Forcepoint DLP Administrator

Lab Guide

Rev: CC0074

Public

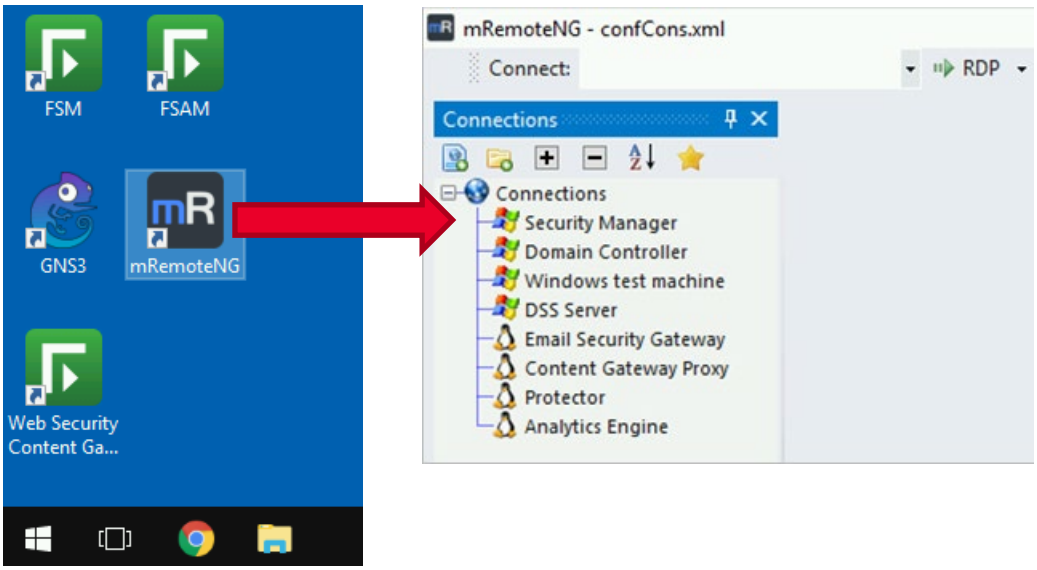
Forcepoint

forcepoint.com

Contents

Lab Environments

You have your own lab environment that has two main parts, the Landing Machine and the Virtual Machines. The Landing Machine is a Windows 10 host that provides access to the lab environment. It is not used for any testing during the labs. On the desktop of the Landing Machine is a shortcut to **mRemoteNG**. When launched, this application provides a list of virtual machines that are used in various labs. To access the console of a desired virtual machine, simply double-click on the name.



The connections list shows you all the devices that are available in this lab.

- You can change the resolution of the remote desktop session using **Config > Appearance**. You will need to close the tab and re-open the connection for this to take effect.
- When you double click on the device in the **Connections** list, it will open in a new tab.

During this lab you will be using:

- **Security Manager** This is the management server and has Forcepoint Security Manager installed. You will log in with

  Username: Administrator
  Password: Forcepoint1!

- **Windows test machine** This is the machine that you will use to test your policies. You will log with

  Username: tmuller
  Password: Forcepoint1!

1 Introduction to Forcepoint DLP

1.1 Access Forcepoint Security Manager and perform initial configuration

Scenario:

In this walk-through, you will sign in to the lab environment in Go4Labs and gain access to the Forcepoint Security Manager. In the process, you will begin to familiarize yourself with the Forcepoint DLP Interface.

Tasks:

1. Use the mRemote application to access the Forcepoint Security Manager.
2. Navigate to the Forcepoint DLP dashboard.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

Open the web browser of your choice and navigate to the lab URL you were provided with by your instructor. You will be presented with a login prompt for Apache Guacamole. Enter the credentials you were provided with by your instructor.

1.1.1 Use the mRemote application to access the Forcepoint Security Manager

1. The first screen you will see in the lab is the Landing Machine desktop.
2. Double click the **mRemoteNG** shortcut and the mRemote application will load.
3. Double-click the **Security Manager** link in the Connections tab.
   A remote desktop session will begin.
4. You will be automatically logged in as the Administrator user, and the Security Manager machine's desktop will load.

5. Double-click the **Forcepoint Security Manager** shortcut on the desktop.
   A browser window will open and the Forcepoint Security Manager login screen will load.
6. If you receive a certificate error, click **Advanced**, then click the link to **Proceed to 172.31.0.155**. The Forcepoint Security Manager login screen will load.

1.1.2 Navigate to the Forcepoint DLP dashboard

1. Enter the credentials you were provided by your instructor, then click **Log On**.
   The Forcepoint Security Manager dashboard will load.
2. Confirm you are on the **Data** dashboard by verifying the product selection in the upper left.

You should now be able to:

- Use the mRemote application to access the Forcepoint Security Manager.
- Navigate to the Forcepoint DLP dashboard.

1.2 Locate and configure registered system modules in a DLP environment

Scenario:

In this walk-through, you will locate the system modules list in the Forcepoint DLP manager and make a necessary configuration change in your web content gateway settings.

Tasks:

1. Navigate to the system modules list in the DLP manager.
2. Identify the system modules registered in your environment.
3. Perform necessary configuration changes on your system modules.
4. Apply Forcepoint DLP licenses.

Environment Credentials:

Go4labs information sent via instructor

Site:	(generatedname).go4labs.net
Username:	generatedfirst.generatedlast
Password:	generated

Security Manager Server

Domain:	Fpcert
Username:	Administrator
Password:	Forcepoint1!

Security Manager UI

Username:	admin
Password:	Forcepoint1!

1.2.1 Navigate to the system modules list in the DLP manager

1. In your Go4Labs environment, resume the session in **mRemote** and access the Forcepoint Security Manager. Navigate to the **Data** tab.
2. Scroll down, and in the left-hand menu, select **Deployment > System Modules**.
   The dashboard will load the system modules list.

1.2.2 Identify the system modules registered in your environment

1. Identify each registered system module and recall their function.
2. Click the **+** symbol next to the **Forcepoint Content Gateway Server**.
   The entry will expand to show the components of that module.

1.2.3 Perform necessary configuration changes on your system modules

1. Click on the title line of the **Forcepoint Content Gateway Server**.
   This will load the details tabs for that module.
2. Click on the **HTTP/HTTPS** tab to access those configuration settings.
3. Change the **Mode** from **Monitoring** to **Blocking**.
   This will ensure the web content gateway is capable of enforcing block actions on any detected web incidents.
4. Click on **OK** in the bottom right to save your configuration changes.
5. You should see a **Deployment Needed** pop-up window, indicating there is a configuration change awaiting deployment. Click the **Yes** button.
6. Confirm that each system module on the resulting Deployment Process page shows a green check mark and “Success” in the Status column when the deployment is done.

1.2.4 Apply Forcepoint DLP licenses.

1. Navigate to **General > Subscription** in the left menu of the DLP manager.
2. Note that all subscription information currently shows as N/A – this is because the license currently in effect is a limited one shared from the Web and Email products, not a full DLP license.
3. Without clicking, hover your mouse over **Deployment** in the left-hand menu. Note that there is no option for **Endpoint Profiles**, as the current license is not a full DLP license.
4. Click on **Update** on the Subscription tab, then click **Choose File** and browse to *C:\Forcepoint\License_Keys* in the browser that pops up.
5. Double click the file *DLP–subscription.xml*. Then click **OK** to save your changes.
6. In the next pop-up, click **OK** to be logged out, then log back in using your credentials.
7. Without clicking, hover your mouse over **Deployment** in the left-hand menu. Note that there is now an option for **Endpoint Profiles**.
8. Navigate to **General > Subscription** in the left-hand menu.
   You will now see your updated license information.
9. Click the **Deploy** button in the top right, which should now be blue, indicating there are changes awaiting deployment. This will push the new license out to all system modules and activate them.
10. Confirm that each system module on the resulting **Deployment Process** page shows a green check mark and “Success” in the Status column when the deployment is done.

