## Contents

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Getting Started with Forcepoint DLP</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entering a subscription key</td>
<td>1</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Configuring the Protector for Use with SMTP</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Set up SMTP in monitoring mode</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Set up SMTP in MTA mode</td>
<td>4</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Configuring the Mobile Agent</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Configure the mobile agent module</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Configuring a mobile DLP policy</td>
<td>9</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Configuring the Web Content Gateway</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Enter a subscription key in the Content Gateway manager</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Register Content Gateway with Forcepoint DLP</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Enabling web DLP</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Configure the Content Gateway policy engine</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Set up Content Gateway</td>
<td>13</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Configuring the Analytics Engine</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Reporting and health monitoring options</td>
<td>16</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Configuring the CASB Service</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Connect and enabled the CASB service</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Configure DLP policy enforcement</td>
<td>17</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Configuring Third-Party Proxies</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Configuration example 1: Symantec Proxy SG</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Enabling HTTPS forward proxy configuration</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuring the protector for ICAP</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuring the ICAP service on Symantec</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Setting up forwarding</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Configuring HTTPS policies</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Recommended Symantec filtering rules</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Configuration example 2: Squid</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Configure the protector for ICAP</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>ICAP server error and response codes</td>
<td>27</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Configuring User Directory Integration</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Define user directory settings</td>
<td>29</td>
</tr>
</tbody>
</table>
Contents

Chapter 9

Getting Started with File Discovery ......................................................... 33
Performing discovery on Micro Focus file systems ................................. 33
  Prepare the Micro Focus server ......................................................... 33
  Prepare the Forcepoint DLP server ..................................................... 34
    Step 1: Install the Micro Focus Client ............................................. 34
    Step 2: Prepare the system for discovery ......................................... 34
    Step 3: Create a new discovery task ............................................... 34
Performing discovery on Windows NFS shares ....................................... 35
  Configure the Forcepoint DLP server ............................................... 35
  Configure the domain controller ...................................................... 37
  Configure Identity Management for UNIX .......................................... 38
  Configure Forcepoint DLP to scan NFS ............................................ 42
Performing discovery on Exchange servers ......................................... 44
  Prepare to run discovery on Exchange Online 365 ............................. 44
  Prepare to run discovery on Exchange 2013 ....................................... 45
  Prepare to run discovery on Exchange 2010 ....................................... 47
Performing discovery on IBM Domino and Notes .................................. 48

Chapter 10

Configuring Labels .................................................................................. 49
Import and enable Boldon James Classifier labels ................................... 49
Import and enable Microsoft Information Protection labels ....................... 50
Configure an action plan to apply labels 52
After installing Forcepoint DLP, log on to the Forcepoint Security Manager and enter a subscription key (see "Entering a subscription key").

Next, follow the initial configuration instructions for the components that have been deployed.

- **Configuring the Protector for Use with SMTP**, page 3
- **Configuring the Mobile Agent**, page 7
- **Configuring the Web Content Gateway**, page 11
- **Configuring the Analytics Engine**, page 15
- **Configuring the CASB Service**, page 17
- **Configuring Third-Party Proxies**, page 19

To get started with Forcepoint DLP, also configure commonly used features:

- **Configuring User Directory Integration**, page 29
- **Getting Started with File Discovery**, page 33

---

**Tip**

Administrators who have not yet deployed Forcepoint DLP can find planning information in the [Forcepoint DLP Deployment Guide](#).

For installation instructions, see the [Forcepoint DLP Installation Guide](#).

---

### Entering a subscription key

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

1. Open a browser and enter the Security Manager URL:
   ```plaintext
   https://<IP_address_or_hostname>:9443
   ```
2. Enter the User name **admin** and the password configured during installation, then click **Log On**.

3. If the Data Security module of the Security Manager is not displayed by default, select **Data** from the Product Module drop-down menu to open it.
   - Until a subscription key is entered, a subscription prompt appears automatically.
   - Once a key has been entered, administrators can review subscription information on the **Settings > General > Subscription** page.

4. Browse to the subscription file, then click **Submit**.
   Current subscription information is displayed.

5. Click **Deploy** in the Security Manager toolbar to complete the process.
Configuring the Protector for Use with SMTP

Getting Started Guide | Forcepoint DLP | v8.7.x

When the protector is used for monitoring or protecting data transfer in email (SMTP) traffic, it can be configured in monitoring or MTA mode.

More information about the different protector deployment modes can be found in the Deployment Guide.

More information about configuring the protector to monitor other protocols can be found in the Administrator Help.

For initial SMTP configuration instructions, see:

- Set up SMTP in monitoring mode, page 3
- Set up SMTP in MTA mode, page 4

Set up SMTP in monitoring mode

Preparing for configuration

The steps in this procedure assume that the protector has already been installed as described in the Forcepoint DLP Installation Guide, with the following configuration:

- The time, date, and time zone are precise.
- Network interface eth0 is mapped and located on the main board.
- Interface eth0 is connected to the LAN.

Before beginning the configuration process, make sure the protector is powered on.

Configuring the protector

Use the Forcepoint Security Manager to configure the protector to monitor SMTP:

1. Go to the Settings > Deployment > System Modules page.
2. Select the protector instance.
4. On the Local Networks tab, select **Include specific networks**, then add all of the internal networks for all sites.
   - This list is used to identify the direction of the traffic.
   - The mail servers and mail relays should be considered part of the internal network.
5. On the Services tab:
   a. Select the **SMTP** service.
   b. On the General tab, set the Mode to **Monitoring bridge**.
   c. On the Traffic Filter tab, set the Direction to **Outbound**.
   d. Click **OK**.
6. Click **OK** to save the configuration.
7. Click **Deploy** to activate the settings.
8. Connect the protector to the outgoing connection and to the organization’s internal network.
   This should be done last, after the protector is fully configured.

