Wizard - Field Selection .......... 215
  Database Fingerprinting Wizard - Scheduler .................. 217
  Database Fingerprinting Wizard - Fingerprinting Type .... 217
Performing database discovery ........................................... 268
Performing Exchange discovery ......................................... 268
Performing Outlook PST discovery ....................................... 269
Performing endpoint discovery ........................................... 270
Viewing discovery status .................................................. 270
Viewing discovery results .................................................. 271
Updating discovery ......................................................... 271
Configuring discovery incidents ......................................... 271
Copying or moving discovered files ..................................... 272
Preparing and running the remediation scripts ....................... 272

**Scheduling Discovery Tasks** ........................................ 275
Manually deleting discovery tasks ....................................... 278
Scheduling network discovery tasks .................................... 279
File System tasks ......................................................... 280
File System Discovery Task Wizard - Networks ....................... 281
File System Discovery Task Wizard - Scanned Folders ............... 281
File System Discovery Task Wizard - Scheduler ....................... 282
File System Discovery Task Wizard - Policies ......................... 283
File System Discovery Task Wizard - File Filtering .................... 283
File System Discovery Task Wizard - Advanced ....................... 284
File System Discovery Task Wizard - Finish ......................... 285
SharePoint tasks ............................................................ 285
SharePoint Discovery Task Wizard - Site Root ........................ 285
SharePoint Discovery Task Wizard - Scanned Documents ............ 286
SharePoint Discovery Task Wizard - Scheduler ....................... 286
SharePoint Discovery Task Wizard - Policies ......................... 287
SharePoint Discovery Task Wizard - File Filtering .................... 287
SharePoint Discovery Task Wizard - Advanced ....................... 288
SharePoint Discovery Task Wizard - Finish ......................... 288
Box tasks ................................................................. 288
Box Discovery Task Wizard - Permissions ............................. 289
Box Discovery Task Wizard - Scanned Accounts ..................... 290
Box Discovery Task Wizard - Scheduler ............................... 290
Box Discovery Task Wizard - Policies ................................ 291
Box Discovery Task Wizard - File Filtering .......................... 291
Box Discovery Task Wizard - Advanced .............................. 292
Box Discovery Task Wizard - Finish ................................ 292
Database tasks ............................................................. 293
Exchange tasks ............................................................. 297
Exchange Discovery Task Wizard - Exchange Servers (online) .... 297
Exchange Discovery Task Wizard - Mailboxes ......................... 298
Exchange Discovery Task Wizard - Scheduler ....................... 298
Exchange Discovery Task Wizard - Policies ........................................... 299
Exchange Discovery Task Wizard - Filtering ...................................... 299
Exchange Discovery Task Wizard - Advanced .................................... 300
Exchange Discovery Task Wizard - Finish ........................................ 300
Outlook PST tasks ............................................................................. 301
Outlook Discovery Task Wizard - Scanned Folder ............................... 301
Outlook Discovery Task Wizard - Scheduler ...................................... 301
Outlook Task Discovery Wizard - Policies ......................................... 302
Outlook Discovery Task Wizard - Filtering ....................................... 302
Outlook Discovery Task Wizard - Advanced ..................................... 303
Outlook Discovery Task Wizard - Finish .......................................... 304
Domino tasks .................................................................................. 304
Emailing discovery task status reports ............................................. 310
Scheduling endpoint discovery tasks ................................................. 311
Endpoint Discovery Task Wizard - Endpoints .................................... 311
Endpoint Discovery Task Wizard - Scheduler .................................... 311
Endpoint Discovery Task Wizard - Policies ...................................... 312
Endpoint Discovery Task Wizard - File Filtering ............................... 312
Endpoint Discovery Task Wizard - Advanced .................................. 313
Endpoint Discovery Task Wizard - Finish ........................................ 313

**Topic 16**

Viewing Forcepoint DLP Logs ......................................................... 315
The Forcepoint DLP traffic log ......................................................... 316
The Forcepoint DLP system log ....................................................... 319
The Forcepoint DLP audit log .......................................................... 320

**Topic 17**

General System Settings ............................................................... 323
Setting reporting preferences ......................................................... 324
  Setting general reporting preferences ........................................... 325
  Setting preferences for data loss prevention reports .................... 326
  Setting preferences for Incident Risk Ranking reports ............... 326
  Setting preferences for discovery reports .................................. 327
  Setting preferences for mobile incident reports ....................... 327
Back up the system ........................................................................ 328
  Scheduling backups .................................................................. 329
  Backup folder contents .............................................................. 330
  Restoring the system ................................................................. 330
Exporting incidents to a file .......................................................... 331
Configuring endpoint settings ......................................................... 333
  Endpoint settings: the Email Domains tab ................................. 334
  Endpoint settings: the Disk Space tab ...................................... 335
  Endpoint settings: the Advanced tab ....................................... 335
Mobile device settings ................................................................. 336
## Contents

- **Remediation** ................................................................. 338
- **Mail servers** ............................................................... 340
- **Alerts** ............................................................. 342
  - Setting up email properties ........................................ 342
- **Archive storage** ..................................................... 343
- **Services** ............................................................ 345
  - Configuring Linking Service ..................................... 345
  - Configuring Microsoft RMS ................................. 346
  - Configuring the CASB service ............................. 348
  - Configuring classification tagging ....................... 349
  - The RAP service ................................................ 350
  - Configuring the RAP service ............................. 350
- **Analytics** .......................................................... 351
  - Adding a high-risk resource .................................. 352
- **User directory settings** ........................................ 352
  - Adding or editing user directory server information ..... 353
  - Rearranging user directory servers ...................... 355
  - Importing users ................................................ 355
  - Importing user entries from a CSV file ............... 356
- **Archiving incident partitions** .................................. 359
  - Remote SQL Server machines ............................. 360
  - Archiving a partition ........................................ 361
  - Restoring a partition ........................................ 362
  - Deleting a partition ........................................ 362
  - Archive threshold ........................................... 363
- **Updating predefined policies and classifiers** ............. 363
  - Viewing your update history ................................ 364
  - Installing policy updates ................................. 365
  - Restoring policies to a previous version ............ 366
- **Entering subscription settings** ................................ 367
  - Subscription alerts ........................................... 367

### Topic 18
**Configuring Authorization** ............................................. 369

- Defining administrators ........................................... 369
  - Viewing administrators ..................................... 371
  - Editing administrators ..................................... 372
- Working with roles ................................................ 374
  - Adding a new role ............................................ 376
- Customizing your own administrator account settings .... 379

### Topic 19
**Managing Forcepoint DLP System Modules** ................. 381

- Adding Forcepoint DLP system modules ................ 382
- Configuring Forcepoint DLP system modules ........ 383
<table>
<thead>
<tr>
<th>Topic 20</th>
<th>Configuring Endpoint Deployment.</th>
<th>417</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring protector services.</td>
<td>405</td>
</tr>
<tr>
<td></td>
<td>Protector: Configuring SMTP.</td>
<td>406</td>
</tr>
<tr>
<td></td>
<td>Protector: Configuring HTTP.</td>
<td>409</td>
</tr>
<tr>
<td></td>
<td>Protector: Configuring FTP.</td>
<td>411</td>
</tr>
<tr>
<td></td>
<td>Protector: Configuring plain text</td>
<td>412</td>
</tr>
<tr>
<td></td>
<td>Removing Forcepoint DLP modules.</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>Balancing the load.</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>Defining load balancing distribution.</td>
<td>414</td>
</tr>
<tr>
<td></td>
<td>Viewing and managing endpoint profiles.</td>
<td>418</td>
</tr>
<tr>
<td></td>
<td>Adding an endpoint profile.</td>
<td>419</td>
</tr>
<tr>
<td></td>
<td>Endpoint profile: Servers tab.</td>
<td>420</td>
</tr>
<tr>
<td></td>
<td>Endpoint profile: Properties tab.</td>
<td>421</td>
</tr>
<tr>
<td></td>
<td>Endpoint profile: Encryption tab.</td>
<td>422</td>
</tr>
<tr>
<td></td>
<td>Configuring encryption for removable media.</td>
<td>424</td>
</tr>
<tr>
<td></td>
<td>Backing up encryption keys.</td>
<td>425</td>
</tr>
<tr>
<td></td>
<td>Restoring encryption keys.</td>
<td>425</td>
</tr>
<tr>
<td></td>
<td>Selecting endpoint destination channels to monitor.</td>
<td>427</td>
</tr>
<tr>
<td></td>
<td>Bypassing endpoint clients.</td>
<td>430</td>
</tr>
<tr>
<td></td>
<td>Rearranging and deploying endpoint profiles</td>
<td>431</td>
</tr>
<tr>
<td></td>
<td>Using the endpoint client software.</td>
<td>431</td>
</tr>
<tr>
<td>Topic 21</td>
<td>Troubleshooting</td>
<td>433</td>
</tr>
<tr>
<td></td>
<td>Discovery</td>
<td>433</td>
</tr>
<tr>
<td></td>
<td>Endpoint</td>
<td>434</td>
</tr>
<tr>
<td></td>
<td>Endpoint Status page does not show user name</td>
<td>434</td>
</tr>
</tbody>
</table>
Overview

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.

Note

Version 8.5 of Forcepoint DLP does not include the Forcepoint Web Security or Forcepoint Email Security modules.
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.

A mobile agent applies DLP policies to corporate email traffic that is synchronized to mobile devices using Microsoft Exchange ActiveSync.

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, protector, or a mobile agent 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.
- The mobile agent is a soft appliance that secures the type of email content synchronized to users’ mobile devices via Exchange ActiveSync when they connect to the network. This includes content in email messages, calendar events, and tasks.

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, page 353.

- 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*, page 382.

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

**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.

**Related topics:**

- *Classifying Content*, page 165
- *Defining Resources*, page 223
- *Remediation*, page 237
Overview

- **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.

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.
Overview

- Create customized scripts, dictionaries, file-types, regular expression patterns, and key phrases for specific (described) data. As a shortcut, edit a 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, page 165.

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 using the Data Security module of the Security Manager to work with Forcepoint DLP. For a more general overview of the Security Manager as a whole, as well as information about the settings that effect all modules of the Security Manager:

1. Click the Global Settings icon ( ) on the Security Manager toolbar.
2. Click the Help icon ( ), then select Help Contents.
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.

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.
Navigating the System

The Data Security module of the Forcepoint Security Manager is displayed in 2 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 2 sections:
  - **Main** has options for creating and fine-tuning policies, performing discovery, managing incidents, and viewing system status and logs. See *Main options*, page 10.
  - **Settings** has options for administrating the system; performing system maintenance; and configuring endpoint deployment, settings, modules, and roles. See *Settings options*, page 12.

---

**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*, page 23.
  - 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.

---

Related topics:

- *Deploy button*, page 13
- *Global and status icons*, page 14
In the image below, Status is selected in the navigation pane, and the Status > Dashboard page appears in the content pane.

Main options

Related topics:

- Viewing Incidents and Reports, page 35
- Creating Custom DLP Policies, page 141
- Creating Discovery Policies, page 255
- Scheduling Discovery Tasks, page 269
- Classifying Content, page 165
- Defining Resources, page 223
- Viewing Status, page 23
- Viewing Forcepoint DLP Logs, page 309

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.)
Navigating the System

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*, page 23.
- **System Health** helps administrators to monitor Forcepoint DLP performance. See *Monitoring system health*, page 26.
- **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*, page 29.
- **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*, page 29.

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*, page 310.
- **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*, page 313.
Navigating the System

- **Audit Log** displays a list of actions that administrators have performed in the system. See *The Forcepoint DLP audit log*, page 314.

## 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.

### 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.
- **Linking Service**: Make sure the connection to the Linking Service is intact, and configure how to use the URL categories and user names in Forcepoint DLP.
Navigating the System

- **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 system reminders about pending deployment.

Deployment

- **System Modules**: Manage system components such as Forcepoint DLP servers, fingerprint repositories, policy engines, 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
Navigating the System

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

Deployment 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 for tips on how to solve failed deployments.

Global and status icons

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

Severity and Incident Status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>High</td>
</tr>
<tr>
<td>🔴</td>
<td>Medium</td>
</tr>
<tr>
<td>🔴</td>
<td>Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔵</td>
<td>New</td>
</tr>
<tr>
<td>🔴</td>
<td>In Process</td>
</tr>
<tr>
<td>🔴</td>
<td>Closed</td>
</tr>
</tbody>
</table>
## System-wide

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="http://example.com/error-icon" alt="Error Icon" /></td>
<td>When a problem occurs, the Error icon is displayed at the top of the page with an explanation.</td>
</tr>
<tr>
<td><img src="http://example.com/success-icon" alt="Success Icon" /></td>
<td>When an update succeeds, the Success icon is displayed at the top of the page with a description of what has been done.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="http://example.com/information-icon" alt="Information Icon" /></td>
<td>Click the Information icon to get additional details.</td>
</tr>
<tr>
<td><img src="http://example.com/note-icon" alt="Note Icon" /></td>
<td>The Note icon marks additional, pertinent information displayed on a page to assist with configuration.</td>
</tr>
</tbody>
</table>
Initial Setup

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*, page 19.
2. Select and define attributes for the web DLP or email DLP policy. See:
   - *Configuring web DLP policy attributes*, page 124
   - *Configuring outbound and inbound email DLP attributes*, page 117
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*, page 18.
2. Define the general system settings, such as user directories and alerts, as well as notifications. See *Defining general system settings and notifications*, page 19.
3. Configure system modules (protector deployments only). See *Configuring system modules*, page 19.
4. Configure predefined policies. See *Adding a predefined DLP or discovery policy*, page 137.
5. To deploy all of the configured settings, click **Deploy** in the Data Security toolbar.
Entering a subscription key

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

1. Log on to the Security Manager. If the Data Security module is not displayed by default, click **Data** to open it.
   - If no subscription information has been provided, the subscription page appears automatically.
   - 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.
3. If the subscription is about to expire, a notice appears on this screen. Click **Update** to update the subscription.
   After an update, log off of the Security Manager and then log on again to see accurate information on the subscription screen.
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.
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:

- 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, page 346, and Adding or editing user directory server information, page 347.

- 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, page 336, and Setting up email properties, page 336.

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, page 251, and Adding a new message, page 252.

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.
Configuring the protector

Administrator Help | Forcepoint DLP | Version 8.5.x

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*, page 387
   b. *Edit Protector: Networking tab*, page 388
   c. *Edit Protector: Local Networks tab*, page 389
   d. *Edit Protector: Services tab*, page 390

---

**Note**

Refer to *Configuring Forcepoint DLP system modules*, page 377, for information on the default settings of system modules.
Viewing Status

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.

![Health Alert Summary]

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.

---

**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** 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.

● **Synchronized mobile devices** shows the number of mobile devices that have synchronized with the mobile agent in the last 24 hours (may be fewer than the number of registered devices).

### Data Loss Prevention Incidents

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Number of incidents that have been set to the most severe setting and should be handled immediately.</td>
</tr>
<tr>
<td>Medium</td>
<td>Number of incidents that have been set to the medium severity setting and should be handled soon.</td>
</tr>
<tr>
<td>Low</td>
<td>Number of incidents that have been set to the most lenient severity setting and should be handled.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Summary</td>
<td>Information about the server, including operating system and version, time zone, and free disk space.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The percentage of the CPU that is being used by the machine’s processes over the specified time frame.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The percentage of memory that is being used by the machine’s processes over the specified time frame.</td>
</tr>
</tbody>
</table>

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:
Viewing Status

- 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:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet loss and dropped transaction indication</td>
<td>Indicates the levels of packet loss and dropped transaction rates.</td>
</tr>
<tr>
<td>Number of events sent to analysis</td>
<td>The number of events sent for analysis by this protector in the specified time frame.</td>
</tr>
<tr>
<td>Load average</td>
<td>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.</td>
</tr>
<tr>
<td>Memory usage</td>
<td>The percentage of memory used by machine processes.</td>
</tr>
<tr>
<td>Total Throughput</td>
<td>Total amount of traffic (in KB per second) monitored by the protector. This includes both interesting and non-interesting sessions.</td>
</tr>
<tr>
<td>Data sent to analysis throughput</td>
<td>Total amount of traffic (in KB per second) sent for analysis by this protector.</td>
</tr>
</tbody>
</table>

- For the policy engine:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis status</td>
<td>Displays the request load on the policy engine for analysis by time period.</td>
</tr>
<tr>
<td>DLP—number of analyzed events</td>
<td>Number of DLP events analyzed by this policy engine in the specified time frame.</td>
</tr>
<tr>
<td>DLP—number of incidents</td>
<td>Number of DLP incidents detected by this policy engine in the specified time frame.</td>
</tr>
</tbody>
</table>
Viewing Status

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery—number of analyzed items</td>
<td>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.</td>
</tr>
<tr>
<td>Discovery—number of incidents</td>
<td>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.</td>
</tr>
</tbody>
</table>

- For the fingerprint repository:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database fingerprint repository synchronization</td>
<td>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.</td>
</tr>
<tr>
<td>Secondary database fingerprint repository synchronization trend</td>
<td>Shows how much database data was synchronized from the primary repository to this one over time, in KB.</td>
</tr>
<tr>
<td>Number of fingerprinted files</td>
<td>Displays the total number of files fingerprinted in the specified time frame.</td>
</tr>
<tr>
<td>Number of fingerprinted database cells</td>
<td>Displays the total number of database cells fingerprinted in the specified time frame.</td>
</tr>
</tbody>
</table>

- 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:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue load</td>
<td>Shows the load of OCR server queue during the selected time period.</td>
</tr>
<tr>
<td>Number of textual requests</td>
<td>Shows the total number of OCR requests containing textual data during the selected time period.</td>
</tr>
<tr>
<td>Number of requests</td>
<td>Shows the total number of requests made to the OCR server during the selected time period.</td>
</tr>
</tbody>
</table>
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)

### Chart Description

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average image size</td>
<td>Shows the average size of images (in bytes) that were handled by the OCR server during the selected time period.</td>
</tr>
<tr>
<td>Average processing time</td>
<td>Shows the average processing time (in milliseconds) of images that were handled by the OCR server during the selected time period.</td>
</tr>
</tbody>
</table>

Related topics:

- Configuring Endpoint Deployment, page 411
- Bypassing endpoint clients, page 424
Viewing Status

- 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 name is out of sync.

- 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, page 31.

There are also many options for filtering the data in the table. See Applying column filters, page 33.

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
  
Enter the hostname in the Find host field, then click Find.

- Temporarily disable the selected endpoint
  
Click Bypass Endpoint (see Bypassing endpoint clients, page 424).

- View and edit system settings for endpoint clients
  
Click Settings (see Configuring endpoint settings, page 327).

---

**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.
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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Installation Version</td>
<td>Version of the endpoint client software that is installed on the endpoint machine.</td>
</tr>
<tr>
<td>Client Status</td>
<td>Status of the endpoint client: enabled or disabled.</td>
</tr>
<tr>
<td>Discovery Status</td>
<td>The status of the discovery service on the endpoint.</td>
</tr>
<tr>
<td>Endpoint Server</td>
<td>Name of the server associated with this endpoint.</td>
</tr>
<tr>
<td>Files Scanned</td>
<td>The number of files that were scanned on the endpoint in the most recent scan.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the endpoint machine.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the endpoint machine.</td>
</tr>
<tr>
<td>Last Scan End Time</td>
<td>The time that the latest endpoint scan ended.</td>
</tr>
<tr>
<td>Last Scan Start Time</td>
<td>The time that the latest endpoint scan began.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Last time the endpoint received updates from the management server (profiles, policies, etc.).</td>
</tr>
<tr>
<td>Logged-in Users</td>
<td>Users who have logged into the endpoint.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the endpoint client machine.</td>
</tr>
<tr>
<td>Microsoft RMS</td>
<td>Whether Microsoft Rights Management Service (RMS) decryption and analysis is active or inactive.</td>
</tr>
<tr>
<td>Next Scan Time</td>
<td>The time scheduled for the next endpoint scan.</td>
</tr>
<tr>
<td>Policy Engine Version</td>
<td>Version of the policy engine machine that is associated with this endpoint.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>The name of the endpoint profile on this machine.</td>
</tr>
<tr>
<td>Synced</td>
<td>Indicates whether the endpoint is updated with the latest settings. The sync status shows an “X” when the policy, fingerprint, or profile version is not synchronized with the management server or when the endpoint’s profile name is out of sync.</td>
</tr>
</tbody>
</table>
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.

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

**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*, page 33.
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**.

Status is sent from the mobile agent to the management server in intervals between 1 and 60 minutes. This is configurable by clicking **Settings** in the toolbar at the top of the content pane.

## 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:

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

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.
Viewing Incidents and Reports

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, page 318, 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.
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, page 82
- Mobile devices reports, page 94
- Discovery reports, page 96

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.

Click Expand All or Collapse All to expand or collapse all folders, or click New Folder to create a new folder. 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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td>🎁</td>
<td>Run the selected report and display it.</td>
</tr>
<tr>
<td>Edit</td>
<td>📊</td>
<td>Edit or apply filters to the report. See Editing a report, page 37.</td>
</tr>
<tr>
<td>Save As</td>
<td>🗂️</td>
<td>Save the report with a new name.</td>
</tr>
<tr>
<td>Export to PDF</td>
<td>📝</td>
<td>Export the report to a PDF file.</td>
</tr>
<tr>
<td>Export to CSV</td>
<td>📋</td>
<td>Export the report to a CSV file.</td>
</tr>
<tr>
<td>Schedule a task</td>
<td>⌛️</td>
<td>Schedule this report for automatic email delivery.</td>
</tr>
<tr>
<td>Delete</td>
<td>✖</td>
<td>Delete the selected report. Predefined reports cannot be deleted.</td>
</tr>
</tbody>
</table>

**Note**

The operations administrators can perform on folders and reports in the catalog depend on their privileges. Superusers can perform these functions on all user-defined reports and folders. Other users can perform these functions only on reports and folders they created.

There are additional buttons in the report catalog toolbar:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Tasks</td>
<td>⌛️</td>
<td>Used to create a schedule for emailing incident reports. Create a scheduled task, define sender and recipient names, and define the outgoing mail gateway.</td>
</tr>
<tr>
<td>Settings</td>
<td>🏷</td>
<td>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 Setting reporting preferences, page 318.</td>
</tr>
</tbody>
</table>

**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.

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the report.</td>
</tr>
<tr>
<td>Description</td>
<td>A description to help administrators understand the purpose of the report.</td>
</tr>
</tbody>
</table>
| Availability | Which administrators can access the report:  
• Only the *Report owner*  
• *All administrators* with access to the Data Security module of the Forcepoint Security Manager|
| Show top  | *(Summary reports only)* 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.
### 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**, page 39
- **Mobile Device filters**, page 44
- **Discovery filters**, page 49

### Data Loss Prevention filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Action          | 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. Incidents with the following actions can be displayed:  
  - Permitted  
  - Blocked  
  - Attachment(s) dropped  
  - Quarantined  
  - Encrypted with profile key  
  - Encrypted with user password  
  - Denied (confirmed)  
  - Continued (confirmed)  
  In addition to the default actions, DLP actions configured in the Forcepoint Security Manager are listed (Forcepoint Email Security only). |
| Application Name| Filter incidents by the name of applications found in the incidents. Select the applications to include in the report. |
### Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assigned to</strong></td>
<td>Filter incidents by the person to whom they are assigned. <strong>Unassigned</strong> displays all incidents that have not been assigned to any administrator. Because filters can be available for all administrators, checking the <strong>Assigned to current administrator</strong> check box displays incidents assigned to the administrator who is currently logged onto the Security Manager. <strong>Assigned to selected administrators</strong> enables you to select specific administrators whose assigned incidents you want to display.</td>
</tr>
<tr>
<td><strong>Business Unit</strong></td>
<td>Filter to filter incidents by the business unit to which they’re assigned.</td>
</tr>
<tr>
<td><strong>Channel</strong></td>
<td>Limit which channels’ incidents are displayed in the report. The list of available channels depends on channels configured in the Security Manager. 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. 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. It is also possible to view incidents from the Discovery channel or CASB Service channel. Select <strong>CASB Service</strong> to view incidents detected when users synced or shared files with cloud applications such as Microsoft OneDrive for Business or Box. (Enable the CASB Service on the Settings &gt; General &gt; Service page.)</td>
</tr>
<tr>
<td><strong>Classifier</strong></td>
<td>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 <strong>Edit</strong> to add or remove content classifiers to the filter, then select a threshold for each.</td>
</tr>
<tr>
<td><strong>Classifier Type</strong></td>
<td>Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.).</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Set the incident list to display only incidents that were directed at specific destinations. Select <strong>Enable filter</strong> to select destinations from your resource list or enter them as free text. Choose which method you want to use from the drop-down list. If your free text includes a comma, enclose the value in quotes. For example: “Doe, John”. If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available. Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain. Complex filters can affect performance. See Selecting items to include or exclude in a policy, page 112 for more details on using this selector.</td>
</tr>
<tr>
<td><strong>Detected by</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Type</strong></td>
<td>Filter incidents according to the type of endpoint client, e.g., laptop or static device (such as workstations). In the <strong>Filter Properties</strong> pane, select the endpoint type.</td>
</tr>
</tbody>
</table>
| **Event Time** | 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.) Select a date range, then select a time of day. **Date Range**  
  - **Last n days** - Select this option to display incidents from the last $n$ days, then select the number of interest. For example, display incidents from the last 30 days.  
  - **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.  
  - **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the **From** and **To** dates and times from the drop-down lists. For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (**Entire day**) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30. **Time of Day**  
  - **Entire day** - Select **Entire day** to show all incidents during the date range, no matter what time of day they took place.  
  - **From ... to ...** - Select this option to show only incidents from a specific period. For example, if you select **Last 60 days** and **From 8 a.m. to 5 p.m.**, the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m. If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around.  
| **File Name** | 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. Note that complex filters can affect performance. |

**Note:** Filters are applied chronologically, so a file name filter will be applied before an endpoint type filter.
Viewing Incidents and Reports

Filter | Description
--- | ---
History | 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.
  - 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.
    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.
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.
Note that complex filters can affect performance.

Ignored Incident | Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.

Incident Tag | Filter incidents by a previously-defined tag. (See **Tagging incidents**, page 70). Select the tags by which to filter the report and click **Add**. Continue until all required tags have been added.
These can be used to group incidents for external applications.
Note that complex filters can affect performance.
Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Time</td>
<td>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.) Select a date range, then select a time of day.</td>
</tr>
<tr>
<td><strong>Date Range</strong></td>
<td></td>
</tr>
<tr>
<td>Last n days</td>
<td>Select this option to display incidents from the last n days, then select the number of interest. For example, display incidents from the last 30 days.</td>
</tr>
<tr>
<td>Time period</td>
<td>Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.</td>
</tr>
<tr>
<td>Exact date and time</td>
<td>Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Time of Day</strong></td>
<td></td>
</tr>
<tr>
<td>Entire day</td>
<td>Select Entire day to show all incidents during the date range, no matter what time of day they took place.</td>
</tr>
<tr>
<td>From ... to ...</td>
<td>Select this option to show only incidents from a specific period. For example, if you select Last 60 days and From 8 a.m. to 5 p.m., the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Use the check boxes provided to set which policy’s incidents are displayed in the incident list.</td>
</tr>
<tr>
<td>Released Incident</td>
<td>Filter in or out SMTP incidents that have been released by an administrator (a reports remediation option).</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Filter incidents by the rules they triggered.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the severity of incidents to display. Select High if you want to display incidents of high severity, and so on. Select as many severity levels as desired.</td>
</tr>
</tbody>
</table>
### Mobile Device filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Filter incidents by the action that was performed on the incident. Select the check box for each action to be displayed.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Filter incidents by the person to whom they are assigned. <strong>Unassigned</strong> displays all incidents that have not been assigned to any administrator. Because filters can be available for all administrators, checking the <strong>Assigned to current administrator</strong> check box displays incidents assigned to the administrator who is currently logged onto the Forcepoint Security Manager. <strong>Assigned to selected administrators</strong> enables you to select specific administrators whose assigned incidents you want to display.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Filter incidents by the business unit to which they’re assigned.</td>
</tr>
<tr>
<td>Classifier Matches</td>
<td>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 <strong>Edit</strong> to add or remove content classifiers to the filter, then select a threshold for each.</td>
</tr>
<tr>
<td>Classifier Type</td>
<td>Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)</td>
</tr>
<tr>
<td>Filter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination</td>
<td>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”. If you have a role in which source and destination information is hidden for privacy reasons, this filter is not available. Note that the filter returns values from all columns describing the destination, such as URL category, hostname, IP address, and domain. Complex filters can affect performance. See Selecting items to include or exclude in a policy, page 112 for more details on using this selector.</td>
</tr>
<tr>
<td>Detected by</td>
<td>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.</td>
</tr>
<tr>
<td>Device Details</td>
<td>Display incidents that match certain device criteria. 1. In the Field menu, indicate whether to filter by device name, ID, user agent, model, operating system, or type. 2. Indicate whether the field should contain a certain value or be empty. 3. Enter a value in the blank text box. 4. Click Add.</td>
</tr>
<tr>
<td>Device User</td>
<td>Display only incidents for specific mobile-device users. Select users from the resource list or enter identifying information manually. When using the resource list:  ● Use the Display field to indicate whether to pick from directory entries, business units, or custom users.  ● Enter a search term in the Filter by field.  ● Click the filter button.  ● Select items from the available list. See Selecting items to include or exclude in a policy, page 112. For free text, type a name, email address, or other information in the text box. Note that complex filters can affect performance.</td>
</tr>
</tbody>
</table>
Viewing Incidents and Reports

Filter | Description
--- | ---
Event Time | 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.)

Select a date range, then select a time of day.

**Date Range**

- **Last n days** - Select this option to display incidents from the last \( n \) days, then select the number of interest. For example, display incidents from the last 30 days.

- **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.

- **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the **From** and **To** dates and times from the drop-down lists.

For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30.