You should now be able to:

- Navigate to the system modules list in the DLP manager.
- Identify the system modules registered in your environment.
- Perform necessary configuration changes on your system modules.
- Apply Forcepoint DLP Licenses.

2 Configuring Forcepoint DLP Classifiers

2.1 Create simple classifiers

Scenario:

In this walk-through, you will create a key phrase classifier and dictionary classifier that can work in tandem to increase the overall accuracy of a DLP rule.

Tasks:

1. Create a key phrase classifier.
2. Create a dictionary classifier.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

2.1.1 Create a key phrase classifier.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Content Classifiers > Patterns & Phrases** in the left-hand menu bar.
3. Click **New > Key Phrase** in the **Patterns & Phrases** menu bar.
4. Enter the key phrase classifier information.

   Name: FTKW
   Phrase to search: FactoryTestKeyWord
   Note that the **Name** of the classifier and the **Phrase to search** do not need to be identical.
5. Click **OK** in the bottom right to save your changes.
6. Click **Cancel** in the pop-up window to save the classifier without adding it to a rule.

2.1.2 Create a dictionary classifier.

1. Click **New > Dictionary** in the **Patterns & Phrases** menu bar.

   Name: Test Phrase Dictionary
   Description: A dictionary to test phrases to compliment the FTKW key phrase classifier.

2. Enter the dictionary classifier information.

Top Secret	1
Internal-Use-Only	1
Confidential	1
Approved for Release	- 4

3. Click **OK** in the bottom right to save your changes.
4. Click **Cancel** in the pop-up window to save the classifier without adding it to a rule.

You should now be able to:

- Create a key phrase classifier.
- Create a dictionary classifier.

2.2 Create a regular expression classifier

Scenario:

In this walk-through, you will use a third-party resource to create and analyze the function of a regular expression classifier.

Tasks:

1. Analyze the function of a regular expression using a third-party tool.
2. Create a regular expression classifier.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

2.2.1 Analyze the function of a regular expression using a third-party tool.

1. Open a new tab in your web browser and browse to https://regex101.com
2. Enter the following regular expression:
   `^\d{1,2}\/\d{1,2}\/\d{4}$`
3. Test the regular expression by entering date strings in the format *mm/dd/yyyy*.
   Note that the explanation and test results will show on the right.

2.2.2 Create a regular expression classifier.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Content Classifiers > Patterns and Phrases** in the left-hand menu bar.
3. Click **New > Regular Expression** in the **Patterns & Phrases** menu bar.

4. Enter in the regex classifier information.

   Name: Date with Slashes
   Description: A regex to detect a simple date format
   Value: `^\d{1,2}\/\d{1,2}\/\d{4}$`

   Note there are fields where you can enter in patterns to exclude from your search. Leave them blank.
5. Click **OK** in the bottom right to save the classifier.
6. Click **Cancel** in the pop-up window to save the classifier without adding it to a rule.

You should now be able to:

- Analyze the function of a regular expression using a third-party tool.
- Create a regular expression classifier.

2.3 Configure the parameters of a predefined script classifier.

Scenario:

In this walk-through, you will modify a configurable parameter in a commonly used script classifier, with the intent of identifying transactions that contain the email addresses of competing companies.

Tasks:

1. Filter the predefined classifier list to locate the Email to Competitors script classifier.
2. Edit the parameter values of the Email to Competitors classifier.
3. Save a renamed copy of the Email to Competitors classifier.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

2.3.1 Filter the predefined classifier list to locate the Email to Competitors script classifier.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Content Classifiers > Patterns & Phrases** in the left-hand menu bar.
3. Click the down arrow next to the header of the **Name** column, and then click **Filter by this Column**.
4. Enter the string *Email to Competitors* into the filter, then click **OK**.
5. Click on the name of the filtered result. The classifier configuration page will load.

2.3.2 Edit the parameter values of the Email to Competitors classifier.

1. Check the box next to **Edit parameter values**.
2. In the **Value** column, enter the list of domain names, separated by semicolons as indicated: *gmail.com;outlook.com;test.com*
3. Click **Save As** in the top left, and a new window will open.

2.3.3 Save a renamed copy of the Email to Competitors classifier.

1. Enter the new classifier name: “Test – List of Domains”
2. Click **OK** to save your renamed copy of the *Email to Competitors* classifier.

You should now be able to:

- Filter the predefined classifier list to locate a script classifier.
- Edit the parameter values of the classifier.
- Save a renamed copy of the classifier.

2.4 Exercise: Create simple classifiers

Scenario

You need to create classifiers that can be used in a DLP rule to find the names of projects and products used in your organization.

Tasks

1. Create a keyword classifier for the project name: UnderMilkWood.
2. Create a dictionary classifier for the product names:
    - Captain Cat
    - Mog Edwards
    - Cherry Owen

3 Configuring Forcepoint DLP Resources

3.1 Configure a connection to and import a user list from Active Directory.

Scenario:

In this walk-through, you will configure a user directory import from Microsoft Active Directory, while first testing the connection to ensure it is functional.

Tasks:

1. Configure an Active Directory connection.
2. Test the connection to ensure it is functional.
3. Change the default time for the Active Directory daily import.
4. Manually import a user list from a configured Active Directory connection.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

3.1.1 Configure an Active Directory connection.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **General > User Directories** in the left-hand menu bar.
3. Click **New** in the User Directories menu bar.
   The **Add/Edit directory server** configuration page will load.
4. Enter the **Name**: “Domain Controller”. Select the **Type**: “Active Directory”.
5. Configure the connection, entering only the information below.

Hostname: dc.fpcert.com
User distinguished name: fpcert\administrator
Password: Forcepoint1!

3.1.2 Test the connection to ensure it is functional.

1. Click the **Test Connection** button.
2. If successful, a green banner message will load at the top of the page.
3. In the **Test Attributes** box, enter the **Sample email address**: "*tmuller@fpcert.com*".
4. Click **Test Attributes**.
   The page will refresh, and a link to **View Results** will appear next to the button.
5. Click the **View Results** link. This sends a live query to the Active Directory. A successful test will cause a pop-up to display with the specified user's attributes.

3.1.3 Change the default time for the Active Directory daily import.

1. Click **OK** at the bottom right to save the configured settings.
2. After returning to the User Directories page, click the **Import daily at 11:00 PM** link in the top right.
   The **Schedule User Directory Import** window opens.
3. Configure the import to run once weekly, at midnight on Saturdays. This is ideal in environments where the user directory structure does not change on a daily basis.
4. Click **OK** at the bottom right to save your configuration settings.

3.1.4 Manually import a user list from a configured Active Directory connection.

1. After returning to the User Directories page, check the box next to the newly configured connection, and then click **Import Now** at the top of the page.
2. Click **OK** on the pop-up that appears to proceed with the manual import.
3. When all scheduled imports are complete, the line above the server list will indicate that **Entries are ready for policy engines**.

You should now be able to:

- Configure an Active Directory connection.
- Test the connection to ensure it is functional.
- Change the default time for the Active Directory daily import.
- Manually import a user list from a configured Active Directory connection.

3.2 Create a functional example of each Forcepoint DLP resource.

Scenario:

In this walk-through, you will create multiple resources you will use for testing purposes in later walk-throughs.

Tasks:

1. Create a custom user directory group.
2. Create a custom user.
3. Create a custom computer.
4. Create a network.
5. Create a domain.
6. Create a business unit.
7. Create an endpoint device.
8. Create a custom endpoint application and add it to an application group.
9. Configure endpoint operations for an endpoint application group.
10. Update the URL categories list.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

3.2.1 Create a custom user directory group

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Resources > Custom User Directory Groups** in the left-hand menu bar.
3. Click **New** in the Custom User Directory Groups menu bar.
4. Call the group *Engineering and MyDLPGroup*.

