Module 6: Managing message security in Exchange Online

Security has always been one of the biggest priorities of messaging administrators, whether they work with Exchange Server or Exchange Online. Multiple threats such as spam, malware, and phishing use email transport to attack computer systems worldwide. Microsoft 365 includes technologies for message security, such as Exchange Online Protection and Microsoft Defender for Office 365. Messaging administrators should work together with security administrators and security information officers to create a security strategy and provide comprehensive protection for their organizations. Furthermore, it's important that users are trained on how to protect sensitive information sent over email or other collaboration technologies.

In this module, you'll learn about email protection, threat protection, and message encryption. You'll learn how to use tools such as Exchange Online Protection, Microsoft Defender, and Microsoft Purview to manage message security and encryption.

By completing this module, you'll achieve the knowledge and skills to:

- Plan message security for Exchange Online.
- Describe Microsoft Defender for Office 365.
- Provide message security with Microsoft Defender for Office 365.
- Implement message encryption in Exchange Online.

SAMPLE

Lesson 1: Planning message security for Exchange Online

Planning messaging security for Exchange Online involves analyzing potential threats and defining the security technologies that you will use to protect your organization's data. You'll also need to choose the Microsoft 365 subscription that will best meet your organization's business requirements, because the types of message security technologies available to you will differ between subscriptions.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Exchange Online Protection.
- Plan mail flow for Exchange Online Protection.
- Explain how email protection works.

Overview of Exchange Online Protection

Exchange Online Protection is a cloud-based service that protects users' mailboxes from email threats. You can also use Exchange Online Protection as a standalone product to protect mailboxes that are stored in an on-premises Exchange Server.

When a Microsoft 365 tenant subscription is activated, Exchange Online Protection is automatically configured with the following default protection policies:

- **Anti-malware protection**. Protection from viruses, spyware, and ransomware.
- **Anti-spam protection**. Protection from spam, junk email, and bulk email.
- **Anti-phishing (spoof) protection**. Protection from phishing (spoof) email; provides spoof intelligence.

Before a message is sent to a user's mailbox in Exchange Online, Exchange Online Protection performs the following filtering:

1. **Connection filtering**. Connection filtering checks the sender's reputation. If the sender's reputation doesn't match the security criteria, the email will not be delivered to the user's mailbox; it will be stored in quarantine or the junk email folder, depending on the configuration. If the sender's reputation matches the security criteria, the message will be forwarded to anti-malware filtering.
2. **Anti-malware filtering**. Anti-malware filtering inspects the message for malware. If the email contains malware, the message will be delivered to quarantine. If the message doesn't contain malware, it will be forwarded to policy filtering.
3. **Policy filtering and Data Loss Prevention (DLP)**. Policy filtering includes mail flow rules (transport rules) that are created by messaging admins. DLP policies include criteria that are based on the organization's compliance policies. Mail flow rules and DLP policies perform actions on the message depending on different criteria. If the message meets the filtering criteria, then the message will be stored in quarantine or the junk email folder, depending on the configuration. If the message doesn't match the filtering criteria, it will be forwarded to content filtering.
4. **Content filtering**. Content filtering inspects the message for spam, spoofing, phishing, or bulk. If the message contains content that indicates spam, spoofing, phishing, or bulk email, then the message will be stored in quarantine or the junk email folder, depending on the configuration. If the message doesn't contain spam, spoofing, phishing, or bulk email, the message will finally be delivered to the user's mailbox.

SAMPLE

Planning mail flow for Exchange Online Protection

Planning mail flow for Exchange Online Protection is dependent on the Exchange Online deployment process. It involves analyzing the current messaging environment and the organization's business and compliance requirements, and deciding how messages will be directed to Exchange Online Protection.

Planning mail flow from the internet to Exchange Online Protection

To direct their incoming email to Exchange Online Protection, organizations will need to configure their public DNS MX record during the Microsoft 365 tenant setup, or later, depending on the deployment scenario. The Microsoft 365 deployment setup process will include instructions for the messaging administrator about the values that should be provided for the MX record. For example, an organization with an SMTP domain name **contoso.com** will have the MX record depicted in the following table.