**Time of Day**

By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select **From** and choose a time range.

- **Entire day** - Select **Entire day** to show all incidents during the date range, no matter what time of day they took place.

- **From ... to ...** - Select this option to show only incidents from a specific period.

For example, if you select **Last 60 days** and **From 8 a.m. to 5 p.m.**, the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m.

If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around.

File Name | Filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click **Add**. Continue until you’ve added all you need.

Note that complex filters can affect performance.
Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| History         | 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.  
  - 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.  
    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.  
    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. Not that complex filters can affect performance. |
| Ignored Incident| Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports. |
| Incident Tag    | Filter incidents by a previously-defined tag (see Tagging incidents, page 70). Select the tags by which to filter the report and click Add. Continue until all required tags have been added.  
  Use these tags to group incidents for external applications.  
  Note that complex filters can affect performance. |
Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Time</td>
<td>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.) Select a date range, then select a time of day.</td>
</tr>
</tbody>
</table>
| Date Range         | **Last n days** - Select this option to display incidents from the last n days, then select the number of interest. For example, display incidents from the last 30 days.  
|                    | **Time period** - Select this option to display incidents that transpired in a set period of time, then select the period. Example: last 24 hours, this week, or last month.  
|                    | **Exact date and time** - Select this option to display incidents that transpired during a time period that you define, then select the From and To dates and times from the drop-down lists. For example, you can show incidents starting from 5:00 a.m. on April 1, 2009 to midnight April 30, 2009. Using the Time of Day options below this, you can specify whether to show all incidents from this period (Entire day) or just those from a time range, for example, 8 a.m. to 5 p.m. If you choose this From/To option, the report would include incidents from 8-5:00 on April 1, 8-5:00 on April 2, and 8-5:00 all other days of April, up to and including April 30. |
| Time of Day        | By default, incidents are displayed no matter what time of day they occurred, as long as the date range matches. To display only those incidents that occurred at certain times of day, select From and choose a time range.  
|                    | **Entire day** - Select Entire day to show all incidents during the date range, no matter what time of day they took place.  
|                    | **From ... to ...** - Select this option to show only incidents from a specific period. For example, if you select Last 60 days and From 8 a.m. to 5 p.m., the report displays all incidents from the last 60 days that were detected between 8 a.m. and 5 p.m. If you prefer, you can view incidents that occurred during off-peak hours, such as 5 p.m. to 8 a.m. the next day. That way you know if information is being leaked at night when no one is around. |
| Policy             | Use the check boxes provided to set which policy’s incidents are displayed in the incident list. |
| 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. |
Viewing Incidents and Reports

### Discovery filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source          | 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”. If there is a role in which source and destination information is hidden for privacy reasons, optionally enter one or more source IDs. Note that the filter returns values from all columns describing the source, such as URL category, hostname, IP address, and domain. Complex filters can affect performance.
|                 | See Selecting items to include or exclude in a policy, page 112.                                                                                                                                  |
| 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       | Display incidents on messages that were synchronized by a certain number of mobile-device users. For example, you want to know when the same violating message was synchronized by more than 10 users. |
| Top Matches     | 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 | Select which incident triggers to display in the incident list. In the field, enter a violation trigger of interest and click Add. Continue until you’ve added all you need. Note that complex filters can affect performance. |

### Filter Description

- **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.
### Viewing Incidents and Reports

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Classifier Name</td>
<td>Select which specific content classifiers should be displayed in the incident list.</td>
</tr>
<tr>
<td>Content Classifier Type</td>
<td>Select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.).</td>
</tr>
<tr>
<td>Date Accessed</td>
<td>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.</td>
</tr>
<tr>
<td>Date Created</td>
<td>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.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>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.</td>
</tr>
<tr>
<td>Detected by</td>
<td>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.</td>
</tr>
<tr>
<td>Discovery Task</td>
<td>Select the discovery tasks to display in the report.</td>
</tr>
<tr>
<td>Discovery Type</td>
<td>Select the type of discovery to display in the report: File System, Endpoint, SharePoint, SharePoint Online, Database, Exchange, Exchange Online, Outlook PST, and/or Domino.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>Filter incidents according to the type of endpoint client, e.g., laptop or static device.</td>
</tr>
<tr>
<td>Event Time</td>
<td>Select incidents by the date and time the policy engine first saw the transaction. For filter properties, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last nn days</strong> - Select the number of days from the spinner.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Time period</strong> - Select the range from the drop-down list. Example: last 24 hours or this week.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exact dates</strong> - Select the <strong>From</strong> and <strong>To</strong> dates from the drop-down lists.</td>
</tr>
<tr>
<td>Folder</td>
<td>View incidents from a certain folder or folders. Type a valid folder name into the field box, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>File Name</td>
<td>Filter in or out incidents involving certain files. Enter the file name (wildcards can be used), and click <strong>Add</strong>. Continue until all required files have been added. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>File Owner</td>
<td>Filter incidents by file owner. Type a valid owner name into the field box, then click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
### Filter Description

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Permissions</td>
<td>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--</td>
</tr>
<tr>
<td>File Size</td>
<td>Filter incidents by file size, then choose the size of the file to include in the report.</td>
</tr>
<tr>
<td>Folder Owner</td>
<td>Filter incidents by folder owner. Type a valid owner name into the field box, then click Add.</td>
</tr>
<tr>
<td>History</td>
<td>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. 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 &gt; Add Comments), those are appended to the workflow details. 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. 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. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Filter incidents by the host on which they were detected. Type a valid hostname into the field box, then click Add.</td>
</tr>
<tr>
<td>Ignored Incident</td>
<td>Filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td>Filter incidents by a previously-defined tag (see Tagging incidents, page 70). Select the tags by which to filter the report and click Add. Continue until all required tags have been added. Use these tags to group incidents for external applications. Note that complex filters can affect performance.</td>
</tr>
<tr>
<td>Incident Time</td>
<td>Filter incidents by the date and time they were written to the database. Select the time for the incidents to display.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Filter incidents by the host on which they were detected. Type a valid IP address into the field box, then click Add.</td>
</tr>
</tbody>
</table>
Table Properties tab

Administrator Help | Forcepoint DLP | Version 8.5.x

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**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The action taken on the incident, as determined by the action plan.</td>
</tr>
<tr>
<td>Analyzed by</td>
<td>Displays the name of the server component that analyzed the incident.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Either Unassigned or the name of the administrator assigned to handle this incident. (See Assigning incidents, page 67.)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel where the incident occurred. Possible channels include:</td>
</tr>
<tr>
<td></td>
<td>● Email</td>
</tr>
<tr>
<td></td>
<td>● Web</td>
</tr>
<tr>
<td></td>
<td>● FTP</td>
</tr>
<tr>
<td></td>
<td>● Endpoint application</td>
</tr>
<tr>
<td></td>
<td>● Endpoint printing</td>
</tr>
<tr>
<td></td>
<td>● Network printing</td>
</tr>
<tr>
<td>Destination</td>
<td>The intended destination or destinations of the content that violated policy.</td>
</tr>
<tr>
<td>Details</td>
<td>Details about the incident. Shows the subject in an SMTP incident, the URL in a Web incident, etc.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the name of the Forcepoint DLP device or component that detected this incident.</td>
</tr>
<tr>
<td>Endpoint type</td>
<td>The type of endpoint involved in the incident: PC, laptop, etc.</td>
</tr>
<tr>
<td>Email direction</td>
<td>This column displays the direction of the email message that triggers an incident:</td>
</tr>
<tr>
<td></td>
<td>● Inbound</td>
</tr>
<tr>
<td></td>
<td>● Outbound</td>
</tr>
<tr>
<td></td>
<td>● Internal</td>
</tr>
<tr>
<td></td>
<td>If you are using the Forcepoint Email Security module, endpoint agent, or protector to monitor email, then all 3 directions are possible.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The ID number assigned to the event or transaction.</td>
</tr>
<tr>
<td>Event time</td>
<td>The date and time the policy engine first saw a transaction.</td>
</tr>
<tr>
<td>File name</td>
<td>The name and size of the attachment for this incident.</td>
</tr>
<tr>
<td>ID</td>
<td>The incident’s unique ID number.</td>
</tr>
</tbody>
</table>
### Viewing Incidents and Reports

**Column** | **Description**
--- | ---
Incident Tag | Displays any incident tag set for the incident. (See *Tagging incidents*, page 70.)
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 incidents severity (see *Changing incident severity*, page 69).
Source | The source of the incident. Could be a person, computer, or other.
Status | The status of the incident. For example:
  - New
  - In process
  - Closed
  - False Positive
  - Escalated
You can also add and filter by up to 17 custom statuses. See *Changing incident status*, page 68.
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 *Assigning incidents*, page 67.)
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.
Detected by | Displays the name of the Forcepoint DLP device or component that detected this incident.
### Viewing Incidents and Reports

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Email direction         | This column displays the direction of the email message that triggers an incident:  
  ● 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                | 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 Tagging incidents, page 70.)                                                                                                                                                                                                                                                               |
| Incident Time           | The time and date the incident was written to the database.                                                                                                                                                                                                                                                                                     |
| Top Matches             | The maximum number of violations triggered by any given rule in the incident.                                                                                                                                                                                                                                                                  |
| Policy                  | The policies that were violated by the content.                                                                                                                                                                                                                                                                                                 |
| Severity                | The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incidents severity (see Changing incident severity, page 69). |
| Source                  | The source of the incident. Could be a person, computer, or other.                                                                                                                                                                                                                                                                            |
| Status                  | The status of the incident. For example:  
  ● New  
  ● In process  
  ● Closed  
  You can also add and filter by up to 17 custom statuses.  
  See Changing incident status, page 68.                                                                                                                                                                                                                                       |
| 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.                                                                                                                                                       |
| 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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzed by</td>
<td>Displays the name of the server component that analyzed the incident.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Either Unassigned or the name of the administrator assigned to handle this incident. (See Assigning incidents, page 67.)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel where the incident occurred. Possible channels include:</td>
</tr>
<tr>
<td></td>
<td>● Email</td>
</tr>
<tr>
<td></td>
<td>● Web</td>
</tr>
<tr>
<td></td>
<td>● FTP</td>
</tr>
<tr>
<td></td>
<td>● Endpoint application</td>
</tr>
<tr>
<td></td>
<td>● Endpoint printing</td>
</tr>
<tr>
<td></td>
<td>● Network printing</td>
</tr>
<tr>
<td>Details</td>
<td>The details listed in the forensics Properties tab. Shows the subject in an SMTP incident, the URL in a Web incident, etc.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the name of the Forcepoint DLP device or component that detected this incident</td>
</tr>
<tr>
<td>Discovery task</td>
<td>The discovery task that identified the incident.</td>
</tr>
<tr>
<td>Discovery type</td>
<td>The type of resource that was scanned: File System, Endpoint, SharePoint, SharePoint Online, Database, Exchange, Exchange Online, and/or Outlook PST.</td>
</tr>
<tr>
<td>Endpoint type</td>
<td>The type of endpoint involved in the incident: PC, laptop, etc.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The ID number assigned to the event or transaction.</td>
</tr>
<tr>
<td>Event time</td>
<td>The date and time the policy engine first saw a transaction.</td>
</tr>
<tr>
<td>File extension</td>
<td>The file extension of the file that violated policy. For example: .docx or .pptx.</td>
</tr>
<tr>
<td>File full path</td>
<td>The full directory path of the file that violated policy.</td>
</tr>
<tr>
<td>File name</td>
<td>The name of the file that violated policy.</td>
</tr>
<tr>
<td>File owner</td>
<td>The owner of the file that contained the policy violation.</td>
</tr>
<tr>
<td>File size</td>
<td>The size of the file that violated policy.</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder of the file that violated policy.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the host on which the violation was detected.</td>
</tr>
<tr>
<td>ID</td>
<td>The incident’s unique ID number.</td>
</tr>
<tr>
<td>Ignored incident</td>
<td>The incidents marked as ignored.</td>
</tr>
<tr>
<td>Incident Tag</td>
<td>Displays any incident tag set for the incident. (See Tagging incidents, page 70.)</td>
</tr>
<tr>
<td>Incident Time</td>
<td>The time and date the incident was written to the database.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the host on which the violation was detected.</td>
</tr>
</tbody>
</table>
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, page 58.
- 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.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task name</td>
<td>Enter a name for the task you are scheduling.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select <strong>Enabled</strong> to enable the task for use.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the task.</td>
</tr>
<tr>
<td>Report type</td>
<td>Indicate whether you want to email a data loss prevention, mobile devices, or discovery report.</td>
</tr>
<tr>
<td>Report name</td>
<td>Select a report from the drop-down list. This is the report that will be emailed on the schedule you define.</td>
</tr>
<tr>
<td>Report format</td>
<td>If you selected a details report, select whether you want the report delivered in PDF or CSV format. Summary reports are graphical, so they can be exported to PDF only.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>Enter the name of the person from whom the report should be sent. This is the name that will appear in the email From field.</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom the report should be sent.</td>
</tr>
<tr>
<td>Outgoing mail server</td>
<td>The outgoing mail server that’s been configured appears on screen. If you want to change the server used, click <strong>Edit</strong> (the icon). Please note that changing this setting changes the configuration for the entire system.</td>
</tr>
<tr>
<td>Subject</td>
<td>Type the subject of the message containing the report. This appears in the email Subject: line.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Define the recipient(s) for the notification. Click <strong>Edit</strong> to select to select users or groups from a user directory. Select <strong>Additional email addresses</strong> if you want to send the report to someone not on your user directory list, then enter the email address. Separate multiple addresses with commas.</td>
</tr>
</tbody>
</table>
3. On the **Schedule** tab, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Select the date and time on which to start the schedule. This is the date and time of the Forcepoint DLP Server.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Select this check box to set up a recurrence pattern for the task, then select the pattern:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Daily</strong> - Select daily if you want the task performed every day at the same time.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Weekly</strong> - Select weekly if you want the task to recur every week on a certain day, then select the day of the week.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monthly</strong> - 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”.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following options if you specify a recurrence pattern:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No end date</strong> - Select this option if there is no end date for the recurrence. You want it to continue until you reconfigure the task.</td>
</tr>
<tr>
<td></td>
<td>- <strong>End by</strong> - Select this option if you want the task to end by a certain date, then select the date from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>- <strong>End after</strong> - Select this option if you want the task to end after a set number of occurrences, then select the number from the spinner.</td>
</tr>
</tbody>
</table>

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

### Viewing the incident list

To view a list of data loss prevention incidents from the last 3 or 7 days, and their details:
1. 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*, page 76.)

Click the down arrow on column header to sort, filter, or group incidents by that column. (See *Applying a column filter*, page 77, for more information.) Or click **Table Properties** to change the columns that are displayed, their order, and their width. See *Table Properties tab*, page 52, 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*, page 63, for more information about what is displayed.)

Use toolbar buttons to manage incident workflow, remediate incidents, escalate incidents, change incident filters or table properties, and more.
## Toolbar buttons

There are several buttons on the incident toolbar:

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| Workflow       | ![Image](image-url) | Click this button to manage the workflow of the selected incident, then select one of the following:  
- Assign - Select this option to assign the incident to someone or mark it as unassigned.  
- Lock - Select this option to lock the selected incident, preventing any further changes from future scans of the file. This option applies only to discovery incidents.  
- Unlock - Select this option to unlock a locked incident, allowing information from future scans to overwrite the current data. This option applies only to discovery incidents.  
- Change Status - Select this option to change the incident status or change the status labels.  
- Change Severity - Select this option to change the incident severity assignment.  
- Ignore Incident - Select this option to mark an incident as ignored or unmark an ignored incident. Mark an incident as ignored when you’ve reviewed it and no action is required.  
- Tag Incident - Select this option to associate an incident with a custom tag that you can later use in filters.  
- 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 incidents, all incidents that match the filter criteria for the current report, or all incidents.  
(See Managing incident workflow, page 66 for details on all of these options.) |
Remediate Click this button to remediate the selected incident, then select one of the following:

- **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.
- **Run Remediation Script** - Select this option to run a remediation script on the selected incident.
  
  (See *Remediating incidents*, page 72 for details on both options.)

Escalate Click this button to escalate the selected incident to a manager or other person:

- **Email to Manager** - Select this option to email the incident to the manager of the person generated the policy breach.
- **Email to Other** - Select this option to email the incident to another person for action.
  
  (See *Escalating incidents*, page 74 for details on both options.)

Manage Report N/A Click this button to edit the filter or table properties applied to the current report, then select one of the following:

- **Edit Filter** - Select this option to edit the filters applied to the report—for example, choosing a longer time period or single channel.
- **Table Properties** - Select this option to customize the properties of the incident table.
- **Save** - Select this option to save the changes you made to current report.
- **Save As** - Select this option to save the current report with a new name.
  
  (See *Managing incident reports*, page 76. for details on all of these options.)

Settings Lets you set preferences for incident lists and reports. For example, for data loss prevention incidents, you can define attachment size and forensics settings. For discovery incidents, you can set database thresholds. You can also define general settings, like filtering and printing, that apply to all types of incidents.

For information on configuring these settings, see *Setting reporting preferences*, page 318.
To preview an incident and learn more about it, click on the table row of the incident in the Incidents List. See Previewing incidents, page 63 for details on this portion of the window.

**Previewing incidents**

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

- **Violations**
- **Forensics**
- **Properties**
- **History**

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

**Violations**

In this section, you can display violation triggers or violated rules.

- **Violated rules** displays which rules were violated by the incident. Click the information icon to view more details, such as the policy and action plan for the rule. Only the first 500 rules or 500 MB for the incident are displayed.
- **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.

---

Click **Tune Policy** to update your policy for this incident. You can select any of the following:

- **Exclude Source from Rules** - Select this option to exclude the incident source from one or more of the rules. You cannot exclude an incident source from an email or Web data loss prevention policy.

- **Disable Policies** - Select this option to disable a policy if it is not producing the desired effect. You cannot disable an email or Web data loss prevention policy; you can only disable attributes.

- **Disable Rules** - Select this option to disable a rule if it is not producing the desired effect. To disable attributes in an email or Web data loss prevention policy, highlight the policy, click **Edit**, then de-select **Enabled** for the desired attributes.

See *Tuning policies*, page 80 for more information.

**Forensics**

The **Forensics** tab shows information about the original transaction.

For data loss prevention incidents that occurred on an email or a mobile channel, it displays the message subject, from, to, attachments, and message body. You can click links for details about the source or destination of the incident, such as email address, manager, and manager’s manager. You can retrieve thumbnail photos, if configured. You can also open attachments. The bottom portion of the incident screen displays the message body.

For data loss prevention incidents that occurred on a Web channel, the forensics could include the URL category property.

For discovery incidents, forensics includes the hostname and file name.

Use the **Show as** field to select how you want the text displayed: Marked HTML, plain text, or HTML.

Marked HTML includes the HTML markup language. HTML does not.

Forensics are stored in the `\forensics_repository\data` directory on the management server.

Note that the extracted text may appear slightly different from channel to channel. This is due to the way the policy engine works in different environments.
Properties

The Properties tab displays incident details, such as:

- Incident number
- Severity
- Status
- Action
- Channel

It also shows information about the source and destination of the incident.

For discovery incidents, this tab also displays:

- Detection information
- Discovery task name
- File permissions
- File details

History

The History tab displays the incident history, such as when it was received, released, or assigned to someone. These are automatically generated when a workflow operation is performed.

This tab also displays comments that were added by administrators using the Workflow > Add Comments option.

Each event in the incident’s history is shown in a separate row. You can expand or collapse events to view details.
Managing incident workflow

Click this button to manage the workflow of the selected incident, then select one of the following:

- **Assign** - Select this option to assign the incident to someone or mark it as unassigned.
- **Change Status** - Select this option to change the incident status or change the status labels.
- **Change Severity** - Select this option to change the incident severity assignment.
- **Ignore Incident** - Select this option to mark an incident as ignored or unmark and ignored incident. Mark an incident as ignored when you’ve reviewed it and no action is required.
- **Tag Incident** - Select this option to associate an incident with a custom tag that you can later use in filters.
- **Add Comments** - Select this option to comment on the incident. Comments are added to the incident history.
- **Delete** - Select this option to delete selected incidents (all types), all incidents in the current report (network, endpoint, and mobile DLP incidents only), or all incidents at once (mobile DLP and discovery only).

The following option is available only for data loss prevention and mobile incidents:

- **Download Incident** - Select this option to download a data loss prevention incident.

The following options are available only for discovery incidents:

- **Lock** - Select this option to lock an incident, preventing the addition of any information from subsequent scans.

---

Related topics:

- Assigning incidents, page 67
- Changing incident status, page 68
- Changing incident severity, page 69
- Ignoring incidents, page 69
- Tagging incidents, page 70
- Adding comments, page 70
- Downloading incidents, page 70
- Deleting incidents, page 71
Assigning incidents

You can assign specific administrators to an incident. When you do, other administrators—those to whom it has not been assigned—no longer have the ability to perform actions on this incident, with the exception of Superusers. Administrators with the proper role may still be able to view the incident however.

To assign an incident to someone for action:

1. Select the incident.
2. From the toolbar, select Workflow > Assign.
3. Select the Assign to option.
4. From the drop-down list, select the person to whom to assign the incident.
5. Add comments if desired.
6. Click OK.

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

1. Select the incident.
2. From the toolbar, select Workflow > Assign.
3. Select the Unassigned option.
4. Add comments if desired.
5. Click OK.

Locking and unlocking incidents

During discovery, a file may be scanned several times as a part of consecutive scans. Each scan may detect different policy breaches, if either the file or the policy has changed. If this happens, the incident for that file is overwritten with the most recent information.

If you want to keep the current stored information for a particular incident, you can choose to lock it. Information logged from subsequent scans on this file is then discarded.

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.)
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

To change the status of an incident:
1. Select the incident.
2. From the toolbar, select Workflow > Change Status.
3. Select a new status from the menu.

There are 5 predefined statuses:

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

Although you cannot change these statuses, you can add and maintain up to 17 more. To add a new status:
1. Select Workflow > Change Status > Edit Statuses.
2. Click New in the resulting window.
3. Enter a name for the status. It must be unique and fewer than 32 characters.
4. Enter a description for the status, up to 1024 characters.
5. Select from one of 12 available flags. If you add more than 12 statuses, you must reuse a flag.
6. Click OK.
The new status is added to the top of the status list. Rearrange the order of the list by selecting a status and clicking the up or down arrow. The order is reflected in reports and in the incident list when it’s sorted by the status column.

Click a status name to edit its properties (predefined statuses are uneditable). If you rename a status, all incidents with that status are updated with the new name.

If you delete a status, incidents with that status retain their designation; however, the status is no longer available in report filters.

## Changing incident severity

The incident’s severity setting is a measure of how important it is to the organization that this incident is handled. The severity of an incident is automatically decided by 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 the incident.
2. From the toolbar, select **Workflow > Change Severity**.
3. Select a new severity from the menu.

Possible severities include:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>High. This breach is significant and may have a broad impact on the organization.</td>
</tr>
<tr>
<td>📢</td>
<td>Medium. This breach is moderate and should be reviewed.</td>
</tr>
<tr>
<td>🔴</td>
<td>Low. This breach is insignificant.</td>
</tr>
</tbody>
</table>

## 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.

To mark an incident as ignored:

1. Select the incident.
2. From the toolbar, select **Workflow > Ignore Incident**.
3. Select **Mark as ignored incident**.

If you no longer want the incident to be ignored, you can unmark it:

1. Select the incident.
2. From the toolbar, select **Workflow > Ignore Incident**.
3. Select **Unmark ignored incident**.

### Tagging incidents

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. Enter the desired text string into the **Incident tag** field.
4. Add comments if desired.
5. 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. Enter the notes in the Comment field.
4. 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

With Forcepoint DLP, you can delete incidents that are known to be false positives or that are the product of a policy that is no longer relevant to your organization. There may be other reasons as well, depending on your security policies and practices.

- You can delete selected incidents.
- For discovery and mobile DLP, you can delete all incidents at once. Choosing this option deletes all discovery incidents or all mobile DLP incidents in the system (depending on your selection).
- For network, endpoint, and mobile DLP, you can delete all the incidents in the current report. For example, you can create a report that lists all email incidents originating from your company president, and then delete all those incidents in a single batch operation.

To delete incidents, you must be a Global Security Administrator or Super Administrator.

---

### Important

You cannot undo this action.

---

**To delete selected incidents:**

1. Select the incidents to delete.
2. From the toolbar, select **Workflow > Delete > Selected Incidents**.
3. When prompted, select a reason for the action—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.
4. Click **OK** to confirm the action.

**To delete all the incidents in the report** (network, endpoint, and mobile DLP only):

1. Set your report filters as desired. To do so, select **Manage Report > Edit Filter**.
2. When the report contains all the incidents you want to delete and no more, select **Workflow > Delete > Report Incidents** from the toolbar.
3. When prompted, select a reason for the action—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.
4. Click **OK** to confirm the action.

**To delete all incidents** (discovery and mobile DLP only):
1. From the toolbar, select Workflow > Delete > All Mobile Incidents / All Discovery Incidents.

2. For mobile DLP, skip to step #3. For discovery, select a reason for the action when prompted—for instance, the incidents are false positives or no longer relevant. If you choose Other, enter a reason for the deletion in the field provided.

3. Click OK to confirm the action.

If you are deleting mobile or network DLP incidents, you can continue working while the operation runs in the background.

When incidents are deleted, their forensics are deleted from the forensic repository.

If the system is set up to do so, an email message is sent to all configured recipients notifying them that incidents were deleted from the incident database.

Incident deletions are also logged in the Audit Log, showing who deleted the incidents, when, and why.

---

**Remediating incidents**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

---

**Releasing incidents**

Administrator Help | Forcepoint DLP | Version 8.5.x

This option is only available for blocked incidents sent from the mobile agent, protector, or Forcepoint Email Security module—that is, for email transactions that have been quarantined.

If an SMTP email transaction was quarantined, the administrator responsible for handling this incident can release this incident to the recipients originally blocked from receiving the content.

All messages are released through the configured release gateway. You configure the release gateway at Settings > General > Remediation. By default, the release gateway is the agent that delivered the message to the policy engine for analysis (the mobile agent, protector MTA, or Forcepoint Email Security).
There are 2 ways to release an incident: From the Incident Details report or By replying to the notification message.

**From the Incident Details report**

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**.

For mobile incidents, you’re asked to select the users to release the message to. (Many users may have had the same message blocked when they synchronized their email to their mobile devices.) You can release the blocked message to all users who tried to sync it, or to selected users. If desired, you can release the message to everyone who syncs this message in the future.

If the system is set up to do so, an email message is sent to all configured recipients notifying them that incidents were released from the incident database.

The release status (success or failure) is also logged in the Audit Log.

**By replying to the notification message**

When an email incident is blocked, or indeed any policy breach is discovered, notifications are sent to all the users configured in **Main > Policy Management > Resources > Notifications**. Users can release email incident by replying to the notification message.

If the message was successfully released, the user who released the message receives a confirmation email.

See the knowledge base article, [Releasing email blocked by Forcepoint DLP](#), 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**.

**Escalating incidents**

Click this button to escalate the selected incident to the manager of the person who caused the incident or to another person.

For data loss prevention incidents, the following options are available:

- **Email to Manager** 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.

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

1. Select the incident or incidents you want to email.
2. From the toolbar, select **Escalate > Email to Manager**. A screen appears.
3. By default, the message is sent to the manager of the person who generated the incident. For most DLP incidents, this is the incident source—the person who tried to move sensitive data. For mobile incidents, it is the person who received sensitive data and tried to synchronize it to a mobile device.
If you want to send a copy or blind copy to other people, enter their email addresses in the **Cc** and **Bcc** fields.

4. Enter a subject in the **Subject** field or accept the default. Click the right arrow to choose variables to include in the subject, such as “This is to notify you that an employee’s message was %Action% because it breached corporate policy.” Maximum length: 4000 characters.

5. Select **Include original message as an attachment** if you want to attach the message.

6. Select **High importance** if this is a priority message.

7. Edit the predefined message body as desired. Click the right arrow to choose variables to include, such as %Incident Time% or %Severity%.

8. Click **OK**.

The selected incidents are immediately emailed to the manager.

### Email incidents to another

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%.

8. Click **OK**.

The selected incidents are immediately emailed to the people you selected.
Managing incident reports

You can change the incident report by applying different filters or editing table properties. You can then save the report with your changes or create a new report by saving it as another file.

Click the Manage Report link and 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.

Editing report filters

To change the filters that are applied to this report, select Manage Report > Edit Filter. See Filter tab, page 39 for instructions on selecting filters and defining filter properties.

Editing table properties

To edit the properties of the incident table—the one displayed at the top of the Incidents (last 3 days) report—select Manage Report > Table Properties.

Using the check boxes provided, select each column to be displayed and set the maximum width in number of characters. See Table Properties tab, page 52 for a description of the columns.
Set the maximum number of incidents to be displayed per page (20 to 200). By default this is set to 100. This setting is saved for each administrator.

Use the up/down arrows to the right of the incident table to customize the order of columns.

Click OK to apply these settings.

**Applying a column filter**

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

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

For example: If the main filter is set to display only SMTP channel incidents, and the column filter is then set to display severity - high, only high severity SMTP incidents are displayed. Column filters are not saved, so when a custom filter is applied, the column filter that was applied before it is lost.

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

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

To filter columns:

1. Click the down arrow button in a column header. A drop menu with 5 options appears. Different columns display different options.
2. Select from one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Ascending</td>
<td>Sorts the column’s entries by A-Z, from top to bottom.</td>
</tr>
<tr>
<td>Sort Descending</td>
<td>Sorts the column’s entries by Z-A, from top to bottom.</td>
</tr>
<tr>
<td>Group by this Column...</td>
<td>Incidents in the incident list screens can be grouped, allowing an alternative filtered report. Grouping incidents enables deep drill down into a problem. For more information, refer to Grouping Incidents (on page 212).</td>
</tr>
</tbody>
</table>
Saving reports

Once you’ve applied the filters and table properties you desire, click Manage Report > Save or Save As to save your custom report. Save saves your changes to the current report. Save As lets you specify a new report name.