### Set up SMTP in MTA mode

#### Preparing for configuration

The steps in this procedure assume that the protector has already been installed as described in the [Forcepoint DLP Installation Guide](#), with the following configuration:

- The time, date, and time zone are precise.
- The network interface selected during installation is mapped and located on the main board.
- The interface is connected to the LAN.

Before beginning the configuration process, make sure the protector is powered on.

#### Configuring the protector

Configure the protector in the Forcepoint Security Manager:

1. Go to the **Settings > Deployment > System Modules** page.
2. Select the protector instance.
3. On the General tab, select **Enabled**.
4. On the Local Networks tab, select **Include specific networks**, then add all of the internal networks for all sites.
   - This list is used to identify the direction of the traffic.
   - The mail servers and mail relays should be considered part of the internal network.
5. On the Services tab:
   a. Select the **SMTP** service.
   b. On the General tab, set the Mode to **Mail Transfer Agent (MTA)**.
   c. On the Mail Transfer Agent (MTA) tab, set the Operation Mode to **Blocking** and select the behavior desired when an unspecified error occurs during analysis.
   d. Set the **SMTP HELO name**. This is required.
   e. Set the next hop MTA (for example, the organization’s mail relay), if needed.
   f. Set the addresses of all networks that are permitted to relay email messages through the protector.
      - This is required, as it is important that not all networks have permission to send email via the protector’s SMTP service. Otherwise, the protector can be used as a mail relay.
      - This list should include the addresses of any previous hops, such as the mail server.

6. Click **OK** to save the configuration.
7. Go to the **Main > Policy Management > DLP Policies** page.
8. Select a policy rule to use for email management, then click **Edit**.
9. Complete the fields as follows:
   a. Select **Destinations**, and check the **Network Email** box.
   b. Select **Severity & Action**, then select an action plan that includes notifications.

   **Note**
   For more information about action plans, see the [Forcepoint DLP Administrator Help](#).

   c. Click **OK** to save the policy configuration.
10. Click **Deploy** to activate the settings.

### Connecting the protector

1. Connect the protector to the outgoing connection and to the organization’s internal network.
   Do this last, after the protector is fully configured.
2. If a next hop server exists (for example, a company mail relay), add the protector’s IP address to its allowed relay list.
3. *(Optional)* Set the mail server’s next hop (smart host) to the protector’s IP address.
Configuring the Mobile Agent

To get started with the mobile agent, first verify or update the mobile agent configuration in the Forcepoint Security Manager, then create mobile DLP policies for the mobile agent to enforce. A predefined mobile DLP quick policy is provided to simplify the process.

See:
- Configure the mobile agent module, page 7
- Configuring a mobile DLP policy, page 9

Configure the mobile agent module

To configure mobile agent settings:

1. Log on to the Data Security module of the Security Manager.
2. Go to the Settings > Deployment > System Modules page.
3. Select the mobile agent instance.
4. Click the Connection tab, then define the Exchange and Mobile Devices connections:
   a. For Exchange Connection, supply the domain and hostname or IP address of the Exchange server.
   b. Specify a port number:
      - If Use secure connection (SSL), is selected, the port number defaults to 443.
      - Otherwise, the port number defaults to 80.

---

**Important**

If the Exchange server is specified by name, make sure local resolving is properly configured to resolve this name. In addition, if an edge-like device is used, ensure there are no loops through the device.
c. For Mobile Devices Connection, supply the IP address of the mobile agent and port number.
    To use all IP addresses, select **All IP addresses** from the IP address drop-down list.

---

**Note**

The IP address of the mobile agent was defined during the installation of the mobile device, when configuring the network settings.

---

More detailed information about these connections is available in the [Forcepoint DLP Administrator Help](#).

5. *(Optional)* If connections between mobile devices and the mobile agent are secured, select the appropriate certificate option:
   - **Self-signed certificate** (default) uses a certificate signed by Forcepoint.
   - **Custom certificate** uses a certificate signed by a Certificate Authority (CA).
     a. Click **Browse** to locate and upload the public certificate.
     b. Click **Browse** to locate and upload the private key.
     c. Optionally, select **Add chained certificate**, then click **Browse** to locate and upload the chained certificate.

For more information, see the [Forcepoint DLP Administrator Help](#).

6. Click the Analysis tab, then select a mode: **Blocking** or **Monitoring**.

---

**Note**

When Blocking mode is enabled, it is best practice to:

- Select the **Allow on fail** option, which allows failed messages to be received on the mobile device. When this option is not selected, failed messages are dropped, and are neither tracked nor released.
- Define the sender’s email address, outgoing mail server, and port for breach notifications on the **Settings > General > Alerts > Email Properties** page.

For more information, see the [Forcepoint DLP Administrator Help](#).

---

7. Go to the **Main > Policy Management > Resources > Notifications** page and select the mobile policy violation template.

8. Add sender details, then use the Outgoing mail server field to define a next hop relay for outbound mail.
   If you do not, the mobile agent may not send block notifications.

9. Click **Deploy**.
Wait for the agent to fully deploy. This may take a few minutes.

---

**Tip**

The mobile agent can also be configured for high-availability. High-availability enables mobile devices to run seamlessly and continuously in the event of a system outage (such as hardware or software failure).

