

```
#####
Lab 09 - Implementing DLP & Anti-Malware Policies
Exercise 1 - Implementing Data Loss Prevention (DLP)
#####
```

Overview:

In this exercise, we will implement **Data Loss Prevention (DLP)** policies in Exchange Server using both the **Exchange Admin Center (EAC)** and **Exchange Management Shell (EMS)**. These policies allow administrators to detect, monitor, and act on email content that includes sensitive information such as **credit card numbers, Canadian personal health data, and financial data**.

We will **begin** by **using** the **EAC** to create DLP policies from **built-in templates** as well as configure **custom rules** that trigger actions or warnings. Then, we will **switch** to **PowerShell-based EMS configuration** to script similar policies and link them to **transport rules** for automated content scanning. By the **end** of this lab, you'll have a **clear** understanding of how to deploy, customize, and validate DLP strategies across your Exchange environment.

Exercise 1 - Task 1: Create a DLP Policy from a Template (EAC)

Objective:

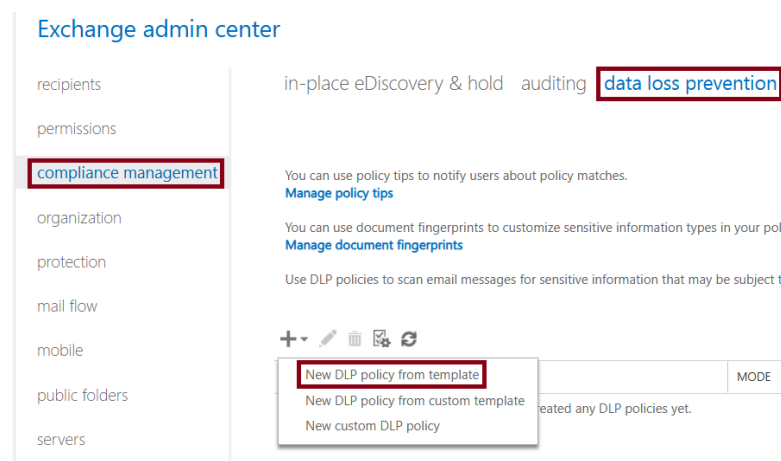
Use the Exchange Admin Center (EAC) to create a new **Data Loss Prevention (DLP)** policy using a predefined Canadian PII template. This task introduces how to deploy content-inspection policies for sensitive data such as Social Insurance Numbers and credit card numbers in a non-enforcing mode for testing.

Action:

Create a new DLP policy using a built-in template and configure it to test and display Policy Tips to users.

Navigation:

1. Open **Exchange Admin Center (EAC)** via browser → <https://ad07.domain07.local/ecp> or your Exchange Servers URL.
2. In the left-hand menu, click **Compliance Management**.
3. Select the **Data Loss Prevention** tab.
4. Click the **plus (+)** button → Choose **New DLP Policy from Template**.



Configuration:

- **Name**: Confidential Info - Canada
- **Template**: Canada Personally Identifiable Information (PII)
- **Mode**: Test with Policy Tips

DLP policy from template

Confidential Info - Canada

Description:
This DLP policy monitors emails for Canadian Personally Identifiable Information (PII) such as SINs, government IDs, and financial data.

*Choose a template:

Australia Financial Data

Australia Health Records Act (HRIP Act)

Australia Personally Identifiable Information (PII) Data

Australia Privacy Act

Canada Financial Data

Canada Health Information Act (HIA)

Canada Personal Health Act (PHIPA) - Ontario

Canada Personal Health Information Act (PHIA) - Manitoba

Canada Personal Information Protection Act (PIPA)

Canada Personal Information Protection Act (PIPEDA)

Canada Personally Identifiable Information (PII) Data

France Data Protection Act

France Financial Data

France Personally Identifiable Information (PII) Data

Canada Personally Identifiable Information (PII) Data 15.0.3.0

Helps detect the presence of information commonly considered to be personally identifiable information (PII) in Canada, like health ID number and social insurance number. Use of this policy does not ensure compliance with any regulation. After your testing is complete, make the necessary configuration changes in Exchange so the transmission of information complies with your organization's policies. Examples include configuring TLS with known business partners or adding more restrictive transport rule actions, such as adding rights protection to messages that contain this type of data.

Find more DLP policy templates from Microsoft partners. [Learn more](#)

Choose the state of this DLP policy:

☒ Enabled

☐ Disabled

Choose a mode for the requirements in this DLP policy:

☐ Enforce

☒ Test DLP policy with Policy Tips

Explanation:

This step creates a **template-based DLP policy** designed to detect Canadian Personally Identifiable Information (PII), including Social Insurance Numbers and government-issued IDs.

By setting the **enforcement mode** to "Test with Policy Tips", the policy will **not block email messages**, but will **alert the sender** with an in-app notification banner when a potential policy violation is detected. This is a recommended practice **for** evaluating the impact of DLP policies **in** a live environment without disrupting user communication.

Validation:

After saving the policy, ensure it appears **in** the **DLP policy list**.