5. Enter the following string into the Query field, with no spaces or new lines in the middle or after it:
   `(&(objectClass=user)(&(department=Engineering)(memberOf=CN=MyDlpGroup,CN=Users,DC=fpcert,DC=com)))`
6. Click **View Sample Data** and confirm that two users are returned, Tim Muller and Tom Crowne.
7. Click **OK** to save your custom user directory group.

3.2.2 Create a custom user

1. Click **Policy Management > Resources > Custom Users** in the left-hand menu bar.
2. Click **New** in the Custom Users menu bar.
3. Configure the user, then click **OK** to save the user.

Name:	Guest User 1
Email Address:	guest1@fpcert.com
User name:	guest1

3.2.3 Create a custom computer

1. Click **Policy Management > Resources > Custom Computers** in the left-hand menu bar.
2. Click **New** in the Custom Computers menu bar.
3. Configure the computer, then click **OK** to save the computer.

IP address or hostname:	172.31.0.159
FQDN:	DSS-server.fpcert.com

3.2.4 Create a network

1. Click **Policy Management > Resources > Networks** in the left-hand menu bar.
2. Click **New** in the Networks menu bar.
3. Configure the network, then click **OK** to save the network.

Name:	Server Farm
IP address range:	172.31.0.150 to 172.31.0.160

3.2.5 Create a domain

1. Click **Policy Management > Resources > Domains** in the left-hand menu bar.
2. Click **New** in the Networks menu bar.
3. Configure the domain, then click **OK** to save the domain.

Domain:	*.dlptest.com
Description:	all subdomains of dlptest.com

3.2.6 Create a business unit

1. Click **Policy Management > Resources > Business Units** in the left-hand menu bar.
2. Click **New** in the Business Units menu bar. Name the business unit *MyDLPGroup and Server Farm*.
3. Change **Display** to *Custom User Directory Groups* and add the **Engineering and MyDLPGroup** into the business unit using the selection arrows.
4. Change **Display** to *Networks* and add the **Server Farm** into the business unit using the selection arrows.
5. Click **OK** to save the business unit.

3.2.7 Create an endpoint device

1. Click **Policy Management > Resources > Endpoint Devices** in the left-hand menu.
2. Click **New** in the Endpoint Devices menu bar.
3. Configure the endpoint device, then click **OK** to save the device.

   Name: Virtual Flash Drive
   Value: *sandisk*

3.2.8 Create a custom end point application

1. Click **Policy Management > Resources > Endpoint Applications** in the left-hand menu bar.
2. Click **New** then **Application** in the **Endpoint Applications** menu bar.
3. Add the application name and add it to the **Office Applications** endpoint group.

   Name: Notepad++
   Initiated by: notepad++.exe
4. Check the box to make this application a **Trusted Application**.
5. Change the **Screen Capture** action to **Permit & audit**.
6. Click **OK** to save the application.

3.2.9 Configure endpoint operations for an endpoint application group

1. Click **Policy Management > Resources > Endpoint Application Groups** in the left-hand menu.
2. Click the link for the **Office Applications** group in the list.
3. Check the boxes for the **Cut/Copy**, **Paste** and **File Access** operations, then click **Save & Close**.

3.2.10 Update the URL Categories list

1. Click **Policy Management > Resources > URL Categories** in the left-hand menu bar.
2. Click the **Update Now** button in the top left of the page. The page will refresh while polling the Web product database for any changes and import them if any exist.
3. Click **Deploy** in the top right of the FSM dashboard to make all new configuration changes active.

You should now be able to:

- Create a custom user directory group.
- Create a custom user.
- Create a custom computer.
- Create a network.
- Create a domain.
- Create a business unit.
- Create an endpoint device.
- Create a custom endpoint application and add it to an application group.
- Configure endpoint operations for an endpoint application group.
- Update the URL categories list.

3.3 Create a custom action plan.

Scenario:

You have been tasked with configuring DLP to protect local files using the endpoint, specifically to prevent files from being copied to unapproved devices or network locations.

We will put this action plan to use in a later walk-through.

Task:

- Configure actions for individual channels in a custom action plan.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Resources > Action Plans** in the left-hand menu bar.
3. Click **New** in the Action plans menu bar.
4. Call the action plan *Block Lan – Encrypt RM*.
5. Under **Endpoint Channels**, change **Removable media** to **Encrypt with profile key**, and **LAN** to **Block**.
6. Click **OK** to save your new action plan.

You should now be able to:

- Configure actions for individual channels in a custom action plan.

3.4 Configure the default notification.

Scenario:

In a new DLP environment, it is necessary to provide configuration information in the default notification template, in order to ensure that administrators and management receive information when incidents of critical sensitivity are created.

Tasks:

1. Configure the settings of the default notification template.
2. Configure the message body of the default notification template.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

3.4.1 Configure the settings of the default notification template.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Resources > Notifications** in the left-hand menu bar.
3. Click **Default notification** to edit the notification settings.
4. Configure the notification settings.
   Sender name: DLP Administrator
   Sender email address: administrator@fpcert.com
   Subject: Your organization's DLP policy was breached at %Event Time%
   Additional email addresses: %Policy Owners%,%Source's Manager%
   Use **Directory Entries** to add **Tmuller@fpcert.com** as a recipient.
5. Click the **Notification Body** tab to edit the message body of the notification template.

3.4.2 Configure the message body of the default notification template.

1. Configure the message body.

   A policy breach of severity %Severity% was found and action %Action% was taken.
   Sender: %Source%.
   Message Subject: %Details%

2. Click **OK** to save the changes to the notification settings and body.

You should now be able to:

- Configure the settings of the default notification template.
- Configure the message body of the default notification template.

3.5 Exercise: Create a custom action plan

Scenario

You want an action plan to stop data leaving your organization. Emails need to be quarantined until they can be inspected. All FTP on the network must be blocked.

Tasks

- Create a custom action plan to quarantine network emails and block FTP.

4 Configuring DLP Policies and Rules

4.1 Configure and test the quick web policy

Scenario:

In this walk-through, you will enable the quick web policy and establish basic Payment Card Industry (PCI) regulatory compliance, supplemented by several other attributes.

Tasks:

1. Enable and configure attributes of the quick web policy.
2. Deploy your policy changes.
3. Test your quick policy and confirm that regulatory compliance is in effect.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

4.1.1 Enable and configure attributes of the quick web policy.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > DLP Policies > Web DLP Policy** in the left-hand menu bar.
3. Click **Regulatory and Compliance** in the list of attributes. Check the box to **Enable attribute**.
4. Click the **No regions selected** link and set the region to **USA** and click **OK**.
5. Check the box next to **Payment Card Industry (PCI DSS)** to enable it.
6. Click the now active link for **Payment Card Industry (PCI DSS)** and check the box to enable **PCI**. Set the sensitivity to **Narrow**.

7. Click **OK** in the bottom right to save your PCI policy settings.
8. Click **Patterns & phrases** in the list of attributes.
9. Check the box to **Enable attribute**.

4.1.2 Deploy your policy changes.

1. Click **Add** and enter the key phrase “Customer List”. Click **OK** to save your key phrase.
2. Click **OK** in the bottom right to save your quick policy configuration.
3. Click **Deploy** in the top right to deploy your new quick policy out to your policy engines.

4.1.3 Test your quick policy and confirm that regulatory compliance is in effect.

1. In **mRemote**, open a session to the Windows test machine.
2. Open a browser and navigate to https://dlptest.com/sample-data/nameccnzip/ . Highlight and copy five rows of sample data.
3. Navigate to http://dlptest.com/http-post/
4. Paste your sample data into the **Test Message** field. Below it, type the phrase “Customer List”.
5. Click **Submit**. A block page should load indicating your transaction has been stopped by Forcepoint DLP.

You should now be able to:

- Enable and configure attributes of the quick web policy.
- Deploy your policy changes.
- Test your quick policy and confirm that regulatory compliance is in effect.

4.2 Configure and test a predefined policy.

Scenario:

In this walk-through, you will enable a predefined policy to protect PHI (Protected Health Information) using Forcepoint DLP. With minimal configuration, detect and block uploads of filled out-patient medical forms.