For more information about configuring the mobile agent for high-availability, refer to the document [Mobile DLP agent using cluster solutions](#).

---

### Configuring a mobile DLP policy

To begin analysis, configure the mobile DLP policy or create a custom policy.

- Configure the mobile DLP policy on the **Main > Policy Management > DLP Policies > Mobile DLP Policy** page in the Security Manager.
  
  A quick start guide with instructions for setting up the mobile DLP policy is available from the **Help > Getting Started** menu in the Security Manager.

- Create a custom policy on the **Main > Policy Management > DLP Policies > Create Custom Policy** page.
  
  Select **Mobile Email** on the Destination tab for each rule to support Mobile events.

  See the [Forcepoint DLP Administrator Help](#) for details.
Configuring the Web Content Gateway

Getting Started Guide | Forcepoint DLP | v8.7.x

After installing the Web Content Gateway module, configure it in both the Content Gateway manager and the Forcepoint Security Manager. See:

- Enter a subscription key in the Content Gateway manager, page 11
- Register Content Gateway with Forcepoint DLP, page 11
- Configure the Content Gateway policy engine, page 13
- Set up Content Gateway, page 13

Enter a subscription key in the Content Gateway manager

Enter a subscription key in the Content Gateway manager to activate the Web Content Gateway:

1. Open a web browser and enter the Content Gateway manager URL:
   
   https://<ip_address>:8081

2. Log on as admin with the password created during installation.

3. Go to the Configure > Subscription page.

4. Enter the subscription key.

5. Go to the Configure > My Proxy > Basic page.

6. Click Restart to restart Content Gateway.

Register Content Gateway with Forcepoint DLP

After Content Gateway is activated, it must be registered with the Forcepoint management server.

Preparing for registration

1. Synchronize the date and time on the Content Gateway and management server machines to within a few minutes.
2. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface (“C” on a V Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.

3. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). This is the NIC used by the management server during the registration process.

4. After registration, the IP address can move to another network interface.

5. Verify connectivity between Content Gateway and the management server.

## Registering Content Gateway

Register Content Gateway in the Content Gateway manager:

1. Go to the Configure > My Proxy > Basic > General page.
2. In the Networking section, enable Web DLP > Integrated on-box if needed.
   If a change was made, restart Content Gateway when prompted.
3. Go to the Configure > Security > Web DLP page and enter the IP address of the management server.
4. Enter a user name and password for a Forcepoint Security Manager administrator with Deploy Settings privileges in the Data Security module.
5. Click Register.
6. Go to the Configure > My Proxy > Basic page and click Restart to restart the Content Gateway machine.

## Enabling web DLP

After Content Gateway has registered with Forcepoint DLP, use the Content Gateway manager to perform the following steps:

1. Go to the Configure > Security > Web DLP page.
2. Enable Analyze FTP Uploads to send FTP uploads to web DLP components for analysis and policy enforcement.
3. Enable Analyze Secure Content to send decrypted HTTPS posts to web DLP components for analysis and policy enforcement.
   This option requires that SSL Manager be enabled. See the Content Gateway Manager Help for details.
4. Click Apply and restart Content Gateway.
Configure the Content Gateway policy engine

When Content Gateway is registered with the management server, a Content Gateway module is added to the System Modules in the Data Security module of the Forcepoint Security Manager.

By default, this agent is configured to monitor web traffic, not block it, and for a default violation message to appear when an incident is triggered. To continue using this default behavior, no Content Gateway configuration changes are needed. Simply deploy settings in the Security Manager to activate the default configuration.

To instead block web traffic that breaches policy, or to customize the violation message, do the following:

1. Log on to the Data Security module of the Security Manager.
2. Go to the Settings > Deployment > System Modules page.
3. Select the Web Content Gateway module in the tree view (click the module name itself, not the plus sign next to it).
   It will be listed as “Forcepoint Web Security Server on <FQDN> (<PE_version>),” where <FQDN> is the fully-qualified domain name of the Content Gateway machine and <PE_version> is the version of the Content Gateway policy engine.
4. Select the HTTP/HTTPS tab to configure HTTP(S) blocking behavior.
   Select Help > Explain This Page for instructions for each option.
5. Select the FTP tab to configure FTP blocking behavior.
   Select Help > Explain This Page for instructions for each option.
6. Click Save to save the changes.
7. Click Deploy to deploy the settings.

---

**Important**

Even if the default configuration is not changed, it is still necessary to click Deploy to finalize the Content Gateway deployment process.

---

Set up Content Gateway

Additional Content Gateway configuration is performed in the Content Gateway manager:

- Log onto Content Gateway Manager and run a basic test (Getting Started)
- If there are multiple instances of Content Gateway, consider configuring a managed cluster.
- Configure protocols to proxy in addition to HTTP:
Complete the explicit or transparent proxy deployment.

- **Content Gateway explicit and transparent proxy deployments**
- **Explicit proxy**
- **Transparent proxy**

- If proxy user authentication will be used, [configure user authentication](#).
- If content caching was enabled during installation, [configure content caching](#).

After the base configuration has been tested, consider these additional activities:

- In explicit proxy deployments, [customize the PAC file](#).
- In transparent proxy deployments, use [ARM dynamic and static bypass](#), or use router ACL lists to bypass Content Gateway (see the router documentation).
Configuring the Analytics Engine

Configure the analytics engine, incident risk reporting, and risk-related policies in the Data Security module of the Forcepoint Security Manager.

