Forcepoint

Forcepoint DLP

9.0

Forcepoint Email Security Cloud and Forcepoint DLP Integration Guide

Revision A

© 2022 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 12 August 2022

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

Contents

1 Introduction 5
Getting Started 5
Additional documentation 6

2 License Information 7
New Forcepoint Email Security Cloud and Forcepoint DLP customers 7
Existing Forcepoint Email Security Cloud and Forcepoint DLP customers 9

3 Integrating Forcepoint DLP and Forcepoint Email Security Cloud 11
General Flow 11
Step 1: Configure Data Protection Service in Forcepoint Security Manager 12
Step 2: Connect Forcepoint Email Security Cloud to Data Protection Service in the cloud portal 15
Step 3: Configure Data Protection Service in the cloud portal 17
Step 4: Configure Email DLP policies in the Forcepoint Security Manager 18
Step 5: Deploy to Data Protection Service in the Forcepoint Security Manager 18
Step 6:View DLP incident reports in the Forcepoint Security Manager 19

Chapter 1

Introduction

Contents

- Getting Started on page 5
- Additional documentation on page 6

Forcepoint Cloud Security Gateway is an integrated cloud security service that merges web security, network security, and cloud application security into one easy-to- consume service. With the introduction of Data Protection Service, email security and data loss prevention are now available as an additional integration with Forcepoint Cloud Security Gateway. Data Protection Service connects the Forcepoint Security Manager with Forcepoint Email Security Cloud, allowing you to enjoy the benefits of Forcepoint DLP analysis in the cloud.

Forcepoint Email Security Cloud protects your organization against the threats of malware, spam, and other unwanted content in email traffic. When combined with Forcepoint DLP, email messages that present potential data loss are sent to Forcepoint DLP for further inspection. Forcepoint DLP then returns its finding to the cloud service for policy enforcement.

The integration between Forcepoint DLP and Forcepoint Email Security Cloud is available starting in Forcepoint DLP 8.8.2 and the June 2021 release of Forcepoint Email Security Cloud.

Getting Started

This section provides a high-level overview of the Forcepoint Email Security Cloud and Forcepoint DLP access and integration process.

Steps

1) Purchase the Data Protection for Email license.

   See *License Information* for more information about the Data Protection for Email license and licensing information if you purchase the products separately.

2) Review your fulfillment email. The fulfillment email contains:

   a) License information, including the subscription keys for the products.

   b) Credentials to sign in to the products.

   c) A JSON file with unique configuration information. This JSON file is used to connect Data Protection Service with Forcepoint Security Manager.

   d) An XML license file. This file is used to activate your Forcepoint DLP subscription in the Forcepoint Security Manager.

3) Check your Forcepoint Cloud Security Gateway access.
   Verify that you can sign in to the products using the credentials in the fulfillment email:
   a) Sign in to the Forcepoint Cloud Security Gateway Portal to access Forcepoint Email Security Cloud.
   b) Sign in to the Forcepoint Security Manager and use the XML license file to access Forcepoint DLP.
4) Start the integration process.
   For more information about setting up this integration, see *Integrating Forcepoint DLP and Forcepoint Email Security Cloud*.

Related concepts
License Information on page 7
Integrating Forcepoint DLP and Forcepoint Email Security Cloud on page 11

Additional documentation

- Forcepoint DLP v9.0 Administrator Guide
- Forcepoint Email Security Cloud Help
- Forcepoint Cloud Security Gateway Integration Guide: Forcepoint Web Security, Forcepoint DLP, and Forcepoint CASB

Chapter 2

License Information

Contents

- New Forcepoint Email Security Cloud and Forcepoint DLP customers on page 7
- Existing Forcepoint Email Security Cloud and Forcepoint DLP customers on page 9

To enjoy the benefits of the data loss protection for your organization's email system, new customers need a license for Forcepoint Email Security Cloud and a license for Forcepoint DLP.