When you select Save As, indicate whether you want the report saved in one of the existing report folders or in a new folder.

The new report then appears in the report catalog for future use.

Grouping incidents

In the active report, you can group incidents by the person they’re assigned to, by source, by status, by channel, or a number of other headings in the incident table. Each column header has a down arrow next to it.

Select the down arrow next to the column header of interest, then select Group by [column].
Your report is now grouped by that function.

Grouping incidents is an effective way to drill-down into a problem.

For example, grouping can be used as follows:

An administrator who wants to take a look at the most problematic channel can group by channel. This enables the administrator to quickly see that HTTP is by far the problematic channel, and can then drill-down into HTTP. Now the administrator groups by the policy category to learn that finance is the information that is most frequently leaked and within that group, the administrator can group by IP addresses to find the most problematic employee and drill down to that employee’s incidents.

See *Applying a column filter*, page 77, for additional information.

**Deleting incidents**

Only discovery incidents can be deleted.

To delete one or more selected incidents:

1. 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.
2. 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:

![Example Incident Report]

To configure how incidents are grouped when exported to PDF, see *Setting general reporting preferences*, page 319.

**Tuning policies**

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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*, page 81
   - *Disabling policies*, page 81
   - *Disabling rules*, page 81
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) | 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. Select this report when to manage incident workflow, remediation, and escalation. It is also possible to view Incidents by Severity, which shows detailed information about each incident, ranked in severity order. |

**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 | Find out which policies were violated most frequently over the last 7 days. Assess the security risk to your organization. ● 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. |
| 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. |
### Viewing Incidents and Reports

| Incident Risk Ranking - Top Cases | Shows up to 20 cases with the highest risk scores during the selected time period, along with details for those cases. Requires the Forcepoint DLP analytics engine on a Linux machine. |
| My Cases | Shows the cases that you have flagged for later reference. Requires the Forcepoint DLP analytics engine on a Linux machine. |

### Severity & Action

<table>
<thead>
<tr>
<th>Violations by Severity &amp; Action</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Last 7 Days</td>
<td>shows incidents by the actions (permit, block, notify) and severities from the last 7 days.</td>
</tr>
<tr>
<td>● Credit Card Violations</td>
<td>shows credit card-related incidents by the actions and severities applied to them.</td>
</tr>
<tr>
<td>● Violations of Personally Identifiable Information (PII)</td>
<td>shows PII incidents by the actions and severities applied to them.</td>
</tr>
</tbody>
</table>

### Sources & Destinations

<table>
<thead>
<tr>
<th>Top Sources &amp; Destinations</th>
<th>Find out who are the top violators involved in data leakage and the top domains where sensitive data was posted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Last 7 Days</td>
<td>shows the top violators involved in data leakage and the top domains where sensitive data was posted from the last 7 days.</td>
</tr>
<tr>
<td>● Leaks to Public EMail Web Sites</td>
<td>shows the top violators involved in leaking data to public email websites and the top domains of those websites.</td>
</tr>
<tr>
<td>● Leaks to Malicious Web Sites</td>
<td>shows the top violators involved in leaking data to malicious websites and the top domains of those websites.</td>
</tr>
<tr>
<td>● Credit Card Number Violations</td>
<td>shows who attempted to leak credit card information in plain text and the top destinations to which this information was leaked.</td>
</tr>
<tr>
<td>● PII Violations</td>
<td>shows who violated a PII policy and the top destinations to which PII information was leaked.</td>
</tr>
<tr>
<td>● PCI Violations</td>
<td>shows who violated a PCI policy and the top destinations to which PCI information was leaked.</td>
</tr>
</tbody>
</table>
Trends

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

Status

| Incident Status (last 7 days) | View the status of all DLP incidents from the last 7 days. |

Geographical Location

| Web DLP - Destinations by Severity | View the destinations of the most severe outbound web incidents, by geographical region. |

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:

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.

The dashboard includes the following sections:

- **Incidents by Severity** - This table displays incidents over the last 7 days by severity.
- **Incidents by Action** - This table displays incidents by the action taken on them.
- **Top 5 Channels** - This table displays incidents by channel. The corresponding pie chart displays the percentage of the total incidents represented by these channels.
• **Top 5 Policies** - This table displays incidents in the order of which policy was violated, therefore generating the most incidents. Click **Show All** to show all policies that were violated.

• **Top 5 Destination URL Categories** - This table displays URL categories with the most violations.

• **Top 5 Sources** - This table displays the sources that violated policy the most and their severity level. Click **Show All** to show all sources that violated policy.

• **Top 5 Destinations** - This table displays the destinations with the most violations and their severity level. Click **Show All** to show all destinations that were violated.

• **Top Incidents** - This table displays the top incidents as determined by severity, the maximum number of matches, and incident time. This table lists the incident ID, source, destination, severity, policy, and date/time for each incident. Click an ID number for details on the incident. Click **Show All** to show all incidents.

You can export the dashboard report to a PDF file or view a Print Preview of it.

You can also customize the report by selecting **Manage Report > Edit Filter**. (See *Managing incident reports*, page 76 for more details.)

To schedule this report to be delivered by email, see *Scheduling tasks*, page 57.

### Top violated policies

Administrator Help | Forcepoint DLP | Version 8.5.x

To assess risk to your organization’s security, you should review incidents in a few key reports and consider making policy changes.

To view data loss prevention risk:

1. Select **Main > Reporting > Data Loss Prevention**.
2. From the report catalog, expand the Risk Assessment folder and select **Top Violated Policies (last 7 days)**.
3. Click **Run** to generate the report.

### User risk summary (all incidents)

Administrator Help | Forcepoint DLP | Version 8.5.x

This report shows the users who generated the most incidents across all active DLP policies.

It contains the user’s full name, login name, department, manager, title, and business unit according to details imported from the user directory.

It also shows incident counts by severity.

To view this report:

1. Select **Main > Reporting > Data Loss Prevention**.
2. From the report catalog, expand the Risk Assessment folder and select **User Risk Summary (All Incidents)**.
3. Click **Run** to generate the report.

**User risk summary (data theft risk indicators)**

This report shows which users generated the most incidents across all active Data Theft Risk Indicator policies, including suspicious user activity, indicators of compromise, and employee discontent.

- Suspicious user activity policies include Data Sent During Unusual Hours, 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.
Viewing Incidents and Reports

- 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.

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, page 318.)

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?, page 89, 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.

**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.

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.

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.

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**

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.

- 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.

- 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:
  1. Go to the **Main > Policy Management > Manage Policies** page and open or create a custom policy.
  2. On the Destination page, under Web, click **Edit**.
  3. 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:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
</table>
| Incident List                       | View a list of all the mobile email incidents for a certain period of time—that is, incidents discovered when users synchronize their mobile devices to their network email systems.  
                                        | See detailed information on each incident. Investigate the violated policies and the actions taken by Forcepoint software. Evaluate whether policy changes are needed.  
                                        | Select this report when you want to manage incident workflow, remediation, and escalation.  
                                        | See *Viewing the incident list, page 59*, for an explanation of how to read and customize reports like this one. |
| 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)  | Find out the messages that were synchronized to mobile devices most frequently.  
                                        | View a list of incidents with details such as the time the message was sent, the source and destination of the message, the severity and more.                                                                 |
| Severity & Action                   | Find out when personally identifiable information was being synchronized to mobile devices, the users performing the sync, and the action taken.                                                              |
| Mobile PII 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.

## Top violated mobile policies

This report shows which mobile DLP policies were violated most frequently over the last 7 days, so you can assess the security risk to your organization.
The bar chart shows how many times the policies were violated.

The table shows how many devices were involved in each breach—that is, how many tried to synchronize email that violated those policies. It also shows whether each violation was a high, medium, or low security breach. This setting is determined by which attribute was matched.

Click a link to view details about each incident.

**Top synced messages**

This report shows the messages that were synchronized to mobile devices most frequently.

View a list of incidents with details such as the time the message was sent, the source and destination of the message, the severity and more. (These properties are configurable.) View the message itself under incident forensics.

See *Viewing the incident list, page 59*, for an explanation of how to read and customize incident reports like this one.

**Mobile PII violations**

This report shows the severity of personally identifiable information incidents and the action taken.

The top portion shows incidents by severity.

- The table shows how many high, medium, and low severity PII incidents occurred during email sync. Click a link to view details about each incident, such as the source and destination of the violating email message.
- The pie chart shows the percentage of PII violations that were of high, medium, and low severity.
  
  Severity is determined by which attribute was matched.

The bottom portion of the report shows the actions taken for each PII incident. The bar chart and table both show how many PII incidents were quarantined or permitted. Click a link in the table to view details about each incident.

**Mobile credit card violations**

This report shows when credit card information was being synchronized to mobile devices, the users performing the sync, and the action taken.

The top portion shows incidents by severity.
Viewing Incidents and Reports

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

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. |
Discovering Sensitive Data

<table>
<thead>
<tr>
<th>Sensitive data on shared folders accessible by everyone</th>
<th>Find out was sensitive data was found in shared folders.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data on file servers, SharePoint servers, and cloud servers</td>
<td>Find out was sensitive data was found on file, SharePoint, and cloud servers (for example, SharePoint 365 and Box).</td>
</tr>
<tr>
<td>Sensitive data on laptops</td>
<td>Find out was sensitive data was found on laptops</td>
</tr>
<tr>
<td>Sensitive data in databases</td>
<td>Find out was sensitive data was found in databases.</td>
</tr>
<tr>
<td>Sensitive data in private mailboxes</td>
<td>Find out was sensitive data was found in private mailboxes.</td>
</tr>
<tr>
<td>Sensitive data in public mailboxes</td>
<td>Find out was sensitive data was found in public mailboxes.</td>
</tr>
</tbody>
</table>

Discovering Databases

<table>
<thead>
<tr>
<th>Databases with credit card numbers</th>
<th>Find out which databases contain credit card numbers, and assess any violated policies on each database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases with personally identifiable information</td>
<td>Find out which databases contain personally identifiable information, and assess any violated policies on each database.</td>
</tr>
<tr>
<td>Databases with sensitive data</td>
<td>Find out which databases contain sensitive information, and assess any violated policies on each database.</td>
</tr>
<tr>
<td>Databases with PCI data</td>
<td>Find out which databases contain PCI data, and assess any violated policies on each database.</td>
</tr>
</tbody>
</table>

Discovering Mailboxes

<table>
<thead>
<tr>
<th>Mailboxes with credit card numbers</th>
<th>View which mailboxes contain credit card numbers, and assess any violated policies in each mailbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailboxes with personally identifiable information</td>
<td>View which mailboxes contain personally identifiable information, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Mailboxes with sensitive data</td>
<td>View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Mailboxes with PCI data</td>
<td>View which mailboxes contain PCI data, and assess any violated policies in each mailbox.</td>
</tr>
</tbody>
</table>
Executive Dashboard

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Provides an at-a-glance view of system metrics for information leaks in the system and the actions being taken on them.</th>
</tr>
</thead>
</table>

Status

<table>
<thead>
<tr>
<th>Incident status</th>
<th>View the status of all discovery incidents from the last 7 days.</th>
</tr>
</thead>
</table>

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.
- Customize the report via the Manage Report > Edit Filter page (see Managing incident reports, page 76).
- Schedule the report to be delivered by email (see Scheduling tasks, page 57).

**Sensitive data reports**

The sensitive data reports enable you to see where potentially sensitive data is located in your organization, and review any violated policies for those locations.

Note that for these reports to contain information, you must first run appropriate discovery tasks. For hosts, run a discovery task for endpoints, network folders, or SharePoint sites. For mailboxes or databases, run a network discovery task for Exchange servers or databases respectively.

1. Go to the **Main > Reporting > Discovery** page.
2. From the report catalog, expand the Discovered Sensitive Data folder and select one of the following reports:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data on file servers, SharePoint servers, and cloud servers</td>
<td>Find out what vulnerable data was most violated and where it is stored. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Sensitive data in private mailboxes</td>
<td>Find out which policies were violated most, and in which mailboxes the violations occurred. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Sensitive data in databases</td>
<td>Find out which policies were violated most, and in which databases the violations are located. Assess the security risk to your organization.</td>
</tr>
<tr>
<td>Mailboxes with sensitive data</td>
<td>View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.</td>
</tr>
<tr>
<td>Hosts with sensitive data</td>
<td>Find out which hosts contain sensitive information, and assess any violated policies on each host.</td>
</tr>
<tr>
<td>Databases with sensitive data</td>
<td>Find out which databases contain sensitive information, and assess any violated policies on each database.</td>
</tr>
</tbody>
</table>

3. Click **Run** to generate the report.
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*, page 115.

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

  For more information, see *Configuring the Web DLP Policy*, page 123.

- 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*, page 131.

- A rich set of predefined policies that cover the data requirements for a wide variety of organizations. They include:

  Related topics:
  - *Viewing policies*, page 104
  - *Creating Custom DLP Policies*, page 141
  - *Creating Discovery Policies*, page 255
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*, page 137.

- 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*, page 141.

---

**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?*, page 103.
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.

### Related topics:
- Managing rules, page 160
- Managing exceptions, page 161
- Classifying Content, page 165
- Defining Resources, page 223

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>Provide the logic for the policy. They are the conditions that govern the behavior of the policy. When should something be blocked? When should managers be notified? Rules can apply to a single breach or to the accumulation of breaches over a period of time. Standard rules create incidents every time a rule is matched. Cumulative rules accumulate matches over time and create incidents when a threshold is met. This is known as drip DLP.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Define the conditions that should be exempt from the rules. An exception is part of a rule and checked only when its rule is triggered. You cannot add exceptions to cumulative rules, and exceptions themselves cannot be cumulative.</td>
</tr>
</tbody>
</table>
These components are the building blocks of a policy. When you create a policy from a policy template, it 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.

### 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 policy toolbar

The policy toolbar provides many functions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Create a new policy, rule, or exception.</td>
</tr>
<tr>
<td>Edit</td>
<td>Update the selected policy, rule, or exception.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected policy, rule, or exception.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If you do not want to see incidents for a deleted policy, clear the check box for the policy in your Incident report list.</td>
</tr>
<tr>
<td>Show Disabled Rules</td>
<td>Show disabled rules in the policy tree.</td>
</tr>
<tr>
<td>Hide Disabled Rules</td>
<td>Hide disabled rules so they do not appear in the policy tree.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| ![More Actions](icon)| ● Use **Batch Operations** to update or delete multiple items at once. For example:  
  ■ Select **Update rules of current policy** to change one or more rules in the selected policy at the same time. This overrides the settings in the policy and reduces time and effort involved in updating multiple settings.  
  ■ Select **Update exceptions of current rule** to change one or more exceptions in the selected rule at the same time. This overrides the settings in the rule.  
  ■ Select **Update rules of multiple policies** to make changes to selected rules or all rules across multiple policies.  
  ■ Select **Update exceptions of multiple rules** to change selected exceptions or all exceptions across multiple rules.  
  ■ Select **Delete policies** to delete a batch of policies at once: a screen appears so you can choose which policies to delete.  
● Use **Rearrange Exceptions** to set the order of exceptions under the selected rule.  
● Use **Manage Policy Levels** to configure policy execution priority order. See **Policy levels**. |
| ![Export](icon)| 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. |
| ![Refresh](icon)| Refreshes the policy list. |

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

**Editing a policy**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The name for this policy.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this box to enable the rule for this policy. If this box is unselected, the rule is present, but disabled.</td>
</tr>
<tr>
<td>Policy description</td>
<td>Enter a description for this policy.</td>
</tr>
</tbody>
</table>
| Policy owners | If configured, policy owners receive notifications of breaches.  
To define an owner or owners for this DLP policy:  
1. Click **Edit**.  
2. Select one or more owners from the resulting box. See **Selecting items to include or exclude in a policy**, page 112, for instructions.  
3. Click **OK**. |
Update rules of current policy

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether to enable or disable all the selected rules. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of the selected rules.</td>
</tr>
<tr>
<td></td>
<td>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). 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 UEBA. Click  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 Custom Policy Wizard - Severity and Action, page 147, for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data to analyze. These sources are applied to all of the selected rules. See Custom Policy Wizard - Source, page 150, for more details. Any changes made here override all other configurations of source in the rule.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations to analyze. These destinations are applied to all of the selected rules. See Custom Policy Wizard - Destination, page 150, for more details. Any changes made here override all other configurations of destination in the rule.</td>
</tr>
</tbody>
</table>

6. Click OK.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the selected exceptions. This changes their state.</td>
</tr>
</tbody>
</table>
| Severity & Action | Specify the incident severity and action plan to apply to all of the selected rules.  
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). 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 UEBA. Click 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 Custom Policy Wizard - Severity and Action, page 147, for more details. |
| Source          | Select the sources of data you’d like to analyze. These sources are applied to all of the selected exceptions. See Custom Policy Wizard - Source, page 150, for more details. |
| Destination     | Select the data destinations that you want to analyze. These destinations are applied to all of the selected exceptions. See Custom Policy Wizard - Destination, page 150, for more details. |

6. Click **OK**.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the rules in the current policy. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of 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). 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 UEBA. Click 🔳 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 <em>Custom Policy Wizard - Severity and Action</em>, page 147, for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data you’d like to analyze. These sources are applied to all of the rules in the policy. See <em>Custom Policy Wizard - Source</em>, page 150, for more details.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations that you want to analyze. These destinations are applied to all of the rules in the policy. See <em>Custom Policy Wizard - Destination</em>, page 150, for more details.</td>
</tr>
</tbody>
</table>

7. Click **OK**.

**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:
Policies Overview

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether you want to enable or disable all the exceptions to the current rule. This changes their state.</td>
</tr>
<tr>
<td>Severity &amp; Action</td>
<td>Specify the incident severity and action plan to apply to all of this rule’s exceptions. 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). 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 UEBA. Click 👇 to create a new action plan and add it to all risk level action. See <a href="#">Custom Policy Wizard - Severity and Action</a>, page 147, for more details.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the sources of data you’d like to analyze. These sources are applied to all of this rule’s exceptions. See <a href="#">Custom Policy Wizard - Source</a>, page 150, for more details.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the data destinations that you want to analyze. These destinations are applied to all of this rule’s exceptions. See <a href="#">Custom Policy Wizard - Destination</a>, page 150, for more details.</td>
</tr>
</tbody>
</table>

7. Click **OK**.

**Delete policies**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

### 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**.

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**

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**

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, you would add user bsmith to the exclusions list.

A rule can have multiple exclusions.
To use the selector, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Select the entity—such as computers or networks if you are selecting a source—to display in the 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 Defining Resources, page 223, for instructions.</td>
</tr>
<tr>
<td>Filter by</td>
<td>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 “<em>jones</em>”. You can use additional wildcards in your filter string if desired. For example, “?” represents any single character, as in the example “file_.txt”. Click the search icon to filter the data.</td>
</tr>
<tr>
<td>Available items</td>
<td>Lists the items that are available for selection in the current display category. Use the page forward/backward controls to navigate from one page to the next, or to the first or last page. In some cases, a folder icon or up arrow appears. Click the icon to display the directory one level up in the directory tree. You can also click the breadcrumbs above the list to navigate to another level. If you chose Directory Entries in the Display field, hover over an item in this list to see all the fields that will be searched—login, full name, domain name, and email address.</td>
</tr>
<tr>
<td>Selected items</td>
<td>Use the right and left arrows to move items into and out of the selected list. If you want to include a computer named Bob_Computer, then highlight it on the left. Make sure the Include tab is active, and then click &gt;. If you want to exclude Bob_Computer, make sure the Exclude tab is active when you click &gt;. 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. Tip: you can move a group of users, computers, networks, etc. into the Include box, then remove one user, computer, or network by highlighting it on the right and clicking Remove.</td>
</tr>
</tbody>
</table>

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

On the sources and destinations selector:

1. From the drop-down list box, select one of the following:
   - Use Predefined lists to select from lists.
   - Use Free text to type the name of an item to include.
2. If you choose Predefined lists, complete the fields described above.
If you choose Free text, use the space provided to specify the entity to include:

When selecting a source, for example, to select an owner, type the corresponding email address. To select a computer, type the hostname or IP address.

- Optionally enter multiple items in a comma-separated list. For example:
  
  ssmith@example.com, mjones@example.com

- By default, the system searches for all entities containing the word or words you enter. For example, if you type “jones” for policy owner, it might return mjones@example.com, jjones@acme.com, and sjones@abc.com.

  Entering “jones” is equivalent to searching “*jones*”. Additional wildcards are allowed.

3. Click **OK**.
Forcepoint DLP can help administrators control how sensitive data moves through their organization via email using the email DLP quick policy. (Note that the email DLP policy applies to network channels only. To monitor email on endpoint machines, such as laptops that are off-network, create a custom policy.)

- 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.

---

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 and click **Email** to open the Email Security module.
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. Click **Data** in the Security Manager toolbar 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*, page 117.
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*, page 120.
9. Identify trusted domains, if any. See *Identifying email DLP trusted domains*, page 121.
10. Click **OK**.

---

**Note**

The email DLP policy cannot be deleted or renamed, but its attributes can be enabled or disabled.
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.
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*, page 240.
   - 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size</td>
<td>The size of email messages to monitor. Only messages of the specified size or higher are monitored. The default size is 10 MB. Default severity: low. Available actions: quarantine (default), permit.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Regulatory & compliance | 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.)
- **Personally Identifiable Information (PII)**
- **Protected Health Information (PHI)**
- **Payment Card Industry (PCI DSS)**
After selecting a law, click its name to view or edit the specific policies to enforce, then select a sensitivity for each policy.
- **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.
Default severity: **high**.
Available actions: **quarantine** (default), **permit**.

Attachment name | One by one, enter the names of the exact files that should be monitored when they're attached to an email message. Include the filename and extension. Click **Add** after each entry.
For example, 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.
Note that only Forcepoint Email Security can drop attachments. If the drop attachments options is selected when the protector is monitoring email, messages are quarantined when a policy is triggered.
Default severity: **low**.
Available actions: **quarantine, permit, drop attachments** (default).

Attachment type | Click **Add** to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files.
Select the type or types of files to monitor. If there are more file types than can appear on the page, enter search criteria to find the file type you want. The system searches in the file type group, description, and file type for the data you enter.
If the file type does not exist, specify exact files of this type using the **Attachment name** attribute instead.
Default severity: **low**.
Available actions: **quarantine, permit, drop attachments** (default).
**Note:** Only Forcepoint Email Security can drop attachments. If the drop attachments options is selected when the protector is monitoring email, messages triggering a policy are quarantined.
Configuring the Email DLP Policy

Patterns & phrases
Click Add to define key phrases or regular expression (regex) patterns that should be monitored. Regex patterns are used to identify alphanumeric strings of a certain format. Enter the precise phrase (for example “Internal Only”) or regex pattern (for example – m/H.?e/) to include. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1. Define whether to search for the phrase or regex pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields. Default severity: medium. Available actions: quarantine (default), permit.

Note: Although you do not define whether to search only for unique strings, the system uses the following defaults:
- Key phrase searches are non-unique. All matches are reported.
- For regular expression searches, only unique matches are reported as triggered values.

Acceptable use
Select the dictionaries that define unacceptable use in your organization. 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. Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce.

You cannot add or delete terms from predefined dictionaries, but you can exclude 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.

By default, the policy is triggered by a single match from the dictionary or dictionaries you select. Default severity: medium. Available actions: quarantine (default), permit.

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

Number of attachments
Specify the number of attachments to detect. Email messages with this number of attachments (or more) trigger the policy. The default number of attachments is 20. Default severity: low. Available actions: quarantine (default), permit.
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, page 112, 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, page 251, for more information.
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.

To define trusted domains:

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

**Note**

Trusted domain definitions apply to outbound email traffic only.
Configuring the Web DLP Policy

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.

**Web DLP policy configuration overview**

To configure the web DLP quick policy:

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, page 124.
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, page 128.
4. Select the Policy Owners tab, then identify an owner for the policy.
   See Defining web DLP policy owners, page 130.
5. Click OK.

---

**Note**

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

**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, page 240.*

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*, page 123.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post size</td>
<td>Disabled by default. 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). Default severity: low. Available actions: block (default), permit.</td>
</tr>
<tr>
<td>Regulatory &amp; Compliance</td>
<td>Enabled by default. 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.) After selecting a category, click its name to view or edit the specific policies to enforce. Applying specific policies improves performance and reduces resource consumption. Select a sensitivity for each policy. ● <strong>Wide</strong> 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). ● <strong>Default</strong> balances the number of false positives and false negatives and is recommended for most customers. ● <strong>Narrow</strong> is the least restrictive. It is more likely to let content through than to produce an unintended match. For best practice, use this level when you first start using the block action. You might also use it if the system is detecting too many false positives. Default severity: high. Available actions: block (default), permit.</td>
</tr>
</tbody>
</table>
Configuring the Web DLP Policy

Data theft: Disabled by default.
- 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. Select the type of data to search for in outbound transactions. When sent outside your network, this data can indicate a serious vulnerability.
- **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.

Select a sensitivity for each policy. Sensitivity levels are described in more detail in the Regulatory & Compliance section, above.

**Note:** The selected number of policies and their sensitivity levels affect performance.

Default severity: **high**.
Available actions: **block** (default), **permit**.

Name of uploaded file: Disabled by default.
- One by one, enter the names of the exact files that should be monitored when they’re posted or uploaded to the Web. Include the file name and extension. Click **Add** after each entry.
- 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.
- The system can detect files even when they’ve been compressed into an archive, such as a .zip file.
- Default severity: **low**.
- Available actions: **block** (default), **permit**.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data theft</td>
<td>Disabled by default. The system protects against content being posted to the Web after your computer is infected. This complements Forcepoint Web Security, which protects against infected content downloaded from the Web. Select the type of data to search for in outbound transactions. When sent outside your network, this data can indicate a serious vulnerability.</td>
</tr>
<tr>
<td></td>
<td><strong>Suspected malware communication</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Encrypted files - unknown format</strong> searches for outbound files that were encrypted using unknown encryption formats, based on advanced pattern and statistical analysis of the data.</td>
</tr>
<tr>
<td></td>
<td><strong>Encrypted files - known format</strong> searches for outbound transactions comprising common encrypted file formats, such as password-protected Microsoft Word files.</td>
</tr>
<tr>
<td></td>
<td><strong>Password files</strong> searches for password files, such as a SAM database and UNIX/Linux password files.</td>
</tr>
<tr>
<td></td>
<td><strong>Common password information</strong> searches for password information in plain text by looking for common password patterns and using various heuristics.</td>
</tr>
<tr>
<td></td>
<td><strong>IT asset information</strong> searches for electronic data containing suspicious content, such as network data, software license keys, and database files.</td>
</tr>
<tr>
<td></td>
<td><strong>Suspicious behavior over time</strong> searches for activity considered to be potentially malicious, such as numerous posts in a designated period or numerous transactions containing encrypted data.</td>
</tr>
<tr>
<td></td>
<td>Select a sensitivity for each policy. Sensitivity levels are described in more detail in the Regulatory &amp; Compliance section, above.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The selected number of policies and their sensitivity levels affect performance.</td>
</tr>
<tr>
<td></td>
<td>Default severity: <strong>high</strong>. Available actions: <strong>block</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Name of uploaded file</td>
<td>Disabled by default. One by one, enter the names of the exact files that should be monitored when they’re posted or uploaded to the Web. Include the file name and extension. Click <strong>Add</strong> after each entry.</td>
</tr>
<tr>
<td></td>
<td>For example, after adding a file named <strong>confidential.docx</strong>, when a user attempts to post a file with that name, the system detects it and takes the configured action.</td>
</tr>
<tr>
<td></td>
<td>The system can detect files even when they’ve been compressed into an archive, such as a .zip file.</td>
</tr>
<tr>
<td></td>
<td>Default severity: <strong>low</strong>. Available actions: <strong>block</strong> (default), <strong>permit</strong>.</td>
</tr>
</tbody>
</table>
Configuring the Web DLP Policy

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.
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:

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**, page 231.
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, page 112, 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, page 251, for more information.
Configuring the Mobile DLP Policy

Use the Forcepoint DLP mobile DLP quick policy to define what content can and cannot be sent to mobile devices—such as phones and iPads—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. In addition, the mobile agent must be installed in the DMZ and connected to both an Exchange server and the Forcepoint management server. (See Configuring the mobile agent, page 395, for more information.)

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.

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.
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, page 132.
2. Identify users that don’t need to be monitored (trusted users), if any.
   See Defining mobile DLP trusted users, page 134.
3. Identify one or more owners for the policy.
   See Defining policy owners, page 135.
4. Click OK.