1. Go the Settings > Deployment > System Modules page.
2. Make sure the analytics engine module appears in the tree, then:
   a. Click the module to view details.
   b. If needed, change the module name and description.
3. Go to the Settings > General > Reporting page to configure the Top Risks report derived from the user analytics.
   a. Specify the risk scores to show in the report and on the dashboard.
   b. Define the organization’s typical work week to help identify aberrant behavior.
4. For optimal accuracy and efficacy, go to the Main > Policy Management > DLP Policies page and add the following policies:
   ■ Disgruntled Employee
   ■ Self CV Distribution
   ■ Password Files
   ■ PKCS #12 Files
   ■ Deep Web URLs
   ■ Email to Competitors
     Be sure to provide the competitors’ domain names (case-insensitive, separated by semicolons).
   ■ Suspected Mail to Self
     Add or edit the sources to monitor via the possible_sources_domains parameter in the Email Similarity script classifier.
5. Click Deploy.

See Reporting and health monitoring options, page 16, for information about the reports that the analytics engine enables.
Reporting and health monitoring options

Once the system is running and capturing metrics, use the following reports to review analytics data:

- On the Main > Status > Dashboard page, monitor the charts under Data Loss Prevention - Incident Risk Ranking.
- Use the Incident Risk Ranking report to investigate risks in more detail. To access the report, do either of the following:
  - Click an Incident Risk Ranking dashboard chart.
  - Go to the Main > Reporting > Data Loss Prevention > Report Catalog page, then expand the Security Analytics tree and select Incident Risk Ranking.

To view the health of the analytics engine, go to the Main > Status > System Health page, then click the Analytics Engine module.
Configuring the CASB Service

After receiving CASB service connection information from Forcepoint, first use the Forcepoint Security Manager to enable the CASB service to the cloud service, then enable DLP policy enforcement and discovery for specific cloud applications. See:

- Connect and enabled the CASB service, page 17
- Configure DLP policy enforcement, page 17

Connect and enabled the CASB service

To connect and enable the CASB service:

1. Make sure to have the Forcepoint fulfillment message that contains the CASB service activation information at hand.
2. Log on to the Data Security module of the Security Manager.
3. Go to the Settings > General > Services page and select the CASB Service tab.
4. Click Connect.
5. In the CASB Service Connection dialog box, enter the following information from the fulfillment letter:
   a. The Access key ID for the account
   b. The Access key secret for the account
   c. The Service URL
6. Click Connect.

When the connection process is complete, the CASB service is automatically enabled and the CASB Service tab is updated.

Configure DLP policy enforcement

To allow the CASB service to apply DLP policies to cloud applications, configure a connection to the organization’s cloud applications:
1. On the **Settings > General > Services > CASB Service** tab, click **Add** under the Cloud Applications list.

2. In the Add Cloud Application window, select an application.
   The CASB portal opens in a new window 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.

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 than can be left in place of quarantined files to explain to users that their file has been moved.
   Click **Test Connection** to verify that the message file can be copied to the cloud application.

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 window in the CASB portal, which can be used to update configuration for the application.

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.
Configuration example 1: Symantec Proxy SG

Follow the instructions in the Symantec installation guide to set up an initial ProxySG configuration with a direct serial port connection. This process requires the following information:

1. IP address and netmask of the main interface
2. Default gateway IP address
3. DNS server IP address
4. Console user name and password
5. Enable password
Once the initial configuration is complete, configure the second interface on the Symantec proxy for use with the Forcepoint DLP ICAP server:

1. Log on to the ProxySG management console as described in the Symantec installation guide.
2. Configure Adapter #1 with the IP address and netmask of the ICAP interface using the steps in the “Adapters” section of the Symantec configuration guide. (Adapter #0 is configured during the serial port configuration)

Enabling HTTPS forward proxy configuration

To enable scanning of HTTPS posted documents, the ProxySG must be configured for HTTPS forward proxy.

To configure the HTTPS forward proxy, follow the steps in the following sections of the Symantec configuration guide:

1. Setting up the SSL proxy in transparent proxy mode
2. Creating an issuer keyring for SSL interception
3. Downloading an issuer certificate

Refer to Symantec documentation for more information.

Configuring the protector for ICAP

Configure the protector to use ICAP in the Data Security module of the Forcepoint Security Manager:

1. Go to Settings > Deployment > System Modules page.
2. Expand the node for a protector instance.
3. Select the ICAP server for the selected protector.

For more information, see the Forcepoint DLP Administrator Help.

Configuring the ICAP service on Symantec

This procedure assumes the ProxySG is operating minimally with only the initial configuration, and that the administrator performing the procedure is logged on to the Symantec management console.

If the deployment includes multiple protectors with ICAP servers, create a unique ProxySG service for each one.

To configure the ProxySG ICAP service:

1. In the Symantec management console, go to the Configuration > External Services > ICAP page. The ICAP Services tab is selected by default.
2. To add a new service, click **New**.

The Add list item window appears.

3. In the **Add ICAP Service** field, enter an alphanumeric name, then click **OK**.
4. In the Services list, select the new ICAP service name and click **Edit**.

5. In the Edit ICAP Service dialog box, enter the **Service URL**.
   This includes the URL schema, the ICAP server hostname or IP address, and the ICAP port number.
   Use different service URLs to distinguish between encapsulated protocols. For example:
   ```
   icap://10.1.1.1/reqmod/ftp
   ```

6. Specify the **Maximum number of connections** between the ProxySG and the ICAP server. This can be any number between 1 and 65535 (default 5).

7. Specify the **Connection timeout** period in seconds.
   - This is the number of seconds the ProxySG waits for replies from the ICAP server.
   - It can be any number between 60 and 65535 (default 70).