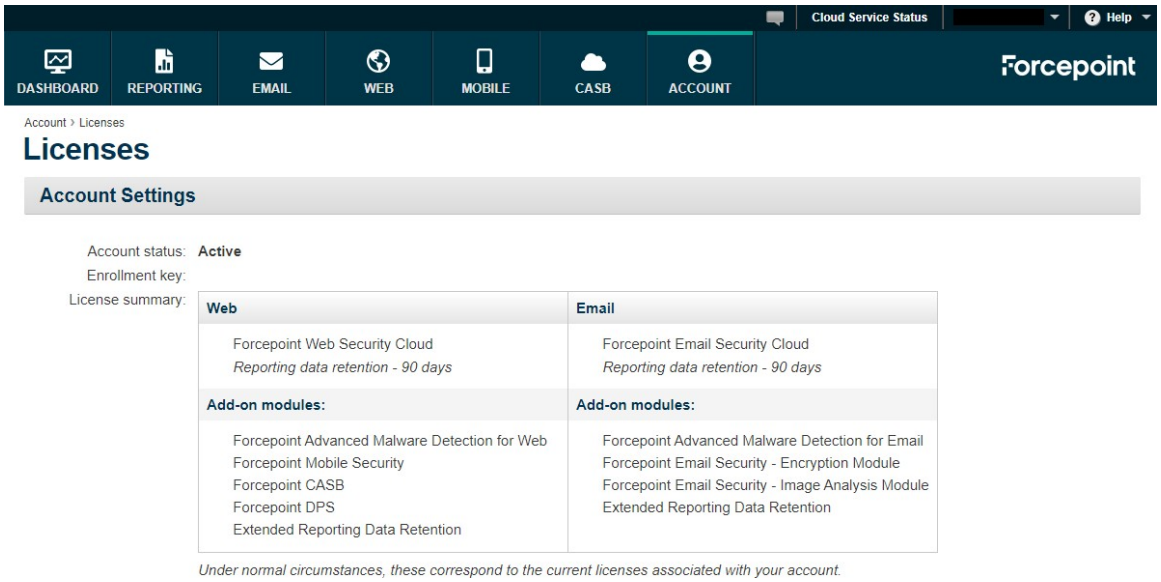
New Forcepoint Email Security Cloud and Forcepoint DLP customers

When you purchase Data Protection for Email, you will receive a fulfillment email on purchase, which contains:

- License information, including the subscription keys for the products.
- Credentials to sign in to the products.
- A JSON file with unique configuration information. This JSON file is used to connect Data Protection Service with Forcepoint Security Manager.
- A Forcepoint Email Security Cloud XML license file. This file is used to activate your Forcepoint DLP subscription in the Forcepoint Security Manager.

Check your license in Forcepoint Cloud Security Gateway Portal

After you receive your fulfillment email, verify that "Forcepoint DPS" is listed on the **Account** > **Licenses** page in the Forcepoint Cloud Security Gateway Portal (also known as the cloud portal). Your account is automatically updated on purchase:



After the license is active, configure the Forcepoint DLP and Forcepoint Email Security Cloud integration. For more information, see *Integrating Forcepoint DLP and Forcepoint Email Security Cloud*.

Related concepts

Integrating Forcepoint DLP and Forcepoint Email Security Cloud on page 11

Upload your license in Forcepoint DLP

Before you begin

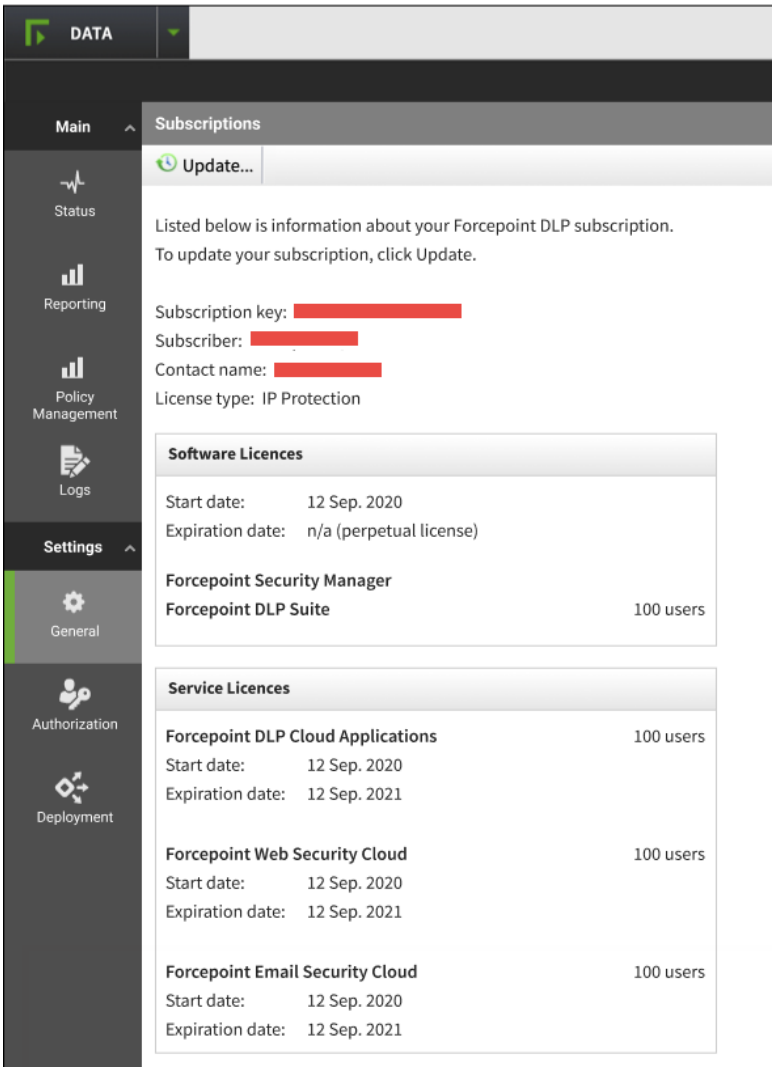
To enable Forcepoint DLP configuration, upload your XML license file in the Forcepoint Security Manager:

Steps

1) Log on to the Forcepoint Security Manager. If the Data Security module is not displayed by default, hover over the Forcepoint logo at the top of the Forcepoint header and select Data from the drop-down list.
   a) If this is your first login, the subscription page appears automatically.
   b) To navigate to the subscription page, select **Settings** > **General** > **Subscription**

2) Browse to the subscription file, then click **Submit**. Current subscription information is displayed, and the Forcepoint DLP application restarts.

Your subscription terms displayed on this page include the license name (**Forcepoint Email Security Cloud** for this new license), the start and expiration dates (or "n/a" if you have a perpetual subscription), the number of subscribed users, and the modules and services to which you subscribe.



See Entering a subscription key in *Forcepoint DLP Administrator Help* for more information.

Existing Forcepoint Email Security Cloud and Forcepoint DLP customers

Existing customers using Forcepoint DLP v8.8.2 or upgrading from Forcepoint DLP v8.8.2 to v8.9 can use the DLP Network XML license to subscribe and use the Data Protection for Email in the Forcepoint Security Manager.

If you already have Forcepoint Email Security Cloud deployment with the on- premises Forcepoint Email Security DLP Module, you can switch to this license. Contact Forcepoint Support for more information.

If you already have the Forcepoint Web Security Cloud integration with Data Protection Service, you need to purchase the Data Protection for Email license. You need a new JSON file for reconnecting Data Protection Service with the cloud portal, and you do not need to reconnect Data Protection Service with Forcepoint Security Manager. However, you need to configure your email policies for Data Protection Service. See *Step 3: Configure Data Protection Service in the cloud portal*.

Related tasks

Step 3: Configure Data Protection Service in the cloud portal on page 17

Chapter 3

Integrating Forcepoint DLP and Forcepoint Email Security Cloud

Contents

- General Flow on page 11
- Step 1: Configure Data Protection Service in Forcepoint Security Manager on page 12
- Step 2: Connect Forcepoint Email Security Cloud to Data Protection Service in the cloud portal on page 15
- Step 3: Configure Data Protection Service in the cloud portal on page 17
- Step 4: Configure Email DLP policies in the Forcepoint Security Manager on page 18
- Step 5: Deploy to Data Protection Service in the Forcepoint Security Manager on page 18
- Step 6:View DLP incident reports in the Forcepoint Security Manager on page 19

This chapter provides an overview of how to configure the integration between Forcepoint DLP and Forcepoint Email Security Cloud.

General Flow

Before you begin

Before beginning your configuration, ensure that you have connected the cloud portal and Forcepoint Security Manager by following the steps in *License Information*.

Steps

1) Connect the Forcepoint Security Manager with Data Protection Service by uploading the JSON tenant information to the Data Protection Service tab (**Settings** > **General** > **Services**). See *Connect Forcepoint DLP to Data Protection Service*.

2) Configure Data Protection Service in the Forcepoint Cloud Security Gateway Portal by uploading the JSON tenant information to the Data Protection Service tab (**Account** > **Data Protection Settings**). See *Step 2: Connect Forcepoint Email Security Cloud to Data Protection Service in the cloud portal*.