Tasks:

1. Enable and configure PHI predefined policies.
2. Deploy your policy changes.
3. Test your policies and confirm that regulatory compliance is in effect.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

4.2.1 Enable and configure PHI predefined policies.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > DLP Policies > Manage Policies** in the left-hand menu bar.
3. Click **Add > Predefined Policy** in the top left. The predefined policy wizard will load.
4. Click **Next**.
5. Set the region to **USA** and click **Next**.
6. Select the industry to **Healthcare and Pharma** and click **Finish**.
7. From the policy list, select **PHI: Protected Health Information**.
8. Click **Use Policies** in the bottom right to save your selections.

4.2.2 Deploy your policy changes.

1. Click **Deploy** in the top right to deploy your new policies out to your policy engines.

4.2.3 Test your policies and confirm that regulatory compliance is in effect.

1. Using **mRemote**, open a session to the Windows test machine.
2. Navigate to http://dlptest.com/http-post/ . Use the file upload to attempt to upload each of the files in *C:\Forcepoint\Test Files*.
   The uploads will not be blocked. You will examine the resulting incidents in more detail in a later unit.

You should now be able to:

- Enable and configure PHI predefined policies.
- Deploy your policy changes.
- Test your policies and confirm that regulatory compliance is in effect.

4.3 Configure and test a custom policy.

Scenario:

In this walk-through, you will configure a custom policy to work with previously established custom classifiers and resources, using advanced policy logic.

Tasks:

1. Configure a custom policy.
2. Deploy your policy changes.
3. Test your policies and confirm that regulatory compliance is in effect.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

4.3.1 Configure a custom policy.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > DLP Policies > Manage Policies** in the left-hand menu bar.
3. Click **Add > Custom Policy** in the top left. The custom policy wizard will load.
4. Name this policy “Custom Test Policy”. Click **Next** in the bottom right to proceed.
5. Click **Add > Patterns & Phrases** to bring up a list of classifiers to choose from.
6. Include the classifiers created previously: key phrase **FTKW** and dictionary **Test Phrase Dictionary**. Click **Next** in the bottom right to proceed.
7. Change the action under **Action Plan** to **Block All**. Click **Next** in the bottom right to proceed.
8. Click **Edit** to open the source selection wizard.

9. Change **Display** to **Business Units** and include **MyDLPGroup and Server Farm** into the rule. Click **OK** to save your settings.
10. Click **Finish** in the bottom right to save your custom policy.

4.3.2 Deploy your policy changes.

1. Click **Deploy** in the top right to deploy your policy updates.

4.3.3 Test your policies and confirm that regulatory compliance is in effect.

1. Use **mRemote** to open a session to the Windows test machine.
2. Open a web browser and navigate to http://dlptest.com/http-post/
3. In the **Test Message** field, first type in “FactoryTestKeyword” and “Confidential”. Click **Submit**. The transaction should be blocked.
4. Submit a new transaction, this time with “FactoryTestKeyword”, “Confidential”, and “Approved for Release”. The transaction should be allowed.

You should now be able to:

- Configure a custom policy.
- Deploy your policy changes.
- Test your policies and confirm they are functioning as expected.

4.4 Create a new policy level and assign policies to it.

Scenario:

In this walk-through, you will establish execution order for your policies using policy levels, in order to ensure that your most critical policies run first.

Tasks:

1. Create a new policy level.
2. Rearrange policy levels and assign policies to the appropriate levels.
3. Deploy your changes.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

4.4.1 Create a new policy level.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > DLP Policies > Manage Policies** in the left-hand menu bar.
3. Click **More Actions > Manage Policy Levels** in the menu bar. The custom policy wizard will load.
4. Click **New** in the top left and name the new level “High Priority Policies”.
5. Click **Select from list** in the bottom right to move policies into the new policy level. (Include Health Data, US PHI, and the Web DLP policies).
6. Click **OK** in the bottom right to save your changes.

4.4.2 Rearrange policy levels and assign policies to the appropriate levels.

1. Click **OK** on the bottom right of the policy level details page to save the new configuration. Do not deploy.
2. Click **Rearrange Levels** in the menu bar.
3. Move the *High Priority Policies* level above the *Default level*.

4.4.3 Deploy your changes.

1. Click **Save** in the bottom right to save the new policy level order.
2. Click **Deploy** in the top right to deploy your policy updates.

You should now be able to:

- Create a new policy level.
- Rearrange policy levels and assign policies to the appropriate levels.
- Deploy your changes.

4.5 Exercise: Create a custom policy

Scenario

You want to create a policy that monitors files for the project name UnderMilkWood and the product names Captain Cat, Mog Edwards and Cherry Owen. Network emails containing these names must be quarantined. FTP must be blocked for files containing these names. There should be 4 matches before an incident is created. Matches should accumulate over 30 minutes.

Tasks

1. Create a custom policy.
2. Select the classifiers.
3. Set the threshold.
4. Select the action plan and severity.
5. Deploy your policy.
6. Test your policy.

5 The Forcepoint One Endpoint

5.1 Install and configure the Forcepoint One Endpoint and browser extension.

Scenario:

Your company is concerned about users copying sensitive data in Office documents to flash drives and leaking it outside the network. They want to retain control of an encryption process rather than putting it in the hands of the users

Tasks:

1. Download the latest version of the Forcepoint One Endpoint.
2. Extract the endpoint files to the DLP endpoint folder.
3. Build an endpoint package.
4. Install the endpoint package, and confirm it updates successfully.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Forcepoint Support Site
Use your credentials, or ask instructor.

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

5.1.1 Download the latest version of the Forcepoint One Endpoint

1. Sign in to the Security Manager Windows Desktop using the same Windows account used for the Websense Data Security Manager service (in your lab, this is *fpcert\Administrator*). Note that crypto keys are associated to this account.

2. On the **Security Manager** machine, open a web browser and navigate to: https://support.forcepoint.com/Downloads
3. Sign in with your support site credentials.
   If you do not have credentials for the site, ask the course instructor to provide you with the endpoint files.
4. Download the latest version of the Forcepoint One Endpoint Package Builder.

5.1.2 Extract the endpoint files to the DLP Endpoint folder

1. Open Windows File Explorer and browse to the DLP endpoint folder:
   C:\Program Files (x86)\Websense\Data Security\client
2. Copy the downloaded .zip file to this folder and extract the files.
   Make sure they do not extract into a new sub-folder.

5.1.3 Build an endpoint package

1. Double click the endpoint package builder file to run it, and create a new Windows Forcepoint DLP endpoint:
   C:\Program Files (x86)\Websense\Data Security\client\WebsenseEndpointPackageBuilder.exe
2. Save the newly created endpoint package to the network shared folder:
   C:\Forcepoint\My_Share

5.1.4 Install the endpoint package

1. On **Windows test machine**, locate the shared network folder *\\fp-sec-svr\my_share* from the **Security Manager** machine.
2. Copy the endpoint installer package from the shared folder to the desktop, then double click it to install the endpoint.
3. Reboot **Windows test machine**, and confirm the endpoint is running after the machine reboots.
4. Open the Endpoint UI from the system tray, and then click **Update**.
   Ensure the endpoint is able to connect and that the timestamp changes.

You should now be able to:

- Download the latest version of the Forcepoint One Endpoint.
- Extract the endpoint files to the DLP endpoint folder.
- Build an endpoint package.
- Install the endpoint package, and confirm it updates successfully.

5.2 Use the Forcepoint One Endpoint to encrypt files copied to removable media.

Scenario:

Your company is concerned about users copying sensitive data in Office documents to flash drives and leaking it outside the network. They want to retain control of an encryption process rather than putting it in the hands of the users.

You will need to configure a policy that will encrypt files copied to removable media, using a method that retains control of the encryption algorithm.