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

### 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, page 240.
   See Mobile DLP attribute properties, page 133, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size</td>
<td>The size of email messages to monitor. Only messages of the specified size or higher are monitored. The default size is 10 MB. Default severity: <strong>low</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Regulatory &amp; Compliance</td>
<td>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 <strong>Select regions</strong> to address the issue.)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Personally Identifiable Information (PII)</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Protected Health Information (PHI)</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Payment Card Industry (PCI DSS)</strong></td>
</tr>
<tr>
<td></td>
<td>After selecting a law, click its name to view or edit the specific policies to enforce, then select a sensitivity for each policy.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wide</strong> is highly sensitive and errs on the restrictive side. To avoid leaking sensitive data, it is more likely to produce a false positive (unintended match) than a false negative (content that is not detected).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong> balances the number of false positives and false negatives.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Narrow</strong> is the least restrictive. It is more likely to let content through than to produce an unintended match.</td>
</tr>
<tr>
<td>Default severity: <strong>high</strong>.</td>
<td>Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Attachment name</td>
<td>One by one, enter the names of the exact files that should be monitored when they’re attached to an email message. Include the filename and extension. Click <strong>Add</strong> after each entry. For example, after adding a file named <strong>confidential.docx</strong>, when a user attaches a file with that name to an email message, the system detects it and takes the configured action. Default severity: <strong>low</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Attachment type</td>
<td>Click <strong>Add</strong> to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files. Select the type or types of files to monitor. If there are more file types than can appear on the page, enter search criteria to find the file type you want. The system searches in the file type group, description, and file type for the data you enter. If the file type does not exist, specify exact files of this type using the <strong>Attachment name</strong> attribute instead. Default severity: <strong>low</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
</tbody>
</table>
Configuring the Mobile DLP Policy

### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patterns &amp; phrases</td>
<td>Click <strong>Add</strong> to define key phrases or regular expression (regex) patterns that should be monitored. Regex patterns are used to identify alphanumeric strings of a certain format. On the resulting dialog box, enter the precise phrase (for example “Internal Only”) or regex pattern (for example ~ m/H.?e/) to include. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1. Define whether to search for the phrase or regex pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields. Default severity: <strong>medium</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>. Note: Although you do not define whether to search only for unique strings, the system uses the following defaults: ■ Key phrase searches are non-unique. All matches are reported. ■ For regular expression searches, only unique matches are reported as triggered values.</td>
</tr>
<tr>
<td>Acceptable use</td>
<td>Select the dictionaries that define unacceptable use in your organization. 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. Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce. You cannot add or delete terms from predefined dictionaries, but you can exclude terms from detection, if needed. Do this on the <strong>Main &gt; Content Classifiers &gt; Patterns &amp; Phrases</strong> page. Select the dictionary to edit, then enter the phrases to exclude. By default, the policy is triggered by a single match from the dictionary or dictionaries you select. Default severity: <strong>medium</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Questionable images</td>
<td>Select this attribute to prevent pornographic images from entering your organization. Pornographic images pose a legal liability to organizations in many countries. The system judges images based on the amount of flesh tone they contain. Default severity: <strong>low</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
</tbody>
</table>

---

Administrator Help | Forcepoint DLP | Version 8.5.x
If you have users that should not receive mobile DLP policy enforcement:

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, page 112, 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, page 251, for more information.
Using Predefined DLP and Discovery Policies

Administrator Help | Forcepoint DLP | Version 8.5.x

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 to 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

Administrator Help | Forcepoint DLP | Version 8.5.x

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

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
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, page 138**, for information about the resulting page.

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.
Using Predefined DLP and Discovery Policies

- 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.

---

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, page 223.
- To create discovery policies, see Creating Discovery Policies, page 255.

---

**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.

---

**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:

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

Administrator Help | Forcepoint DLP | Version 8.5.x

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

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.
Creating Custom DLP Policies

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, page 142.
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 topics:
- Managing rules, page 160
- Managing exceptions, page 161
- Defining Resources, page 223
Creating Custom DLP Policies

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:

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, page 112.
   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, page 142.

Related topics:
- Classifying Content, page 165
- Custom Policy Wizard - Severity and Action, page 147

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*, page 144.

With dictionary classifiers, the weights of the dictionary’s phrases are taken into account when determining if a threshold is reached. See *Adding a dictionary classifier*, page 177, 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.

**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* for information about additional configurable properties that are unique to fingerprint classifiers.
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*, page 177.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File/attachment</td>
<td>Search files or attachments for each chosen destination channel.</td>
</tr>
<tr>
<td>File metadata</td>
<td>Search the metadata of files or attachments.</td>
</tr>
<tr>
<td>Subject</td>
<td>Search only the subject line of messages.</td>
</tr>
<tr>
<td>Body</td>
<td>Search only the main body of a messages.</td>
</tr>
<tr>
<td>From</td>
<td>Search only the From field of a message.</td>
</tr>
<tr>
<td>To</td>
<td>Search only the To field of a message (email only).</td>
</tr>
<tr>
<td>Cc</td>
<td>Search only the carbon copy field of a message (email only).</td>
</tr>
</tbody>
</table>
Creating Custom DLP Policies

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.

**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.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bcc</td>
<td>Search only the blind carbon copy field of a message (email only).</td>
</tr>
<tr>
<td>Other header</td>
<td>Search in headers that are not covered by the above options:</td>
</tr>
<tr>
<td></td>
<td>• Search in <strong>All headers</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• Search in <strong>User-defined header</strong>. 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.</td>
</tr>
</tbody>
</table>
• 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.)

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

**Note**

If 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*, page 199.

**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.
Creating Custom DLP Policies

- **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*, page 239, 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 Plan** table, 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.
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). 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 UEBA.

Click 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 The RAP service, page 344 and Configuring the RAP service, page 344.

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.

Note
The Risk Adaptive Protection section only affects users that were defined as risk adaptive users (see Custom user directory groups, page 226 and Custom users, page 228 pages on how to define such users.)
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.

**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.

1. To define specific sources of data, click **Edit**, then see *Selecting items to include or exclude in a policy*, page 112.
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*, page 150.

**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**
Creating Custom DLP Policies

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, page 112.

---

### Standard Forcepoint DLP options

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.
     - Although Forcepoint Email Security will analyze all 3 directions, Forcepoint DLP Email Gateway will analyze only outbound traffic.
     - Protectors monitor all traffic directed to them. All transactions are regarded as outbound.

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 endpoint applications.

3. Select **CASB Service** to analyze files sent to supported cloud applications.
   - This option is available only when the CASB service is enabled on the Settings > General > Services page.

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*, page 231.

- 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*, page 421.

6. Select **Cloud Services** (enabled by default) to analyze content that is sent to cloud services, such as Microsoft OneDrive for Business or Box.

7. Select **Endpoint Printing** to analyze files that endpoint users send to printers.
   (Requires Forcepoint DLP Endpoint.)
   
   To select the printers to analyze click **Edit**.

8. 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*. 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.

9. 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*, page 421.
   - Linux-based endpoints cannot share removable media devices through NFS.

10. 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.

---

**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.

Click **Edit** to select the email destination to analyze.
Rule Wizard - Finish

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.
Patterns & Phrases

Administrator Help | Forcepoint DLP | Version 8.5.x

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, page 181*.

Properties tab

Administrator Help | Forcepoint DLP | Version 8.5.x

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

1. Set the **Threshold** that determines the number of matches that trigger an incident:
Creating Custom DLP Policies

- 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File/attachment</td>
<td>Search files or attachments for each chosen destination channel.</td>
</tr>
<tr>
<td>File metadata</td>
<td>Search the metadata of files or attachments.</td>
</tr>
<tr>
<td>Subject</td>
<td>Search only the subject line of messages.</td>
</tr>
<tr>
<td>Body</td>
<td>Search only the main body of a messages.</td>
</tr>
<tr>
<td>From</td>
<td>Search only the From field of a message.</td>
</tr>
<tr>
<td>To</td>
<td>Search only the To field of a message (email only).</td>
</tr>
<tr>
<td>Cc</td>
<td>Search only the carbon copy field of a message (email only).</td>
</tr>
<tr>
<td>Bcc</td>
<td>Search only the blind carbon copy field of a message (email only).</td>
</tr>
<tr>
<td>Other header</td>
<td>Search in headers that are not covered by the above options:</td>
</tr>
<tr>
<td></td>
<td>- Search in <strong>All headers</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>- Search in <strong>User-defined header</strong>. 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”.</td>
</tr>
<tr>
<td></td>
<td>After selecting this option, enter the header name.</td>
</tr>
</tbody>
</table>
### 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*, page 179).
  - 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.

### Properties tab

Use the Properties tab to configure the threshold for matches.

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

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.)

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

Note

If 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, page 199.
## Properties tab

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>A condition’s threshold is the number of matches that trigger an incident.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>At least</strong> - select the minimum number of matches that must be</td>
</tr>
<tr>
<td></td>
<td>made. Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Between</strong> - select an exact range of matches that must be made.</td>
</tr>
<tr>
<td></td>
<td>Valid values are 1-999.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No match exists</strong> - trigger the rule if there are no matches.</td>
</tr>
</tbody>
</table>

| Email Fields           | Click **Email Fields** to view and select the email fields to search for  |
|                       | this condition.                                                            |

| Search in all the      | Select to search the entire email message for the key phrase, regular      |
| email fields           | expression, or dictionary terms. This is the default.                     |

| Search only in         | Select to search only specific parts of the email message. Choose one or   |
| these fields           | more of the following:                                                     |
|                       |   - **Attachment** - search only in email attachments                      |
|                       |   - **Subject** - search only in the subject line of the email message     |
|                       |   - **Body** - search only in the main body of the email message           |
|                       |   - **From** - search only in the From field of the email message          |
|                       |   - **To** - search only in the To field of the email message              |
|                       |   - **Cc** - search only in the carbon copy field of the email message     |
|                       |   - **Bcc** - search only in the blind carbon copy field of the 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:
Creating Custom DLP Policies

- 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*, page 221.)
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*.

**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, the 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, page 162*, for information on ordering exceptions.

**Rearranging exceptions**

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:

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, page 163*.

Complete the information on each page and click **Next** to proceed through the wizard.
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, page 163).

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, page 142, for explanations of the condition properties.
- Select Source to change the source of data defined for the rule.
  See Custom Policy Wizard - Source, page 150, for explanations of the source properties.
- Select Destination to change the destination of data defined for the rule.
  See Custom Policy Wizard - Destination, page 150, 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, page 164).
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*, page 239.

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). 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 UEBA.

4. Click ☐ 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, page 226 and Custom users, page 228 pages on how to define such users.)

5. Click **Next** to continue to the Finish page of the exception wizard. See Exception Wizard - Finish, page 165.

### 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.

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.
Classifying Content

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.

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td></td>
</tr>
<tr>
<td><strong>Patterns &amp; Phrases</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>File properties</strong></td>
<td>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).</td>
</tr>
<tr>
<td>Fingerprints</td>
<td></td>
</tr>
<tr>
<td><strong>File fingerprinting</strong></td>
<td>Fingerprint files or directories, including Microsoft SharePoint and IBM Domino directories.</td>
</tr>
<tr>
<td><strong>Database fingerprinting</strong></td>
<td>Fingerprint database records directly from your database table, Salesforce table, or CSV file.</td>
</tr>
<tr>
<td>Machine Learning</td>
<td></td>
</tr>
<tr>
<td><strong>Machine learning</strong></td>
<td>Provide examples of the data to protect, so the system can learn from them and identify data of a similar nature.</td>
</tr>
</tbody>
</table>

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*, page 201, and *Creating a validation script*, page 202.

Forcepoint DLP automatically runs validation scripts on your new database fingerprinting classifiers if the scripts are set up properly.
Content classifier menu bar

When working with most content classifiers, the toolbar at the top of the content pane offers the following options:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Opens a dialog so you can create a new classifier of the selected type.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected classifier. Be sure to check where the classifier’s used before deleting it. (See Where Used, below.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can delete only one classifier at a time. If you’re deleting a fingerprint classifier and the crawler is unresponsive, you’re asked to delete the classifier manually. (See Manually deleting fingerprinting classifiers, page 168 for instructions.)</td>
</tr>
<tr>
<td>Create Rule from Classifier</td>
<td>Creates a rule from the selected classifier and lets you mark it for use in an existing or new policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can create a rule from only one classifier at a time.</td>
</tr>
<tr>
<td></td>
<td>See Creating a rule from a content classifier for more details on this shortcut.</td>
</tr>
<tr>
<td>Where Used</td>
<td>Shows which policies, rules, and exceptions use this classifier.</td>
</tr>
</tbody>
</table>

The fingerprinting and machine learning classifiers have additional menu options.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Begins the fingerprinting or machine learning scan. Alerts that the task will be moved into manual mode.</td>
</tr>
<tr>
<td>Pause</td>
<td>Fingerprinting only. Pauses the scan.</td>
</tr>
<tr>
<td>Stop</td>
<td>Stops the fingerprinting or machine learning scan. Alerts that the task will resume at the next scheduled time or the next time it is run manually.</td>
</tr>
<tr>
<td>More Actions</td>
<td>In addition to Create Rule from Classifier and Where Used, fingerprinting and machine learning classifiers offer a reporting option under More Actions:</td>
</tr>
<tr>
<td></td>
<td><strong>Download Fingerprinting Report</strong> - Database fingerprinting only. Downloads a detailed report on fingerprinting activities.</td>
</tr>
<tr>
<td></td>
<td><strong>Download Machine Learning Report</strong> - Machine learning classifiers only. Downloads a detailed report on machine learning processes. Using this report, you can:</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
</tbody>
</table>
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, page 169.

**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:
   a. 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.

   b. 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:

```
<jobj 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.pyc -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* (below) and *Machine learning details*, page 171.

### Fingerprinting details

For fingerprinting classifiers, the details pane shows the following Scan details:

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

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.)

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

In addition, statistics are displayed for the most recently run scan, or the scan in progress (if any).

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanned files</td>
<td>The total number of items detected in the last scan</td>
</tr>
<tr>
<td>Scanned size</td>
<td>The size of items detected in the scan, all totaled. (Does not apply to database scans.)</td>
</tr>
<tr>
<td>Scan/fingerprinting progress</td>
<td>The progress of the scan, in percentage completed</td>
</tr>
<tr>
<td>Fingerprinted files/records</td>
<td>The number of items sent to the policy engine’s fingerprint repository</td>
</tr>
<tr>
<td>Failed files</td>
<td>The number of files that could not be fingerprinted for some reason—such as access to the folder was denied or the file was not found. Click the link to see why fingerprinting failed for these files.</td>
</tr>
<tr>
<td>Filtered-out files</td>
<td>The files that were not included in the scan because of the file filters you specified when you defined the task. (These files that were ignored by the crawler because they matched a filter.) Click the link to see the precise file type, age, or size filter that was matched.</td>
</tr>
<tr>
<td>Estimated total files/records</td>
<td>An estimate of the total number of items</td>
</tr>
<tr>
<td>Estimated total size</td>
<td>An estimate of the total size of items</td>
</tr>
</tbody>
</table>
Machine learning details

For machine learning classifiers, the Active Classifier section of the details pane shows the following information:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>Expected rate of unintended and undetected matches (false positives and false negatives).</td>
</tr>
<tr>
<td>Last successful scan time</td>
<td>The time and date of the last successful scan</td>
</tr>
<tr>
<td>All documents folder</td>
<td>Path to the all documents folder</td>
</tr>
<tr>
<td>Positive examples folder</td>
<td>Path to the positive examples folder</td>
</tr>
<tr>
<td>Negative examples folder</td>
<td>Path to the negative examples folder</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>How sensitive the classifier is when detecting matches—in other words, how closely content has to match the positive examples to be considered an incident.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Wide</strong> is highly sensitive and errs on the restrictive side. To avoid leaking sensitive data, it is more likely to produce a false positive (unintended match) than a false negative (content that is not detected).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong> balances the number of false positives and false negatives.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Narrow</strong> is the least restrictive. It is more likely to let content through than to produce an unintended match. Click the link to adjust the sensitivity level. Your choice depends on how important it is to prevent sensitive data loss.</td>
</tr>
<tr>
<td>Ignore inconsistent examples</td>
<td>Indicates whether to ignore documents that do not appear to belong to the positive examples folder or to use them as positive examples anyway. To view a list of inconsistent example documents, download the Machine Learning report.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run time</td>
<td>The time and date that the machine learning process last ran</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the current content scan. See <em>Machine learning current scan status options</em>, page 172, for an explanation of each status option. 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.</td>
</tr>
<tr>
<td>All documents folder</td>
<td>Path to the all documents folder</td>
</tr>
</tbody>
</table>
Classification Content

### 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.
Classifying Content

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.

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\d+” matches all strings that start with the letter “a” and are followed by at least one digit, where “\d” represents any digit and “+” represents “at least one.” When the extracted text from a transaction is scanned, 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}[-\s]\d{4}[-\s]\d{4}[-\s]\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 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 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.

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. (Refer to File-type classifiers for details about each predefined file-type classifier.)

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

File-size classifiers identify files by their size.

Tip
For a list of supported file types, see Supported File Formats.

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

Adding a file-type classifier

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.

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.

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 Size 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.

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.

**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.

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.
   - Refer to 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.

Use the Main > 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.

1. The File Fingerprinting page displays a list of fingerprinting classifiers:
   - Expand the right pane to view more details, such as last run time and next run time, or you can collapse it to show fewer.
   - Click the links in the details pane to learn more about the fingerprinted files and folders.
   - Start, stop, or pause a fingerprinting task using buttons in the toolbar at the top of the content pane.

2. To create a fingerprinting classifier, 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, page 184)
   - SharePoint Fingerprinting (see SharePoint Fingerprinting Wizard - General, page 188)

You can fingerprint data on sites running the following versions of Microsoft SharePoint:
- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Related topics:
- Managing Forcepoint DLP, page 6
- Classifying Content, page 165
Domino Fingerprinting (see *Domino Fingerprinting Wizard - General, page 193*)

**Important**

To use this feature:

- 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.

See the [Forcepoint DLP Deployment Guide](#) for step-by-step instructions.

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

**Note**

To import an existing fingerprinting classifier—one that has been exported and copied to a network location—select **Import** from the toolbar. See *Imported fingerprinting, page 215*.

---

**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:

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.

6. Click **Next** to continue. See *File System Fingerprinting Wizard - Root Folder*, page 185.

**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:
   ```plaintext
   \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*, page 186.

When you click Next, Forcepoint DLP tries to connect to the root folder using the given credentials. You are alerted if the attempt fails.
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.

- Click Edit to modify the list.
- 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, page 186.

File System Fingerprinting Wizard - Scheduler

Use the Scheduler page of the file system fingerprinting wizard to determine when to start the scan:

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.

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.
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**, page 187.
   - Otherwise, see **File System Fingerprinting Wizard - Finish**, page 188.

### 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**, page 215, for details. (The disconnected network must also have a management server.)
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*, page 188.

### 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:

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.
Classifying Content

- 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, page 189.*

**SharePoint Fingerprinting Wizard - Site Root**

Use the Site Root page of the SharePoint fingerprinting wizard to identify the folders to scan:

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*, page 190.

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.

**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*, page 190.

**SharePoint Fingerprinting Wizard - Scheduler**

Use the Scheduler page of the SharePoint fingerprinting wizard to determine when to start the scan:

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*, page 191.

**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.

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*, page 192.
   - Otherwise, see *SharePoint Fingerprinting Wizard - Finish*, page 192.
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*, page 215, for details. (The disconnected network must also have a management server.)

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*, page 192

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

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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*, page 194.

**Domino Fingerprinting Wizard - Server**

Use the Server page of the Domino fingerprinting wizard to specify which IBM Domino server to scan.

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*, page 194.

**Domino Fingerprinting Wizard - Scanned Documents**

Use the Scanned Documents page of the Domino fingerprinting wizard to define which documents and folders to scan.

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.
Classifying Content

- 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, page 195.

Domino Fingerprinting Wizard - Scheduler

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Scheduler page of the Domino fingerprinting wizard to determine when to start the scan:

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*, page 196.

**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.

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*, page 196.

**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.
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*, page 197.
   - Otherwise, see *Domino Fingerprinting Wizard - Finish*, page 198.

**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*, page 215, for details. (The disconnected network must also have a management server.)

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*, page 198

**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.
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 Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (32- and 64-bit)
  - Microsoft SQL Server Express (SQL Server Express ODBC driver)
  - IBM DB2 9.5 (ODBC driver 8.2.9)
  - IBM Informix Dynamic Server 11.50 (IBM Informix ODBC driver 3.50)
  - MySQL 5.1 (ODBC driver 5.1.5)
    - Due to MySQL limitations, you must define “string” columns with UTF-8 encoding to fingerprint them.
  - Sybase ASE 15.0 (Sybase ODBC driver 15.0.0.152)
  - Teradata v13 and v14
- Salesforce.com
- CSV files (UNC path needs to be specified. For example, `\server\share\path_to_file.csv`)

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:

- CHAR
- VARCHAR
- WCHAR
- WVARCHAR
- TINYINT
- SMALLINT
- INTEGER
- BIGINT
- DECIMAL
- NUMERIC
- REAL
- FLOAT
- DOUBLE
- TIME
Preparing for database fingerprinting

Administrator Help | Forcepoint DLP | Version 8.5.x

Before creating a database fingerprinting classifier, there are several preparatory steps to perform to streamline the process and optimize the results. See:

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

Creating a Data Source Name (DSN) in Windows

Administrator Help | Forcepoint DLP | Version 8.5.x

---

**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:

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**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.
Classifying Content

- *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, page 208*. 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.

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

The first 3 files are also included (with the .sample extension, for the batch and ini files) in the 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).
Classifying Content

- 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

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

1. Avoid fingerprinting short values

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

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

- 4 digits easily match years (frequently appearing in email)
Classifying Content

- 3 digits are quite common
- 1 and 2 digits numbers match days of month

The validation script template is a script that removes numbers with values less than the configured minimum (see Patterns & Phrases, page 173, for more details).

---

**Note**

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

---

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

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

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

---

**Note**

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

---

2. Avoid fingerprinting columns with repetitive values

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

For now, 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.
3. Avoid fingerprinting uninteresting / irrelevant values

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

The validation script template (described under Creating a validation script, page 202) allows you to ignore values that are specified in an external “ignored dictionary” file. If preferred, you can write your own scripts that filter any custom type of irrelevant data.

How matches are counted

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

For example, consider the following table:

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

And a condition specifying the combination of Column_A and Column_B.

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

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

Use the Main > Policy Management > Content Classifiers > Database Fingerprinting page to classify your content by fingerprinting database records.

1. The Database Fingerprinting page displays a fingerprint list appears.
   - Expand the right pane to view more details, such as last run time and next run time, or collapse it to show fewer details.
   - Click the links in the details pane to learn more about the fingerprinted records.
   - Start, stop, or pause a fingerprinting task using buttons in the toolbar at the top of the content pane.

2. To create a new classifier, 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, page 209.

---

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, page 201, 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, page 215*, for more information.

---

**Database Fingerprinting Wizard - General**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the General page of the database fingerprinting wizard to name the classifier and configure its high-level properties:

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, page 209*.

**Database Fingerprinting Wizard - Data Source/Site**

Administrator Help | Forcepoint DLP | Version 8.5.x

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

- **Database table, page 210**
- **Salesforce site, page 210**
- **CSV file, page 210**

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, page 211*. 
Database table

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*, page 201.
     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*, page 200.
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.

Salesforce site

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

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, page 211
- Salesforce site, page 212

After clicking Next on this page, see Database Fingerprinting Wizard - Scheduler, page 213.

Database table or CSV file

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.

---

**Tip**

When selecting the fields to fingerprint, be sure to follow the guidelines in Selecting the data to fingerprint, page 205. Avoid fingerprinting short values, columns with repetitive values, and uninteresting or irrelevant values.
Classifying Content

**Note to Informix users**
The system cannot fingerprint Informix tables that have names containing a backslash character. There is a workaround, however.

1. Mark **Select up to 32 fields from a table**.
2. Select the table and fields.
3. Copy the query from the **Selection as SQL query** field.
4. Mark **Use the following SQL query to select records**.
5. Paste the query into the box.
6. Surround the table name with double quotes. For example:
   ```sql
   SELECT "name","id","cc","phone" FROM "blade2\informix".custdb.
   ```

---

**Salesforce site**

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 use 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:

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*, page 213.

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.
  a. 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.
  b. 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*, page 214
- *Database Fingerprinting Wizard - Finish*, page 214

**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*, page 215, for details. (The disconnected network must also have a management server.)

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*, page 214.

**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.


Import Fingerprint Wizard - Import Source

Use the Source page of the import fingerprint wizard to specify the classifier location and select a crawler.

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, page 216.
Import Fingerprint Wizard - Properties

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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, page 216*.

Import Fingerprint Wizard - Scheduler

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Scheduler page of the import fingerprint wizard to determine when to start the scan:

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, page 217*. 
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 propriety marketing plans
Classifying Content

- 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, refer to Introduction to Machine Learning for Forcepoint DLP.

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, page 218.

Machine Learning Wizard - General

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the General tab of the machine learning wizard to set a name and description for the classifier.

1. Enter a meaningful Name for the machine learning classifier, such as “Engineering source code.”
2. Enter a Description of this set of classifier.

Machine Learning Wizard - Credentials

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Credentials tab of the machine learning wizard to identify which crawler to use to scan documents, and where the documents are located.

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.
**Classifying Content**

- 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).


**Machine Learning Wizard - Scanned Folders**

*Administrator Help | Forcepoint DLP | Version 8.5.x*

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.

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
Classifying Content

- 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, page 220.

**Machine Learning Wizard - Scheduler**

Administrator Help | Forcepoint DLP | Version 8.5.x

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, page 221.

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.
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**.
     e. Click **Edit** to select one or more **Policy Owners** from a list.
3. Click **OK** to save your changes.
Defining Resources

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 3 general areas: General, 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.
Defining Resources

- *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.

**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.

**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.

**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 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.
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 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, where level 1 gets the most permissive actions. The values are determined by Forcepoint UEBA and sent to Forcepoint DLP.

---

**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**, page 231, for more information).

---

To add a custom user directory group to a policy, first add it to a business unit. Then, 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:

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] [: 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).
Custom users

To add a custom user, click New, then:

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:

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:

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:

1. Complete the fields as follows:
2. 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.
3. Enter a **Description** for this domain.
4. 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*, page 231, for more information.
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. (Note that the system does not monitor URL categories on endpoint web channels.)

URL categories are imported from the Forcepoint Master Database, and can therefore be viewed but not changed. Periodically click Update Now to reconnect with the database and update your category list.

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 Configuring Linking Service, page 339.

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 Settings > General > 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)
   - Custom User Directory Groups
   The selected entry appears in the **Available List** grouping at the bottom of the page.
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 and 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.
6. Click **OK**.

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.

Endpoint Devices

Use the Main > Policy Management > Resources > Business Units 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:

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.
5. Click OK.

Tip
To filter reports by device serial number, use free text under Filter by Destination.

Endpoint Applications

Forcepoint provides a long list of built-in applications that you can choose to monitor on the endpoint when you set up your endpoint policy. These applications, including web applications and SaaS 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.
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.

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

To define your own application group, click **New > Application Group** or **New > Cloud Application Group**, then see *Adding custom application groups*, page 236, for instructions.

### 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).

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. This may include:

- **Action Plans**, page 239
- **Remediation scripts**, page 247
• *Notifications*, page 251
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and Notify</td>
<td>Audit incidents from all channels, and if configured, generate notifications.</td>
</tr>
<tr>
<td>Audit Only (Default)</td>
<td>(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.</td>
</tr>
<tr>
<td>Audit Without Forensics</td>
<td>Same as Audit Only, but does not store forensic data for the incident.</td>
</tr>
<tr>
<td>Block All</td>
<td>Block all incidents on all channels, audit them, and, if configured, generate notifications. This action plan is designed for severe breaches.</td>
</tr>
<tr>
<td>Block Without Forensics</td>
<td>Same as Block All, but does not store forensic data for the incident.</td>
</tr>
<tr>
<td>Drop Email Attachments</td>
<td>Drop email attachments that breach policy.</td>
</tr>
</tbody>
</table>

**Note**

The predefined action plans use the Default notification. You can edit the action plans to use a different notification—see *Notifications, page 251*, and *Adding a new message, page 252*, 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, page 240*.
- 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.

**Adding or editing an action plan**

Use the Policy Management > Resources > Action Plans > Action Plan Details page to create or edit an action plan.

To access this page, do one of the following:

- Click **New** in the toolbar at the top of the content pane on the Action Plans page.
- Click the name of an action plan in the list on the Action Plans page.

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**, page 240
   - **Forcepoint Data Discovery options**, page 242
   - **Forcepoint Web Security mode**, page 243
   - **Forcepoint Email Security mode**, page 243

**Standard Forcepoint DLP options**

On the Data Loss Prevention tab, complete the fields as follows. See Possible actions for an action plan, page 245, for a description of each possible action.

1. Under Network Channels:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Select an action to take when a breach is discovered on network email channels.</td>
</tr>
<tr>
<td>Mobile email</td>
<td>Select an action to take when a breach is discovered in content being sent to a user’s mobile device.</td>
</tr>
<tr>
<td>FTP</td>
<td>Select an action to take when a breach is discovered over FTP.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>Select an action to take when a breach is discovered over HTTP or secure HTTP.</td>
</tr>
<tr>
<td>Chat</td>
<td>Select an action to take when a breach is discovered over chat.</td>
</tr>
<tr>
<td>Plain text</td>
<td>Select an action to take when a breach is discovered via plain text.</td>
</tr>
</tbody>
</table>
2. Under Endpoint Channels:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>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.</td>
</tr>
<tr>
<td>Application control</td>
<td>Select an action to take when a breach is discovered on an endpoint application such as Word.</td>
</tr>
<tr>
<td>Removable media</td>
<td>Select an action to take when a breach is discovered on an endpoint device such as a thumb drive.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>Select an action to take when a breach is discovered on an endpoint device over HTTP or secure HTTP.</td>
</tr>
<tr>
<td>LAN</td>
<td>Select an action to take when a breach is discovered on an endpoint LAN, such as when a user copies sensitive data from a workstation to a laptop.</td>
</tr>
<tr>
<td>Printing</td>
<td>Select an action to take when a breach is discovered on a local or network printer that is connected to an endpoint.</td>
</tr>
</tbody>
</table>

3. For Cloud Channels, use the **CASB service** drop-down list to select an action to take when an incident involves files uploaded to, downloaded from, or used by a cloud application.

- Select **Permit** to allow files to be uploaded, synchronized, downloaded, shared, and so on.
- 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 internal** to remove sharing permissions for any internal address.
- 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 select, also select one or more of the following 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*, page 247, 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*, page 251, and *Adding a new message*, page 252, for details.

---

**Tip**

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

5. To configure discovery options, continue to the next section. Otherwise, click **OK** to save the changes.

**Forcepoint Data Discovery options**

On the *Discovery* tab:

1. To have the system run a remediation script for network discovery incidents, select **Run remediation script**, then select a script from the drop-down list. See *Remediation scripts*, page 247.