3) Enable Data Protection Service in the Forcepoint Cloud Security Gateway portal and configure email policies. See *Step 3: Configure Data Protection Service in the cloud portal*.

4) Configure email policies in Forcepoint Security Manager. See *Step 4: Configure Email DLP policies in the Forcepoint Security Manager*.

5) Deploy the configuration to Data Protection Service and begin receiving incidents in Forcepoint Security Manager. See *Step 5: Deploy to Data Protection Service in the Forcepoint Security Manager*.

6) View incident reports using Data Protection Service in Forcepoint Security Manager. See *Step 6: View DLP incident reports in the Forcepoint Security Manager*.

Related concepts

License Information on page 7
Step 4: Configure Email DLP policies in the Forcepoint Security Manager on page 18
Step 5: Deploy to Data Protection Service in the Forcepoint Security Manager on page 18
Step 6:View DLP incident reports in the Forcepoint Security Manager on page 19

Related tasks

Connect Forcepoint DLP to Data Protection Service on page 12
Step 2: Connect Forcepoint Email Security Cloud to Data Protection Service in the cloud portal on page 15
Step 3: Configure Data Protection Service in the cloud portal on page 17

Step 1: Configure Data Protection Service in Forcepoint Security Manager

Data Protection Service connects to both Forcepoint DLP in the Forcepoint Security Manager and Forcepoint Email Security Cloud in the Cloud Security Gateway Portal, or cloud portal.

Each of these steps requires you to upload the configuration file provided by Forcepoint in the fulfillment email you received. This file provides the information needed to connect both products to Data Protection Service.

Important

Make sure you update your subscription before connecting to Data Protection Service. If you connected first, the new license is not reaching Data Protection Service. To resolve this issue, follow the instructions provided in the Knowledge Base article "Failure to deploy a subscription XML to Data Protection Service after subscription change."

Connect Forcepoint DLP to Data Protection Service

Forcepoint DLP and Data Protection Service are connected in Forcepoint Security Manager DLP in the Data Protection Service tab **General** > **Services** > **Data Protection Service**, as follows:

Steps

1) Click **Select File**, and in the dialog box that appears, click **Choose File**, and browse to the JSON file you received from Forcepoint, and then click **OK**.

   The file is uploaded to the server, and the information begins to appear in the Connection area of the Data Protection Service tab.

2) Click **Connect** to establish the connection with Data Protection Service.

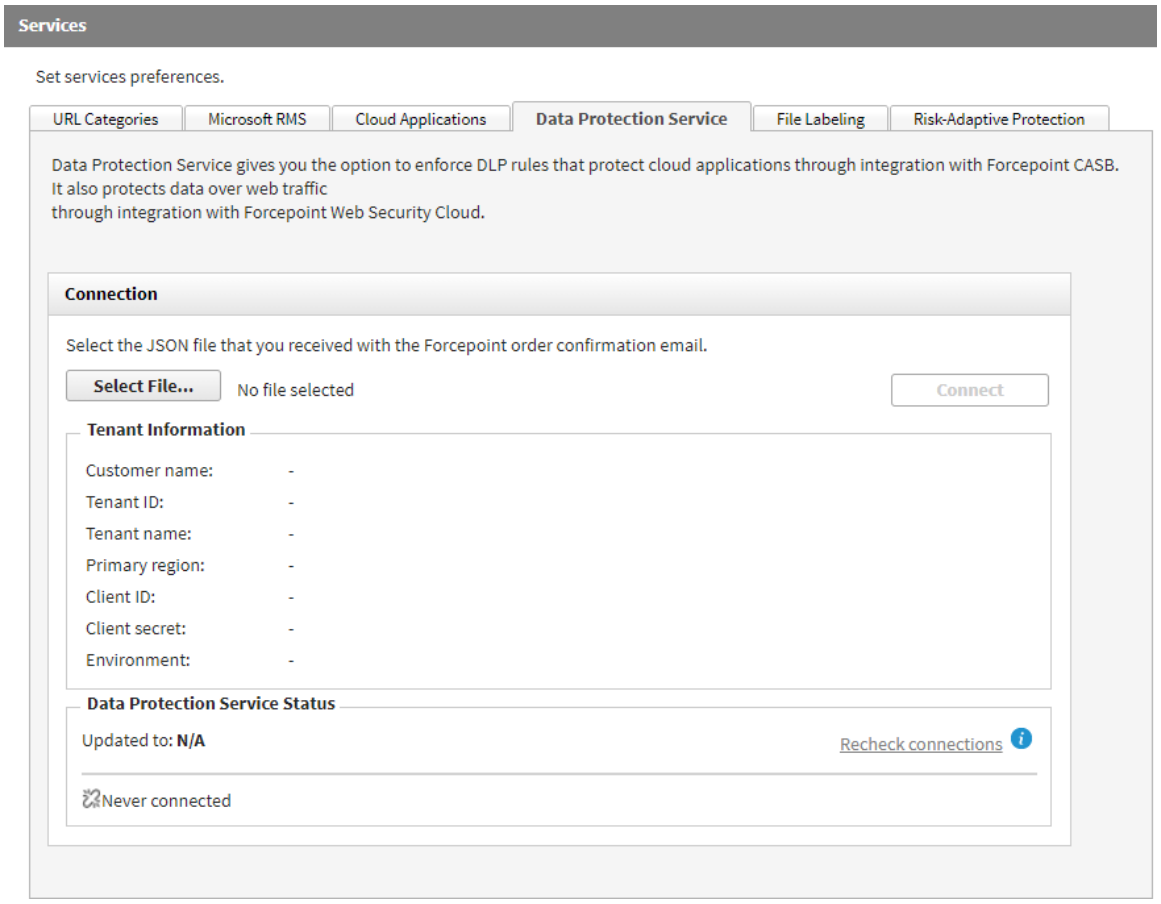
3) Click **OK** at the bottom of the screen to complete the process.