Verify:

- **Name**: Confidential Info - Canada
- **Template**: Canada Personally Identifiable Information (PII)
- **Mode**: Test with Policy Tips

Exercise 1 – Task 2: Add a Custom Rule to the DLP Policy (EAC)
#####

Objective:

Modify the existing DLP policy "Confidential Info - Canada" to include a custom rule that detects sensitive **data** (e.g., PII or credit card numbers) **in** outgoing messages and ****warns the sender** if** the email is being sent ****outside the organization****.

Action:

Create a new custom rule under the existing DLP policy to apply warnings when sensitive **data** is detected **in** messages sent externally.

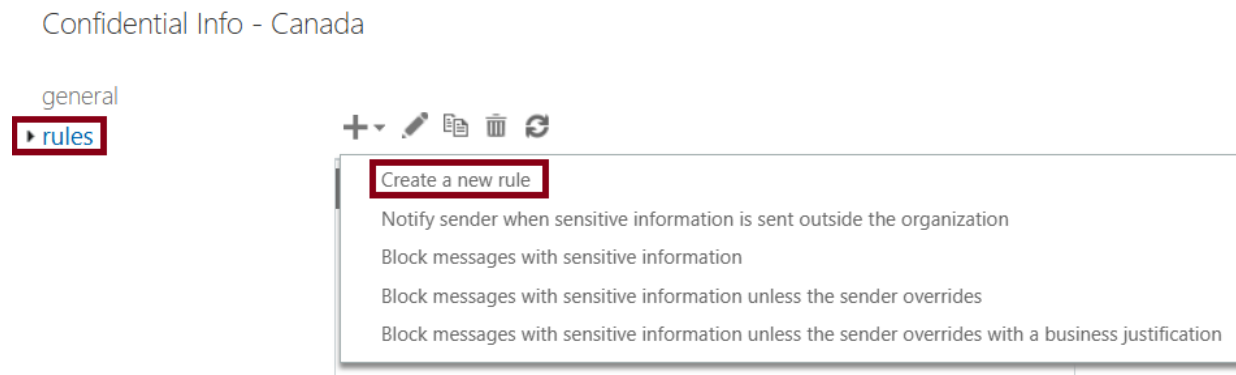
Navigation:

1. Open ****Exchange Admin Center**** at:
`https://ad07.domain07.local/ecp`
2. Go to ****Compliance Management**** → ****Data Loss Prevention****
3. Double-click the DLP policy named ****Confidential Info - Canada****



+ - ✎ 🗑️ 🔄		
ON	NAME	MODE
✓	Confidential Info - Canada	Testing with Policy Tips

4. **In** the ****Rules**** tab, click the ****plus (+)**** icon → Choose ****Create a new rule****



Confidential Info - Canada

general

rules

+ - ✎ 🗑️ 🔄

Create a new rule

Notify sender when sensitive information is sent outside the organization

Block messages with sensitive information

Block messages with sensitive information unless the sender overrides

Block messages with sensitive information unless the sender overrides with a business justification

5. Configure the rule as follows:

Configuration:

- **Name**: `External PII Warning`
- **Apply this rule if...**:
 - `The recipient is located...` → `Outside the organization`
 - `The message contains any of these sensitive information types...`
→ `Canada Social Insurance Number` or `Canada Bank Account Number`
- **Do the following...**:
 - `Notify the sender with a Policy Tip`
→ `Notify the sender, but allow them to send`
- **Except if...**: `(Leave blank – no exception)`
- **Audit this rule with severity level**: `High`
- **Choose a mode for this rule**: `Test with Policy Tips`
- **Activate this rule on the following date**: `Tue 7/1/2025 - 11:30 AM`
- **Deactivate this rule on the following date**: `Wed 7/1/2026 - 11:30 AM`
- **Match sender address in message**: `Header`
- **Comments**:
`Warns sender when PII is found in outbound emails.`

new rule

Name:

*Apply this rule if...

☒ The recipient is located...

and

☒ The message contains any of these sensitive information types...

*Do the following...

Except if...

Properties of this rule:

☒ Audit this rule with severity level:

Choose a mode for this rule:

☐ Enforce

☒ Test with Policy Tips

☐ Test without Policy Tips

☒ Activate this rule on the following date:

☒ Deactivate this rule on the following date:

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:

Comments:

Explanation:

This rule enhances the existing DLP policy by **detecting outbound emails containing sensitive information** and **alerting the sender before they send the message externally**.

This does not block the message – it simply displays a ****Policy Tip****, encouraging awareness of organizational compliance policies.

This proactive step helps reduce accidental **data** leakage **while** building user accountability.

Validation:

Once saved, the new rule ****External PII Warning**** should appear under the Rules tab of the ****Confidential Info - Canada**** policy.

Verify the rule:

- Triggers on external recipients
- Is tied to sensitive **data** types
- Uses ****Policy Tip**** notification
- Remains **in **Test mode**** for safe evaluation

Confidential Info - Canada

general

- rules

- ☒ Canada PII: Allow override
- ☒ Canada PII: Scan email sent outside - low count
- ☒ Canada PII: Scan email sent outside - high count
- ☒ Canada PII: Scan text limit exceeded
- ☒ Canada PII: Attachment not supported
- ☒ **External PII Warning**

1 selected of 6 total

External PII Warning

If the message...