8. Next to Notify administrator, select **Virus detected** to send an email message to the administrator if the virus scan detects a match.
   The notification is also sent to the Event Log and the Event Log email list.

9. Next to Method supported, select **request modification**.

10. For the Send options, select **Client address**, **Authenticated user**, or both.

11. **(Optional)** Click **Sense settings** to automatically configure the ICAP service using the ICAP server parameters.
12. Click **OK**, then click **Apply**.

**Setting up forwarding**

The procedure in this section assumes that ProxySG is operating with initial configuration settings and ICAP configuration, and that the administrator performing the procedure is logged on to the Symantec management console.

To configure the ProxySG ICAP policies:

1. Go to the **Configuration > Policy > Visual Policy Manager** page, then click **Launch**.

![Visual Policy Manager](image)

2. In the Visual Policy Manager, select **Add a policy**.
3. To add a content layer, click the **Web Content Layer** tab, then click **Add Rule**.
4. Enter a policy name, then click **OK**.
5. Right click the **Action** option and select **Set** from the menu.

6. Under **Show**, select **Set ICAP Request Service Objects**.

7. Click **New > Set ICAP Request Service**.
8. Enter a name for the ICAP request service.
9. Select **Use ICAP request service**, choose a service from the drop-down list, and click **Add**.

![Add ICAP Request Service Object](image)

10. Click **OK** twice.
11. Click **Install policy**.

### Configuring HTTPS policies

To configure an HTTPS policy, follow the steps in these sections of your Symantec configuration guide:

1. Using the SSL intercept layer
2. Using the SSL access layer

Refer to Symantec documentation for more information.

### Recommended Symantec filtering rules

The table below lists filters that should be applied to the Symantec policy layer before the data is sent to the protector’s ICAP server.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Filter</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>GET</td>
<td>Allow always</td>
</tr>
<tr>
<td>HTTP</td>
<td>POST &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>HTTP</td>
<td>POST &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
<tr>
<td>HTTP</td>
<td>PUT &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
</tbody>
</table>
Configuring Third-Party Proxies

### Configuration example 2: Squid

Configure the Squid proxy to send requests to the ICAP server that is part of the Forcepoint DLP protector.

This example is for Squid-3.1:

```bash
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
adaptation_access service_req allow all
```

This example is for Squid-3.0:

```bash
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
icap_class class_req service_req
icap_access class_req allow all
```


### Configure the protector for ICAP

Configure the protector to use ICAP in the Data Security module of the Forcepoint Security Manager:

1. Go to **Settings > Deployment > System Modules** page.
2. Expand the node for a protector instance.
3. Select the ICAP server for the selected protector.

For more information, see “Configuring ICAP” in the [Forcepoint DLP Administrator Help](#).
## ICAP server error and response codes

<table>
<thead>
<tr>
<th>Response Condition</th>
<th>Forcepoint Block Decision</th>
<th>Control Exceeds Size Limit</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>“pana_response”</td>
<td>“huge_content”</td>
<td>“pana_error”</td>
</tr>
<tr>
<td>Error Code</td>
<td>500</td>
<td>500</td>
<td>512</td>
</tr>
<tr>
<td>“X-Response-Info”</td>
<td>PA-block</td>
<td></td>
<td>PA-error</td>
</tr>
<tr>
<td>“X-Response-Desc”</td>
<td>Forcepoint blocked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plain URL</td>
<td>/usr/local/spicer/etc/blockmessageexample.plain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Markup URL</td>
<td>/usr/local/spicer/etc/blockmessageexample.markup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring User Directory Integration

Getting Started Guide | Forcepoint DLP | v8.7.x

Import information from a supported directory server, such as Microsoft Active Directory or IBM Domino, into Forcepoint DLP in order to:

- Allow administrators to use their network credentials to log on to the Forcepoint Security Manager.
- Include user details in analysis.
- Enhance the incident details displayed to administrators.

For configuration instructions, see:

- Define user directory settings, page 29
- Configure the directory import, page 31
- Rearrange user directory servers, page 31

Define user directory settings

Use the Forcepoint Security Manager to configure Forcepoint DLP to import user directory data.

Configuring general settings

1. Log on to the Data Security module of the Security Manager.
2. Go to the Settings > General > User Directories page.
3. Click New in the toolbar at the top of the page.
4. At the top of the Add/Edit directory server page:
   a. Enter a display Name for the directory server. This is displayed in the list on the User Directories page.
   b. Mark the Enabled check box.
   c. Select the directory Type from the drop-down list: Active Directory, Domino, or Comma-Separated Values (CSV) File.
Configuring connection settings

Connection settings vary, based on whether a network user directory or a CSV file was selected in the previous section.

For network user directories (Active Directory or Domino), enter:

1. 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 directory server access.
3. To secure the connection to the directory server, mark **Use SSL encryption**.
4. To prompt Forcepoint DLP to follow server referrals, if they exist, mark **Follow referrals**.
5. Click **Test Connection** to verify the connection to the directory server.
6. Continue with the next section,

For CSV files:

1. Enter the **Path** to the file.
2. Enter the **User name** and **Password** for an account with at least read permissions to the file.
3. Click **Test Connection** to verify that Forcepoint DLP can read the file.
4. Click **OK**.

Configuring directory usage settings

This section applies only to network user directories (Active Directory or Domino).