Table 1: MX record

Priority	Hostname	Value	Time to Live (TTL)
0	@	contoso.mail.protection.outlook.com	1 hour

The MX record shows that, for example, if an email is sent from a person in the organization **Northwind Traders**, to a person in the organization **Contoso** with an SMTP domain **contoso.com**, then the sending SMTP server in **Northwind Traders** will perform a DNS lookup and send an email to the receiving SMTP server in **Contoso**. The receiving SMTP server can be found under the DNS name **contoso.mail.protection.outlook.com**, which, in this example, represents the Exchange Online Protection service in the Microsoft 365 cloud.

There are several scenarios for Exchange Online deployment, which influence the decision on when the MX record should be configured.

- **Exchange Online-only deployment.** This scenario is most common for new organizations that plan to deploy Exchange Online in Microsoft 365. For this deployment, the MX record is created during the Microsoft 365 tenant setup.
- **Exchange hybrid deployment.** This scenario is most common for organizations that already have Exchange Server and plan to migrate to Exchange Online. Before introducing Exchange Online, the MX record points to the on-premises Exchange Server or a third-party SMTP gateway; for example, **mail.contoso.com**. Messaging administrators might choose to keep the mail flow to on-premises Exchange Server during the mailbox migration from Exchange Server to Exchange Online, which means that they will not update the MX record during the Microsoft 365 tenant setup. After all mailboxes are migrated to Exchange Online, the MX record can be updated, and the value **mail.contoso.com** will be replaced with **contoso.mail.protection.otulook.com** .

> **Note:** Because of DNS propagation latency through the internet, the MX record change won't take effect immediately. Therefore, it's recommended that you don't turn off the on-premises SMTP gateway, because some of the email might still go through **mail.contoso.com** until the internet DNS servers are updated with the new MX record value.

SAMPLE

- **Microsoft 365 tenant to tenant migration**. This scenario is common in organizations that perform mergers and acquisitions or are created by separating a unit from the existing organization. After the organizational merger, acquisition, or split, messaging administrators should decide when to update the MX record based on the organization's decision about the SMTP domain name. For example, if two organizations merge into a new one, and users' mailboxes will be migrated to a new Microsoft 365 tenant, then the MX record will be created during the Microsoft 365 tenant setup.
- **Third-party messaging solution to Exchange Online migration.** This scenario is common for organizations that use third-party messaging solutions, both on-premises or in the cloud, and plan to migrate to Exchange Online or Microsoft 365. Before the migration, the MX record points to an on-premises messaging solution; for example, **mail.contoso.com**, or a cloud messaging solution; for example, **contoso.cloudprovider.com**. Messaging administrators might also choose to not update the MX record to **contoso.mail.protection.outlook.com** until all mailboxes from the third-party solution are migrated to Exchange Online.

> **Note:** Because of DNS propagation latency through the internet, the MX record change won't take effect immediately. Therefore, it's recommended that you don't turn off the third-party messaging solution, because some of the email might still go through it, until the internet DNS servers are updated with the new MX record value.

SAMPLE

Planning mail flow from Exchange Online Protection to the internet

In organizations that only use Exchange Online, messaging administrators don't need to configure mail flow from Exchange Online Protection to the internet. Exchange Online will send all outgoing email from the organization's employees to the internet through Exchange Online Protection.

However, if organizations that use Exchange Online in hybrid mode need to send email to the internet through Exchange Server, then the messaging administrators will need to configure the send connector. The send connector will direct outgoing email from Exchange Online Protection to on-premises Exchange Server, and Exchange Server will be responsible for sending emails to the internet.

Furthermore, some organizations might need to redirect their outgoing email to a third-party service before email is sent to the internet. This could be a service that archives messages or applies digital signatures to these emails. In such cases, messaging administrators will also need to create a send connector that sends outgoing email to the third-party service, instead of directly to the internet.