4) To deploy all the configured changes, click **Deploy**.

Next steps

When the connection is active, the Connect button turns into a Disconnect button, enabling disconnection of Data Protection Service from Forcepoint DLP.

In the Data Protection Service Status area, upon successful connection, the status is marked as **Connected successfully**, the time and date of the connection is displayed, and the **Recheck connection** link is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as **Failed to connect**.



Upon successful connection, you can see Data Protection Service on the System Modules page (**Settings** > **Deployment** > **System Modules**).

Error handling

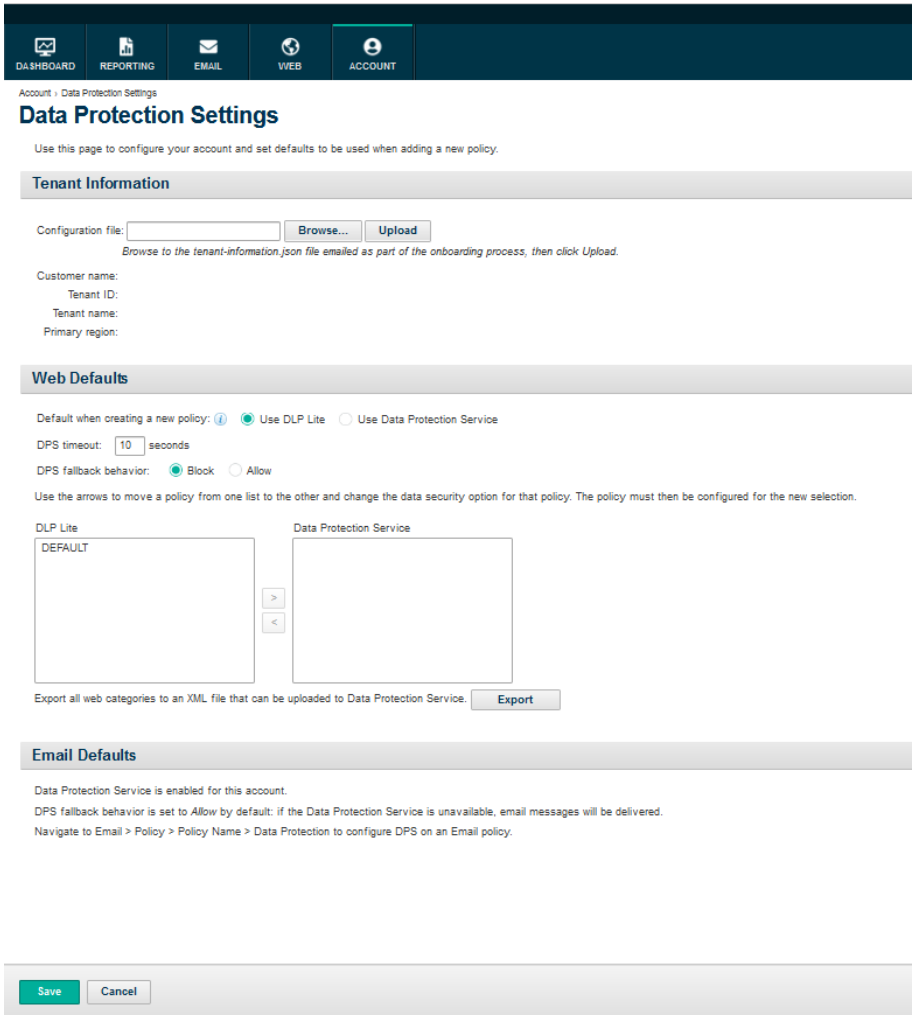
- If Data Protection Service shows the status **Failed to connect**, the module is temporarily unavailable. Click **Connect** or **Recheck connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is **Never connected**. This is because the Forcepoint Security Manager has never successfully connected to the Cloud Policy Engine. In this case, it is probable that a Cloud Policy Engine was not created. Contact Forcepoint Technical Support for assistance.
- When you contact Forcepoint Technical Support, you can share the following files to help troubleshoot the issue:
  - `%DSS_HOME%tomcat\logs\dlp\dlp-all.log`
  - `%DSS_HOME%mediator\logs\mediator.out`