1. Mark **Get user attributes** to retrieve specified user attributes from the directory server.
2. Use the **Attributes to retrieve** field to enter the user attributes that should be collected for all users. Use commas to separate entries.
3. If the directory includes user photos, enter the photo attribute name in the **User’s photo attribute** field.
4. Under Test Attributes, enter a **Sample email address** to use to perform an import test. Use a valid email address from the directory.
5. Click **Test Attributes** to retrieve user information that corresponds to the sample email address.
6. Click **OK**.

The server is listed on the User Directories page.
Configuring User Directory Integration

Configure the directory import

By default, Forcepoint DLP imports data from user directory servers daily at a set time. To change the import time:

1. In the Security Manager, go to the Settings > General > User Directories page.
2. Click the Import daily at... link (to the left of the page, above the list of directories).
3. Set a new time or schedule, then click OK.

In addition to the scheduled import, user directory information can also be imported manually. To start the import process at any time:

1. Go to the User Directories page.
2. Select a directory server in the list.
3. Click Import Now in the toolbar at the top of the page.
4. Click Yes to continue.

To view user directory entries after they have been imported:

1. Go to the Main > Policy Management > Resources page.

Rearrange user directory servers

If more than one user directory has been configured, users are imported from directories in the order listed on the User Directories page. If a user is in more than one directory, the first directory record takes precedence.

To rearrange the order of the servers:

1. Go to the Settings > General > User Directories page.
2. Click Rearrange Servers in the toolbar at the top of the page.
3. Select a server and use the arrow buttons to move it up or down the list.
4. Click OK.
Getting Started with File Discovery

Discovery is the act of determining where sensitive content is located in the organization. If the network includes Windows or Micro Focus shared drives, administrators can create a data discovery task that describes where and when to discover content on the drives. Discovery can also be performed on Exchange servers and IBM Domino and Notes.

For more information, see:

- Performing discovery on Micro Focus file systems, page 33
- Performing discovery on Windows NFS shares, page 35
- Performing discovery on Exchange servers, page 44
- Performing discovery on IBM Domino and Notes, page 48

Performing discovery on Micro Focus file systems

The following definitions are used in this section:

- Using Micro Focus Directory Services, a network administrator can set up and control a database of users and manage them using a directory with an easy-to-use graphical user interface. Users at remote locations can be added, updated, and managed centrally. Applications can be distributed electronically and maintained centrally. The concept is similar to Microsoft’s Active Directory.
- Micro Focus Client for Windows allows Windows machines to authenticate through NDS and access shared resources on Micro Focus servers.

Prepare the Micro Focus server

1. Create a user account in NDS.
   - This user will be used by the Forcepoint DLP crawler agent to authenticate with Micro Focus eDirectory and access files and folders.
   - The user account must have the same logon name and password as the Forcepoint DLP service account.
2. Make sure the newly created user has at least “Read” permissions on all files and folders on which discovery will be run.
Prepare the Forcepoint DLP server

Step 1: Install the Micro Focus Client

1. Download the latest Micro Focus Client for Windows from the Micro Focus website.
2. Run setupnw.exe and select Custom Installation.
3. Make sure Distributed Print Services is not selected, then click Next.
4. Make sure NetIdentity Agent and NMAS are selected, then click Next.
5. Select IP and IPX protocols, then click Next.
6. Select eDirectory, then click Next.
7. Wait for the installation to complete, then reboot the server.
   After the reboot, the logon window should appear instead of the regular Windows logon.

Step 2: Prepare the system for discovery

1. Log on to Windows and Micro Focus using the Forcepoint DLP service account (it should be the same user for both platforms as stated above).
2. On the eDirectory tab, select the tree and its relevant context for the folders on which discovery will be run.
3. Right-click the Micro Focus icon in the task bar and select Properties.
4. Click Cancel.
5. Ensure the files on which discovery will be run are accessible from Windows by UNC (for example, \FileSrv\vol1\Data).
6. Right-click the icon in the task bar and select Connections.
7. On all connections, click Detach until no connections remain.

Step 3: Create a new discovery task

1. Log on to the Data Security module of the Forcepoint Security Manager.
2. Go to the Main > Policy Management > Discovery Policies page.
4. On the Networks page, click Edit to select the server’s IP address.
5. Click Advanced, then add the Micro Focus access port number 524.
6. On the Scanned Folders page, use the Forcepoint DLP service account for authentication.
7. Configure the remaining discovery options as needed.
Performing discovery on Windows NFS shares

If you want to perform data discovery on Windows file shares, you need to install NFS client on your Forcepoint DLP server. If you have more than one Forcepoint DLP server, install NFS client on the one with the crawler you will use to perform discovery.

Do not install Forcepoint DLP on the same machine as the NFS server.

Configure the Forcepoint DLP server

The instructions in this section are for supported versions of Windows Server 2008 R2.

1. To activate Network File System (NFS) on the Forcepoint DLP server, open the Server Manager.

2. Select Server > Role Services > Add Role > Services for Network File System.

4. Right-click **Client for NFS** and select **Properties**.

5. On the Client Settings tab, set the Transport protocol to **TCP** and the Default mount type to **Use hard mounts**.

6. On the File Permissions tab, set all file permissions to **Read, Write, and Execute**.

7. Click **OK**.

8. Right-click **Services for NFS** again and select **Properties**.
9. Mark the **Active Directory domain name** check box and enter a **Active Directory domain name**.

10. Click **OK**.

**Configure the domain controller**

1. Log onto a Domain Controller to configure Active Directory to use Identity Management for UNIX.
2. Remove any installed NIS tools under Server Manager > Features.

3. Click Add Role Services to launch the Add Role Services wizard.
4. Select Identity Management for UNIX.

5. Click Next, then click Install.
6. Reboot the server when prompted.

Identity Management for UNIX is now installed.