Tasks:

1. Create a policy to encrypt files using a profile key.
2. Test the policy by copying files to a virtual flash drive.
3. Confirm an incident was created and review the report.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

5.2.1 Create a policy to encrypt files using a profile key.

1. In your Go4Labs environment, resume the session in **mRemote** and access the **Security Manager** machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > DLP Policies > Manage Policies** in the left-hand menu bar.
3. Click **Add > Custom Policy** in the menu bar. Call the new policy “Flash Drive Encryption – Profile Key” and click **Next**.
4. Click **Add > File Properties** and select the classifier **Microsoft Office File – All Versions** from the list. Click **OK** to add it to the rule.

5. Click **Next** to proceed to **Severity and Action**.
6. Change the action plan for the rule to **Block Lan – Encrypt RM** that you created in the Resources module. Click **Finish** to save the new rule.
7. Click **Deploy** in the top right to send your changes to the endpoint server.

5.2.2 Test the policy by copying files to a virtual flash drive.

1. From the **Windows test machine**, open the endpoint UI from the system tray and click **Update**. Confirm that the endpoint receives the new policy version.
2. Copy the file *C:\Forcepoint\Test Files\common-health-conditions* to the virtual flash dive, *Removable Disk (F:)*.
   If everything was configured and updated successfully, you will be prompted for approval and the file will be encrypted.

5.2.3 Confirm an incident was created and review the report.

1. From the **Security Manager** machine, open the FSM and click on **Reporting > Data Loss Prevention > Incidents (Last 3 Days)**.
   Review the incident information and confirm your policies functioned as expected.

You should now be able to:

- Create a policy to encrypt files using a profile key.
- Test the policy by copying files to a virtual flash drive.
- Confirm an incident was created and review the report.

5.3 Temporarily bypass the Forcepoint One Endpoint.

Scenario:

A user in your company is attempting to copying files for a work order to a flash drive, but the files are being encrypted by a profile key, making them unusable for an external customer.

The user has requested that you bypass their endpoint temporarily to disable the file encryption.

Tasks:

1. Obtain the bypass request code.
2. Specify a time frame and generate the bypass code.
3. Activate the bypass on the endpoint.
4. Test the bypass by uploading a file.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

5.3.1 Obtain the bypass request code.

1. Begin on the **Windows test machine**.
2. Open the endpoint UI from the system tray and click **Disable** in the top left.
   A pop up will load with a bypass ID.

5.3.2 Specify a time frame and generate the bypass code.

1. Return to the **Security Manager** and click **Status > Endpoint Status > Bypass Endpoint**.
2. Set the bypass to last for 15 minutes and enter the Bypass ID from the endpoint.

3. Click **Generate Code**, and the page will refresh, showing a generated code next to the button.

5.3.3 Activate the bypass on the endpoint.

1. Return to the **Windows test machine** and paste the generated bypass code into the endpoint UI. Click **OK**.
2. The status of the endpoint shown under **Endpoint Settings** should now change to *disabled*.
3. Copy the file *C:\Forcepoint\Test Files\common-health-conditions* to the virtual flash dive, *Removable Disk (F:)*.
   If the endpoint was bypassed successfully, the file will now copy without prompting for approval or encrypting the file.

You should now be able to:

- Obtain the bypass request code.
- Specify a time frame and generate the bypass code.
- Activate the bypass on the endpoint.
- Test the bypass by uploading a file.

5.4 Configure the mode of the endpoint browser extension.

Scenario:

Users in your environment have been reporting system instability or slowness when using Chrome, and the suspected culprit is a proprietary extension conflicting with the DLP endpoint browser extension.

For troubleshooting purposes, you will temporarily switch the mode of the browser extension to monitoring for Chrome browsers.

Tasks:

1. Create a rule to test the browser extension.
2. Configure the Chrome endpoint browser extension to operate in Monitoring only mode.
3. Test the browser extension in Monitoring only mode.
4. Configure the browser extension to operate in Enabled mode.
5. Test the browser extension in Enabled mode.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

5.4.1 Create a rule to test the browser extension

1. Access the DLP Policy Management page: **Policy Management > DLP Policies > Manage Policies**.
2. Click the **Add** button and then select **Custom Policy**.
3. On the **General** tab, name the new policy “Browser Extension Test Policy”, and then click **Next**.

4. On the **Condition** tab, click the **Add** button, and choose **File Properties** to open the **Select a Content Classifier** window.
5. Find the **ZIP File** classifier in the list. (Optionally, use the **Filter by** text box to refine the list.) Select it and click **OK**.
6. Change the action plan to **Block All**. Then proceed to the **Destination** tab.
   Confirm that the check boxes in the **Web** section for **Endpoint HTTP** and **Endpoint HTTPS** are selected. Do not make any other changes to this tab.
7. Click **Finish** to complete creating the policy and rule.
8. Click **Yes** on the **Deployment Needed** pop-up window.

5.4.2 Configure the browser extension to operate in Monitoring only mode

1. On the **Security Manager** machine, open the DLP tab of Forcepoint Security Manager and navigate to: **Deployment > Endpoint Profiles**.
2. Click on **Default Profile**, then select the **Properties** tab.
3. In the **Forcepoint Browser Extension** section, change the **Chrome Extension Mode** to **Monitoring only**.
4. Click on **Save and Close**, then **Deploy**.

5.4.3 Test the browser extension in Monitoring only mode

1. On the **Windows test machine**, update the Forcepoint One Endpoint.
2. Confirm that the endpoint has received the update.
3. Open Chrome browser and navigate to *dataleaktest.com*.
4. Click **Upload Test** and upload *test_zip_file.zip* in *C:/Forcepoint/Data Class Resource Files*. The upload should succeed.
5. If you check incident reporting in Security Manager, there should be a new incident created with **Permitted** as the action.

5.4.4 Configure the browser extension to operate in Enabled mode

1. On the **Security Manager** machine, open the DLP tab of Forcepoint Security Manager and navigate to: **Deployment > Endpoint Profiles**.
2. Click on **Default Profile**, then select the **Properties** tab.
3. In the **Forcepoint Browser Extension** section, change the **Chrome Extension Mode** to **Enabled**.
4. Click on **Save and Close**, then **Deploy**.

5.4.5 Test the browser extension in Enabled mode

1. Confirm the endpoint receives the update.
2. Upload *test_zip_file.zip* again from **Windows test machine** to *dataleaktest.com*.
3. You should see a block warning. If you check incident reporting in Security Manager, there should be a new incident created with **Blocked** as the action.

You should now be able to:

- Create a rule to test the browser extension.
- Configure the Chrome endpoint browser extension to operate in Monitoring only mode.
- Test the browser extension in Monitoring only mode.
- Configure the browser extension to operate in Enabled mode.
- Test the browser extension in Enabled mode.

5.5 Enable and test the employee coaching feature.

Scenario:

A new company security policy requires that users receive immediate education about potential security breaches. You have been directed to enable the employee coaching feature at the endpoint level as one means of satisfying this request.

Tasks:

1. Enable the employee coaching feature.
2. Test the employee coaching feature.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

5.5.1 Enable the employee coaching feature.

1. On the **Security Manager** machine, open the DLP tab of Forcepoint Security Manager and navigate to: **Deployment > Endpoint Profiles**.
2. Click on **Default Profile**, then select the **Properties** tab.
3. In the **Interactive Mode Options** section, select the **Show incident details in the confirm dialog and the Log Viewer** option.
4. Click on **Save and Close**, then deploy.

5.5.2 Confirm the employee coaching feature functions correctly.

On the Security Manager:

1. Edit your *Browser Extension Test Policy* and edit the action plan to use the **Confirm** action for the endpoint HTTP/S channels.
2. Deploy your settings and confirm that the endpoint on **Windows test machine** receives the update.

On the Windows test machine:

1. Upload the *test.zip* file to *dataleaktest.com*.
2. The upload should cause a confirmation window to appear. Confirm that the window contains information regarding policies and number of violations. Select any reason and click **Allow**.
3. Confirm that an incident was created in incident reporting, and that it shows the **Continued (confirmed)** action.