Is sent to 'Outside the organization'
and The message contains any of these sensitive information types: 'Canada Social Insurance Number' or 'Canada Bank Account Number'

Do the following...

Set audit severity level to 'High'
and Notify the sender that the message violates a DLP policy, but send the message

Policy group membership

Confidential Info - Canada

Rule comments

Warns sender when PII is found in outbound emails.

Rule mode

Audit and notify

Additional properties

Activation date: 7/1/2025 11:30 AM

Expiry date: 7/1/2026 11:30 AM

Sender address matches: Header

Exercise 1 – Task 3: Create a Custom DLP Policy from Scratch (EAC)

Objective:

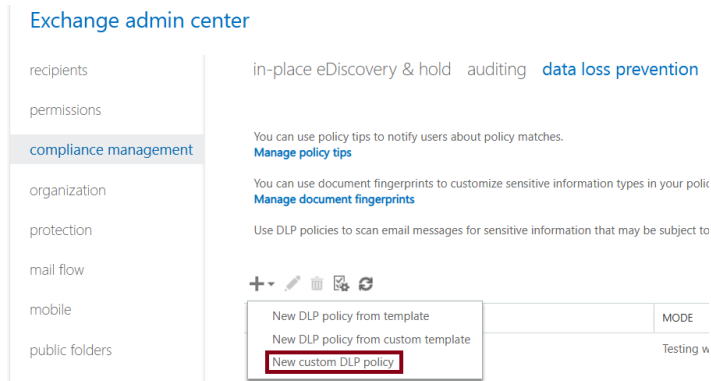
Create a new **Data Loss Prevention (DLP)** policy from scratch **using** the Exchange Admin Center. This custom policy will detect ****credit card numbers**** **in** outgoing messages, ****block the email****, but allow the sender to ****override the block**** **if** a valid business justification is provided.

Action:

Use the EAC to define a custom policy and configure a rule that applies strict control over sensitive financial **data while** offering a controlled override option.

Navigation:

1. Go to ****https://ad07.domain07.local/ecp****
2. Open ****Compliance Management**** → ****Data Loss Prevention****
3. Click ****+**** → **Select **New Custom DLP Policy (without template)****



4. Fill **in** the following fields:
 - ****Name****: `Custom Credit Card **Filter**`
 - ****Description**** (optional):
`Blocks messages containing credit card numbers unless a business justification is provided.`

new custom DLP policy

*Name:

Description:

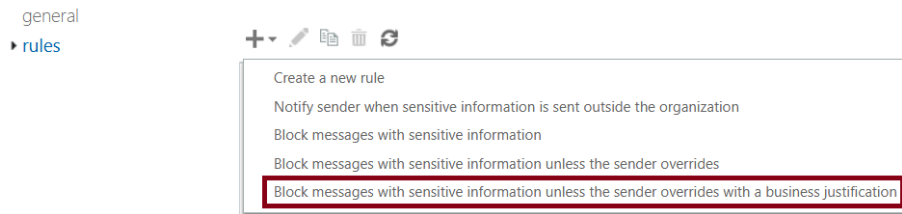
Choose the state of this DLP policy:
☒ Enabled
☐ Disabled

Choose a mode for the requirements in this DLP policy:
☐ Enforce
☐ Test DLP policy with Policy Tips
☒ Test DLP policy without Policy Tips

- Click ****Save****

5. After saving, double-click the new policy and go to the **Rules** tab
6. Click **+** → **Select** **Block messages with sensitive content unless the sender provides a business justification**

Custom Credit Card Filter



Configuration:

- **Rule Name**: `Block Credit Card with Override`
- **Apply this rule if...:**
 - `The recipient is located...` → `Outside the organization`
 - Click **Add condition** and **select**:
 - `The message contains any of these sensitive information types...`
 - **In** the selection dialog, choose: `Credit Card Number`
- **Do the following...:**
 - `Block the message, but allow the sender to override with a business justification and send`
 - (Optional but recommended) Click **Add action** and **select**:
 - `Generate incident report and send it to...`
 - Choose `Administrator` or an appropriate monitoring address
 - Use `Custom content` **for** the report **if** needed
- **Audit this rule with severity level**: `High`
- **Choose a mode for this rule**: `Enforce`
- **Activate this rule on**: ***(Optional)*** You may leave this unchecked or choose a valid future date
- **Deactivate this rule on**: ***(Optional)*** Leave unchecked unless the rule is temporary
- **Match sender address in message**: `Header` ***(Default, no change needed)***
- **Comments**:
 - `Blocks messages with credit card numbers unless sender provides justification. Incident report sent to administrator.`

new rule

Name:
Block Credit Card with Override

*Apply this rule if...

✖ The recipient is located...
Outside the organization

and

✖ The message contains any of these sensitive information types...
'Credit Card Number'

add condition

*Do the following...