  The default location for *%DSS_HOME%* is `C:\Program Files (x86)\Websense\Data Security\`. If you cannot find these files at the default location, check with your Forcepoint Security Manager administrator.

Step 2: Connect Forcepoint Email Security Cloud to Data Protection Service in the cloud portal

Before you begin

Use the **Account** > **Data Protection Settings** page of the cloud portal to enable and configure the integration with Forcepoint Email Security Cloud and Forcepoint DLP.



Upload the configuration file provided by Forcepoint in the fulfillment email you received. This file provides the information needed to connect the cloud service to Data Protection Service and is the same file used when configuring Data Protection Service in the Data module of the on-premises Forcepoint Security Manager.

Steps

1) Click **Browse**, then locate and select the JSON file you received from Forcepoint.
   The filename appears in the Configuration file entry.

2) Click **Upload**.

   When the upload is successful, the remaining fields are automatically populated.

3) Verify that the correct **Customer Name** is shown in the Forcepoint Security Manager. If the Customer Name is incorrect, contact Forcepoint Technical Support.

   The **Browse** and **Upload** buttons are not available for users with **View Configuration** web permissions.

4) Use the Email Defaults section to view how data security is handled in new email policies. DPS fallback behavior is set to Allow by default and cannot be changed.

   DPS fallback behavior is configured as a backup in the event of a Data Protection Service timeout or other error. With this behavior set to Allow, all email messages received while Data Protection Service is unreachable are delivered. This ensures that emails are not unnecessarily quarantined.

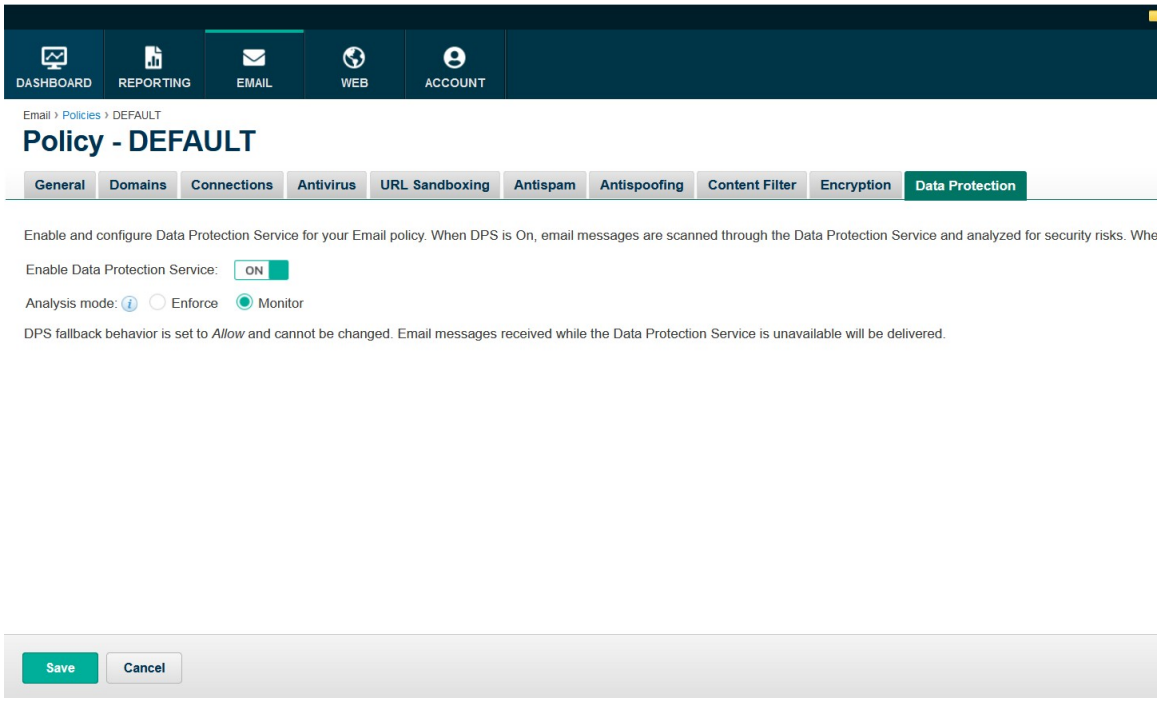
   Navigate to **Email** > **Policy** > **Policy Name** > **Data Protection** to configure your email policies with the new data security option.