You should now be able to:

- Enable the employee coaching feature.
- Test the employee coaching feature.

6 Implementing OCR Analysis

6.1 Configure a policy engine to work with an OCR server.

Scenario:

In this walk-through, you will enable OCR for the policy engine handling web traffic, in order to analyze potentially sensitive images uploaded over web channels.

Tasks:

- Enable OCR analysis for the web content gateway.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

MRSRV
Domain: fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Deployment > System Modules** in the left-hand menu bar.
3. Click the **+** icon to expand the entry for the **Forcepoint Content Gateway Server** and click on the **Policy Engine** component.
4. Check the box next to **Enable OCR by** to enable OCR analysis.
5. Click **OK** in the bottom right to save your changes.
6. Click **Deploy** in the top right to send the new configuration to the policy engine.

You should now be able to:

- Enable OCR analysis for the web content gateway.

6.2 Submit a transaction to the OCR engine and examine the results.

Scenario:

You will evaluate the function of the OCR server using a test image and examine the resulting incidents to confirm that all text was extracted successfully.

Tasks:

1. Submit a test transaction for OCR analysis.
2. Adjust the accuracy of the OCR server and retest.
3. Examine the created incident.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

MRSRV
Domain: fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

6.2.1 Submit a test transaction for OCR analysis.

1. From the Windows test machine, open a browser and navigate to http://dlptest.com/http-post/ .
2. Upload the file *C:\Forcepoint\Test Files\peter-piper-confidential.png*.
   The upload will not be blocked.

6.2.2 Adjust the accuracy of the OCR server and retest.

1. Return to the Security Manager and click **Deployment > System Modules** in the left-hand menu bar.
2. Click the **+** icon next to **Forcepoint DLP Server on DSS-Server.fpcert.com** to expand it, then click the **OCR Server** component.
3. Change the **Accuracy** setting from **Balanced** to **Accurate**. Click **OK** at the bottom right to save your change.
4. Deploy your changes.
5. Return to the Windows test machine and attempt again to upload *peter-piper-confidential.png*.
   The upload should now fail.

6.2.3 Examine the created incident.

1. Return to the Security Manager machine and click **Reporting > Data Loss Prevention > Incidents (Last 3 Days)** in the left-hand menu bar.
2. Inspect the created incident.

You should now be able to:

- Submit a test transaction for OCR analysis.
- Adjust the accuracy of the OCR server and retest.
- Examine the created incident.

7 Implementing Discovery

7.1 Configure and run a Forcepoint discovery policy and task

Scenario:

Your company handles intake and user data for medical practices, and you need to ensure that no Protected Health Information (PHI) belonging to patients exists outside of the correct repository.

Using a predefined PHI discovery policy and a configured endpoint discovery task, you will search for and generate a report on any misplaced PHI on an end user's machine.

Tasks:

1. Select and enable a predefined discovery policy to identify PHI.
2. Create an endpoint discovery task which will leverage the new policy.
3. Run the discovery task and wait for it to complete.
4. Generate a report on the result.
5. Analyze the report and navigate to the location of the identified sensitive data.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

7.1.1 Select and enable a predefined discovery policy to identify PHI.

1. On the **Security Manager** machine, sign in to Forcepoint Security Manager and go to **Data > Policy Management > Discovery Policies > Manage Policies**.
2. Click **Add > Predefined Policy** in the menu bar.

3. Select **USA** for the region, **Healthcare & Pharma** for the industry, then click **Finish** to display those policies. Enable the **PHI: Protected Health Information** policy.
4. Click **Use Policies** in the bottom right to save your changes and return to the **Manage Discovery Policies** page. Do not deploy.
5. Navigate to **Policy Management > Discovery Policies > Endpoint Discovery Tasks**. Click **New** to create a new task.
6. Name this task “Out of Place PHI” and click **Next** to proceed to the **Endpoint Hosts** step.

7.1.2 Create an endpoint discovery task which will leverage the new policy.

1. Leave the endpoint host selection set to **All**. Click **Next** to proceed to the **Scheduler** tab.
2. Change the Run Scan setting to **Once** to make the task run manually rather than on a schedule. Make sure to uncheck the option for **Scan only when computer is idle**. Click **Next**.
3. Leave the policy selection set to **All discovery policies**. Click **Next** to proceed to the **File Filtering** tab.
4. Check **Filter by Type**.
5. Click **File Types** to open the file type selection window. Select **Office Documents** and click **OK**.
6. Click **Finish** to save the configured task.

7.1.3 Run the discovery task and wait for it to complete.

1. Click **Deploy** to deploy your changes.
2. On the **Windows test machine**, open the endpoint UI and click **Update**.
   Confirm that the timestamp changes, and that the endpoint displays a running discovery task.

7.1.4 Generate a report on the result.

1. It is possible to review incoming incidents before the scan is complete.
   On the **Security Manager** machine, navigate to **Reporting > Discovery > Incidents**.
2. Browse through the incidents shown and look for files matching the PHI policies.
   Note the file path in the **Properties** tab.

7.1.5 Analyze the report and navigate to the location of the identified sensitive data.

1. On the **Windows test machine**, browse to *C:\Users\administrator\Documents\saved data\misc forms* and delete only the identified files containing PHI.

You should now be able to:

- Select and enable a predefined discovery policy to identify PHI.
- Create an endpoint discovery task which will leverage the new policy.
- Run the discovery task and wait for it to complete.
- Generate a report on the result.
- Analyze the report and navigate to the location of the identified sensitive data.

8 Analyzing DLP Incidents and Reports

8.1 Perform a remediation operation on a batch of incidents.

Scenario:

A new DLP policy in your environment has produced an unexpectedly large number of incidents in a short period of time. You need to remediate these incidents altogether, and in a manner that will allow to you continue working on your other assigned projects.

Tasks:

1. Run the provided script to generate incidents.
2. Open an incident report.
3. Select all incidents created by a specific policy.
4. Run a batch operation on the selected incidents.
5. Confirm the desired changes have been made.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

8.1.1 Run the provided script to generate incidents

1. Earlier in this unit, you created a rule to detect zip files (Browser extension test policy). Confirm that this rule is enabled and deployed.
2. On the **Security Manager** machine, locate the file: *C:\Forcepoint\Data Security Resource Files\bulk_incident_creation.bat*
3. Right click the file and select **Run as Administrator**.
   A command prompt window will open and execute a series of commands. Wait for the script to complete and the command prompt window to disappear.

8.1.2 Open an incident report

1. While still on the **Security Manager** machine, access the DLP Security Manager.
2. Open an incident report: **Reporting > Data Loss Prevention > Incidents (last 3 days)**.

8.1.3 Select all incidents created by a specific policy

1. Using the arrow button in the column header, filter the **Policies** column to show only incidents created by the .zip file detection policy (Browser Extension test policy).

8.1.4 Run a batch operation on the selected incidents

1. Click on **Workflow**, then **Change Status**. Choose **Change Status > Closed** to mark these incidents as resolved.
2. When the **Change Status** batch operation pop-up window appears, select **All Filtered Incidents** and then click **OK**.

8.1.5 Confirm the desired changes have been made.

1. Wait for the **Batch action completed successfully** message to appear, then click on **Refresh** to update the report.
2. Confirm that the status of the selected incidents has changed to **closed**.

You should now be able to:

- Run a script to generate incidents.
- Open an incident report.
- Select all incidents created by a specific policy.
- Run a batch operation on the selected incidents.
- Confirm the desired changes have been made.

8.2 Exercise: Perform each UI-based incident workflow action

Scenario:

You are responsible for monitoring the incidents that are reported by Forcepoint DLP. Without step-by-step instructions, perform workflow actions on reported incidents.

Tasks:

1. Filter the Incident List to show new incidents.
2. Change the status of 5 incidents to “In Process”.
3. Change the severity of 3 incidents.
4. Mark one of the incidents as an ignored incident.
5. Close 2 incidents.
6. View the history chain of the incidents.