✖ Generate incident report and send it to...
Send incident report to: Administrator, with content: Custom content

and

✖ Notify the sender with a Policy Tip...
Block the message, but allow the sender to override with a business justification and send

add action

Except if...

add exception

☐ Stop processing more rules
☐ Defer the message if rule processing doesn't complete

Match sender address in message:
Header

Comments:
Blocks messages with credit card numbers unless sender provides justification. Incident report sent to administrator.

Properties of this rule:

☒ Audit this rule with severity level:
High

Choose a mode for this rule:
☒ Enforce
☐ Test with Policy Tips
☐ Test without Policy Tips

☒ Activate this rule on the following date:
Tue 7/1/2025 7:00 PM

☒ Deactivate this rule on the following date:
Wed 7/1/2026 7:00 PM

Explanation:

This **configuration** uses a **custom DLP policy** to implement a strict but flexible control over **credit card numbers**. The system will:

- **Detect financial data** using Microsoft's built-in **data** classification engine

- **Block transmission** by default

- **Allow override** if the sender includes a justification, giving flexibility for legitimate business needs

This approach balances **security** and **business continuity** and is useful in financial services, HR, and legal teams.

Validation:

After saving the rule, ensure it appears under the **Rules** tab in the "Custom Credit Card Filter" policy. Validate:

- The condition targets **credit card numbers**
- The **block action** is present
- **Override with justification** is enabled
- Mode is **Enforce**

Block Credit Card with Override

If the message...

Is sent to 'Outside the organization' and The message contains any of these sensitive information types: 'Credit Card Number'

Do the following...

Set audit severity level to 'High' and Notify the sender that the message can't be sent, but allow the sender to override and provide justification. Include the explanation 'Delivery not authorized, message refused' with status code '5.7.1' and Send the incident report to _@domain07.ca, include these message properties in the report: original mail

[View the Incident management mailbox](#)

Policy group membership

Custom Credit Card Filter

Rule comments

Blocks messages with credit card numbers unless sender provides justification.
Incident report sent to administrator.

Rule mode

Enforce

Additional properties

Activation date: 7/1/2025 7:00 PM
Expiry date: 7/1/2026 7:00 PM
Sender address matches: Header

Exercise 1 – Task 4: Review and Analyze All DLP Policies and Rules (EAC)
#####

Objective:

Verify that all previously created **Data** Loss Prevention (DLP) policies and custom rules are properly configured **in** the Exchange Admin Center. This task ensures visibility into how each rule functions, how they are enforced, and whether they meet the intended security objectives.

Action:

Inspect and validate each DLP policy, checking their:

- Name and enforcement mode
- Assigned sensitive information types
- Conditions, actions, and exceptions (**if** any)
- Audit severity
- Rule behavior (e.g., test vs enforce, notification **type**)

Navigation:

1. Go to ****https://ad07.domain07.local/ecp****
2. Open ****Compliance Management**** → ****Data** Loss Prevention******
3. **In** the DLP policies list, confirm that the following appear:

- `Confidential Info - Canada` (Template: Canada PII, Mode: Test with Policy Tips)
- `Custom Credit Card **Filter**` (Custom Policy, Mode: Enforce)

4. Double-click each policy to review details **in** the ****Rules**** tab

ON	NAME	MODE
<input checked="" type="checkbox"/>	Confidential Info - Canada	Testing with Policy Tips
<input checked="" type="checkbox"/>	Custom Credit Card Filter	Enforcing

Custom Credit Card Filter

Blocks messages containing credit card numbers unless a business justification is provided.

Policy Mode

Enforcing

Test without Policy Tips

Test with Policy Tips

Version: 15.00.0002.000

Validation Steps:

****A. Confidential Info - Canada****

- ****Rule****: `External PII Warning`
- ****Conditions****:
 - Recipient is ****Outside the organization****
 - Contains ****Canada Social Insurance Number**** or ****Canada Bank Account Number****
- ****Action****: Notify sender with ****Policy Tip****
- ****Mode****: `Test with Policy Tips`
- ****Audit Severity****: `High`
- ****Comment**** (**if** added): Explains purpose to warn user before sending PII externally

****B. Custom Credit Card Filter****

- ****Rule****: `Block Credit Card with Override`
- ****Conditions****:
 - Recipient is ****Outside the organization****
 - Contains ****Credit Card Number****
- ****Actions****:
 - ****Block the message****, but allow sender to override with ****business justification****
 - ****Notify the sender**** with Policy Tip
 - (Optional) Generate incident report to Administrator
- ****Mode****: `Enforce`
- ****Audit Severity****: `High`
- ****Warning Shown****: "NotifySender action may reject the message" → expected behavior

```
#####
Exercise 1 - EMS Section: Implementing DLP Using PowerShell
#####
```

```
#####
Step 1 - List All Available DLP Policy Templates
#####
```