Configure Identity Management for UNIX

Identity Management for UNIX requires:

1. A primary group that includes all LDAP users
2. A bind or anonymous bind user

Create the primary group for all UNIX user accounts

2. Navigate to the Organization Unit (OU) that will contain the group, then select Action > New > Group.
5. Click OK.

6. Right-click the new group and select Properties.
7. On the UNIX Attributes tab, select the NIS Domain from the drop-down menu and accept the default Group ID (GID), then click OK.

**Note**
If the GID is not 10000, there is already a UNIX-enabled group in the directory. The GID must be unique and match the GID of the UNIX Group.
Create a new UNIX user / service account

1. Still in the Active Directory Users and Computers tool, select the OU that will hold the UNIX Service Account, then **Action > New > User**.

2. Enter a **Password** and select the following:
   - User cannot change password
   - Password never expires
   All other features must be disabled.

3. Click **Next**, then click **Finish** to create the account.

4. Right-click the new user and select **Properties**.

5. On the Member Of tab, click **Set Primary Group** and add the group created in the previous section.
6. Remove the **Domain Users** group.

7. Select the **UNIX Attributes** tab.

8. Set the following parameters, then click **OK**.
   a. Select the user’s **NIS Domain**.
   b. Enter the **UID** on the UNIX computer that matches the UID of the user on the UNIX machine.
   c. Enter the user account **Login Shell**.
   d. Enter the user **Home Directory** on the UNIX computer.
e. Enter the **Primary group name/GID** of the user configured previously.

Configure Forcepoint DLP to scan NFS

1. Log on to the Data Security module of the Security Manager.
2. Create a data discovery policy. (See [Creating a data discovery policy](#) for instructions.)
3. On the Main > Policy Management > Discovery Policies page, select **Add network task** > **File System Task**.
4. On the General page, add a name and description for the discovery task and select the crawler hosted on the machine that also hosts the NFS client. This is the crawler that will perform the file system discovery.
5. On the Networks page, click **Advanced** and add port **2049** to the existing list of scanned ports.
6. On the Scanned Folders page, specify the shares to scan and the user name and password of the Windows user mapped to the UNIX account as follows:

   a. Select the Shared Folders to scan:
      ○ Select **Administrative shares** to scan administrative share drives such as C$.
      ○ 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 entries.

   b. Select the Method to use when scanning network shares: **TCP** or **ICMP**.

   c. Enter the **User name** and **Password** of the Windows user that was previously mapped to a UNIX account.

   ![Image of Scanned Folders and Network Credentials]

   **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.

7. Deploy your changes.

For more information on the wizard for creating file system discovery tasks, see File System tasks.
Performing discovery on Exchange servers

Forcepoint DLP can be used to perform discovery on Microsoft Exchange servers. See:

- Prepare to run discovery on Exchange Online 365, page 44
- Prepare to run discovery on Exchange 2013, page 45
- Prepare to run discovery on Exchange 2010, page 47

Prepare to run discovery on Exchange Online 365

1. Create or identify an Exchange 365 account for Exchange discovery scanning.
2. Grant the account one of the following roles to allow the Forcepoint DLP crawler to discover messages and display results:
   - Organization Management
   - View Only Organization Management

   The crawler account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery.

   Log onto OWA with this account, and try switching between mailboxes as shown below:

3. Configure Exchange impersonation for the service account used for discovery:
   a. Open the Windows PowerShell as administrator.
   b. Enter the following command:

      ```powershell
      $LiveCred = Get-Credential
      ```
   c. When prompted for credentials, enter the user name (email address) and password for the Exchange 365 account to be used for discovery.
   d. Enter the following command:

      ```powershell
      ```
   e. Enter the following commands:
Getting Started Guide

Getting Started with File Discovery

1. Define a service account for Exchange discovery scanning.
2. Grant the account one of the following roles. This is necessary so that the system can discover messages and display results.
   - Organization Management

Prepare to run discovery on Exchange 2013

3. Log on to the Data Security module of the Forcepoint Security Manager.
4. Go to the Main > Policy Management > Discovery Policies page, then click Add network task > Exchange Task.
5. Complete the wizard as explained in the Forcepoint DLP Administrator Help. On the Exchange Servers page, enter the credentials set up above.

5. Make sure that Integrated Windows authentication is turned on (default). If it is not:
   a. In the Exchange admin center, go to servers > virtual directories > EWS (Default Web Site).
   b. Select Integrated Windows authentication.
   c. Click Save.
3. Configure Exchange impersonation for the service account used for the discovery:
   a. Open the Exchange Management Shell.
   b. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate to the specified user.

   For example, to enable a service account to impersonate all other users in an organization, enter the following:
   ```powershell
   New-ManagementRoleAssignment -
   Name:impersonationAssignmentName -
   Role:ApplicationImpersonation -User:ServiceAccount
   ```


4. Configure an Exchange discovery task as follows:
   a. Log on to the Data Security module of the Forcepoint Security Manager.
   b. Go to the Main > Policy Management > Discovery Policies page, then click Add network task > Exchange Task.
   c. Complete the wizard as explained in the [Forcepoint DLP Administrator Help](#). On the Exchange Servers page, enter the credentials set up above.

5. Check that Integrated Windows authentication is turned on (it should be on by default). If it is not:
   a. In the Exchange admin center, go to servers > virtual directories > EWS (Default Web Site).
b. Select **Integrated Windows authentication**.