It does not matter which incidents you chose to update.

9 Creating Fingerprinting and Machine Learning Classifiers

9.1 Create file fingerprint classifiers

Scenario:

In this walk-through, you will create a file fingerprint classifier and apply it to a DLP policy. You will then create a policy with the newly created classifier and test it.

Tasks:

1. Create a file fingerprint classifier.
2. Create a file fingerprint policy.
3. Test the file fingerprinting policy.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

9.1.1 Create a file fingerprint classifier

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Content Classifiers > File Fingerprinting** in the left-hand menu bar.
3. Click **New > File System Fingerprinting** in the File Fingerprinting menu bar.
4. Enter a name for the fingerprinting classifier: “Books”
   Note the options available for Crawler and Fingerprinting Mode, but leave the options on their default setting.

5. Click **Next** in the bottom right to move onto the next step.
6. Open Windows File Explorer, navigate to *C:\Forcepoint\My_Share\class_files* and right click on the *fingerprinting-unstructured* folder. Select the **Sharing** tab, and copy the **Network Path**:
   \\FP-SEC-SVR\My_Share\class_files\fingerprinting-unstructured
7. Copy the network path information to Root folder: *\\FP-SEC-SVR\My_Share\class_files\fingerprinting- unstructured* and enter the administrator login information into the **Network Credentials** section.

   User name: administrator
   Password: Forcepoint1!
   Domain: fpcert
8. Click **Next** again and then select **Edit**.
9. Select the checkbox next to the root folder and remove it from the list of folders to include by clicking on the **Left Arrow** button.
10. Select the checkbox next to **books** and add it to the list of folders to include by clicking on the **Right Arrow** button. Click **OK** and then **Next**.
11. Next to **Run Scan** select **Once** from the dropdown. Click **Next**.
12. Select the checkbox next to **Filter by Type**.
13. Click on the **File Types** button.
14. Select the checkbox next to **Office Documents**. Click **OK**.
15. Click on the **Finish** button.
16. Select **Cancel** to the dialog box prompting to add the classifier to a policy.
17. Click the **Start** button to begin the fingerprinting task.
18. Once the fingerprinting task is completed, verify the number of files that have been fingerprinted.

9.1.2 Create a file fingerprint policy

1. Navigate to **Policy Management > DLP Policies > Manage Policies**.
2. Click **Add** and then select **Custom Policy**.
3. Enter a name for the policy: “Book Fingerprint” and click **Next**.
4. Click **Add** and then **Fingerprinting**.
5. Select the fingerprint classifier that was just created, click **OK**, and then **Next**.
6. Select **Block All** as the action plan from the dropdown and select **Finish**.
7. Click **Yes** to deploy the policy.

9.1.3 Test the file fingerprinting policy

1. In **mRemote**, open a session to the **Windows test machine**.
2. Open **Outlook** and create a new email message to an external email address.
3. Attach the file *Gullivers Travels* from *My Share (Z:)\class_files\fingerprinting-unstructured\books* and click **Send**.
4. In **mRemote**, access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.

5. Click **Reporting > Data Loss Prevention > Incidents (last 3 days)**.
6. Investigate the **Network email** incident created from the file fingerprinting policy violation.

You should now be able to:

- Create a file fingerprint classifier.
- Create a file fingerprint policy.
- Test the file fingerprinting policy.

9.2 Create database fingerprint classifiers

Scenario:

In this walk-through, you will create a database fingerprint classifier and apply it to a DLP policy. You will then create a policy with the newly created classifier and test it.

Tasks:

1. Create a database fingerprint classifier.
2. Create a database fingerprint policy.
3. Test the database fingerprint policy.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

9.2.1 Create a database fingerprint classifier

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click **Policy Management > Content Classifiers > Database Fingerprinting** in the left-hand menu bar.
3. Click **New > CSV File Fingerprinting** in the Database Fingerprinting menu bar.
4. Enter a name for the fingerprinting classifier: “DB Fingerprint”
   Note the options available for the crawler, but leave the option on the default setting.
5. Click **Next** in the bottom right to move onto the next step.
6. Open Windows File Explorer, navigate to *C:\Forcepoint\My_Share\class_files\fingerprinting-structured* and right click on the *csv* folder, select the **Sharing**, and copy the **Network Path**: *\\FP-SEC-SVR\My_Share\class_files\fingerprinting-structured\csv*

7. Enter the administrator login information into the **Network Credentials** section.

   User name: administrator
   Password: Forcepoint1!
   Domain: fpcert

8. Copy the network path information *\\FP-SEC-SVR\My_Share\class_files\fingerprinting-structured\csv* and then click **Browse**.
9. Select the **Customer Records.csv** file and click **OK**. Click **Next**.
10. From the **Available Fields** box select **CustomerID**, **SSN**, **ContactName**, **Credit Card** and click **Next**.
11. Next to **Run Scan** select **Once** from the dropdown. Click **Next**.
12. Leave the radial button next to **Full Fingerprinting** but take note of the ability to perform differential fingerprints on a database.
13. Click on the **Finish** button.
14. Select **Cancel** to the dialog box prompting to add the classifier to a policy.
15. Click the **Start** button to begin the fingerprinting task.

9.2.2 Create a database fingerprint policy

1. Once the fingerprinting task is complete, navigate to **Policy Management > DLP Policies > Manage Policies**.
2. Click **Add** and then select **Custom Policy**.
3. Enter a name for the policy: “Customer DB Fingerprint” and click **Next**.
4. Click **Add** and then **Fingerprinting**.
5. Select the database classifier that was just created, select the checkbox next to **Field Name**, click **OK**, and then **Next**.
6. Select **Block All** as the action plan from the dropdown and select **Finish**.
7. Click **Yes** to deploy the policy.

9.2.3 Test the database fingerprint policy

1. In **mRemote**, open a session to the **Windows test machine**.
2. Open **Outlook** and create a new email message to an external email address.
3. Attach the file *Customer Records.xls* from *My Share (Z:)\class_files\fingerprinting-structured\csv* and click **Send**.
4. In **mRemote**, access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
5. Click **Reporting > Data Loss Prevention > Incidents (last 3 days)**.
6. Investigate the **Network email** incident created from the database fingerprint policy violation.

You should now be able to:

- Create a database fingerprint classifier.
- Create a database fingerprint policy.
- Test the database fingerprint policy.

10 Importing File Tagging Labels

10.1 Integrate Boldon James into the DLP data labeling framework

Scenario:

Your company wants to use the Boldon James Classifier system to manage sensitivity levels of files.

Tasks:

1. Select which type of file labeling system to use.
2. Import the file labeling tags.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

10.1.1 Select which type of file labeling system to use

1. On the **Security Manager** machine, sign in to Forcepoint Security Manager and go to **Data > Settings > General > Services**.
2. Select the **File Labeling** tab.
3. Select **Boldon James Classifier** from the list.

10.1.2 Import the file labeling tags

1. Click the **Import Labels** button to import the Boldon James labels.
2. Click the **Choose File** button and select the file to import.
3. Choose the file *spif.xml* located in the *Boldon James spif.xml* folder, which is located on the desktop of the **Security Manager** machine.
4. You should now see a list of the labels that have been imported.

5. If you have not imported labels for Boldon James Classifier (or Microsoft Information Protection), a message displays to indicate that you must first import labels before selecting labels for detection.
6. Select the **Apply file labels** check box to define DLP action plans using Boldon James Classifier file labels.
7. Click the **OK** button. Do not deploy.

You should now be able to:

- Select which type of file labeling system to use.
- Import the file labeling tags.

10.2 Create a file labeling classifier to manage sensitive or proprietary information

Scenario:

You need to enable and configure this file classifier system.