Get-DlpPolicyTemplate

```
[PS] C:\Users\Administrator>Get-DlpPolicyTemplate
```

Name	Publisher	Version
----	-----	-----
Australia Financial Data	Microsoft	15.0.3.0
Australia Health Records Act (HRIP Act)	Microsoft	15.0.3.0
Australia Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
Australia Privacy Act	Microsoft	15.0.3.0
Canada Financial Data	Microsoft	15.0.3.0
Canada Health Information Act (HIA)	Microsoft	15.0.3.0
Canada Personal Health Act (PHIPA) - Ontario	Microsoft	15.0.3.0
Canada Personal Health Information Act (PHIA) - Manitoba	Microsoft	15.0.3.0
Canada Personal Information Protection Act (PIPA)	Microsoft	15.0.3.0
Canada Personal Information Protection Act (PIPEDA)	Microsoft	15.0.3.0
Canada Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
France Data Protection Act	Microsoft	15.0.3.0
France Financial Data	Microsoft	15.0.3.0
France Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
Germany Financial Data	Microsoft	15.0.3.0
Germany Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
Israel Financial Data	Microsoft	15.0.3.0
Israel Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
Israel Protection of Privacy	Microsoft	15.0.3.0
Japan Financial Data	Microsoft	15.0.3.0
Japan Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
Japan Protection of Personal Information	Microsoft	15.0.3.0
PCI Data Security Standard (PCI DSS)	Microsoft	15.0.3.0
Saudi Arabia - Anti-Cyber Crime Law	Microsoft	15.0.3.0
Saudi Arabia Financial Data	Microsoft	15.0.3.0
Saudi Arabia Personally Identifiable Information (PII)...	Microsoft	15.0.3.0
U.K. Access to Medical Reports Act	Microsoft	15.0.3.0
U.K. Data Protection Act	Microsoft	15.0.3.0
U.K. Financial Data	Microsoft	15.0.3.0
U.K. Personal Information Online Code of Practice (PI...	Microsoft	15.0.3.0
U.K. Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
U.K. Privacy and Electronic Communications Regulations	Microsoft	15.0.3.0
U.S. Federal Trade Commission (FTC) Consumer Rules	Microsoft	15.0.3.0
U.S. Financial Data	Microsoft	15.0.3.0
U.S. Gramm-Leach-Bliley Act (GLBA)	Microsoft	15.0.3.0
U.S. Health Insurance Act (HIPAA)	Microsoft	15.0.3.0
U.S. Patriot Act	Microsoft	15.0.3.0
U.S. Personally Identifiable Information (PII) Data	Microsoft	15.0.3.0
U.S. State Breach Notification Laws	Microsoft	15.0.3.0
U.S. State Social Security Number Confidentiality Laws	Microsoft	15.0.3.0

Displays all built-in DLP templates available **in** your Exchange organization. These templates contain pre-defined rules **for** detecting sensitive **data** such as personal information, credit card numbers, or health records.

Templates support compliance needs such as:

- Canada Personally Identifiable Information (PII)
- Canada Financial **Data**
- Canada Health Information Act (HIA)

This helps administrators **select** standardized frameworks **for** their region or industry.

Optional formatting **for** easier reading:

Get-DlpPolicyTemplate | **Format-Table** Name, Description

```
#####  
Step 2 - Create a DLP Policy from Template  
#####
```

New-DlpPolicy -Name "Finance DLP Block" -Template "Canada Financial Data" -
Mode Enforce

```
[PS] C:\Users\Administrator>New-DlpPolicy -Name "Finance DLP Block" -Template "Canada Financial Data" -Mode Enforce  
WARNING: The rule contains NotifySender action with an option that may reject the message. In case the message gets rejected, other actions won't be applied.  
[PS] C:\Users\Administrator>
```

Creates a new DLP policy named "Finance DLP Block" **using** the Canadian financial template. This policy is **set** to Enforce mode, which means **it** will actively restrict or block emails containing protected financial **data**.

This is ideal **for** organizations subject to PIPEDA or internal financial privacy standards. Templates reduce **setup** time and ensure reliable, tested detection mechanisms.

A warning may appear about NotifySender actions rejecting the message – this is expected behavior and does not affect functionality.

```
#####  
Step 3 - Create a Transport Rule Linked to the DLP Policy  
#####
```

New-TransportRule -Name "Notify Finance Block" `
-NotifySender NotifyOnly `
-RuleSubType DLP `
-DlpPolicy "Finance DLP Block" `
-Mode Enforce `
-SentToScope NotInOrganization `
-MessageContainsDataClassification @{Name="Credit Card Number"}

```
[PS] C:\Users\Administrator>New-TransportRule -Name "Notify Finance Block" `  
>> -NotifySender NotifyOnly `  
>> -RuleSubType DLP `  
>> -DlpPolicy "Finance DLP Block" `  
>> -Mode Enforce `  
>> -SentToScope NotInOrganization `  
>> -MessageContainsDataClassification @{Name="Credit Card Number"}`  
  
Name                State    Mode    Priority Comments  
----                -  
Notify Finance Block Enabled Enforce 13
```

Creates a transport rule that connects to the "Finance DLP Block" policy. This rule looks **for** messages containing credit card numbers sent to external recipients. Instead of blocking the message, **it** sends a Policy Tip to the sender.

This approach is often used **in** training phases to raise awareness without disrupting communication. Once behavior improves, this rule can be changed to block or quarantine messages.