Prepare to run discovery on Exchange 2010

1. Define a service account for Exchange discovery scanning.
2. Grant the account one of the following roles. This is necessary so that the system can discover messages and display results.
   - Exchange Full Administrator
   - Exchange Administrator
   - Exchange View Only Administrator

   The service account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery. Try switching between mailboxes as shown below:

3. Configure Exchange impersonation. Exchange impersonation needs to be enabled for the service account used for the discovery
   a. Open the Exchange Management Shell.
   b. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate to the specified user.

   For example, to enable a service account to impersonate all other users in an organization, enter the following:

   ```powershell
   New-ManagementRoleAssignment -Name:impersonationAssignmentName -Role:ApplicationImpersonation -User:ServiceAccount
   ```
For more information on Exchange impersonation, see msdn.microsoft.com/en-us/library/bb204095.

4. Configure an Exchange discovery task as follows:
   a. Log on to the Data Security module of the Forcepoint Security Manager.
   b. Go to the Main > Policy Management > Discovery Policies page, then click Add network task > Exchange Task.
   c. Complete the wizard as explained in the Forcepoint DLP Administrator Help. On the Exchange Servers page, enter the credentials set up above.

Performing discovery on IBM Domino and Notes

Forcepoint DLP can perform discovery on documents stored in an IBM Domino Data Management System (DMS).

Domino discovery 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 would not cause an incident.

To perform discovery on documents:

1. Log on to the Data Security module of the Forcepoint Security Manager.
2. Go to the Main > Policy Management > Discovery Policies page.
3. Select one of the following:
   - Locate regulatory & compliance data
   - Create custom policy.
4. Complete the steps in the wizard as described in the Forcepoint DLP Administrator Help. Select dictionary, RegEx, fingerprinting, or other classifiers as needed.
5. Go to the Main > Policy Management > Discovery Policies page.
6. Select Add network task > Domino Task.
7. Complete the steps in the wizard as described in the Forcepoint DLP Administrator Help.
8. To deploy the policy and task to the Domino server, click Deploy.

The Domino server will be crawled for sensitive data at the next scheduled time. Incidents are reported in Main > Reporting > Discovery reports.
Configuring Labels

Use the Forcepoint Security Manager to import labels from labeling systems and apply them on files in endpoint discovery scans (available on Windows operating systems only). See:

- Import and enable Boldon James Classifier labels, page 49
- Import and enable Microsoft Information Protection labels, page 50
- Configure an action plan to apply labels, page 52

Import and enable Boldon James Classifier labels

To import Boldon James Classifier labels and enable the option to apply labels, first ensure that the labeling system is installed on the network, and then do the following:

1. Log into the Data Security module of the Security Manager.
2. Go to Settings > General > Services and select the File Labeling tab.
3. Click the Boldon James Classifier link.
5. Click Choose File.
6. Browse to the Boldon James configuration file, and click OK to import it. The file is usually called spif.xml. If the file is not found, contact Boldon James technical support.
7. When the importation is successfully completed, the time and date of the process and a list of imported labels appear in the Last import field.
8. Select the Apply file labels check box. You can now define DLP action plans that use Boldon James Classifier file labels. When this box is unchecked, Boldon James Classifier labels are used only for detection.
9. In the Guidelines section, mark one or more check boxes to specify when Forcepoint DLP should add or modify a label. Note the following aspects of the guidelines:
Configuring Labels

- If a file does not meet a specified condition, its labeling remains unchanged.
- Incident reports provide detailed information about whether labels were found on files and whether they were changed.

10. Click OK to save the changes.

Import and enable Microsoft Information Protection labels

Before you can import Microsoft Information Protection labels for the first time, you must obtain permission for the Forcepoint application to perform the import, as follows:

1. Log into the Microsoft Office 365 Admin Consent page, using your Microsoft Office 365 admin credentials for authentication.
2. Accept the permission statement on the page.

Next, to import enable Microsoft Information Protection labels, first ensure that the labeling system is installed on the network, and then do the following:

1. Log into the Data Security module of the Security Manager.
2. Go to Settings > General > Services and select the File Labeling tab.
3. Click the Microsoft Information Protection link.
4. On the Microsoft Information Protection Properties page, in the Imported Labels section, enter your Microsoft Office 365 admin credentials, and then click Import Labels.
5. Click OK to start the import process. Note that if the consent process was not completed, this step generates an error. Complete the consent process, and then try again.
6. When the importation is successfully completed, the time and date of the process and a list of imported labels appear in the Last import field.
7. Select the Apply file labels check box. You can now define DLP action plans that use Microsoft Information Protection file labels.
   When this box is unchecked, Microsoft Information Protection labels are used only for detection.

---

We recommend that you enter credentials for an administrator who has visibility to all Microsoft Information Protection labels used in the organization. User credentials are not stored on Forcepoint servers. You should also ensure that your web browser does not store this information.
8. Click **OK** to save the changes.

---

**Note**

If Rights Management Service Client 2.1 is installed on the endpoint machine, files that are protected by Microsoft Information Protection can be decrypted automatically during DLP analysis, without having to configure Microsoft RMS (see Forcepoint DLP Administrator guide).
Configure an action plan to apply labels

To configure labels to apply on files for Discovery Policies (endpoint only):

1. Log into the Data Security module of the Security Manager.
2. Go to Policy Management > Resources > Action Plans and select the Discovery tab.
3. In the Endpoint Discovery section, select a labeling system from the drop-down menu.
4. Select the labels you want to apply. Make sure they are from the labeling system you chose.
5. Click OK to save.
6. Add the action plan to the desired Discovery Policy.

For more information, see Forcepoint DLP Administrator Guide.