Tasks:

- Select which file labeling tags to assign.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

1. Go to **Data > Policy Management > Content Classifier > File Labeling** and select **New**. The **File Labeling Properties** page opens.
   Note: The file labeling also keeps track of deleted labels, so they can still be used if these labels are still assigned to files within the system.
2. On the **File Labeling Properties** page, enter “Boldon James” as the name of the classifier.
3. Select **Boldon James Classifier** from the drop-down list of **Labeling systems**.
4. After selecting **Boldon James Classifier**, a list of the imported labels appears. Select the labels to use in the classifier (select all the labels), then click the right arrow to move the selected labels to the **Detected Labels** list.
5. Click the **OK** button to return to the **File Labeling** screen. Click **Cancel**.

You should now be able to:

- Select which file labeling tags to assign.

10.3 Create and deploy a data usage policy using file labeling classifiers

Scenario:

You need to verify the system allows Forcepoint DLP to import labels for detection.

Tasks:

- Create a policy using a file labeling classifier.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

1. Go to **Data > Policy Management > Content Classifier > File Labeling**. Select your *Boldon James* classifier and click **Create Rule from Classifier**.
2. Enter “Boldon James” as the name for your new rule.
3. Select **Add this rule to a new policy** and enter “Boldon James” as the policy name.
4. Click **OK** to create the new rule and policy.
5. Click **Deploy** to deploy your changes.
6. Verify that your new policy has been created from the **Manage DLP Policies** page (**Data > Policy Management > DLP Policies > Manage Policies**).
7. If necessary, click on the **Boldon James** rule to edit the Severity & Action, Source, or Destination settings for the rule.

You should now be able to:

- Create a policy using a file labeling classifier.

10.4 Create and deploy a discovery policy to assign file classification labels

Scenario:

You need to create a policy to label all files that contain the word “Confidential” with the Boldon James Classification “Confidential” label.

Tasks:

- Create an endpoint discovery policy to label files.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

1. Go to **Data > Policy Management > Discovery Policies > Manage Policies** and click **Add > Custom Policy** to create a new Endpoint Discovery policy
2. Enter “BJ Confidential” for the **Policy name**.
3. Ensure that the **Use the policy name for the rule name** option is selected.
4. Click **Next**.
5. Select **Add > Patterns & Phrases** from the drop-down menu.
6. The **Select a Content Classifier** window opens.
7. Select **New > Key Phrase** from the drop-down menu.
8. In the **Add Key Phrase** window, enter “Confidential” for the **Name** and **Phrase to search**.
9. Click **OK** to return to the **Select a Content Classifier** window.
10. Select “Confidential” from the **Content Classifier List**.
11. Click **OK** to return to the **Manage Discovery Policies > Policy Rule** screen.
12. Click **Next** to configure **Severity & Action**.
13. Click on the edit icon for the first **Action Plan** to bring up the **Action Plan Details** window.
14. Click on the **Discovery** tab in the **Action Plan Details** window.
15. In the **Endpoint Discovery** section, select **Apply file labels**.
16. Select the **Labeling system**: *Boldon James Classifier* from the drop-down list.
17. Select the **Label**: *Classification: Confidential*
18. Click the **Add** button.

19. Click **OK** to return to the **Manage Discovery Policies > Policy Rule** screen.
20. Do not deploy your changes yet.
21. Click **Finish**.
22. Deploy your changes.

You should now be able to:

- Create an endpoint discovery policy to label files.

10.5 Exercise: Create a discovery task to apply labels

Scenario:

You need to create a discovery task to label all files that contain the key phrase “Confidential” with the Boldon James Classification “Confidential” label

Tasks:

1. Use the discovery policy that you have created to create a discovery task.
2. Run the task.

11 Managing Delegated Administrators

11.1 Configure a delegated administrator to have role-based permissions.

Scenario:

A new frontline DLP analyst has been hired for your team, and you need to create a delegated administrator role for the user that maintains regulatory compliance.

Tasks:

1. Create a new administrator account and assign it to the DLP product.
2. Create a delegated administrator role.
3. Assign the new role to the new administrator account.
4. Test the new account to confirm it functions as expected.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

11.1.1 Create a new administrator account and assign it to the DLP product.

1. In your Go4Labs environment, resume the session in **mRemote** and access the Security Manager machine. Navigate to the **Data** tab of Forcepoint Security Manager.
2. Click the gear icon for **Global** Settings in the in the top-right corner.
3. Click **General > Administrators** in the left side menu bar.
4. Click **Add Local Account** at the bottom, and the creation wizard will load.

5. Configure the new administrator.

   User name: tmuller
   Email address: tmuller@fpcert.com
   Uncheck *Global Security Administrator*
   Assign access to only the *Data* product only under **Module Access Permissions**.
   Set the new admin's password to Forcepoint1!

6. Click **OK** to save the new administrator.

11.1.2 Create a delegated administrator role.

1. Return to the **Data** tab and click **Authorization > Roles** in the left side menu bar.
2. Create a customized role called **Analyst** and select permissions as you see fit. Also select:

   Check **Hide Source and Destination**.
   Uncheck *Traffic Log*, *System Log*, and *Audit Log*.
   Uncheck *Authorization*.
   Uncheck *Manage system modules*, *Manage endpoint profiles*, and *Deploy settings*.

3. Click **OK** to save the new role settings.

11.1.3 Assign the new role to the new administrator account.

1. Click **Authorization > Administrators** in the left side menu.
2. Click **Tmuller** in the list to access that administrator's settings.
3. Assign the newly created *Analyst* role to the administrator account. Click on **OK** to save your changes.
4. Sign out of the FSM, and sign in again using the new tmuller administrator account. Observe the changes to the UI and incident reporting.

You should now be able to:

- Create a new administrator account and assign it to the DLP product.
- Create a delegated administrator role.
- Assign the new role to the new administrator account.
- Test the new account to confirm it functions as expected.

12 Monitoring System Health

12.1 Configure and perform a DLP backup task

Scenario:

Your fully configured and functional DLP environment requires one last step to be compliant – system protection in the form of restorable backups.

While taking snapshots of virtual machines is an excellent option, you need to provide an extra layer of redundancy by configuring and running the Forcepoint DLP backup task.

Tasks:

1. Create a folder for the backup location.
2. Configure the backup task from the security manager.
3. Enable the Windows task scheduler task and run the backup.
4. Confirm the backup completed successfully.

Environment Credentials:

Go4labs information sent via instructor
Site: (generatedname).go4labs.net
Username: generatedfirst.generatedlast
Password: generated

Security Manager Server
Domain: Fpcert
Username: Administrator
Password: Forcepoint1!

Windows Test Machine
Domain: fpcert
Username: tmuller
Password: Forcepoint1!

Security Manager UI
Username: admin
Password: Forcepoint1!

12.1.1 Create a folder for the backup location.

1. On the Security Manager machine, create a new folder: *C:\Forcepoint\My_Share\backup*.
2. Open the folder properties for the new folder and confirm that all users have full read/write access. Copy the network path.

12.1.2 Configure the backup task from the security manager.

1. Sign in to Forcepoint Security Manager and navigate to **Data > Settings > General > Backup**.
2. Configure the backup task. Enter the network path.

   Domain: fpcert.com
   User name: Administrator
   Password: Forcepoint1!

   Select **Do Not Include Forensics** at the bottom. Click **OK** to save your changes.

12.1.3 Enable the Windows task scheduler task and run the backup.

1. Open Windows **Task Scheduler**. An easy way to locate it is to search for *Task Scheduler* using the windows magnifying glass in the task bar.
2. Click on **Task Scheduler Library** and locate **Websense Triton AP-Data Backup** in the list of tasks.
3. Right click the **Websense Triton AP-Data Backup** task and click **Enable**.
4. Right click the task a second time and click **Run**.
   The status of the task should change to **Running**.

12.1.4 Confirm the backup completed successfully.

1. Navigate to the folder you created for the backup and confirm that a folder named **DSSBackup** has been created.
2. Open the folder and explore the backup folder structure.

You should now be able to:

- Create a folder for the backup location.
- Configure the backup task from the security manager.
- Enable the Windows task scheduler task and run the backup.
- Confirm the backup completed successfully.