Step 3: Configure Data Protection Service in the cloud portal

Before you begin

After Data Protection Service is enabled for your account, it must be enabled for each email policy. A Data Protection tab is available when adding or editing an email policy. Navigate to **Email** > **Policy** and select the policy for which to configure data protection.

Click the Data Protection tab in the policy to configure options for handling potential data issues using Data Protection Service.



Steps

1) When you are ready for Data Protection Service to be used for data security, toggle the Enable Data Protection Service button to **ON**.

   Until this switch has been turned on and the change saved, data security is not monitored for the policy.

2) From Analysis mode, select the type of analysis provided by Data Protection Service: **Enforce** or **Monitor**.

   When Enforce is selected, data security is monitored on the policy and enforced through Data Protection Service. When Monitor is selected, data security is monitored on the policy, but not enforced, and results are logged.

3) The default selection for Data Protection Service fallback behavior is **Allow**. This cannot be changed. In the event of a Data Protection Service timeout or other error, all email messages are allowed.

4) Click **Save**.

Step 4: Configure Email DLP policies in the Forcepoint Security Manager

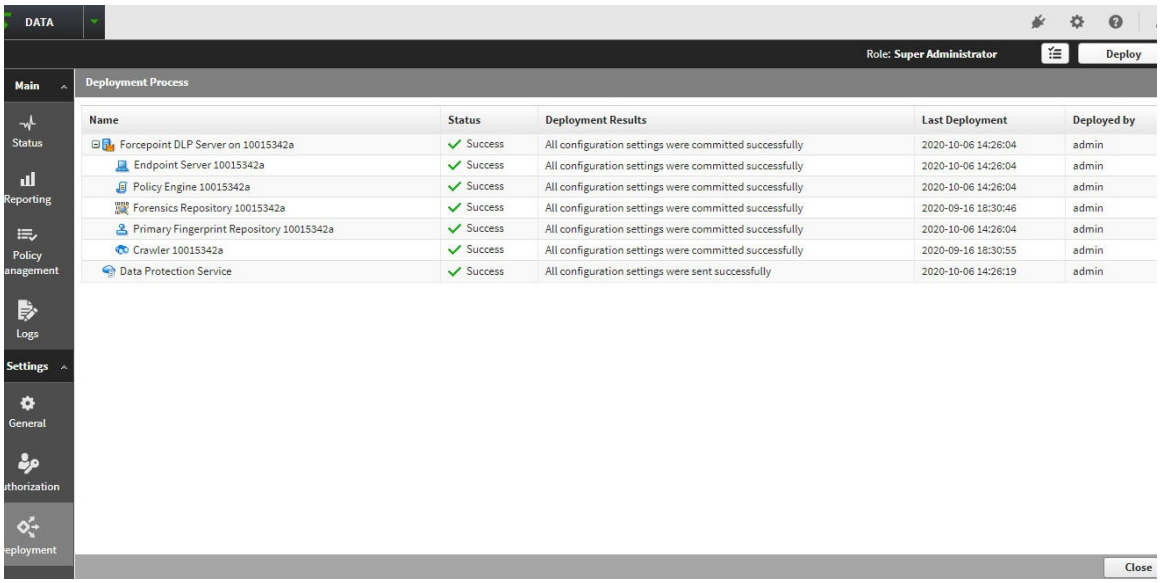
See "Configuring the DLP Email Policy" or "Creating Custom DLP Policies" in *Forcepoint DLP Administrator Help* for information on configuring your policies and editing the email destination for the Network Email channel.