Key details:

- NotifySender NotifyOnly warns but does not block
- SentToScope NotInOrganization ensures **it** only applies to external recipients
- The classifier looks **for** content matching the "Credit Card Number" detection rule

```
#####  
Step 4 - List All Deployed DLP Policies  
#####
```

Get-DlpPolicy

```
[PS] C:\Users\Administrator>Get-DlpPolicy  
  
Name                           Publisher State   Mode  
----                           -  
Confidential Info - Canada Microsoft Enabled AuditAndNotify  
Custom Credit Card Filter      Enabled Enforce  
Finance DLP Block              Microsoft Enabled Enforce
```

Displays all DLP policies that have been created **in** the organization. Use this command to confirm that your configurations exist, and to check their enforcement modes.

The list **should** include:

- Confidential Info - Canada
- Custom Credit Card **Filter**
- Finance DLP Block

Optional formatting **for** reporting:

Get-DlpPolicy | **Format-Table** Name, Mode, Description

```
[PS] C:\Users\Administrator>Get-DlpPolicy | Format-Table Name, Mode, Description  
  
Name                           Mode Description  
----  
Confidential Info - Canada AuditAndNotify This DLP policy monitors emails for Canadian Personal...  
Custom Credit Card Filter      Enforce Blocks messages containing credit card numbers unless...  
Finance DLP Block              Enforce Helps detect the presence of information commonly con...
```

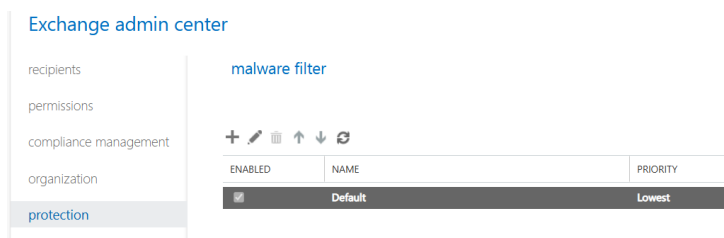
Exercise 2 – Task 1: Review the Default Anti-Malware Policy (EAC)

Objective:

Inspect the default anti-malware policy pre-installed with Microsoft Exchange Server 2019. This policy provides essential threat protection against email-borne malware, such as viruses and trojans, by scanning message attachments.

Navigation:

1. Go to <https://ad07.domain07.local/ecp>
2. In the left-hand panel, click **Protection**
3. Click on the **Malware Filter** tab
4. Locate the policy named **Default** and click to open it



Detected Configuration:

Malware Detection Response:

- `Delete the entire message`

Notifications:

- No recipient, sender, or administrator notifications were configured
- No custom notification text is currently in use

Explanation:

The default policy is extremely basic. When malware is detected in any attachment, the entire message is deleted without notifying the sender or administrator. While this is a valid safety measure, it lacks visibility for both users and IT staff.

This configuration is **functional** but **not ideal** for operational transparency, incident response, or end-user education. In production environments, most organizations will:

- Notify administrators for auditing and follow-up
- Alert senders so they understand what happened
- Provide a custom message with remediation instructions

Real-World Recommendation:

The default policy is meant as a starting point. Organizations should review and customize anti-malware policies to:

- Apply different behaviors per department or domain
- Notify relevant stakeholders
- Integrate with broader incident response and compliance workflows

Malware Detection Response

When malware is detected in any attachment, select whether to delete the entire message or to delete all message attachments.

- ☒ Delete the entire message
- ☐ Delete all attachments and use default alert text
- ☐ Delete all attachments and use custom alert text

This indicates that any email with a detected threat is fully discarded without recourse or visibility.

Exercise 2 – Task 2: Create a New Anti-Malware Policy – Attachment Blocker

Objective:

Create a new anti-malware policy named **Attachment Blocker** that deletes the entire message when malware is detected and notifies the sender. The policy will apply specifically to messages addressed to an external domain (e.g., @domain07.com).

Action:

Define a new policy that targets external communication, helping prevent malware from being distributed beyond the organization. This enhances outbound security and user accountability.

Navigation:

1. Go to <https://ad07.domain07.local/ecp>
2. Click on **Protection** → [Select](#) the **Malware Filter** tab
3. Click the **plus (+)** symbol to create a new malware [filter](#) policy

malware filter

<div><div><div><div><div></div></div></div><div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div></div></div>	
ENABLED	NAME
<input checked="" type="checkbox"/>	Default

Configuration:

Name:

Attachment Blocker

Description:

Deletes entire messages with malware and notifies internal senders **if** emails are sent to @domain07.com.

Malware Detection Response:

[Select](#) the following option:
Delete the entire message

Custom notification text:

Leave blank unless you plan to use a custom replacement file message when deleting attachments. Since we are deleting the entire message (not just attachments), this is not required.

Notifications:

Sender Notifications:

Notify internal senders

Administrator Notifications:

Leave unchecked - Notify administrator about undelivered messages from internal senders

Leave unchecked - Notify administrator about undelivered messages from external senders

Customize Notifications:

Leave this section unchecked **for** now - you can use the default system-generated notification. (Optional: customize later **for** branding or clarity.)

Applied To (Conditions):

Click ****Add condition****, then configure the following:

If...

The recipient domain is → `domain07.com`

No exceptions are needed, so leave the ****Except if...**** section blank.