2. Under Endpoint Discovery, if classification tagging is enabled for the deployment, mark **Add classification tag** to specify the tag or tags to apply to files.

- Tags will be added only to files that meet the conditions set on the Settings > General > Services > Classification Tagging page. (See *Configuring classification tagging*, page 343.)

- Classification tagging must be enabled for this option to display in the action plan.
3. If classification tagging is enabled in the action plan, enter up to two **Tag label** and **Value** pairs.
   
   Each label and value must already exist in the classification tagging system in order for Forcepoint Data Discovery to add a tag to files.

4. To have the system run an endpoint remediation script for endpoint discovery incidents, select **Run endpoint remediation script**, then select a script from the drop-down list.

   Remediation scripts can be added on the Main > Policy Management > Resources > Remediation Scripts page. Select **New > Endpoint Script**.

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

**Forcepoint Web Security mode**

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, page 251,* and *Adding a new message, page 252,* for details.

   **Tip**

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

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

**Forcepoint Email Security mode**

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.
- **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.

---

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 when an administrator selects Remediate > Release on the incident details toolbar.)

- **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, page 251, and Adding a new message, page 252*, for details.

---

**Tip**
There is a benefit to using the same template for each action plan. The system gathers notifications for individual users according to templates and combines them into a single notification. So if an incident contains 10 different rules, each with a different action plan but the same template, the user receives a single notification with the details of all the breaches.

---

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

**Possible actions for an action plan**

The actions available for use in an action plan depend on the channel being configured.

Possible actions include:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Allow data to be maneuvered based on your selection—for example, allow it to be printed or posted to a website.</td>
</tr>
<tr>
<td>Block</td>
<td>Deny or block data from being printed, posted, or emailed, depending on your selection.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Quarantine email messages containing sensitive data. Network email can be encrypted before it’s released. Select <strong>Encrypt on release</strong> to enable this feature. <strong>Note:</strong> When a mobile email message is released from quarantine, it is sent to the mobile device the next time the device is connected to the network.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Drop attachments           | ● Drops email attachments that are in breach of policy.  
|                            | ■ Applies to messages detected by the Forcepoint Email Security module.  
|                            | ■ Applies to rules that monitor data in “each part separately.”  
|                            | ● 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.  
|                            | ■ Are detected when rules are monitoring data in “the transaction as a whole.”  
|                            | ■ Fail to drop attachments when indicated.  
|                            | **Note:** If a violation is found in a uuencoded attachment, the attachment is treated as email body and blocked rather than dropped. This is because additional content is placed between the attachments, including the attachment name. (UNIX-to-UNIX encoding [uuencoding] is a utility that most email applications use for encoding and decoding files.)

Select **Encrypt on release** if you want quarantined messages to be encrypted before they’re released. If an attachment has been dropped, this option reattaches it and encrypts both the body and attachment before releasing the message.

To release an incident, an administrator selects **Remediate > Release** on the incident details toolbar.

| Encrypt                     | Encrypt the affected email message.  
|                            | With Forcepoint DLP agents and Forcepoint Email Security, this option 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.)                  |

| Encrypt with profile key    | 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. |

| Encrypt with user password  | 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.  
|                            | 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.  
|                            | This option is not supported on Mac or Linux endpoints. Removable media transactions are permitted on Mac and Linux when this option is selected. |
Defining Resources

Remediation scripts

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm</td>
<td>Display a confirmation message, such as the following when a security threat is detected:</td>
</tr>
<tr>
<td></td>
<td>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?</td>
</tr>
<tr>
<td></td>
<td>Users can continue if they enter a business reason for the operation, or they can cancel. If they cancel or wait too long, the default action is taken.</td>
</tr>
<tr>
<td></td>
<td>To configure the default action, go to the Settings &gt; General &gt; Endpoint page and select Block or Permit on the General tab.</td>
</tr>
<tr>
<td>Run remediation script</td>
<td>Run a script that performs specific actions when an incident is detected.</td>
</tr>
<tr>
<td></td>
<td>Remediation scripts can be run when network discovery, endpoint discovery, or DLP incidents are detected.</td>
</tr>
<tr>
<td></td>
<td>See Remediation scripts, page 247.</td>
</tr>
<tr>
<td>Add classification tag</td>
<td>Add classification tags to files that trigger a discovery incident, following the guidelines established on the Settings &gt; General &gt; Services &gt; Classification Tagging page.</td>
</tr>
<tr>
<td></td>
<td>Endpoint discovery only.</td>
</tr>
<tr>
<td></td>
<td>Requires a supported, third-party classification tagging system.</td>
</tr>
</tbody>
</table>

Related topics:

- *Adding a new remediation script*, page 250
- *Incident XML interface for use in remediation scripts*, page 249
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.

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.

The system provides 3 scripts for network file system and endpoint discovery. These scripts can be used to copy or move content detected in breaches. See *Copying or moving discovered files*, page 266, for details.

For information on writing your own scripts, see **Creating Remediation Scripts**.

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:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analysisDetails</td>
<td>Root element.</td>
</tr>
<tr>
<td>transactionID</td>
<td>The internal transaction ID (unique ID that the system generates for every analyzed transaction).</td>
</tr>
<tr>
<td>action</td>
<td>The action taken (for example, permit or deny).</td>
</tr>
<tr>
<td>actionDetails</td>
<td>The action taken per destination.</td>
</tr>
<tr>
<td>violations</td>
<td>The detected violations, including the policy name and content.</td>
</tr>
</tbody>
</table>
Adding a new 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, page 247*.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Executable file| 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.  
**Note:** If you are using a remediation script that copies files to a quarantine folder, be sure to exclude this folder from discovery scans.  
Endpoint scripts must be smaller than 5 MB. |
Defining Resources

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.
5. If necessary, update the additional files in the same way.
6. Click OK.

For more information about writing a remediation script, Creating Remediation Scripts. This document describes:

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

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.
Defining Resources

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.

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.

1. Enter a Name for this notification template, such as “Breach notification”.
2. Enter a Description for the template.

On the General tab

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.
3. Information for the currently configured outgoing mail server is displayed. To change the server used, click the Edit (pencil) icon.
   Note that changes to the mail server properties affect all features that use the outgoing mail server, including alerts.
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.

**On the Notification Body tab**

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 display 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 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, page 334, for more information.

4. Select *Attach policy-breacht content* to include the content that violated policy as an attachment to the message.

5. Click *OK* to save your changes.

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: Report, An administrator reviewed this incident, Closed
Escalation: Report to your manager
More actions: Send, 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.
Creating Discovery Policies

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, page 256*
2. *Scheduling Discovery Tasks, page 269*

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.

Related topics:

- *Configuring discovery incidents, page 265*
- *Viewing discovery status, page 264*
- *Viewing discovery results, page 265*
- *Updating discovery, page 265*
- *Copying or moving discovered files, page 266*
Creating Discovery Policies

- SharePoint directories and identify data in breach of policies.
- Documents in a data management system or IBM Domino server.
- Documents, folders, and accounts in Box cloud storage systems.

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.

Creating a discovery policy

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.
## Predefined policies

In the wizard for predefined policies:

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, refer to **Predefined Policies**.)

## Custom policies

In the wizard for custom policies:

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**, page 173, for details.
   - **File Properties**: Select file properties to add to this policy. Click **OK**. See **File properties**, page 179, for details.
   - **Fingerprint**: Select the fingerprint classifier to use for this policy. Click **OK**. See **Fingerprint**, page 158, 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.

The process of adding rules and exceptions to discovery policies is the same as for DLP policies. See *Managing rules, page 160*, and *Managing exceptions, page 161*, for instructions.

### 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, page 269.*
Performing file system discovery

To perform discovery on a network file system:
1. Prepare your file server as described in the Forcepoint DLP Deployment Guide.
2. Create a discovery policy (see Creating a discovery policy, page 256).
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, page 274.
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, page 59.

Performing SharePoint discovery

To perform discovery on SharePoint folders:
1. Create a discovery policy (see Creating a discovery policy, page 256).
2. Go to the Main > Policy Management > Discovery Policies page.

Related topics:
- Scheduling Discovery Tasks, page 269
- Creating a discovery policy, page 256
- Scheduling network discovery tasks, page 273
- File System tasks, page 274
- Scheduling Discovery Tasks, page 269
- Creating a discovery policy, page 256
- Scheduling network discovery tasks, page 273
- SharePoint tasks, page 279
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, page 279.

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, page 59.

Performing Domino discovery

To perform discovery on documents on an IBM Domino server:

1. Create a discovery policy (see Creating a discovery policy, page 256).

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, page 299.

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, page 59.

Related topics:
- Scheduling Discovery Tasks, page 269
- Creating a discovery policy, page 256
- Scheduling network discovery tasks, page 273
- Domino tasks, page 298
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, page 256).
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, page 282.
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, page 59.
Performing database discovery

To perform discovery on a database:

1. Create a discovery policy (see Creating a discovery policy, page 256).
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, page 287.
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, page 59.

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*, page 256 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*, page 291.

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*, page 59.

### Performing Outlook PST discovery

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

To perform discovery on email on Outlook PST data files:

1. Create a discovery policy (see *Creating a discovery policy*, page 256 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*, page 295.

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.

---

**Related topics:**
- *Scheduling Discovery Tasks*, page 269
- *Creating a discovery policy*, page 256
- *Scheduling network discovery tasks*, page 273
- *Outlook PST tasks*, page 295
To view and respond to discovery results, go to the `Main > Reporting > Discovery` page. See `Viewing the incident list, page 59`.

### Performing endpoint discovery

To perform discovery on endpoint systems:

1. Create a discovery policy. (See `Creating a discovery policy, page 256` 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, page 305`.
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, page 59`.

### Viewing discovery status

To view the status of a discovery task:

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.

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

You cannot view the status of endpoint discovery.
Creating Discovery Policies

Viewing discovery results

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*, page 36, and *Viewing the incident list*, page 59, 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.

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:

1. Go to the **Settings > General > Reporting** page.
2. Select the **Discovery** tab.
3. Complete the fields as described in *Setting preferences for discovery reports*, page 321.
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, page 266*, for instructions on using these scripts.

Preparing and running the remediation scripts

**STEP 1: Configure CopyFiles and MoveFiles**

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:
Creating Discovery Policies

- 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.

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**

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**

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.
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.
Scheduling Discovery Tasks

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 **Endpoint discovery tasks** to set up discovery on endpoint hosts.

Related topics:

- *Scheduling network discovery tasks*, page 273
- *Scheduling endpoint discovery tasks*, page 305
- *File System tasks*, page 274
- *SharePoint tasks*, page 279
- *Domino tasks*, page 298
- *Box tasks*, page 282
- *Database tasks*, page 287
- *Exchange tasks*, page 291
- *Outlook PST tasks*, page 295
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:

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

Buttons and controls

For all discovery tasks:

- Click **New** to create a 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.
- Click **Delete** to delete the selected discovery task.

**Note**

If the crawler is unresponsive for any reason, delete the task manually, as prompted (see *Manually deleting discovery tasks*, page 272).

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td></td>
<td>Starts a discovery scan.</td>
</tr>
<tr>
<td>Stop</td>
<td></td>
<td>Stops a discovery scan. When restarted, task starts from the beginning.</td>
</tr>
<tr>
<td>Pause</td>
<td></td>
<td>Pauses a discovery scan. When restarted, task starts from the last point it was paused.</td>
</tr>
<tr>
<td>Download</td>
<td></td>
<td>Downloads a detailed report on discovery scanning activities in CSV format.</td>
</tr>
</tbody>
</table>
## Details pane

Network tasks also offer a Details pane to show statistics about the scan and scheduler. Expand or collapse this pane to show more or fewer details.

### Scan

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

### Task Statistics

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

### Last Scan Statistics*

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

Last Scan Statistics*

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated total items/files/records</td>
<td>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.</td>
</tr>
<tr>
<td>Total records/items to scan</td>
<td>The number of items or records you’ve chosen, out of the total, to scan.</td>
</tr>
<tr>
<td>Estimated total size</td>
<td>An estimate of the total size of items in MB. (Does not apply to database scans.)</td>
</tr>
</tbody>
</table>

* The Last Scan Statistics are derived as follows:

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

Manually deleting discovery tasks

If the crawler is unresponsive for any reason when 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:

```xml
<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.pyc -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*
  - *Box 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.

---

**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:

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*. 
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.

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.

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.

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 semi-colons 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*.

---

**File System Discovery Task Wizard - Scheduler**

---

Use the **Scheduler** page of the file system discovery task wizard to enable and configure task scheduling.

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*.  

---

**Warning**

These credentials aren’t verified until the scan starts. Be careful to enter a valid user name and password.
Scheduling Discovery Tasks

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.

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*.

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.

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 semi-colons.
   - 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 semi-colons. 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*, page 304.
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.

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.**
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 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.

SharePoint Discovery Task Wizard - Site Root

Use the Site Root page of the SharePoint discovery task wizard to identify the site to scan.

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.

3. Optionally, enter the Domain for the administrator account.

4. Click Next, then continue with SharePoint Discovery Task Wizard - Scanned Documents.

SharePoint Discovery Task Wizard - Scanned Documents

Use the Scanned Documents page of the SharePoint discovery task wizard to determine where discovery runs.

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.

SharePoint Discovery Task Wizard - Scheduler

Use the Scheduler page of the SharePoint discovery task wizard to determine when discovery runs.

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*.

**SharePoint Discovery Task Wizard - Policies**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Policies** page of the SharePoint discovery task wizard to determine which policies to apply during the scan.

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*.

**SharePoint Discovery Task Wizard - File Filtering**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

---

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 semi-colons.
   - 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 semi-colons. 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*, page 304.

**SharePoint Discovery Task Wizard - Advanced**

Use the **Advanced** page of the SharePoint discovery task wizard to configure bandwidth limits and full scan options.

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*.

**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:

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*.

### 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.

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*.

**Box Discovery Task Wizard - Scanned Accounts**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Scanned Accounts** page of the Box discovery task wizard to determine what to scan.

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*.

**Box Discovery Task Wizard - Scheduler**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Scheduler** page of the Box discovery task wizard to determine when discovery runs.

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*.

### Box Discovery Task Wizard - Policies

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Policies** page of the Box discovery task wizard to determine which policies to apply during the scan.

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*.

### Box Discovery Task Wizard - File Filtering

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

---

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 semi-colons.
   - 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 semi-colons. 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*, page 304.

**Box Discovery Task Wizard - Advanced**

Use the **Advanced** page of the Box discovery task wizard to configure bandwidth limits and full scan options.

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*.

**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 Express (SQL Server Express ODBC driver)
- IBM DB2 9.5 (ODBC driver 8.2.9)
- IBM Informix Dynamic Server 11.50 (IBM Informix ODBC driver 3.50)
- MySQL 5.1 (ODBC driver 5.1.5)
- Due to MySQL limitations, you must define “string” columns with UTF-8 encoding to fingerprint them.
- Sybase ASE 15.0 (Sybase ODBC driver 15.0.0.152)
- Teradata v13 and v14

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:

- CHAR
- VARCHAR
- TINYINT
- BIGINT
- REAL
- TIME
- DECIMAL
- FLOAT
- LONGVARCHAR
- SMALLINT
- WCHAR
- DOUBLE
- TINYTE

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.

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.

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*.

---

**Database Discovery Task Wizard - Data Source Name**

**Administrator Help | Forcepoint DLP | Version 8.5.x**

Use the **Data Source Name** page of the database discovery task wizard to define how Forcepoint DLP connects to the database.

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*, page 201.
   - For a list of supported databases and field types, see *Connecting to data sources*, page 200.
   - 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 Sever 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*.

---

**Database Discovery Task Wizard - Scheduler**

**Administrator Help | Forcepoint DLP | Version 8.5.x**

Use the **Scheduler** page of the database discovery task wizard to determine when the discovery task runs.

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*.

### Database Discovery Task Wizard - Policies

Use the **Policies** page of the database discovery task wizard to determine which policies to apply during the scan.

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*.

### Database Discovery Task Wizard - Table Filtering

Use the **Table Filtering** page of the database discovery wizard to determine which tables to scan.

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]
Scheduling Discovery Tasks

○ 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, page 304.

Database Discovery Task Wizard - Advanced

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Advanced page of the database discovery task wizard to configure bandwidth limits and full scan options.

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.

Database Discovery Task Wizard - Finish

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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)

Exchange Discovery Task Wizard - Exchange Servers (online)

Use the Exchange Servers (online) page of the Exchange discovery task wizard to provide connection information.

1. Enter the Email address and Password used for logging on to the Exchange Online account.
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.

Exchange Discovery Task Wizard - Exchange Servers (local)

Use the Exchange Servers (local) page of the Exchange discovery task wizard to provide connection information.

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.
Enter the hostname or IP address of each additional server and click Add.

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.

   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*.

### Exchange Discovery Task Wizard - Mailboxes

Use the **Mailboxes** page of the Exchange discovery task wizard to select which mailboxes to scan.

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*.

### Exchange Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Exchange discovery task wizard to determine when the discovery task runs.

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*.

### Exchange Discovery Task Wizard - Policies

**Administrator Help | Forcepoint DLP | Version 8.5.x**

Use the **Policies** page of the Exchange discovery task wizard to determine which policies to apply during the scan.

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*.

### Exchange Discovery Task Wizard - Filtering

**Administrator Help | Forcepoint DLP | Version 8.5.x**

Use the **Filtering** page of the Exchange discovery task wizard to determine which items to scan.

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.
Scheduling Discovery Tasks

- 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, page 304.

Exchange Discovery Task Wizard - Advanced

Use the Advanced page of the Exchange discovery task wizard to configure bandwidth limits and full scan options.

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.

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.

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*.

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.

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*.

Outlook Discovery Task Wizard - Scheduler

Use the **Scheduler** page of the Outlook discovery task wizard to determine when the scan runs.

1. Mark **Enabled** to enable the scheduler for the current task.
Scheduling Discovery Tasks

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.

Outlook Task Discovery Wizard - Policies

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Policies page of the Outlook discovery task wizard to determine which policies to apply during the scan.

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.

Outlook Discovery Task Wizard - Filtering

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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 semi-colons. 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*, page 304.

---

**Outlook Discovery Task Wizard - Advanced**

Use the **Advanced** page of the Outlook discovery task wizard to configure bandwidth limits and full scan options.

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**.

**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*).

**Domino Discovery Task Wizard - General**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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*.

**Domino Discovery Task Wizard - Server**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Server** page of the Domino task wizard to select the Domino server to scan, and to provide connection details.

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.

---

1. 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*.

---

**Domino Discovery Task Wizard - Scanned Documents**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Scanned Documents** page of the Domino discovery task wizard to determine which documents are scanned during the discovery process.

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*.

## Domino Discovery Task Wizard - Scheduler

*Use the Scheduler page of the Domino discovery task wizard to specify when the scan is run:*

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*.

## Domino Discovery Task Wizard - Policies

*Use the Policies page of the Domino discovery task wizard to determine which policies to apply during the scan:*

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*.
**Domino Discovery Task Wizard - Document Filtering**

Use the **Document Filtering** tab of the Domino discovery task wizard to determine which documents are scanned.

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 semi-colons. 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 semi-colons. 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**.

**Domino Discovery Task Wizard - Attachment Filtering**

Use the **Attachment Filtering** page of the Domino discovery task wizard to determine which attachments are scanned.

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 semi-colons.
     - The “*” and “?” wildcards are supported. For example, “*.doc; *.xls; *.ppt; *.pdf”.

Scheduling Discovery Tasks

1. Select **Except** to list the file types to exclude from the scan, separated by semi-colons. 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*, page 304.

**Domino Discovery Task Wizard - Advanced**

Use the **Advanced** page of the Domino discovery task wizard to configure bandwidth limits and full scan options.

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*.

**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.

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.
   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**, page 278
   ■ **SharePoint Discovery Task Wizard - Advanced**, page 282
   ■ **Box Discovery Task Wizard - Advanced**, page 286
   ■ **Database Discovery Task Wizard - Advanced**, page 290
   ■ **Exchange Discovery Task Wizard - Advanced**, page 294
   ■ **Outlook Discovery Task Wizard - Advanced**, page 297
   ■ **Domino Discovery Task Wizard - Advanced**, page 303
   ■ **Endpoint Discovery Task Wizard - Advanced**, page 307
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:
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.

Endpoint Discovery Task Wizard - Endpoints

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.

Endpoint Discovery Task Wizard - Scheduler

Use the Scheduler page of the endpoint discovery task wizard to determine how often the discovery task is run.

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*.

---

**Endpoint Discovery Task Wizard - Policies**

Use the **Policies** page of the endpoint discovery task wizard to determine which policies to apply during the scan.

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*.

---

**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.

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 semicolons. 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 semicolons. 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.

---

**Endpoint Discovery Task Wizard - Advanced**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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.

---

**Endpoint Discovery Task Wizard - Finish**

Administrator Help | Forcepoint DLP | Version 8.5.x

The Finish page of the endpoint discovery task wizard displays a summary of the new endpoint discovery task.
Viewing Forcepoint DLP Logs

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, page 310
- The Forcepoint DLP system log, page 313
- The Forcepoint DLP audit log, page 314

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:

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

To view the current filters in use, click the information ("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 tooltip 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*, page 311, 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.
## Changing table properties

After clicking Table Properties, select the properties to display in the table and specify the column width for each property.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Taken</td>
<td>The online action that was performed (allow or block).</td>
</tr>
<tr>
<td>Analysis Canceled</td>
<td>Displays whether analysis was canceled.</td>
</tr>
<tr>
<td>Analysis Failed</td>
<td>Displays whether analysis failure occurred.</td>
</tr>
<tr>
<td>Analyzed By</td>
<td>Displays the name of the policy engine that analyzed the event.</td>
</tr>
<tr>
<td>Channel</td>
<td>Channel on which the event was intercepted, for example SMTP, HTTP, or FTP.</td>
</tr>
<tr>
<td>Classifier Time</td>
<td>Time spent analyzing all classifiers, in milliseconds. Includes the time spent processing dictionaries, scripts, key phrases, patterns, and fingerprints.</td>
</tr>
<tr>
<td>Database Fingerprint Latency</td>
<td>Time in milliseconds that the transaction spent in the policy engine waiting for structured fingerprint analysis.</td>
</tr>
<tr>
<td>Database Fingerprint Search Time</td>
<td>Time in milliseconds spent on searching for structured fingerprint data in this transaction’s content.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination of the event, for example an IP address or an email address.</td>
</tr>
<tr>
<td>Details</td>
<td>Header details from the event. For example, if the breach is in an email message, this column contains the message subject. If the breach was detected in an FTP transfer, this column lists the file name.</td>
</tr>
<tr>
<td>Detected By</td>
<td>Displays the protector or agent that caught the event.</td>
</tr>
<tr>
<td>Dictionary Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for dictionary analysis.</td>
</tr>
<tr>
<td>Dictionary Search Time</td>
<td>Time in milliseconds spent on searching for dictionary phrases in this event’s content.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Unique traffic log event number.</td>
</tr>
<tr>
<td>Event Time</td>
<td>Date and time the event was detected.</td>
</tr>
<tr>
<td>Extraction Time</td>
<td>Time spent extracting text from the event, in milliseconds.</td>
</tr>
<tr>
<td>File Fingerprint Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for unstructured fingerprint analysis.</td>
</tr>
<tr>
<td>File Fingerprint Search Time</td>
<td>Time in milliseconds spent on searching for unstructured fingerprint data in this event’s content.</td>
</tr>
<tr>
<td>Host Name Resolution Time</td>
<td>Time in milliseconds spent on performing external resolution from IP to hostname on this event’s source or destination.</td>
</tr>
<tr>
<td>Incident</td>
<td>Displays a check mark if the event was determined to be an incident (a policy violation).</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Incident Creation Time</td>
<td>Time spent creating an incident when a breach is detected, in milliseconds. If no incident was created, this field is “0”.</td>
</tr>
<tr>
<td>Key Phrase Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for key phrase analysis.</td>
</tr>
<tr>
<td>Key Phrase Search Time</td>
<td>Time in milliseconds spent on searching for key phrases in this event’s content.</td>
</tr>
<tr>
<td>Latency</td>
<td>Time the event spent in the policy engine waiting for analysis, in milliseconds—in other words, Processing Time + Incident Creation Time + Queue Time.</td>
</tr>
<tr>
<td>Regular Expression Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for regular expression analysis.</td>
</tr>
<tr>
<td>Regular Expression Processing Time</td>
<td>Time in milliseconds spent on all regular expression calculations performed on this event’s content.</td>
</tr>
<tr>
<td>Resolution Time</td>
<td>Time spent resolving user names for all sources and destinations in the event, in milliseconds.</td>
</tr>
<tr>
<td>Script Search Time</td>
<td>Time in milliseconds spent on all script classifications performed on this event’s content.</td>
</tr>
<tr>
<td>Search Time</td>
<td>Time it took to search the event for breaches, in milliseconds—in other words, Classifier Time + Extraction Time + Resolution Time.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the event content, for example a file or an email message.</td>
</tr>
<tr>
<td>Source</td>
<td>The source from which the event originated. This could be an email address or IP address or other source.</td>
</tr>
<tr>
<td>Text Extraction Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for text extraction.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Displays whether analysis was stopped due to a timeout restriction.</td>
</tr>
<tr>
<td>Total Queue Time</td>
<td>Total amount of idle time, in milliseconds, that the event spent in internal queues.</td>
</tr>
<tr>
<td>URL Categorization Time</td>
<td>Time in milliseconds spent on categorizing the destination URL of this event.</td>
</tr>
<tr>
<td>User Name Resolution Time</td>
<td>Time in milliseconds spent on performing external resolution from IP to user name on this event’s source.</td>
</tr>
<tr>
<td>User Resolution Latency</td>
<td>Time in milliseconds that the event spent in the policy engine waiting for user name resolution.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Defines whether the action is an error, or is reported for informational purposes.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays either New or Confirmed. Once you view a new action, you can mark it as confirmed to show you’ve reviewed it. To mark a new action as confirmed, select the action and click Mark as Confirmed. To revert a confirmed action to new, select the event and click Mark as New.</td>
</tr>
<tr>
<td>Message</td>
<td>This column may contain variables that are filled by the system, for example a full folder path or a component name. If there are multiple identical messages in a short time interval, a combined message is displayed. The 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.).”</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Date and time the action occurred.</td>
</tr>
<tr>
<td>Local Date &amp; Time</td>
<td>Date and time on the component where the action occurred.</td>
</tr>
</tbody>
</table>
| Topic      | ● System - Displays system messages reported by system components  
             ● Configuration - Displays messages reported by the system after a configuration action is executed (usually by an administrator) |
| Reporter   | Displays the system module’s name, for example 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, it can show when administrators:

- Export incidents to a PDF or CSV file
- Email incidents to a manager or other recipient
- Make changes to a user account, such as user name or password
- View incident details such as trigger values and forensics
  (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.

Audit log records are kept indefinitely.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action ID</td>
<td>ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the <strong>Find Action ID</strong> field and clicking <strong>Find</strong>.</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Date and time the action occurred.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Name and user name of the administrator that initiated the action in the Forcepoint Security Manager.</td>
</tr>
<tr>
<td>Access Role</td>
<td>Role of the administrator.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Topic</td>
<td>You can filter the Audit Log by topic types.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Administration</strong> - Displays actions performed by administrators during the designated period, such as adding a new access role or configuring user directories. Also displays actions made on administrators, such as adding a new administrator or changing an administrator’s permissions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Log on/Log out</strong> - Displays log on and log out actions so you know which administrators were active during the designated period.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong> - Displays actions performed on status reports and logs, such as deleting an entry or creating an audit record.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Policy management</strong> - Displays actions performed on policies, such as updating predefined policies, editing quick policies, or creating a new policy.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reporting</strong> - Displays actions performed on reports during the designated period, such as editing or creating a new report.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Incident management</strong> - Displays actions performed on incidents, such as deleting incidents.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Archiving</strong> - Displays actions performed on incident archives, such as deleting or restoring an archive.</td>
</tr>
<tr>
<td></td>
<td>- <strong>System modules</strong> - Displays actions performed on system modules, such as editing a configuration or adding a module.</td>
</tr>
<tr>
<td>Action Performed</td>
<td>Description of the action performed by the administrator—for example, “exported DLP incident to PDF file”.</td>
</tr>
<tr>
<td>Details</td>
<td>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.</td>
</tr>
<tr>
<td>Modified Item</td>
<td>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.</td>
</tr>
</tbody>
</table>
General System Settings

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, page 318).
- Back up and restore the Forcepoint DLP system (see Backing up the system, page 322).
- Define parameters for exporting incidents to a file (see Exporting incidents to a file, page 325).*
- Configure endpoint hosts (see Configuring endpoint settings, page 327).*
- Configure mobile email devices (included with Forcepoint Email Security). See Mobile device settings, page 330.
- Configure remediation (see Remediation, page 332).*
- Configure incoming and outgoing mail servers (see Mail servers, page 334).
- Set up alerting (see Alerts, page 336).
- Configure archive storage (see Archive storage, page 337).
- Configure Linking Service, Microsoft RMS, the CASB service, classification tagging, and the RAP service (see Services, page 339).
- Configure high-risk resources for incident risk ranking (see Analytics, page 345).
- Configure user directory settings (see User directory settings, page 346).
- Archive incident partitions (see Archiving incident partitions, page 353).
- Update predefined policies and classifiers (see Updating predefined policies and classifiers, page 357).
- Enter subscription settings (Entering subscription settings, page 361).

*These options are not included in the Forcepoint Web Security or Forcepoint Email Security DLP Module.
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.
- For discovery incidents, set database thresholds.
- 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, page 319
- Setting preferences for data loss prevention reports, page 320
- Setting preferences for Incident Risk Ranking reports, page 320
- Setting preferences for discovery reports, page 321
- Setting preferences for mobile incident reports, page 321
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:

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**

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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**

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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 discovery reports

Use the Discovery tab of the Settings > General > Reporting page in the Data Security module of the Forcepoint Security Manager to define settings for discovery incidents:

1. Use the **Maximum discovery incidents** field to enter the maximum number of incidents stored in the discovery database.
   - Enter a number between 10000 and 2000000 (no commas).
   - Assign, view, and monitor these incidents on the Discover Incidents page.
2. Forcepoint DLP has a safety mechanism in place that protects the incident database from being overpopulated. When the same host, database, or mailbox generates many incidents for the same policy, the system quits storing incident details for each incident, and instead stores only general incident information.
   - Use the **Endpoint discovery incidents** and **Network discovery incidents** fields to indicate how many incidents you want to trigger the change (100000, by default). Do not include commas in the number you enter.
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:

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.
Use the Settings > General > Backup 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, page 324, 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.

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.

### Related topics:

- **Scheduling backups**, page 323
- **Monitoring backups**, page 323
- **Backup folder contents**, page 324
- **Restoring the system**, page 324

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Enter the domain for the account.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name for an administrator account with access to this path.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password. It must:</td>
</tr>
<tr>
<td></td>
<td>- Be at least 8 characters</td>
</tr>
<tr>
<td></td>
<td>- Contain upper case characters</td>
</tr>
<tr>
<td></td>
<td>- Contain lower case characters</td>
</tr>
<tr>
<td></td>
<td>- Contain numbers</td>
</tr>
<tr>
<td></td>
<td>- Contain non-alphanumeric characters</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the password a second time.</td>
</tr>
</tbody>
</table>
General System Settings

- 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*, page 323.

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.

---

### 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:

<table>
<thead>
<tr>
<th>Subfolder</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreciseID_DB</td>
<td>The fingerprint repository</td>
</tr>
<tr>
<td>MngDB</td>
<td>The Forcepoint DLP reporting database (containing policies, incidents and configuration)</td>
</tr>
<tr>
<td>Forensics_repository</td>
<td>Encrypted forensic incidents information</td>
</tr>
<tr>
<td>Crawlers</td>
<td>Information on the discovery and fingerprinting crawlers</td>
</tr>
<tr>
<td>Certs</td>
<td>Certificate files used for communication between the Forcepoint Security Manager and Forcepoint DLP network and endpoint agents.</td>
</tr>
</tbody>
</table>

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:

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.

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 (x86)/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 as 12:00 a.m., select **At the start of a new day**.
6. Click **OK** to save your changes.

The following fields are exported:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident ID</td>
<td>External incident ID.</td>
</tr>
<tr>
<td>Insert date</td>
<td>The incident insert date.</td>
</tr>
<tr>
<td>Source hostname</td>
<td>The incident source hostname.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The incident source IP.</td>
</tr>
<tr>
<td>Source full name</td>
<td>The incident source full name.</td>
</tr>
<tr>
<td>Source email</td>
<td>The incident source email.</td>
</tr>
<tr>
<td>Source DN</td>
<td>The distinguished name (DN) of the incident source. A DN is the name that uniquely identifies the entry in the directory. It is made up of attribute=value pairs, separated by commas.</td>
</tr>
<tr>
<td>Destinations list</td>
<td>A list of the incidents destinations, in the format of dest1;dest2;dest3…</td>
</tr>
<tr>
<td>Channel name</td>
<td>The channel name.</td>
</tr>
<tr>
<td>Max action taken</td>
<td>A readable action taken (e.g.: Blocked, Audited).</td>
</tr>
<tr>
<td>Urgency</td>
<td>Incident’s urgency, sometimes called sensitivity (e.g.: Moderate).</td>
</tr>
<tr>
<td>Policy category</td>
<td>A policy category for the current line (an incident can generate multiple lines).</td>
</tr>
<tr>
<td>Filenames</td>
<td>The filename or filenames related to the current incident policy, up to 1024 characters. In the format of [fn1;fn2;…;fnX].</td>
</tr>
<tr>
<td>Filenames trimmed</td>
<td>True if the actual value for the filenames filed is greater than 1024 characters. Please notice that in few cases you do not get the actual file name. For example, for some SMTP incidents you might see the filename as MESSAGE-BODY.</td>
</tr>
</tbody>
</table>
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

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breached contents</td>
<td>The breach content of the incident for the current policy, up to 1024 characters, in the format of [content1;content2;…;contentX].</td>
</tr>
<tr>
<td>Breached content trimmed</td>
<td>True if the actual size of the previous filed is more than 1024 characters.</td>
</tr>
</tbody>
</table>
General System Settings

- Contain numbers
- Contain non-alphanumeric characters

A password is not required to administer endpoint clients.

6. 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.
   - Linux endpoint does not support CD/DVD burners.

7. Click **Save**.

For the next step in configuring endpoint settings, continue with **Endpoint settings: the Email Domains tab**, page 328.

**Endpoint settings: the Email Domains tab**

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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**.

For the next step in configuring endpoint settings, continue with *Endpoint settings: the Disk Space tab*, page 329.

### Endpoint settings: the Disk Space tab

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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**.

For the final step in configuring endpoint settings, continue with *Endpoint settings: the Advanced tab*, page 329.

### Endpoint settings: the Advanced tab

Administrator Help | Forcepoint DLP | Version 8.5.x

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 of 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 can include spaces. For example: `Office application.exe`.
- 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.

---

### Mobile device settings

The mobile agent makes it possible to configure what type of email content to sync to users’ mobile devices when they connect to the network. If content breaches the mobile policy, it is blocked or audited as configured.

Use the **Settings > General > Mobile** page in the Data Security module of the Forcepoint Security Manager to define how Forcepoint DLP manages the mobile devices covered by policy.

1. Use the **Keep released messages for** field to specify, in days (3-30) how long to store released messages (14 days, by default).
When the mobile agent accepts a release operation for a specific message, it stores it for 2 main purposes:

- To wait for the user’s device to sync, which triggers the actual release sequence in Exchange.
- To avoid any subsequent analysis for the same message by the same user syncing to a second device.

This number affects the size of your incident database. A large number requires more storage space than a small one.

2. Use the **Update status every** field to determine how often in minutes (1-60) device status is sent to the management server. The default is 5 minutes.

- Status includes the device owner and type, date of the last synchronization, date of incident detection, and more.
- Status from all registered devices is sent to the management server in a single batch operation.

3. Under Analyze the following components, indicate which Exchange server components you want the mobile agent to analyze:

- Select **Email messages** to analyze all parts of an email message (Subject, Body, To, From, Attachments, etc.).
- Select **Calendar events** to analyze calendar items, including Subject, Location, Attendees, and Description.
- Select **Tasks** to analyze content in To-Do lists.

By default, all message types are analyzed.

4. Under Trusted Devices, define any devices that should not be monitored. These devices are not analyzed by Forcepoint DLP.

a. Select **Enable trusted devices**.

b. One by one, enter a user name and user agent for each trusted device, and then click **Add**.
   - The **User name** of the device user is case insensitive. Do not include the domain name. For example, enter jdoe rather than mydomain\jdoe. If you leave this field blank, all people who use the device specified in the User agent field are trusted.
   - The **User agent** is a case-sensitive identifier used to identify the device operating system and email client software. Similar devices share the same identifier. If you leave this field blank, all devices for the specified users are trusted—for example, all mobile devices used by jdoe. If the device is connected to an Exchange server, you can find the user agent string using an interface such as Outlook Web App (OWA).

   Click **Remove** to remove a device from the trusted device list.

5. Click **OK** to save your changes.
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
- sourceIp = 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,10.0.17.2 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
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 ellipses.

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 the protocol to use for email retrieval: **POP3** or **IMAP**. Most mail servers support both.

2. 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.

3. 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.
   - This email address automatically appears in the To: field of the email message when administrators click a workflow operation link.

4. Enter the **IP address or hostname** and **Port** for the mail server that can open the specified email address.

5. 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.

6. 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.

7. Under Outgoing Mail Server, enter the **IP address or hostname** and **Port** for your outgoing mail server.
   - 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 and alerts is affected.

8. 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.

9. 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.

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:
   - Your subscription is about to expire
   - Policy updates fail during upgrade
   - The number of discovery incidents reaches its limit
   - Disk space for the incident archive reaches its limit
   - Disk space for the forensics repository reaches its limit
   - Incidents have been deleted from the incident repository
2. Click OK to save your changes.

To finish configuring alerts, continue with Setting up email properties, page 336.

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:

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.
3. Review the Outgoing mail server IP address or hostname and Port.
   - 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.
   A 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use existing storage location</td>
<td>Use the drop-down menu to select a previously configured storage location. Click <strong>Delete</strong> to remove unneeded locations.</td>
</tr>
<tr>
<td>Name new storage location</td>
<td>Select this option to define a new storage location. Enter a name for the new location.</td>
</tr>
<tr>
<td>IP address or hostname</td>
<td>Enter an IP address or hostname for the machine on which the storage will be located.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain name for the account used to access the location.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name for the account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the account.</td>
</tr>
<tr>
<td>Archive folder</td>
<td>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.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click <strong>Test Connection</strong> 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.</td>
</tr>
</tbody>
</table>
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:
  \[(\text{number of incidents per quarter}) \times (\text{average transaction size}) \times 12\]

  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:
  \[(\text{number of incidents per quarter}) \times 20 \text{ bytes} \times 12\]

  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.
  

- Forcepoint DLP can decrypt and analyze Microsoft Office files that were encrypted by Azure RMS or Active Directory RMS.
  
  See Configuring Microsoft RMS, page 340.

- With a Forcepoint DLP Cloud Applications subscription, the CASB service can be used to apply DLP policies to files uploaded to or shared within a variety of cloud applications.
  
  See Configuring the CASB service, page 342.

- Organizations that use a supported, third-party classification tagging system to label files used in the network can enable Forcepoint DLP tagging to integrate with the existing system.
  
  See Configuring classification tagging, page 343.

- Integration the Forcepoint DLP with UEBA technology, allows users to provide dynamic, risk-level-based actions per triggered policy rules through the Risk Adaptive Protection feature.
  
  See Configuring the RAP service, page 344.

Configuring Linking Service

Use the Linking Service tab of the Settings > General > Services page to make sure the connection between Forcepoint DLP and Linking Service is intact, and to configure how to use URL categories and user names from Forcepoint Web Security in Forcepoint DLP.

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.

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.

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.

**Configuring Microsoft RMS**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the **Microsoft RMS** tab of the **Settings > General > Services** page to configure Forcepoint DLP to decrypt and analyze Microsoft Office files that were encrypted by Azure RMS or Active Directory (AD) RMS on Windows endpoints. This includes files found on Windows endpoints (discovery) or sent via any endpoint channel.

Office files that are protected by Microsoft RMS include Word, Excel, PowerPoint and other Office documents created in Office 2007 or later, such as those ending in docx and pptx.

The system uses logged-in user credentials to access the Microsoft RMS server. In case of errors, the transaction is permitted without analysis and the error is recorded in a log file.

By default, this setting is disabled.
To enable RMS decryption, select **Enable RMS decryption**, then click **OK**.

The RMS file detection feature has the following prerequisites:

1. The endpoint machine must be in your organization’s domain.
2. Azure Active Directory/Office 365 single sign-on (SSO) must be configured and working. Users must be able to RMS-protect a document without a login request.
3. Either Rights Management Service Client 2.1 or Microsoft Rights Management Sharing application must be installed on the endpoint machine.
4. For Azure AD/Office 365 SSO, Microsoft Online Services Sign-In Assistant must be installed on the endpoint machine.
5. Microsoft RMS predefined templates must have Copy and Extract Content permissions.
6. Make sure that the following Forcepoint DLP predefined policies are not configured to block breaches, because they block the RMS client communication to the RMS server:
   - Encrypted Files - Unknown Format (Script)
   - Encrypted Files - Unknown Format (Wide)

   By default, these policies are set to monitor. If they are enabled, false positive incidents for RMS communication appear in the Security Manager.

To view RMS-related incidents in the Data Security module of the Security Manager, navigate to the **Main > Reporting > DLP > Incidents - Last 3 days** page. The Forensics tab shows when the detected breach was an RMS-protected file.

To determine whether RMS decryption and analysis is active or inactive, check the **Main > Status > Endpoint Status** page.
Configuring the CASB service

Use the CASB Service tab of the Settings > General > Services page to connect, disconnect, and configure the CASB service.

With a Forcepoint DLP Cloud Applications subscription, the CASB service:

- Provides content inspection for files used in cloud collaboration applications, including downloaded, uploaded, shared, and stored files
- Applies DLP policies to sensitive data

The first step in using the CASB service is to connect Forcepoint DLP to the Forcepoint CASB service. To enable the connection:

1. Click Connect.
   The CASB Service Connection dialog box is displayed.
2. Enter the following information from the Forcepoint CASB fulfillment letter:
   a. The Access key ID
   b. The Access key secret for the account
   c. The Service URL
3. Click Connect.
   The connection process is initiated. This may take some time to complete.

Once Forcepoint DLP has connected successfully to the CASB service, it is automatically enabled and the CASB Service tab is updated.

Next, enable DLP policy enforcement for specified cloud applications:

1. Click Add under the Cloud Applications list.
2. In the Add Cloud Application window, select an application.
   The CASB portal opens in a new tab to allow configuration of the selected application.
   - Pop-up blockers may prevent this tab from opening. If this occurs, disable the pop-up blocker and try again.
   - It may take a while for the tab to open. Wait for the tab to load, then complete the steps below. Do not close the tab while it is still loading.
3. Enter a descriptive Application name and Service description to help administrators manage the service, or maintain the default name and description as provided.
4. Under Connection, enter the Key and Secret to enable a connection to the selected cloud application, then click Configure Connection.
   The CASB service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials.
5. Under Service Type, specify whether or not to Enable activity import and allow the CASB service to access and import user activity logs for the selected cloud application.
6. Under Mitigation, configure an **Archive folder** within the cloud service for files moved or copied in response to a DLP incident.

7. Under Quarantine, optionally configure messages that 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.

8. To save the changes and return to the CASB Service tab, 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 in a new CASB window, which can be used to update configuration for the application.
     Note that the new application is added to the cloud applications list even if configuration is canceled before this step is completed. Use the Edit link to finish configuration if necessary.

9. If needed, click **Return to the Security Manager**.
   Functionality can be used to exit the CASB portal at any point and continue working in the Security Manager.

Repeat the steps above as many times as needed to enable the CASB service for each cloud application to which DLP policies will be applied.

### Configuring classification tagging

Use the **Classification Tagging** tab of the Settings > General > Services page to enable and configure file tagging on endpoint machines. This allows Forcepoint DLP to add tags to files and modify tags based on discovery policies.

- File tagging occurs during the endpoint discovery process.
- In order to enable and use this feature, a supported classification tagging system must already be in use on the network.

**Note**

In version 8.5, Boldon James is the only supported classification tagging system.

To enable and configure classification tagging:

1. Mark the **Enable classification tagging** check box.

2. Under Guidelines, mark one or more check boxes to specify when Forcepoint DLP should add or modify a tag:
   - When the file has a lower priority tag (upgrade the classification)
   - When the file has a higher priority tag (downgrade the classification)
   - When the file has a tag whose priority cannot be compared to the new tag
   - When the file is not already tagged
In cases where a file does not meet a selected condition, its tagging remains unchanged. This may mean that the file remains untagged, or that the original tag or tags added by the third-party system remain in place.

In incident reports, the incident details provide information about whether tags were found on a file, and whether tags were changed.

3. Click **OK** to save the changes.

After classification tagging has been enabled, administrators can configure the specific tags to use on the Discovery tab of each of their action plans. See *Action Plans*, page 239.

**The RAP service**

Risk Adaptive Protection (RAP) is a product offering that is built upon existing UEBA and DLP technologies.

The RAP feature combines the power of the DLP and UEBA technologies by ingesting the DLP event and incident data into the UEBA platform which performs modeling and analytics to determine a user profile risk. Then, based on the user risk level, controls are triggered to affect user interactions with sensitive data.

To enable the feature:

1. Deploy a UEBA instance. See Forcepoint UEBA Administrator Help.
2. Enable RAP in DLP. See *Configuring the RAP service*, page 344.
3. Configure relevant policies and rules so that actions will be risk-level-dependent. See *Custom Policy Wizard - Severity and Action*, page 147.
4. Enable/Disable RAP for specific users/groups. Use the RAPUserManager.
   - Users could be either custom or user directory ones.
   - Users get risk level 1 as a default risk level value.
5. Sync the modified list of Risk Adaptive Protection users in the UEBA system. See Forcepoint UEBA Administrator Help.
6. Check DLP incidents. See *Managing incident reports*, page 76.
7. Investigate users. See Forcepoint UEBA Administrator Help.

**Configuring the RAP service**

Risk Adaptive Protection (RAP) is a product offering that is built upon existing Forcepoint UEBA and DLP technologies.

To use the RAP Service go to Settings > General > Services. Select the Risk Adaptive Protection tab.

To enable the feature:
1. Click **Enable Risk Adaptive Protection**.
2. Enter:
   a. The **Forcepoint UEBA hostname or IP Address**
   b. The **Port Number**. The default port number is 2181.
3. Click **Test Connection** to test the UEBA connection to DLP. A confirmation message returns.
   If connection fails, enter again the UEBA hostname or IP Address and the port number; then test again.
4. Click **OK** to save the changes.

---

**Note**

If you already defined DLP rules to determine actions, disabling this option (by clearing the Enable Risk Adaptive Protection checkbox) will disconnect the UEBA from DLP and actions will be determined by DLP matches only.

### 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.

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*, page 346.
   Note that only user resources can be added as high-risk resources. Other resource 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by</td>
<td>If there is a large number of business units listed, use the filter to narrow down the list.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
<tr>
<td>Level</td>
<td>Select the risk level for this business unit. The High-risk source options are:</td>
</tr>
<tr>
<td></td>
<td>- Risk</td>
</tr>
<tr>
<td></td>
<td>- High risk</td>
</tr>
<tr>
<td></td>
<td>- Very high risk</td>
</tr>
<tr>
<td></td>
<td>The Privileged account options are:</td>
</tr>
<tr>
<td></td>
<td>- Privileged</td>
</tr>
<tr>
<td></td>
<td>- High privileged</td>
</tr>
<tr>
<td></td>
<td>- Most highly privileged</td>
</tr>
</tbody>
</table>

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, page 347.
- Update the configuration of an existing directory server. Select an entry in the list, then see Adding or editing user directory server information, page 347.
- Delete an existing directory server.
- Import user information (see Importing users, page 349, and Importing user entries from a CSV file, page 350).

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, page 349.

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:

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, page 348.
   - If you select Comma Separated Value (CSV) file, see Using a CSV file, page 347.

Using a CSV file

If you selected Comma Separated Value (CSV) file, under Connection Settings:

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, page 350, for details.

---
Using Active Directory or Domino

If you selected Active Directory or Domino:

1. Under Connection Settings, enter the **IP address or hostname** and **Port** to use to connect to the user directory server.

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.

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:

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.
  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:

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 page.
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.

---

**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:**
  a. Enclose fields that contain a special character (semicolon, new line, or double quote) in double quotes.
  b. If a field’s value contains a double-quote character, escape it by placing another double-quote character next to it.
- **Omit optional fields and replace them with the delimiter.**
- When a field contains a list, separate the list elements using a semicolon (;) and enclose the entire field in double quotes, unless the list contains 1 element or none.

**Groups file format**

Each row in the groups.csv file should contain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Group name</td>
<td>String</td>
<td>No</td>
<td>Name of user directory group</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>Yes</td>
<td>Description</td>
</tr>
<tr>
<td>memberOf</td>
<td>List of UUID</td>
<td>Yes</td>
<td>UUIDs of which this group is a member (can be empty)</td>
</tr>
</tbody>
</table>

For example:

```
08b3b46b-3631-46cb-adc7-176c2871e94c,Marketing - EMEA, Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05
```

```
40632a33-db39-4f93-bd80-093e0b3230ca,Marketing - APAC, Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05
```

```
7c9d4db6-1737-4b80-9e6e-42f415300a05,Marketing all,All Marketing departments
```

**Users file format**

Each row in the users.csv file should contain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Username</td>
<td>String</td>
<td>No</td>
<td>Login or user ID</td>
</tr>
<tr>
<td>Email</td>
<td>String</td>
<td>Yes</td>
<td>Email address (primary)</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>Yes</td>
<td>Description</td>
</tr>
<tr>
<td>UUID</td>
<td>String</td>
<td>Yes</td>
<td>UUID of the current user’s manager</td>
</tr>
<tr>
<td>memberOf</td>
<td>List of UUID</td>
<td>Yes</td>
<td>UUIDs of which this group is a member (can be empty)</td>
</tr>
</tbody>
</table>

Zero or more “additional attributes” fields

```
| 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:

<table>
<thead>
<tr>
<th>String</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>attr:wbsn_title=/=Manager</td>
<td>wbsn_title</td>
<td>Manager</td>
</tr>
<tr>
<td>aTTr:my amazing attr=/=the value</td>
<td>my amazing attr</td>
<td>the value</td>
</tr>
<tr>
<td>“ATTR:name=/=value1,value2”</td>
<td>name</td>
<td>value1,value2</td>
</tr>
</tbody>
</table>

For example:

```
6278ab76-2ce2-4f16-8e49-aa5104da7d0b, jdoe-mgr, jdoe.manager@example.com,CEO,7c9d4db6-1737-4b80-9e6e-42f415300a05,attr:room/=/201,attr:parkingSpace/=/1
```

```
ff255105-4e43-4e9a-b2bd-e366872cd212, jdoe, jdoe@example.com, administrator, 6278ab76-2ce2-4f16-8e49-aa5104da7d0b,“08b3b46b-3631-46cb-adc7-176c2871e94c;7c9d4db6-1737-4b80-9e6e-42f415300a05”,attr:room=/=101
```

**Computers file format**

Each row in `computers.csv` should contain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>String</td>
<td>No</td>
<td>The record’s universal unique identifier</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>No</td>
<td>Computer name (hostname)</td>
</tr>
<tr>
<td>FQDN</td>
<td>String</td>
<td>Yes</td>
<td>DNS fully qualified domain name</td>
</tr>
</tbody>
</table>
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, page 354, 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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>An internal identification number for the partition, beginning with the year. Click incident partitions to select them for archiving.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status:</td>
</tr>
<tr>
<td></td>
<td>● <strong>Online-Active</strong> marks the partition into which local incidents are dynamically stored.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Online</strong> indicates a former (now full) Online-Active partition. This partition is no longer active, but it has not been archived or deleted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Archive</strong> marks partitions that have been archived in an offline location.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Deleted</strong> marks partitions that have been permanently deleted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Restored</strong> marks partitions that were restored to Online status after having been archived.</td>
</tr>
<tr>
<td>From</td>
<td>The date of the first event logged in the archive.</td>
</tr>
<tr>
<td>To</td>
<td>The date of the last event logged in the archive.</td>
</tr>
<tr>
<td># of Incidents</td>
<td>The number of incidents currently collected in the archive.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the archive, whether local or at an external IP address.</td>
</tr>
<tr>
<td>Path</td>
<td>The complete path to the external storage.</td>
</tr>
<tr>
<td>Comments</td>
<td>Optional, administrator-added comments about the archive.</td>
</tr>
<tr>
<td>Show deleted partitions</td>
<td>When selected, deleted partitions are displayed in the Archiving list.</td>
</tr>
</tbody>
</table>

Use the buttons in the toolbar at the top of the content pane to archive, restore, or delete selected partitions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>Send a selected archive to offline storage. See <em>Archiving a partition</em>, page 355.</td>
</tr>
<tr>
<td>Restore</td>
<td>Restore a selected archived partition. See <em>Restoring a partition</em>, page 356.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently delete a selected partition. See <em>Deleting a partition</em>, page 356.</td>
</tr>
<tr>
<td>Settings</td>
<td>Open a settings paged used to define the archive size and storage location. See <em>Archive storage</em>, page 337.</td>
</tr>
</tbody>
</table>

**Remote SQL Server machines**

Administrator Help | Forcepoint DLP | Version 8.5.x

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:

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**.

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:

1. Go to the **Settings > General > Archive Partitions** 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, page 353.

5. Click OK to continue.

The number of partition archives you can create depends on the size of the partition location.

### 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:

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:

2. Select the partitions of interest.
3. Click Delete in the toolbar. A summary of the partitions to be deleted appears. If one of the partitions is active, a warning message appears: Warning: deleting a partition is irreversible.
4. Click **OK** to continue.

If you delete the Active partition, all of its incidents are removed, but the Active partition itself cannot be deleted. The Status line for the deleted partitions indicates their deletion.

**Archive threshold**

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.

**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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The date the update occurred.</td>
</tr>
<tr>
<td>Administrator</td>
<td>The administrator who performed the update.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of policy that was updated. Standard Policies are those predefined by Forcepoint and available to all customers. Custom policies are those that have been built just for a specific organization.</td>
</tr>
<tr>
<td>From Version</td>
<td>The version of policies, classifiers, and file types installed prior to the update.</td>
</tr>
<tr>
<td>To Version</td>
<td>The version of policies, classifiers, and file types installed during the update.</td>
</tr>
<tr>
<td>Details</td>
<td>A link to a PDF file containing the details of the update. The PDF contains general information, release notes (details about what changed), a snapshot of your policies and classifiers before they were updated, and a list of the components that were updated. Click the link to view the details.</td>
</tr>
<tr>
<td>File name</td>
<td>The name of the update file used to perform the update.</td>
</tr>
</tbody>
</table>

Use the buttons in the toolbar at the top of the content pane to install updates or restore policies to a previous version:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Updates</td>
<td>Install the latest policy updates, content classifiers, and file types on your system. A wizard is launched. (See Installing policy updates, page 359, for instructions on using the wizard.)</td>
</tr>
<tr>
<td>Restore</td>
<td>Restore your policies, content classifiers, and file types to the selected version. (See Restoring policies to a previous version, page 360, for instructions.)</td>
</tr>
</tbody>
</table>
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, page 358, for a description of this page.

Related topics:
- Viewing your update history, page 358
- Restoring policies to a previous version, page 360
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, page 358, for a description of this page.

Note that you cannot restore policies from an older product version. For example, if you are running Forcepoint DLP v8.4, you cannot revert to policies from TRITON AP-DATA v8.3.
Entering subscription settings

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 besides 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’re 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, the number of subscribed users, and the modules to which you subscribe. The Forcepoint DLP application restarts.

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**.
   - The Forcepoint DLP application restarts automatically.

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.
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*, page 363.

- 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*, page 368.

- Configure personal settings for your own administrator account.
  
  See *Customizing your own administrator account settings*, page 373.

### 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 3 types of Forcepoint DLP administrators:

- 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.
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 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 user 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.

   See Editing administrators, page 366, for more information.

Related topics:
- Defining administrators, page 363
- Editing administrators, page 366
- Working with roles, page 368
- Adding a new role, page 370
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:

2. Select the user name for the administrator whose profile you want to edit. Note that changes to administrator profiles are recorded in the audit log.
3. Select a role for this administrator from the drop-down list (see Working with roles, page 368), or click New to create a new role.
   - Click View Permissions to view the permission settings for the selected role.
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.

Related topics:

- Defining administrators, page 363
- Select Incidents, page 367
- Select Policies, page 367
- Select Business Units, page 368
- Working with roles, page 368
- Adding a new role, page 370
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**.

**Select Incidents**

1. When editing an administrator’s profile (see [Editing administrators, page 366](#)), 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.

---

**Select Policies**

1. When editing an administrator’s profile (see [Editing administrators, page 366](#)), 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**.

---

**Note**
The administrator must have a role that permits policy management. If he or she does not, these settings have no effect.

---

### Select Business Units

When editing an administrator’s profile (see *Editing administrators*, page 366), 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.

---

### 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.

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:

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.

Customized role permissions

Configure customized permissions for the role as follows:

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.

Related topics:

- Viewing administrators, page 365
Configuring Authorization

- 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 and destination** to prevent administrators with this role from seeing source and destination information like user names and IP addresses. Instead, reports will show sources and destinations as unique IDs generated by the system.
    This does not affect the source and destination fields in the syslog. Syslog always displays names.

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.
Configuring Authorization

- **Sample database records** - Can view sample database information when editing a database fingerprinting classifier, including database, Salesforce, and CSV classifiers.

  This is offered on the Field Selection page of the fingerprinting wizard when you define the records to fingerprint. It allows you to verify that you’ve set up the classifier as intended. See *Database Fingerprinting Wizard - Field Selection*, page 211, 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.
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 topics:
- Deploy button, page 13
- My cases, page 90
Managing Forcepoint DLP
System Modules

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

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, page 407.

### 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 the Configuring Forcepoint DLP system modules, page 377.

  This requires system modules permissions. (See Adding a new role, page 370, 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).

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, page 21.

To configure a Forcepoint DLP system module:

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

Related topics:

- Adding Forcepoint DLP system modules, page 376
Managing Forcepoint DLP System Modules

- Configuring the Forcepoint Email Security module
- Configuring the Cloud Email module
- Configuring the integration agent
- Configuring protector services
- Configuring the mobile agent
- Configuring the analytics engine

Configuring the Forcepoint DLP management server

Administrator Help | Forcepoint DLP | Version 8.5.x

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**
Managing Forcepoint DLP System Modules

- Configuring the forensics repository
- Configuring the policy engine

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.

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.

To configure the selected repository:
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

Primary Fingerprint Repository

Under Tuning Performance:

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.

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.

## 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.

**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.
Configuring the policy engine

Administrator Help | Forcepoint DLP | Version 8.5.x

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, page 407*, for more information.

---

Policy engines reside on the:

- Management server
- Supplemental Forcepoint DLP servers
- Protectors
- Mobile agents
- 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, page 384*, 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.
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:

- 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](#).

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.

### 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. Under **Languages**, select the languages that might appear inside your textual images.
   - Some languages are included with Forcepoint DLP (see Languages included with Forcepoint DLP (no language pack required), page 386). Other languages require a separate language package on your OCR server (see “Installing the Forcepoint DLP Language Pack”).
   - If you select a language that is not included with the product, and you do not have the language pack installed, matches in that language are not detected.
■ Image analysis can be time consuming. Select fewer languages to optimize performance.
■ 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.