When configuring DLP policies for integration with Forcepoint Email Security Cloud, keep the following in mind:

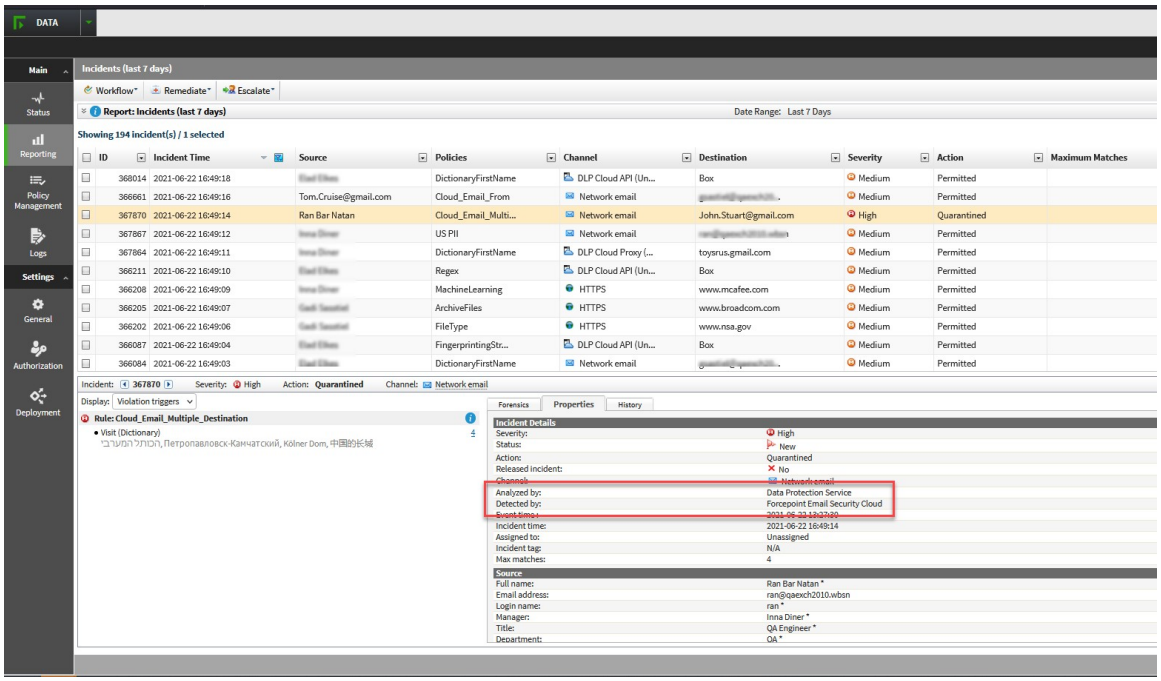
- Email direction: Forcepoint Email Security Cloud only applies to outbound emails.
- Supported actions are Permit, Encrypt, and Quarantine. The "drop attachments" action is not supported for Forcepoint Email Security Cloud. If this option is configured, the actual mitigation that will take place is Quarantine, but the incident report will display "drop attachments" as the action.
- Quarantined email messages cannot be released from the Forcepoint Security Manager. To release quarantined messages, use the cloud portal.
- For multiple recipients (destinations), the strongest mitigation applies to all destinations.

Step 5: Deploy to Data Protection Service in the Forcepoint Security Manager

Deploy the configuration to Data Protection Service by clicking **Deploy**, and begin receiving incidents in Forcepoint Security Manager.



Step 6:View DLP incident reports in the Forcepoint Security Manager



Viewing and managing reports for **SMTP traffic** is the same as in Forcepoint Security Manager. The difference involves what is displayed for a DLP incident:

- **Source:** Email address
- **Destination:** Email address
- **Channel:** Network Email
- **Analyzed by:** Data Protection Service
- **Detected by:** Forcepoint Email Security Cloud

© 2022 Forcepoint