Final Steps:

1. Click ****Save****
2. Ensure the new policy appears **in** the ****Malware Filter**** list

new anti-malware policy

*Name:

Attachment Blocker

Description:

Deletes entire messages with malware and notifies internal senders if emails are sent to @domain07.com.

Malware Detection Response

When malware is detected in any attachment, select whether to delete the entire message or to delete all message attachments.

- ☒ Delete the entire message
☐ Delete all attachments and use default alert text
☐ Delete all attachments and use custom alert text

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is ▼

'domain07.com'

add condition

Except if...

add exception

Notifications

Sender Notifications

Sends a message to the sender of the undelivered message.

- ☒ Notify internal senders
☐ Notify external senders

Explanation:

This policy ensures that **if** any malware is detected **in** a message going to the ****@domain07.com**** domain:

- The message will be deleted entirely (not just the infected attachment)
- The sender will receive a notification, helping them understand that the message was blocked **for** security reasons

Use Cases:

- Prevents malware propagation to external partners or clients
- Enforces sender awareness through proactive notification
- Allows Exchange admins to **set** domain-specific policies – useful **in** B2B email environments or partner filtering

Validation:

After saving the policy:

1. Verify **it** appears under the ****Malware Filter**** tab
2. Ensure the condition reflects the correct domain (``@domain07.com``)
3. Confirm sender notification is enabled

malware filter



ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	Attachment Blocker	0
<input checked="" type="checkbox"/>	Default	Lowest

Exercise 2 – Task 3: Create a New Anti-Malware Policy – Warn Internal Users

Objective:

Create a new anti-malware policy named ****Warn Internal Users**** that deletes only the infected attachment (not the full message), and notifies the ****administrator****. This policy applies to messages sent ****within the organization**** and allows visibility without fully disrupting user communication.

Configuration:

Name:

Warn Internal Users

Description:

Deletes infected attachments from internal emails and notifies the administrator **for** awareness and tracking.

Malware Detection Response:

Select the following option:

Delete all attachments and use default alert text

This setting ensures that:

- The original message is delivered
- The infected file is removed
- A default placeholder file is attached to indicate removal

Notifications:

Sender Notifications:

Notify internal senders

Notify external senders

(No sender notification is needed **for** this policy)

Administrator Notifications:

Check - Notify administrator about undelivered messages from internal senders

→ Administrator email address: `Administrator@domain07.local` (or your lab's designated admin)

Notify administrator about undelivered messages from external senders

→ Leave this unchecked

Customize Notifications:

Leave this section unchecked (default alert text will be used **for** administrator notifications)

Applied To (Conditions):

Click Add condition, then configure:

The recipient domain is → domain07.local

This ensures the policy only applies to messages being delivered ****within the internal Exchange organization****.

Even though we cannot scope based on the sender directly, applying to internal recipients effectively captures the same intent **in** the lab scenario.

No exceptions are needed, so leave the ****Except if...**** section blank.

new anti-malware policy

*Name:

Description:

Malware Detection Response
When malware is detected in any attachment, select whether to delete the entire message or to delete all message attachments.

☐ Delete the entire message
☒ Delete all attachments and use default alert text
☐ Delete all attachments and use custom alert text

Administrator Notifications
Sends a message to the administrator of the undelivered message.

☒ Notify administrator about undelivered messages from internal senders
Administrator email address:

Applied To
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is

Except if...

Explanation:

This policy is focused on ****internal traffic****, which is common **for** file sharing. Instead of deleting the entire email, only infected files are removed. The administrator receives an alert, allowing security staff to monitor and react without interrupting user productivity.

Use Cases:

- Promotes internal safety without being overly disruptive
- Keeps administrators **in** the loop **for** incident management
- Good balance of automation and oversight

Validation:

After saving the policy:

- Confirm **it** appears under the ****Malware Filter**** tab
- Confirm the condition is "Sender is located inside the organization"
- Confirm the action is "Delete attachment only"
- Confirm admin notification is enabled with a valid email

✓	Warn Internal Users	1
---	---------------------	---

Task 4 - Verify Anti-Malware Policies and Their Settings

Objective:

Review all created anti-malware policies and ensure their configuration matches the intended behavior as defined in Tasks 2 and 3, using the Exchange Admin Center (EAC).

Step 1 - Open the EAC

Action:

Access the Exchange Admin Center.

Navigation:

Log into EAC → Click on **protection** in the left-hand menu → Select the **malware filter** tab.

recipients

permissions

compliance management

organization

protection

mail flow

malware filter

ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	Attachment Blocker	0
<input checked="" type="checkbox"/>	Warn Internal Users	1
<input type="checkbox"/>	Default	Lowest

Explanation:

This section lists all anti-malware policies that are configured in the environment. Each entry represents a policy with unique settings and scope.

Step 2 - Review "Attachment Blocker" Policy

Action:

Click on the **Attachment Blocker** policy to view details.

Attachment Blocker

Enabled

Relative priority: 0

Applied to:

If the message:

recipients's address domain portion belongs to any of these domains: 'domain07.com'

Take the following actions:

Apply malware filter policy "Attachment Blocker".