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.

Languages included with Forcepoint DLP (no language pack required)

- Basque
- Dutch (Netherlands)
- Finnish
- German
- Greek
- Irish
- Old English
- Old Italian
- Portuguese (Brazil)
- Swedish
- Yiddish
- Belorussian
- Dutch (Belgium)
- French
- German (new spelling)
- Hebrew
- Italian
- Old French
- Old Spanish
- Portuguese (Portugal)
- Turkish
- Danish
- English
- Scottish Gaelic
- German (Luxembourg)
- Icelandic
- Norwegian
- Old German
- Polish
- Spanish
- Welsh

Configuring the protector

Related topics:

- *Edit Protector: General tab*, page 387
- *Edit Protector: Networking tab*, page 388
- *Edit Protector: Local Networks tab*, page 389
- *Edit Protector: Services tab*, page 390

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

---

**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:

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.

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.

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.

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, page 399, 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

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
**Edit ICAP: General tab**

Use the General tab of the Edit ICAP page to configure the module name, description, and basic behavior.

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:

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:

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

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, page 392.

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.
Managing Forcepoint DLP System Modules

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, page 393.*

**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.

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*

## Configuring the Cloud Email module

For information on installing and deploying the Cloud Email module, refer to the [Forcepoint DLP Installation Guide](#).

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
Managing Forcepoint DLP System Modules

- 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 mobile agent

The mobile agent is a Linux-based appliance used to secure the type of email content synchronized to users’ mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

- Within the network, the appliance connects to both the management server and a Microsoft Exchange server to provide this function.
- Outside the DMZ, the appliance connects to any Microsoft ActiveSync-compatible mobile device over 3G and wireless networks—devices such as i-pads, Android mobile phones, and i-phones.

Related topics:
- Configuring the Mobile DLP Policy, page 131
- Viewing mobile device status, page 32
- Mobile device settings, page 330
Like the protector, the mobile appliance has an on-board policy engine and fingerprint repository to optimize content analysis.

No software has to be installed on users’ mobile devices.

To configure the mobile agent, select its node on the Settings > Deployment > System Modules page in the Data Security module of the Forcepoint Security Manager. The configuration page opens to the *Edit Mobile Agent: General tab*.

Note that mobile agent include a policy engine and secondary fingerprint repository. To configure these components on the mobile agent, expand the module on the System Modules screen and click the component of interest. See the following for instructions on configuring these other components:

- Configuring the fingerprint repository
- Configuring the policy engine

**Edit Mobile Agent: General tab**

Use the General tab to enable the mobile agent and optionally update its description:

1. Select or clear **Enabled** to enable or disable this module.
2. Enter a **Description** of the module.

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

Continue with *Edit Mobile Agent: Connection tab*, page 396.

**Edit Mobile Agent: Connection tab**

Use the Connection tab to determine how the mobile agent connects to Microsoft Exchange and users’ devices.

1. Under Exchange Connection, select **Use secure connection (SSL)** to use SSL to provide communication security when connecting the mobile agent to Microsoft Exchange.
2. Enter the **Hostname or IP address** of the Microsoft Exchange server. The mobile appliance connects to this server to access email resources. The appliance acts as a reverse proxy to the Exchange server, making mobile devices unaware of the server.
3. Enter the **Port** for connecting to the Exchange server:
   - If Use secure connection (SSL) is selected, use port **443**.
   - If an unsecured connection is being used, use port **80**.

4. Optionally enter the **Domain** used to identify users in the organization.

5. Under Mobile Devices Connection, select **Use secure connection (SSL)** to use SSL to provide communication security when connecting the mobile agent to users’ mobile devices.

6. Enter the **IP address** of the network interface card (NIC) that mobile devices should use to connect to this agent.
   
   This is a NIC on the mobile appliance or machine hosting the mobile agent. It is the IP address that the mobile agent will listen on. The list reflects all of the NICs found on the mobile appliance.
   
   Select **All IP addresses** to allow the agent to listen and accept connections from all available network interface IPs.

   **Note**
   
   To modify the IP addresses available on the mobile agent machine, re-install and re-register the mobile agent. If you enter a user name in the installation wizard, the system resolves it to the correct IP address.

7. Enter one of the following **Port** numbers:
   - If the Use secure connection (SSL) option is selected, enter port **443**.
   - If the SSL option is not selected, enter port **80**.

8. To secure the connection to the mobile agent, users must set up their mobile devices to accept security certificates from the server. Select a certificate option:
   - Select **Use Forcepoint default security certificate** to use the a self-signed certificate automatically generated by Forcepoint.
     
     It enables SSL encryption to secure the ActiveSync public channel that is used by the mobile agent when communicating with mobile devices, but it does not rely on a well known Root CA for authentication.
     
     If you use this option, users may need to configure their mobile devices to accept all SSL certificates. Some devices, such as those using Windows Mobile 7, do not support this.
   - Select **Use the following certificates** to secure the ActiveSync public channel using specified certificates, then upload the certificates to use. This option enables SSL encryption and CA authentication, so it is seamlessly accepted by all mobile devices.
     
     Upload both a public certificate and its associated private key.

     ○ Upload the **Public certificate** the agent should use to identify itself to mobile devices. The signing CA can be a self-signed Root CA or subordinated (possibly untrusted) CA. If your certificate is signed by a subordinated CA, you must also upload its associated certificate chain file. (See **Add chained certificate** below.)
○ Upload the **Private key** that was used to generate the public certificate. The certificate files must conform to these requirements:
  ○ All files should be in .PEM file format.
  ○ The .PEM files for the public certificate and private key must be separate. Concatenation is not supported.
  ○ The files should not be encrypted or passphrase protected.
  ○ You must follow a Certificate Signing Request (CSR) procedure when creating the files. Instructions are readily available online.

9. Select **Add chained certificate** if the public certificate uploaded in the previous step is signed by a subordinated certificate.

The certificate chain, also known as the certification path, should be a list of all of the CA certificates between (but not including) the server certificate and the Root CA stored in the mobile devices. Each certificate in the list should be signed by the entity identified by the next. For example, the chained certificate should include numbers 2, 3, and 4 below, but not numbers 1 or 2.

a. Server certificate, signed by
b. Issuing CA 1, signed by
c. Intermediate CA 2, signed by
d. Intermediate CA 3, signed by
e. Root CA

The SSLCertificateChainFile file is the concatenation of the various PEM-encoded CA certificate files, usually in certificate chain order. In most cases, the CA organization provides this file.

**Edit Mobile Agent: Analysis tab**

Use the Analysis tab to select a deployment mode and configure analysis behavior.

1. Select the deployment Mode for the module:
   - Select **Monitoring** to monitor traffic through the mobile agent but not block it (default).
   - Select **Blocking** to block actions that breach policy. (Note, to prevent disruption, traffic is permitted when there is an unspecified system error.)

2. In Blocking mode, select **Notify users of breach** to notify users when an email message, task, appointment, or other item was blocked by the agent.
Enter the text to include in the email subject line and body, or click the right arrows and select from variables such as %From%, %Attachments%, and %Type%.

---

**Note**

Before users can be notified of breaches, an outgoing mail server and sender details must be configured on the Email Properties tab of the Settings > General > Alerts page.

---

3. Select the **Minimum transaction size** to analyze, in bytes.

### 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:

- **Configuring the policy engine**, page 383
- **Protector: Configuring SMTP**, page 400
- **Protector: Configuring HTTP**, page 403
- **Protector: Configuring FTP**, page 405
- **Protector: Configuring plain text**, page 406
- **Protector: Configuring plain text**, page 406

---
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, page 400)
   - HTTP (see Protector: Configuring HTTP, page 403)
   - FTP (see Protector: Configuring FTP, page 405)
   - Plain text (see Protector: Configuring plain text, page 406)

**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.

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. (Note that 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, page 400.

**Protector SMTP service: Traffic Filter tab**

Use the Traffic Filter tab to configure protector SMTP monitoring:

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, page 401*.

**Protector SMTP service: SMTP Filter tab**

Use the SMTP filter tab to configure SMTP monitoring by domain, direction, and source email address.

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, page 402.

Protector SMTP service: Mail Transfer Agent (MTA) tab

Use the Mail Transfer Agent (MTA) tab to configure MTA settings for the protector.

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, page 402.

Protector SMTP service: Encryption & Bypass tab

Use the Encryption & Bypass tab to configure how the protector handles encrypted messages and messages flagged for bypass.

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.

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**, page 403.

### 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!
1. Under Transaction Size, select the **Minimum transaction size** to monitor, in bytes.

2. Under Direction:
   - Select **Inbound** to monitor incoming HTTP traffic.
   - Select **Outbound** to monitor outgoing HTTP traffic.
   - Select **Internal** to monitor internal HTTP traffic.

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.
   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*, page 404.

**Protector HTTP service: HTTP Filter tab**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the HTTP Filter tab to specify domains that should be excluded from analysis.

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*, page 404.

**Protector HTTP service: Advanced tab**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.
Managing Forcepoint DLP System Modules

- 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**

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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.)

Continue with *Protector FTP service: Traffic Filter tab, page 405*.

**Protector FTP service: Traffic Filter tab**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Traffic Filter tab to configure FTP monitoring.

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.

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).


Protector plain text service: Traffic Filter tab

Use the Traffic Filter tab to configure telnet monitoring.

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, page 406.
   Otherwise, click **OK** to save your changes and return to the Protector Details page.

Protector plain text service: Advanced tab

Use the Advanced tab to configure characteristics of the data being processed.

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.
Managing Forcepoint DLP System Modules

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 or mobile agent 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.

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, page 26).

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, page 408.

---

**Note**
As a best practice, do not distribute the load to the management server.

---

**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
  - Crawler
  - Content Gateway
  - Integration agent
  - Protector
  - ICAP Server
  - Cloud Email
  - Mobile 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.
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 and Rearranging and deploying endpoint profiles.

   Endpoint profiles are templates that set service permissions. A profile describes the required behavior of an endpoint client: how it connects to endpoint servers, which user interface options are available on the client, and how it uses encryption to protect sensitive data. Each profile is deployed to selected endpoint clients.

5. Create endpoint resources. See Endpoint Devices, Endpoint Applications, and Endpoint Application Groups.
6. Create or modify a rule for endpoint channels. See Selecting endpoint destination channels to monitor.
7. Define the type of endpoint machines to monitor, and configure on- and off-network behavior. See Custom Policy Wizard - Source.
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*.
- 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*.

In special circumstances, monitoring and protection can be bypassed for an endpoint client. See *Bypassing endpoint clients, page 424*, 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.

**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, page 413*).
- Delete an existing profile.
- Rearrange existing profiles (see *Rearranging and deploying endpoint profiles, page 425*).
- Back up and restore encryption keys (see *Backing up encryption keys, page 419*, and *Restoring encryption keys, page 419*).

Select a profile from the list to view or edit its properties.
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**.

**Important**
Make sure that “custom computer” resources in the profile have both an FQDN and an IP address defined. Profiles can only be deployed to computers with a known FQDN.

Continue with *Endpoint profile: Servers tab, page 414*.

**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 robs 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.
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.

Continue with *Endpoint profile: Properties tab, page 415*.

**Endpoint profile: Properties tab**

Administrator Help | Forcepoint DLP | Version 8.5.x

Use the Properties tab to enable user notifications, define message templates, and configure policy override settings.

1. To allow end users to disable the Forcepoint DLP Endpoint software on their machines, under Interactive Mode Options, select **Remote bypass**.
   
   This action requires a bypass code from the administrator. (See *Bypassing endpoint clients, page 424*, for additional information.)

2. To alert endpoint users when content scanning is in progress, select **Content scan alerts**. When this option is enabled, a popup caption appears on the bottom of users’ screens.

   Content scan alerts are not displayed when data is copied to removable media using a non-desktop environment, such as an ssh terminal connection.

3. To notify endpoint users when file operations are performed, select **File operation notifications**. Depending on the application, file operations can include cut/copy, paste, file access, printing, LAN, encryption, and copying to removable media.

4. To change the default endpoint message template, under Endpoint Message Template, mark **Set message template to**, then select the template to use from the drop-down list.

   - Message templates are used for messages sent to the endpoint client, such as status details and alerts. The templates are XML files, and are available in the endpoint profile in multiple languages.
   - 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.

5. Under Data Loss Prevention (DLP) Policy Settings, mark **Disable blocking and encryption capabilities when policy violations are detected** to disable blocking and encryption of endpoint traffic. Even if a policy is specifically set up to block or encrypt content, the endpoint client overrides this setting and allows traffic. 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*, page 416.

**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*, page 418.

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.

To create an encryption key:
1. Click **New**.
2. Enter a password and confirm it.
3. Enter a description (for example “Encryption key for March”).
4. Click **OK**.

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:
  a. Settings are deployed.
  b. The endpoint receives the change.

---

**Note**
The default profile contains a default key based on the password of the administrator that installed the Security Manager.

---

**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

---
c. The endpoint is restarted OR the relevant removable media is disconnected from the endpoint.

- To enable a disabled key, select the key and click **Enable**. The key reverts to decryption-only status.
- To delete a pending key, click **Delete**. Only pending keys can be deleted.

Forcepoint recommends backing up the encryption keys every time you modify them. See *Backing up encryption keys*, page 419.

## Configuring encryption for removable media

Forcepoint DLP Endpoint provides 2 methods for encrypting sensitive data that is being copied on removable media devices:

- **(Windows and Linux) 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 Mac endpoints, regardless of your action plan setting.

- **(Windows only) 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 Linux and Mac endpoints, regardless of your action plan setting.

Encrypt with profile key is the most secure method of protecting data on USB devices.

- The encryption key is provided when administrators create endpoint profiles for each user or group of users (see *Endpoint profile: Encryption tab*, page 416).
- 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*, page 419, and *Restoring encryption keys*, page 419).

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 Mac 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’s 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.

---

### 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 topics:

- *Endpoint profile: Encryption tab*, page 416
- *Restoring encryption keys*, page 419
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, page 416.

To restore encryption keys:

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

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.

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, page 223).

To select endpoint destinations for monitoring in a policy:
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.

For a list of supported browser versions, see the [Certified Product Matrix](#).

**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.

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 Internet Explorer, Firefox, Safari, and Opera.

If Linking Service is active, URL category information is included in the incident (see Configuring Linking Service, page 339).

- 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.

- 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.

- 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 Internet Explorer, Firefox, Safari, and Opera.

---

**Note**

If a user’s browser is open, new endpoint policies are not enforced on those browsers. Users must close and reopen their browser for new policies to take effect.

---

The applications that the system supports out of the box are found in the 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.


Linux endpoint does not support CD/DVD burners.

On Windows 7, the system can also monitor unencrypted data being copied to Android devices through the Windows Portable Devices (WPD) protocol.

- **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 Linux endpoints, only removable media is supported.
- On Mac endpoints, all destination channels except the print channel are supported, with one exception: cloud apps are not supported.

<table>
<thead>
<tr>
<th>Destination Channel</th>
<th>Windows</th>
<th>Mac</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web HTTP/HTTPS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Printing</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Removable media</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LAN</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

For more information on monitoring destinations and protecting data on endpoints, see *Custom Policy Wizard - Destination*, page 150.

**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:

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.

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:

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.

### 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’s Guide,” available from support.forcepoint.com/documentation.

### Updating the endpoint client

Endpoint clients check for updates to policies and profile settings at specified intervals (see *Configuring endpoint settings*, page 327).

End users can start an update check at any time by clicking **Update** on the Forcepoint DLP Endpoint screen.
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.

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 Related Topics box to choose a specific area of concern.

### 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*, page 419 for instructions on how to perform these actions.

**Fingerprinting**

This section lists problems related to fingerprinting and their solutions. See the Related Topics box to choose a specific area of concern.

You can monitor the status and view fingerprinting errors in the 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


File has no fingerprint

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

1. Go to the Main > Policy Management > Content Classifiers > File Fingerprinting page.
2. Select the classifier configured for the file, then click Edit.
4. Change parameters in the Filter by Size section of the screen.
5. Click OK.

Validation script timeout

Administrator Help | Forcepoint DLP | Version 8.5.x

During a database fingerprinting scan, if the crawler finds a script matching the name of your fingerprinting classifier, <classifier-name>_validation.[bat|exe|py], it runs that script.

If it does not, it searches for a default script, default_validation.[bat|exe|py], and runs that.

If neither exists, it does not perform validation.

If you are getting validation script timeout errors, you can disable the script by renaming it.

See Creating a validation script, page 202 for more information on validation scripts.

No connectivity to fingerprint database

Administrator Help | Forcepoint DLP | Version 8.5.x

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.

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**

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 Related Topics box to choose a specific area of concern.

**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

Administrator Help | Forcepoint DLP | Version 8.5.x

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

Administrator Help | Forcepoint DLP | Version 8.5.x

This is expected behavior. Incident export exports only data loss prevention and endpoint incidents.

NLP policy isn’t being triggered, and events are undetected

Administrator Help | Forcepoint DLP | Version 8.5.x

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.
This section lists miscellaneous problems and their solutions. See the Related Topics box to choose a specific area of concern.

**Failed user directory import**

There are a few reasons why the user directory import might fail, such as access problems or an incorrect file structure in the import file. Take these steps in the Forcepoint Security Manager:

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*, page 350.

**Wrong default email address displays**

When forwarding events to another user, the email comes from email@mycompany.com rather than a valid email address. To resolve this:

1. In the 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

Administrator Help | Forcepoint DLP | Version 8.5.x

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

Administrator Help | Forcepoint DLP | Version 8.5.x

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

Administrator Help | Forcepoint DLP | Version 8.5.x

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 (x86)%\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, page 436) for help on improving performance.
Linking Service

This section lists problems related to linking and the Linking Service and their solutions. See the Related Topics box to choose a specific area of concern.

Linking Service stops responding

In the Forcepoint Data Security module of the Forcepoint Security Manager, take these steps:

2. Make sure the Enabled check box is selected.
3. Click the Refresh icon to retrieve the latest linking service host and port settings. These settings can change.
4. Click Test Connection to verify that the Linking Service machine can be reached.

System alerts that Linking Service is not accessible

When your 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
Troubleshooting

- 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**.
How Do I...

Use this selection of quick tips to get started with some of the most common Forcepoint DLP tasks and procedures.

**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, page 353.
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.

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, page 137.)
4. Click Deploy.

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.

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, page 115
   - Configuring the Web DLP Policy, page 123
   - Configuring the Mobile DLP Policy, page 131
4. Click Deploy.

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.

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, page 141.
4. Click Deploy.
Define an exception?

Most rules have exceptions. To add an exception to a rule:

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.

To review the process for using the exception wizard and obtain more information on adding (and rearranging) exceptions, see Adding a new exception, page 162.

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:

1. Open the report.
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:

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.

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*, page 183.
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*, page 199.
5. After completing the wizard, click **Run** to perform the scan.
6. Add the fingerprint classifier to a rule/policy when prompted.

---

### 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, page 208. 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, page 142.

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, page 239*, for more information.
Glossary

A

Analysis
The process that the Forcepoint DLP system uses to examine data to determine whether it contains protected content.

Assigned/Unassigned Incident
Incidents can be tracked through the system by administrators. To give a single administrator the responsibility to handle the incident, you can assign the incident to that administrator. Incidents that can be handled by any administrator are considered unassigned.

Authorization
The instruction to override security policy and send blocked email to the intended recipient. This can be performed by a security officer or by a content owner.

Authorization Code
The Forcepoint DLP-generated code in a Block email notification. When a reply is sent to the Block notification, the Authorization Code releases the blocked transmission.

Authorized Recipient
A user who is allowed to receive protected content.

B

Blocking
The prevention of data containing protected information from being sent to an unauthorized recipient.
### Classifier

A description of the content being monitored or protected. Classifiers include characteristics like dictionary terms, file fingerprints, or patterns. The system compares data to classifiers and triggers an incident when it finds a match.

### Content Group

An empty shell to which you later assign directories containing classified information of a certain type. Each directory within a Content Group can be assigned a security level that restricts its contents to users with matching or higher security levels.

### Content Owner

A Content Owner can define and modify a file’s distribution security policy. Content Owners can override security policy and authorize the distribution of a blocked transmission to the intended recipient.

### Crawler

The Crawler is the agent that scans your documents looking for sensitive data. You can have several in your network if you are managing many documents.

### Cumulative Rule

Accumulates matches to violations over time and creates an incident when a threshold is met (drip DLP). In contrast, a standard rule creates an incident each time its conditions are matched.

### Database

A Forcepoint DLP component that stores the system configuration, settings, and roles that determine the behavior of the application; it also stores information about traffic transmitted through the system.

### Event

An event is any transaction that traverses the Forcepoint DLP system. Not all events are stopped by the Forcepoint DLP sniffer and queued for analysis—for that to happen, something has to look suspicious, meaning that something in the event seems to match with a Policy rule.
● **Unmatched events** are events that pass through the system transparently, because they raise no suspicion.

● **Policy matches** are events that are analyzed as they traverse the system, because something in the transaction is suspicious according to the policies. Policy matches are then either deemed **authorized incidents**—events that seemed to match a policy but are in fact allowed—or **incidents**, which are policy violations.

**External User**

A user who is outside the organization or domain.

---

**File System Directories**

Registered directories on the corporate file server that contain files with classified content.

**File Fingerprinter**

A Forcepoint DLP component that scans specified folders and submits files for fingerprinting to the Forcepoint DLP DMS API.

**File Fingerprints**

Information that is protected by Forcepoint DLP. The information will be recognized even after the original file has been deleted from the corporate file server.

**File Type**

A data format, such as .doc, .pdf, or .xls.

**Fingerprint Server**

A Forcepoint DLP component that analyzes corporate file directories at predefined intervals and fingerprints files.

**Forcepoint DLP Administrator**

A user who manages and maintains the Forcepoint DLP system.

**Forcepoint DLP Server**

The server that controls all aspects of the Forcepoint DLP software.

**Forcepoint Security Manager**

A central management console that provides access to Forcepoint DLP, Forcepoint Email Security, and Forcepoint Web Security. A system administrator can define and monitor the distribution of security policies, and view reports for all 3 modules from one location.
**Forensics Repository**

The forensics repository contains complete information about your original transactions. In SMTP, for instance, it stores the original email message that was sent. For other channels, the system translates transactions into EML.

To configure the forensics repository, select it on the System Modules screen.

---

**Ignored Incident**

Incidents that are set as Ignored Incidents. Often files that are determined not to be violations or incidents (files or attachments) that are not malicious, can be set to be ignored. These incidents can then be filtered in or out using the main and quick filters.

Often, it is useful to set an incident as “ignored” when an incident was determined not to be a violation, (it looks like a violation but is not). Understanding ignored incidents can assist you in fine-tuning your policies to avoid blocking traffic unnecessarily. By default, the data presented in the Forcepoint Security Manager does not include incidents marked as ignored. Refer to “Filtering Incidents” to modify this setting.

**Incident**

An incident is a transaction or set of transactions that violate a policy. Depending on how you configure a rule, incidents can be created for every policy breach, or for matches that occur within a defined period.

Assigned/Unassigned Incident: Incidents can be tracked through the system by administrators. To give a single administrator the responsibility to handle the incident, assign the incident to a single administrator. Unassigned Incidents are those that have not been assigned and can therefore be handled by any administrator who has access to the incident.

**Incident Database**

The incident database saves basic information about incidents plus additional information that helps you analyze the data, such as: source, destination, the resolved source/destination hostname, breach information, analyzed by, detected by, and assigned to.

The incident database is part of the main Oracle management database.

**Information Lifecycle**

The changes (over time) to the importance level of information, from its most sensitive level at creation to its general distribution.
LDAP

Lightweight Directory Access Protocol is the protocol standard over TCP/IP that is used by email clients to look up contact information. Forcepoint DLP uses LDAP to automatically add users and groups to the Forcepoint DLP database.

Management Server

The management server includes all core Forcepoint DLP technology, including fingerprinting servers, policy servers, and patented data loss prevention technology.

MAPI

The protocol that sends email to recipients inside an organization/domain.

Matching Keyword

A predefined text string that must be protected; its presence in a document indicates that the document contains confidential information.

Notification

An email alert sent to the Security Officers and Content Owners, indicating that the information was addressed to an unauthorized recipient.

Owner

See Content Owner.

Permissions

Permissions define what a user is authorized to perform within the Forcepoint DLP structure.
Policy
The system can be set to include multiple policies. A policy is a list of criteria to be searched for over your channels. These criteria are set with a certain rule which defines what the system does when it comes across a transmission that meets the designated criteria.

Policy Category
Forcepoint DLP can be set to include multiple policies. These policies are grouped together to create policy categories.

Policy Category Group
Multiple policy categories can be grouped together to form policy category groups. These groups are then assigned to specific administrators for incident management and monitoring purposes. Often a policy category group reflects the corporate department associated with these events, such as Finance or Marketing. For example, the policy categories Intellectual Property, Malicious Concealment, and Source Code may be combined to form a policy category group called Technology. This group can then be assigned to administrators who are the VP of R&D and the CTO. These individuals would then be notified of violations of these policies and would be able to handle and track these incidents.

Registering
The process of identifying a unique set of characteristics for a document’s contents. Forcepoint DLP uses registering to uniquely identify classified content.

Roles
Security profiles that can be applied to several users without having to define security details for each user.

Rule
Provides the logic for a policy. Rules are made up of conditions that govern the behavior of a policy, determining when, for example, to block or audit an action, or send a notification.

Security Level
A label, such as Top Secret, that represents a degree of confidentiality. Both users and classified content are assigned Security Levels. Users with a specific Security Level can only receive information classified with the same or lower Security Level.
**Security Officer**

A user who defines Forcepoint DLP security policies, and monitors security policy distribution within the organization. The Security Officer can override security policy and authorize the distribution of a blocked transmission to the intended recipient.

**Security Policy**

The policy within an organization that defines which classified information can be distributed to which recipients.

**SMTP**

The protocol used for sending email to recipients outside the organization.

**System modules**

These are the various components of Forcepoint DLP. They are either hardware-based physical devices, like the protector; software components, like the Forcepoint Security Manager, or virtual components like channels and services.

**Traffic**

The transmission of email messages sent through the electronic mail system or uploaded to the Internet.

**Unmatched Events**

Unmatched Events are events that pass through the system transparently because they raise no suspicion.

**Urgency**

The incident’s urgency setting is a measure of how important it is to the corporation that this incident is handled. The urgency of an incident is automatically decided by Forcepoint DLP. This calculation takes both the sensitivity of the incident and the number of matched violations into account.

For example, if content triggers a violation because it includes 400 credit card numbers, and the credit card policy was set to medium sensitivity, then the urgency is set to critical due to the large number of violations (400) and the sensitivity (medium). This setting provides you with a relative measure for how urgent it is for someone to deal with this incident.
Users

The personnel within an organization who can distribute and receive information.

V

Views

Views are views into the incident database with filters applied. Several built-in views are provided. The most common are displayed on the main Reporting page. Views are very much like reports; they’re graphical and contain colorful executive charts.
For other copyright information, refer to **Acknowledgments**.

**Acknowledgments**

Portions of this Forcepoint Software may utilize the following copyrighted material, the use of which is hereby acknowledged:

**4suite**

Copyright (c) The Apache Software Foundation (http://www.apache.org/) Fourthought, Inc.
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (www.apache.org/licenses/LICENSE-2.0).

**7zip**

7-Zip Copyright (C) 1999-2015 Igor Pavlov.
Licenses for files are:
1) 7z.dll: GNU LGPL + unRAR restriction
2) All other files: GNU LGPL(https://www.gnu.org/licenses/lgpl-3.0.txt)

The GNU LGPL + unRAR restriction means that you must follow both GNU LGPL rules and unRAR restriction rules.

Note: You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

unRAR restriction

The decompression engine for RAR archives was developed using source code of unRAR program.
All copyrights to original unRAR code are owned by Alexander Roshal. The license for original unRAR code has the following restriction:

The unRAR sources cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified unRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.

Amara

Copyright (c) August 15, 2011. The Apache Software Foundation (http://www.apache.org/)
Amara team
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

Anaconda

Copyright, Continuum Analytics, Inc.
All rights reserved under the 3-clause BSD License (http://opensource.org/licenses/BSD-3-Clause).

Notice of Third Party Software Licenses
Anaconda contains open source software packages from third parties. These are available on an “as is” basis and subject to their individual license agreements. These licenses are available in Anaconda or at http://docs.continuum.io/anaconda/pkg-docs/. Any binary packages of these third party tools you obtain via Anaconda are subject to their individual licenses as well as the Anaconda license. Continuum Analytics (“Continuum”) reserves the right to change which third party tools are provided in Anaconda.

In particular, Anaconda contains re-distributable, run-time, shared-library files from the Intel(TM) Math Kernel Library (“MKL binaries”). You are specifically authorized to use the MKL binaries with your installation of Anaconda. You are also authorized to redistribute the MKL binaries with Anaconda or in the conda package that contains them. If needed, instructions for removing the MKL binaries after installation of Anaconda are available at http://www.continuum.io.

Cryptography Notice
This distribution includes cryptographic software. The country in which you currently reside may have restrictions on the import, possession, use, and/or re-export to another country, of encryption software. BEFORE using any encryption software, please check your country’s laws, regulations and policies concerning the import, possession, or use, and re-export of encryption software, to see if this is permitted. See the Wassenaar Arrangement <http://www.wassenaar.org/> for more information.

Continuum has self-classified this software as Export Commodity Control Number (ECCN) 5D002.C.1, which includes information security software using or performing cryptographic functions with asymmetric algorithms. The form and manner of this distribution makes it eligible for export under the License Exception ENC Technology Software Unrestricted (TSU) exception (see the BIS Export Administration Regulations, Section 740.13) for both object code and source code.