Except if the message:

Summary

Malware detection response:

Delete the entire message

Sender notifications:

Notify internal senders

Administrator notifications:

None

Customized notification text:

Not configured

Validation:

Ensure the following settings are applied:

- **Name**: Attachment Blocker
- **Malware Detection Response**: Delete the entire message
- **Notify internal senders**: Enabled
- **Recipient domain is**: domain07.com

Step 3 - Review "Warn Internal Users" Policy
#####

Action:

Click on the **Warn Internal Users** policy to view details.

Warn Internal Users

Enabled

Relative priority: 1

Applied to:

If the message:

recipients's address domain portion belongs to any of these domain
s: 'domain07.local'

Take the following actions:

Apply malware filter policy "Warn Internal Users".

Except if the message:

Summary

Malware detection response:

Delete all attachments (use default alert text)

Sender notifications:

None

Administrator notifications:

Undelivered messages from internal senders

Customized notification text:

Not configured

Validation:

Ensure the following settings are applied:

- **Name**: Warn Internal Users
- **Malware Detection Response**: Delete all attachments and use default alert text
- **Administrator Notification**: Enabled **for** internal senders
- **Administrator Email**: administrator@domain07.local
- **Recipient domain is**: domain07.local

```
#####
Step 4 - Confirm Policy Priority and Scope
#####
```

Action:

In the malware **filter** list view, confirm the order and target domains of each policy.

ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	Attachment Blocker	0
<input checked="" type="checkbox"/>	Warn Internal Users	1
<input checked="" type="checkbox"/>	Default	Lowest

Validation:

Verify that:

- Each policy is ****enabled****.
- Each policy is correctly ****scoped**** to its target domain via the "Applied To" rule.
- There is no conflicting overlap between policies.

```
#####
Exercise 2 - EMS Section: Managing Anti-Malware Policies via PowerShell
#####
```

Objective:

Use Exchange Management Shell (EMS) to review all configured anti-malware policies, inspect their notification settings, and perform a manual update of the malware definition engine.

```
#####
Step 1 - List All Existing Anti-Malware Policies
#####
```

Command:

Get-MalwareFilterPolicy

```
[PS] C:\Users\Administrator>Get-MalwareFilterPolicy
```

Name	Action	CustomNotifications	IsDefault
Default	DeleteMessage	False	True
Attachment Blocker	DeleteMessage	False	False
Warn Internal Users	DeleteAttachmentAndUseDefaultAlertText	False	False

Explanation:

This command retrieves a list of all anti-malware **filter** policies currently configured **in** the Exchange environment.

It displays basic information including:

- Name of each policy
- Whether **it** is enabled
- Malware response behavior
- Notification status

This is useful **for** auditing policy presence and quickly confirming naming consistency or identifying gaps **in configuration**.

```
#####
Step 2 - Review Notification Settings of a Selected Policy
#####
```

Command:

Get-MalwareFilterPolicy -Identity "Warn Internal Users" | Format-List
Notify*,CustomNotification*

```
[PS] C:\Users\Administrator>Get-MalwareFilterPolicy -Identity "Warn Internal Users" | Format-List N  
otify*,CustomNotification*

CustomNotifications : False
```

Explanation:

This command displays only the ****notification-related settings**** **for** the policy named `Warn Internal Users`.

You will be able to review:

- Whether internal or external senders are notified
- Whether administrators are notified **for** internal or external traffic
- The email address used **for** admin alerts (**if** configured)
- Whether custom notification messages are **in** use

Use this to confirm that:

- Admin notifications are active (e.g., **for** internal senders)
- Default or custom messages are being used correctly

You can also replace `"Warn Internal Users"` with `"Attachment Blocker"` to check the other policy:

```
Get-MalwareFilterPolicy -Identity "Attachment Blocker" | Format-List Notify*,CustomNotification*
```

```
[PS] C:\Users\Administrator>Get-MalwareFilterPolicy -Identity "Attachment Blocker" | Format-List Notify*,CustomNotification*

CustomNotifications : False
```


Step 3 - Force a Malware Definition Update
#####

Command:

```
& "$env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1" -  
Identity ad07.domain07.local
```

```
[PS] C:\Users\Administrator>& "$env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1"  
-Identity ad07.domain07.local  
Running as DOMAIN07\Administrator.  
-----  
Connecting to ad07.domain07.local.  
Dispatched remote command. Start-EngineUpdate -UpdatePath http://amupdated1.microsoft.com/server/am  
update  
-----  
[PS] C:\Users\Administrator>_
```

Explanation:

This command manually initiates an update of the anti-malware engine and signature definitions **for** the specified Exchange server.

- `\$env:ExchangeInstallPath` dynamically pulls the Exchange installation directory
- The script `Update-MalwareFilteringServer.ps1` ensures the latest malware definitions are applied
- The `-Identity` parameter targets your Exchange server (replace with actual FQDN **if** different)

Why it matters:

In production environments, this is used to ensure Exchange has the ****latest** virus and malware signatures****** **for** real-time protection – especially **in** response to emerging threats.

This step ensures your anti-malware component is not relying on outdated detection patterns.