The following packages are included in this distribution that relate to cryptography:

openssl
The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols as well as a full-strength general purpose cryptography library.

pycrypto
A collection of both secure hash functions (such as SHA256 and RIPEMD160), and various encryption algorithms (AES, DES, RSA, ElGamal, etc.).

pyopenssl
A thin Python wrapper around (a subset of) the OpenSSL library.

kerberos (k5b5, non-Windows platforms)
A network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

cryptography
A Python library which exposes cryptographic recipes and primitives.
antlr

Version 2.7.6
Copyright (c) 2012 Terence Parr and Sam Harwell
ANTLR 4 License
Distributed under the BSD 3-Clause license (https://opensource.org/licenses/BSD-3-Clause).

Apache HTTPD

Version 2.4.23
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

aprutils

Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

asm

Versions 3, 1.5.3
Copyright (c) 2000-2011 INRIA, France Telecom
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE

Bash

Version 4.2.46-19.el7
Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version (https://www.gnu.org/licenses/gpl-3.0.en.html).
BeatBox

Copyright (c) 2000-2013 Simon Fell
Licensed under the GNU General Public License, Version 2.0; you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

bitstring

Version 3.1.3
The MIT License (MIT)
Copyright (c) bitstring
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

bonecp

Version 0.8.0
Copyright (c) bonecp
Apache License Version 2.0, January 2004
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

boost

Copyright (c) 2016 boost
Boost Software License - Version 1.0 - August 17, 2003
Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:
The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
BOUNCER

© 2014 github.com/ggrandes, has been modified and is distributed under the Apache License, version 2.0 (apache.org/licenses/LICENSE-2.0).

bouncycastle

Version 1.3.5
Copyright (c) 2000 - 2013 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

centos-release-7.2

Version 7.2.1511
Copyright (c) 2007 The CentOS Project
Creative Commons Attribution-ShareAlike 3.0 license (https://creativecommons.org/licenses/by-sa/3.0/us/).

cglib

Version 2.2
INRIA, France Telecom
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

chardet

Version 2.1.1
Copyright (c) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Chest

Version 0.2.3
New BSD license
Copyright (c) 2014 Continuum Analytics All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: a. Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer. b. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials provided with the
distribution. c. Neither the name of toolz nor the names of its contributors may be used to endorse or
promote products derived from this software without specific prior written permission. THIS SOFTWARE
IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

commons-beanutils

Version 1.8.3
Copyright (c) 2000-2010. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-cli

Version 1.2
Copyright (c) 2001-2009. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-collections

Version 3.2.1
Copyright (c) 2001-2008. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-codec

Version 1.4
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-digester

Version 1.7
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-discovery

Version 0.2
commons-el

Version 1.1.2.1
Copyright (c) 1999-2002. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-httpclient

Version 3.1
Copyright (c) 1997-2007. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-io

Version 2.0.1
Copyright (c) 2002-2010. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-lang

Version 2.5
Copyright (c) 2001-2010. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-logging

Version 1.1.1
Copyright (c) 2001-2007. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-pool

Version 1.5.3
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

commons-vfs

Versions 20061227 and 1.1
Copyright (c) 2002-2006. The Apache Software Foundation (http://www.apache.org/)
css2parser

Version 0.94
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

cURL

COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1996 - 2013 Daniel Stenberg, <daniel@haxx.se>.
All rights reserved.
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

cytoolz

Version 0.7.4
New BSD license
Copyright (c) 2014 Erik Welch All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. c. Neither the name of cytoolz nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

dask

Version 0.7.3
Copyright (c) 2014-2015, Continuum Analytics, Inc. and contributors All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Continuum Analytics nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

defusexml

Version 0.4.1
Copyright (c) Christian Heimes , All rights reserved.
AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 3.5.1 software in source or binary form and its associated documentation. 2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 3.5.1 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001-2016 Python Software Foundation; All Rights Reserved" are retained in Python 3.5.1 alone or in any derivative version prepared by Licensee. 3. In the event Licensee prepares a derivative work that is based on or incorporates Python 3.5.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 3.5.1. 4. PSF is making Python 3.5.1 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY
PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 3.5.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS. 5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 3.5.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 3.5.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. 6. This License Agreement will automatically terminate upon a material breach of its terms and conditions. 7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party. 8. By copying, installing or otherwise using Python 3.5.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

**Dill**

Version 0.2.4

Copyright (c) Dill v0.2.4

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**enum34**

Version 1.1.2

Copyright (c) Ethan Furman All rights reserved.

New BSD license

Copyright (c) 2013 Matthew Rocklin All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. c. Neither the name of toolz nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Fpconst

Copyright (c) February 24, 2005. The Apache Software Foundation (http://www.apache.org/)
Gregory R. Warnes
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

FreeTDS

Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version (http://www.gnu.org/licenses/gpl-3.0).

funcsigs

Version 0.4
AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 3.5.1 software in source or binary form and its associated documentation. 2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 3.5.1 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001-2016 Python Software Foundation; All Rights Reserved" are retained in Python 3.5.1 alone or in any derivative version prepared by Licensee. 3. In the event Licensee prepares a derivative work that is based on or incorporates Python 3.5.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 3.5.1. 4. PSF is making Python 3.5.1 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 3.5.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS. 5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 3.5.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 3.5.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. 6. This License Agreement will automatically terminate upon a material breach of its terms and conditions. 7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party. 8. By copying, installing or otherwise using Python 3.5.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

fuse

Version 2.7.4
Copyright (c) April 15, 2005,
Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version (http://www.gnu.org/licenses/gpl-3.0).

Gdsl

Version 1.3
Licensed under the GNU Lesser General Public License, Version 3.0; you may not use this file except in compliance with the License (https://www.gnu.org/licenses/lgpl-3.0.en.html).
GhostPDL

Version 9.06
Version 3, 19 November 2007
Copyright (c) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Distributed under the GNU Affero General Public License (https://www.gnu.org/licenses/agpl-3.0.en.html).

GhostScript

Version 9.06
Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. (http://www.gnu.org/licenses/gpl-3.0)

glibc

Version 2.17-105.el7
Bash is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. (http://www.gnu.org/licenses/gpl-3.0)

Google Sparse Hash

Version 2.0.3, Copyright (c) 2005, Google Inc. All Rights reserved. Distributed under the BSD 3-Clause License (opensource.org/licenses/BSD-3-Clause).

gtk2

Version 2.4.13-24.el4/2.10.4-20.el5
Copyright (c) 1991, 1999 Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

guava

Version 15
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

HAProxy

Version 1.6
Copyright (c) 2014 Willy Tarreau. All rights reserved.
Historically, haproxy has been covered by GPL version 2 (http://www.gnu.org/licenses/gpl-2.0). However, an issue appeared in GPL which will prevent external non-GPL code from being built using the headers provided with haproxy. My long-term goal is to build a core system able to load external modules to
support specific application protocols.

Since some protocols are found in rare environments (finance, industry, ...), some of them might be accessible only after signing an NDA. Enforcing GPL on such modules would only prevent them from ever being implemented, while not providing anything useful to ordinary users.

For this reason, I *want* to be able to support binary only external modules when needed, with a GPL core and GPL modules for standard protocols, so that people fixing bugs don't keep them secretly to try to stay over competition.

The solution was then to apply the LGPL license (http://www.gnu.org/licenses/lgpl-3.0) to the exportable include files, while keeping the GPL for all the rest. This way, it still is mandatory to redistribute modified code under customer request, but at the same time, it is expressly permitted to write, compile, link and load non-GPL code using the LGPL header files and not to distribute them if it causes a legal problem.

Of course, users are strongly encouraged to continue the work under GPL as long as possible, since this license has allowed useful enhancements, contributions and fixes from talented people around the world.

Due to the incompatibility between the GPL and the OpenSSL licence, you must apply the GPL/LGPL licence with the following exception: This program is released under the GPL with the additional exemption that compiling, linking, and/or using OpenSSL is allowed.

---

**HeapDict**

Version 1.0.0

Copyright (c) 2014 Erik Welch. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. Neither the name of cytoolz nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

**HOWL**

Version 0.1.8

HOWL is OSI Certified Open Source Software licensed under the BSD license.

Copyright (c) 2004, Bull S. A., All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

httpd

Versions 2.4.6-17.el7
Copyright (c) 2012. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

iconv

Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

ICU

Version 4.2.1.-9.1.el7
Copyright (c) 1995-2016 International Business Machines Corporation and others
All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

iptables

Version 1.4.21-16.el7
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Distributed under the GNU General Public License, Version 2 (http://www.gnu.org/licenses/gpl-2.0).

ipython

Version 4.1.0
Copyright (c) ipython. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**ITEXTPDF**

Version 5.5.12  
Copyright (C) 2017, ITEXT GROUP  
Distributed under the GNU Affero General Public License (http://www.gnu.org/licenses/agpl-3.0.en.html)

**Java**

Version 8 Update 131  
Copyright (c) 2017, Oracle and/or its affiliates. All rights reserved.  
Distributed under the terms of the Oracle Java license (http://www.oracle.com/technetwork/java/javase/terms/license/index.html).

**jcifs**

Version 1.3.16  
Copyright (c) 1991,1999 Free Software Foundation, Inc.  
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.  
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

**Jetty**

Version 9  
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).  
Also licensed under the Eclipse Public License 1.0 (https://www.eclipse.org/legal/epl-v10.html).

**jfree**

Version 1.0.13  
Copyright (c) 1991, 1999 Free Software Foundation, Inc.  
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.  
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.
Jinja 2

Version 2.8
Copyright (c) Jinja2
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

joda-time

Version 2.1
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

JsonCpp

Copyright (c) 2007-2010 Baptiste Lepilleur
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jtds

Version 1.3.1
Copyright (c) Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.
junit-addons

Version 1.4
Copyright (c) 2002-2003 Vladimir R. Bossicard. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

kernel

Version 3.10.0-327.el7
Copyright (c) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301
Licensed under the GNU General Public License, Version 2.0; you may not use this file except in compliance with the License.
See BeatBox for the terms and conditions of the GNU General Public License, Version 2.0. You may obtain a copy of the License at http://www.gnu.org/licenses/gpl-2.0.html.

libappr

Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

libnids

Version 1.2
Copyright (c) June 1991 Free Software Foundation, Inc.
nergal@avet.com.pl
Licensed under the GNU General Public License, Version 2.0; you may not use this file except in compliance with the License.
See BeatBox for the terms and conditions of the GNU General Public License, Version 2.0. You may obtain a copy of the License at http://www.gnu.org/licenses/gpl-2.0.html.

Libpcap

Version libpcap-1.5.3-8.el7
The Regents of the University of California
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.
THE SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
libpgm

Version 1.3
Copyright (c) libpgm All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

libsodium

Version 1.0.3
Copyright (c) libsodium
Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Libsvm

Copyright (c) 2000-2013 Chih-Chung Chang and Chih-Jen Lin All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither name of copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
libtool

Version 2.4.2-21.el7_2.x86_64
Copyright (c) GNU
Licensed under the GNU Lesser General Public License, Version 3.0; you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl.html.

libwbxml

Version 0.11.2-1.el7
Copyright (c) 1991, 1999, Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 3.0; you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl.html.

libxml2

Except where otherwise noted in the source code (e.g. the files hash.c,list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:
Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

locket

Version 0.2.0
Copyright (c) locket. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Log4cxx

Version 0.10.0-2
Copyright (c) 2004-2007. The Apache Software Foundation (http://www.apache.org/)
Apache log4cxx
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

log4j

Version 1.2.14
Copyright (c) 1999-2005 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 1.1 (the "License"); you may not use this file except in compliance with the License (https://www.apache.org/licenses/LICENSE-1.1).

Log4Net

Version 1.2.11
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

MarkupSafe

Version 0.23
Copyright (c) MarkeupSafe. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Microsoft JDBC Driver for SQL Server

Version 4.1.5605.100_enu
Copyright (c) All rights reserved.
MICROSOFT SOFTWARE LICENSE TERMS
REDISTRIBUTION LICENSE FOR MICROSOFT JDBC DRIVER 4.0 FOR SQL SERVER
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft updates, supplements, Internet-based services, and support services for this software, unless other terms accompany those items. If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

INSTALLATION AND USE RIGHTS. You may install and use any number of copies of the software on your devices. You may also install the software in a hosted environment.

ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

Distributable Code.

Right to Use and Distribute. You are permitted to distribute the software in programs you develop if you comply with the terms below:

You may copy and distribute the object code form of the software (“Distributable Code”) in programs you develop. You may not modify the software.

You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

Distribution Requirements. For any Distributable Code you distribute, you must add significant primary functionality to it in your programs;

require distributors and external end users to agree to terms that protect it at least as much as this agreement;

display your valid copyright notice on your programs; and

indemnify, defend, and hold harmless Microsoft from any claims, including attorneys’ fees, related to the distribution or use of your programs.

Distribution Restrictions. You may not alter any copyright, trademark or patent notice in the Distributable Code;

use Microsoft’s trademarks in your programs’ names or in a way that suggests your programs come from or are endorsed by Microsoft;

include Distributable Code in malicious, deceptive or unlawful programs; or

modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that the code be disclosed or distributed in source code form; or

others have the right to modify it.

SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways.

You may not disclose the results of any benchmark tests of the software to any third party without Microsoft’s prior written approval;

reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;

publish the software for others to copy;

rent, lease or lend the software; or

TRANSFER TO A THIRD PARTY. The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.

EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

SUPPORT SERVICES. Because this software is “as is,” we may not provide support services for it.

ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

APPLICABLE LAW.

United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

Outside the United States. If you acquired the software in any other country, the laws of that country
apply.

**LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

**DISCLAIMER OF WARRANTY.** THE SOFTWARE IS LICENSED “AS-IS.” YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

**LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES.** YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to anything related to the software, services, content (including code) on third party Internet sites, or third party programs, and

claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

---

**mock**

Version 1.3.0
Copyright (c) 2016 All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

**mod_ssl**

Version 2.4.6-17.el7
Copyright (c) 2012 The Apache Software Foundation (http://www.apache.org/)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

---

**mssql-jdbc**

Version 6.1, Copyright (c) 2017 Microsoft Corporation. All rights reserved. Distributed under the MIT license (https://github.com/Microsoft/mssql-jdbc/blob/master/LICENSE).
myfaces
Verion 1.1.9
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

net.sf.ehcache
Version 2.4.3
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

Nmap
Copyright (c) Licensed under the GNU General Public License, Version 3.0; you may not use this file
except in compliance with the License.
See Bash for the terms and conditions of the GNU General Public License, Version 3.0. You may obtain a
copy of the License at http://www.gnu.org/licenses/gpl.html.

numexpr
Version 2.6.2, © 2007, 2008  David M. Cooke <david.m.cooke@gmail.com> / © 2009, 2010 Francesc
Alted <faltet@pytables.org>. Distributed under the MIT License (https://github.com/pydata/numexpr/
blob/master/LICENSE.txt).

numpy
Version 1.10.1
Copyright (c) numpy. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the
  following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
  following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenBLAS
Version 0.2.14
BSD license
Copyright (c) OpenBLAS v0.2.14
All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the <organization>. The name of the <organization> may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Open CSV

Version 1.8
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

OpenJDK

V8U131, © 1999, 2015, Oracle and/or its affiliates, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html), including SSLContextImpl.txt which was modified in September 2017.

OpenSSH

Version 6.6.1p1-22.el7
Copyright (c) February 15, 2006. The Apache Software Foundation (http://www.apache.org/)
1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.
Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".
The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself, I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf

NO WARRANTY
BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE...
WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under
a BSD-style license.

Cryptographic attack detector for ssh - source code
Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use
in source and binary forms, with or without modification, are permitted provided that this copyright notice
is retained.

THIS SOFTWARE IS PROVIDED `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE
DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM
THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futuransky <futo@core-sdi.com>
<http://www.core-sdi.com>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.
Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
Modification and redistribution in source and binary forms is permitted provided that due credit is given
to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public
domain and distributed with the following license:
@version 3.0 (December 2000)
Optimised ANSI C code for the Rijndael cipher (now AES)
@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>
This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Version 1.0.2k
Copyright (c) 1998-2017 The OpenSSL Project. All rights reserved.
Distributed under a double license: the OpenSSL License and the original SSLeay license. The full license
is available at https://www.openssl.org/source/license.html.

org.apache.activemq

Version 5.14.4
Copyright 2005-2015 The Apache Software Foundation (http://www.apache.org)
Version 3.1.0
Copyright 2005-2008 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).
org.apache.axis

Version 1.4
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

org.apache.camel

Version 2.15.2
Copyright (c) 2016. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

org.apache.geronimo.specs

Versions 1, 1.1.1, 2016
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

org.apache.myfaces.core

Version 1.2.9
Copyright (c) 2016 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

org.apache.xbean

Version 3.4.3
Copyright (c) 2005-2008 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

org.dbunit

Version 2.2
Copyright (c) 1991, 1999 Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See charget for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

org.hibernate

Versions 1.0.1.GA, 4.0.1.Final, 4.1.6.Final, 4.2.0.Final
Copyright (c) 1991, 1999 Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See charget for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may
obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

**org.richfaces.framework**

Version 3.3.3.Final  
Copyright (c) 1991, 1999, Free Software Foundation, Inc.  
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License (http://www.gnu.org/licenses/lgpl-2.1.txt).

**org.richfaces.ui**

Version 3.3.3.Final  
Copyright (c) 1991, 1999, Free Software Foundation, Inc.  
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.  
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

**org.springframework**

Version 3.2.0  
Copyright (c) 2002-2012, SpringSource, a division of VMware, Inc.  
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

**org.springframework.security**

Version 3.0.7.  
Copyright (c) 2002-2012, SpringSource, a division of VMware, Inc.  
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

**oro**

Version 2.0.8  
Copyright (c) 2000-2002 The Apache Software Foundation (http://www.apache.org/)  
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

**pandas**

Version 0.17.0  
Copyright (c) pandas. All rights reserved.  
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:  
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.  
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.  
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
parse

Version 1.6.6
Copyright (c) 2012-2013 Richard Jones <richard@python.org>
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software without restriction, including without
limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the
Software, and to permit persons to whom the Software is furnished to do so, subject to the following
conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions
of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

partd

Version 0.3.2
Copyright (c) partd. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the
  following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
  following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Pbr

Version 1.3.0
Copyright (c) All rights reserved
Apache License Version 2.0, January 2004 (http://www.apache.org/licenses/).
Pcre

Version 4.5-4.el4_6.6/6.6-2.el5_1.7

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk
Copyright (c) 1997-2013 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright (c) 2010-2013 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright (c) 2009-2013 Zoltan Herczeg
All rights reserved.

THE C WRAPPER FUNCTIONS

Contributed by: Google Inc.
Copyright (c) 2007-2012, Google Inc.
All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

pdfkit

Version 0.5.0
Copyright (c) pdfkit. All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

pexpect

Version 4.0.1
Copyright (c) pexpect. All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

pickleshare

Version 0.3
Copyright (c) pickleshare
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
pip

Version 7.1.2
Copyright (c) pip v7.1.2
Distributed under the MIT License (MIT).
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software without restriction, including without
limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the
Software, and to permit persons to whom the Software is furnished to do so, subject to the following
conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions
of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

POLE

POLE Copyright © 2002-2005 Ariya Hidayat<ariya@kde.org>. All rights reserved.
Copyright © 2009 Dmitry Fedorov, Center for Bio-Image Informatics. All rights reserved.
Copyright © 2010 Michel Boudinot. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.
Neither the name of the authors nor the names of its contributors may be used to endorse or promote
products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADvised OF THE POSSIBILITY OF SUCH DAMAGE.

postfix

Version 2.10.1-6.el7
Copyright (c) postfix
Distributed under the IBM Public License Version 1.0 (https://opensource.org/licenses/IPL-1.0).

PostgreSQL

Portions Copyright (c) 1996-2016, The PostgreSQL Global Development Group
Portions Copyright (c) 1994, The Regents of the University of California
Permission to use, copy, modify, and distribute this software and its documentation for any purpose,
without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Procrun

Version 1
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

psutil

Version 4.3.0
Copyright (c) Giampaolo Rodola
Distributed under the BSD 3-Clause License (http://opensource.org/licenses/BSD-3-Clause).
Copyright (c) 2013 Matthew Rocklin All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. c. Neither the name of toolz nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Pycurl

Copyright (c) 2001-2008 Kjetil Jacobsen
Copyright (c) 2001-2008 Markus F.X.J. Oberhumer
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in compliance with the License.
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

pyodbc

Version 3.0.7
Copyright (c) pyodbc
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Python

Version 2.7.5-34.el7
PSF license

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.7.7 software in source or binary form and its associated documentation. 2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.7.11 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001-2016 Python Software Foundation; All Rights Reserved" are retained in Python 2.7.11 alone or in any derivative version prepared by Licensee. 3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.7.11 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.7.11. 4. PSF is making Python 2.7.11 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.7.11 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS. 5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.7.11 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.7.11, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. 6. This License Agreement will automatically terminate upon a material breach of its terms and conditions. 7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party. 8. By copying, installing or otherwise using Python 2.7.11, Licensee agrees to be bound by the terms and conditions of this License Agreement.

python-dateutil

Version 2.4.2
Copyright (c) python-dateutil
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

python-prompt-toolkit

Copyright (c) 2014, Jonathan Slenders All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the {organization} nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

python-twisted-core

Version 12.1.0-4.el7  
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

python-twisted-web

Version 12.1.0-4.el7

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**Pytz**

Version 2015.7
Copyright (c) Stuart Bishop

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**PyYAML**

Version 3.11
Copyright (c) 2006 Kirill Simonov

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**pyzmq**

Version 14.7.-0
Copyright (c) pyzmq All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

quartz

Version 2.2.1
Copyright (c) 2016. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

scipy

Copyright (c) scipy All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

setup tools

Version 18.4
PSF license
1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.7.11 software in source or binary form and its associated documentation. 2. Subject to the terms and conditions of this License Agreement, VersPSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.7.11 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001-2016 Python Software Foundation; All Rights Reserved" are retained in Python 2.7.11 alone or in any derivative version prepared by Licensee. 3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.7.11 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.7.11. 4. PSF is making Python 2.7.11 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.7.11 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS. 5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.7.11 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.7.11, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. 6. This License Agreement will automatically terminate upon a material breach of its terms and conditions. 7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party. 8. By copying, installing or otherwise using Python 2.7.11, Licensee agrees to be bound by the terms and conditions of this License Agreement.
simplegeneric

Version 0.8.1
Zope Public License (ZPL) Version 2.1

A copyright notice accompanies this license document that identifies the copyright holders.
This license has been certified as open source. It has also been designated as GPL compatible by the Free
Software Foundation (FSF).
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
Redistributions in source code must retain the accompanying copyright notice, this list of conditions, and
the following disclaimer.
Redistributions in binary form must reproduce the accompanying copyright notice, this list of conditions,
and the following disclaimer in the documentation and/or other materials provided with the distribution.
Names of the copyright holders must not be used to endorse or promote products derived from this
software without prior written permission from the copyright holders.
The right to distribute this software or to use it for any purpose does not give you the right to use
Servicemarks (sm) or Trademarks (tm) of the copyright holders. Use of them is covered by separate
agreement with the copyright holders.
If any files are modified, you must cause the modified files to carry prominent notices stating that you
changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AS IS AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES, LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

simplejson

Version 3.8.0
Copyright (c) simplejson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software without restriction, including without
limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the
Software, and to permit persons to whom the Software is furnished to do so, subject to the following
conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions
of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
 ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

Single Element CSS Spinners

© 2014 Luke Haas. Distributed under the MIT license (http://www.opensource.org/licenses/mit-
license.html).
six

Version 1.10.0
Copyright (c) six
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

slf4j

Version 1.7.2
Copyright (c) 2004-2013 QOS.ch
All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

snakeyaml

Version 1.16
Distributed under the Apache License Version 2.0, January 2004 (http://www.apache.org/licenses/).

SQLite

Version 3.7.17-8.el7
Copyright SQLite v3.8.4.1
Public domain

SOAPpy

Version 0.12.22
Copyright (c) 20011 Makina Corpus
Copyright (c) 2002-2005, Pfizer, Inc.
Copyright (c) 2001, Cayce Ullman.
Copyright (c) 2001, Brian Matthews.
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.
Neither the name of actzero, inc. nor the names of its contributors may be used to endorse or promote
products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

stomp.py

Version 4.1.8
Copyright (c) 1999-2012 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

SUDS

Copyright (c) 1991, 1999 Free Software Foundation, Inc.
Licensed under the GNU Lesser General Public License, Version 2.1; you may not use this file except in
compliance with the License.
See chardet for the terms and conditions of the GNU Lesser General Public License, Version 2.1. You may
obtain a copy of the License at http://www.gnu.org/licenses/lgpl-2.1.txt.

SUDS-JURKO (PYTHON)

Version 0.6, Copyright (c) 2007 Free Software Foundation, Inc., is distributed under the GNU Lesser
General Public License, version 3 (http://www.gnu.org/licenses/lgpl-3.0).
Some third-party software included in Forcepoint DLP is licensed under the following open source
license(s): GNU Lesser General Public License. If you would like a copy of the source code for such third-
party software included in Forcepoint DLP, you may email your request to opensource@forcepoint.com.

taglibs

Version 1.1.2
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

tg3

Version 3.136e
Licensed under the GNU General Public License, Version 2.0; you may not use this file except in
compliance with the License.
See BeatBox for the terms and conditions of the GNU General Public License, Version 2.0. You may obtain a copy of the License at http://www.gnu.org/licenses/gpl-2.0.html.

**tldextract**

Version 2.0.1
Copyright (c) John Kurkowski
New BSD license
Copyright (c) 2013 Matthew Rocklin All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. c. Neither the name of toolz nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**Tomcat**

Version 7.0.68
Copyright 1999-2012 The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

**toolz**

Version 0.7.4
Copyright (c) 2013 Matthew Rocklin All rights reserved.
Distributed under the new BSD license (http://opensource.org/licenses/BSD-3-Clause).

**traitlets**

Version 4.1.0
Copyright (c) traitlets. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

twistedcore

Copyright (c) 2001-2006, Twisted Matrix Laboratories.
Allen Short
Andrew Bennetts
Apple Computer, Inc.
Benjamin Bruheim
Bob Ippolito
Canonical Limited
Christopher Armstrong
David Reid
Donovan Preston
Eric Mangold
Itamar Shtull-Trauring
James Knight
Jason A. Mobarak
Jonathan Lange
Jonathan D. Simms
Jp Calderone
Jorgen Hermann
Kevin Turner
Mary Gardiner
Matthew Lefkowitz
Massachusetts Institute of Technology
Moshe Zadka
Paul Swartz
Pavel Pergamenshchik
Ralph Meijer
Sean Riley
Travis B. Hartwell

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

twistedweb

Version 0.7.0
See twistedcore.
Unicodecsv

Version 0.14.1
Copyright (c) Unicodecsv. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Universal Character Names conversions

Copyright (c) Universal Character Names conversions
All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal with the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimers.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.
Neither the names of <Name of Development Group, Name of Institution>, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTRIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS WITH THE SOFTWARE.

unixodbc

Version 2.3.4
Copyright (c) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

wheel

Version 0.26.0
Copyright (c) wheel. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

wkhtmltopdf
Copyright (c) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Licensed under the GNU Lesser General Public License, Version 2.1, February 1999 (https://
www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html).

wstools
Version 0.4.3
Copyright (c) wstools
All rights reserved under the 3-clause BSD License (https://opensource.org/licenses/BSD-3-Clause).

xdelta
Copyright (c) 1989, 1991 Free Software Foundation, Inc.
Licensed under the GNU General Public License, Version 2.0; you may not use this file except in
compliance with the License.
See BeatBox for the terms and conditions of the GNU General Public License, Version 2.0. You may obtain
a copy of the License at http://www.gnu.org/licenses/gpl-2.0.html.

xerces
Version 2.6.2
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

XlsxWriter
Version 0.7.7
Copyright (c) 2016 XlsxWriter. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
  following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

xml-apis

Version 1.0.b2
Copyright (c) 2001-2002. The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

xmlrpc

Version 2.0.1
Copyright (c) The Apache Software Foundation (http://www.apache.org/)
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in
compliance with the License (http://www.apache.org/licenses/LICENSE-2.0).

xstream

Version 1.2.1
XStream is open source software, made available under a BSD license.
Copyright (c) 2003-2006, Joe Walnes
Copyright (c) 2006-2009, 2011 XStream Committers
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the
   following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
   following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of XStream nor the names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
zlib

Version 1.2.8

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.8, April 28th, 2013
Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler
This software is provided 'as-is', without any express or implied warranty. In no event will the authors
be held liable for any damages arising from the use of this software. Permission is granted to anyone
to use this software for any purpose, including commercial applications, and to alter it and redistribute
it freely, subject to the following restrictions:
1. The origin of this software must not be misrepresented; you must not claim that you wrote the original
   software. If you use this software in a product, an acknowledgment in the product documentation
   would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the
   original software.
3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly
   Mark Adler
   jloup@gzip.org madler@alumni.caltech.edu.

ZSI

Copyright © 2001, Zolera Systems, Inc. All Rights Reserved.
Copyright © 2002-2003, Rich Salz. All Rights Reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and
to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s)
and this permission notice appear in all copies of the Software and that both the above copyright notice(s)
and this permission notice appear in supporting documentation.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY
RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN
THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL
DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.
Except as contained in this notice, the name of a copyright holder shall not be used in advertising or
otherwise to promote the sale, use or other dealings in this Software without prior written authorization of
the copyright holder.

ZTHREAD/COUNTEDPTR.H

© 2005 Eric Crahen, is distributed under the MIT License (www.opensource.org/licenses/mit-license)

Some third-party software included in #FORCEPOINTPRODUCT is licensed under the following open
source license(s): GNU General Public License with Classpath Exception, Affero General Public License.
If you would like a copy of the source code for such third-party software included in
#FORCEPOINTPRODUCT, you may email your request to opensource@forcepoint.com.