Planning additional mail flow settings in Exchange Online Protection

Exchange Online Protection provides additional functionalities that protect the organization's messaging environment in Exchange Online from unwanted email. These functionalities include:

- **Directory-Based Edge Blocking.** Directory-Based Edge Blocking analyses every incoming message and verifies if an email recipient object exists. If the email recipient object doesn't exist, Exchange Online Protection rejects the message.
- **Manage accepted domains**. Accepted domains are SMTP domains that are assigned to the Exchange Online recipient objects. After an SMTP domain such as contoso.com is assigned, recipient objects such as the user mailbox can have an email address such as Firstname.Lastname@contoso.com configured through the email address policy. The email address is then used for receiving and sending email. You can create an accepted domain in the Microsoft 365 admin center and perform additional configuration in the Exchange Online admin center or Exchange Online PowerShell.

How does email protection work?

In Exchange Online Protection and Defender for Office 365, every email message passes through multiple threat detection scans, such as anti-malware, anti-spam, and anti-phishing. Based on the detection scans, email messages might be flagged by adding information to the following email message headers:

- **X-Forefront-Antispam-Report.** Contains information regarding how the message was processed by the threat detection scans.
- **X-Microsoft-Antispam**. Contains additional information regarding bulk mail and phishing scans.
- **Authentication-results**. Contains information regarding Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) verification.

The X-Forefront-Antispam-Report email message header contains a property called CAT, which describes the threat category. After Exchange Online Protection scans the email message, it will populate the CAT property with the appropriate value, based on which policy is applied to the email message. The following table describes the CAT property categories.

SAMPLE

Table 2: CAT property categories

Order	Email protection	CAT property - Category	Configuration
1	Malware	CAT:MALW	Exchange Online Protection anti-malware policies
2	High confidence phishing	CAT:HPHSH	Exchange Online Protection anti-spam policies
3	Phishing	CAT:PHSH	Exchange Online Protection anti-spam policies

4	High confidence spam	CAT:HSPM	Exchange Online Protection anti-spam policies
5	Spoofing	CAT:SPOOF	Exchange Online Protection Spoof intelligence insight
6	User impersonation (protected users)	CAT:UIMP	Microsoft Defender for Office 365 anti-phishing policies
7	Domain impersonation (protected domains)	CAT:DIMP	Microsoft Defender for Office 365 anti-phishing policies
8	Mailbox intelligence (contact graph)	CAT:GIMP	Microsoft Defender for Office 365 anti-phishing policies
9	Spam	CAT:SPM	Exchange Online Protection anti-spam policies
10	Bulk	CAT:BULK	Exchange Online Protection anti-spam policies

SAMPLE

Lesson 2: Overview of the Microsoft Defender platform

Microsoft Defender XDR (Extended detection and report) is a family of products that protect organizations from different types of threats, and includes prevention, detection, and response functionalities. Microsoft Defender XDR coordinates actions related to threat prevention, detection, investigation, and response across multiple workloads, such as identities, endpoints, email, documents, and applications.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Microsoft Defender.
- Describe Microsoft Defender for Office 365.
- Explain how threat protection works in Microsoft Defender for Office 365.
- Describe Microsoft Defender for Identity.
- Describe attack simulation in Microsoft Defender for Office 365.

What is Microsoft Defender?

Microsoft 365 provides multiple security technologies within Microsoft Defender. These security technologies help protect organizations from different types of threats and attacks that might have different goals and different ways to propagate, including:

- Malicious code over email message
- A link or a document
- Attack on identity

The following Defender products coordinate information between each other to help protect an organization's data, apps, and identities:

- **Microsoft Defender for Endpoint**. An endpoint security solution that prevents, detects, investigates, and responds to endpoint threats.
- **Microsoft Defender for Office 365**. A security solution that protects organizations from threats in Office 365 content, such as email, email attachments, URL links, and documents located in different Office 365 apps.
- **Microsoft Defender for Identity.** An identity security solution that monitors and secures organizations' identities located both in on-premises Active Directory and in the cloud.
- **Microsoft Defender for Cloud Apps.** A security solution that discovers and monitors cloud apps used by organizations and prevents security threats from different cloud apps.
- **Microsoft Defender Vulnerability Management**. A security solution that provides asset visibility, intelligent assessments, and built-in remediation tools for different platforms, such as Windows, macOS, Linux, Android, iOS, and network devices.
- **Microsoft Entra ID Protection**. A security solution that provides organizations with functionalities to detect, investigate, and remediate identity-based risks.
- **Microsoft Data Loss Prevention**. A component of Microsoft Purview that protects sensitive data and reduces the risk of unauthorized sharing of sensitive data.
- **Microsoft Apps Governance**. A functionality in Microsoft Defender for Cloud Apps that provides visibility and control over cloud apps that access sensitive data in Microsoft 365.

SAMPLE

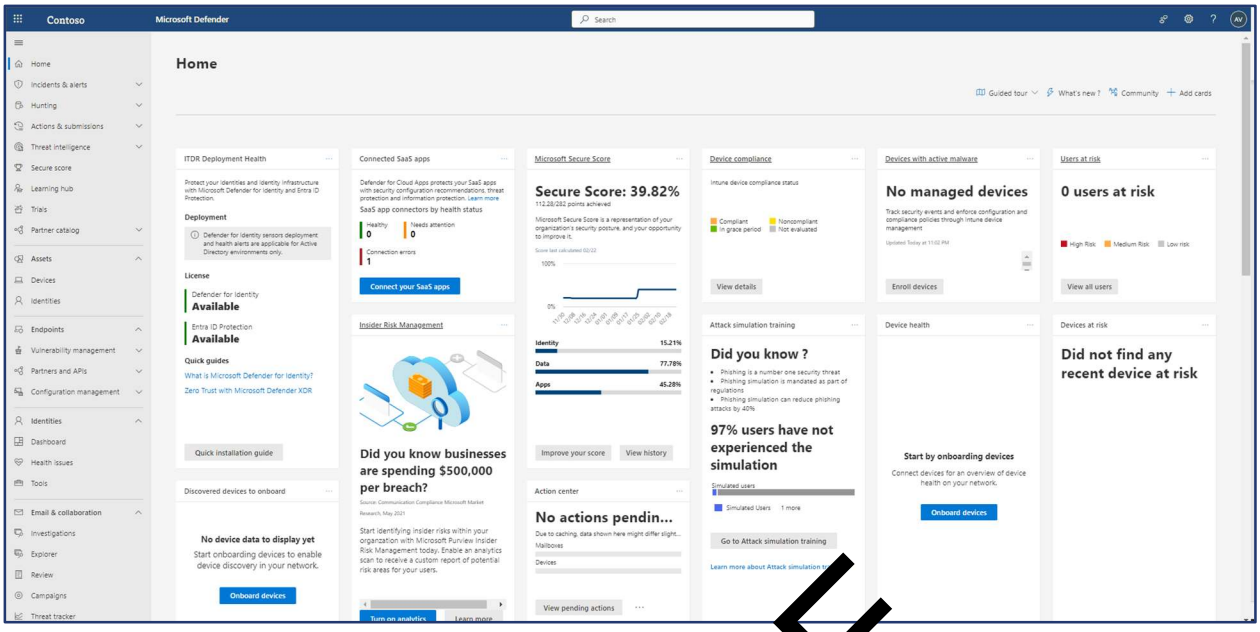


Figure 1: Defender admin center

Overview of Microsoft Defender for Office 365

Organizations can deploy multiple components of email message protection, depending on their business requirements. Microsoft 365 includes three products for email messaging security, which are available as separate subscriptions:

- **Exchange Online Protection**. Included in every Microsoft 365 and Exchange Online subscription, and provides protection from broad, volume-based known attacks.
- **Microsoft Defender for Office 365 Plan 1 (P1)**. Provides all Exchange Online Protection functionalities, in addition to more advanced threat protection, such as protection from zero-day malware attacks, phishing attacks, and protection from malicious links and attachments in email messages.
- **Microsoft Defender for Office 365 Plan 2 (P2)**. Provides all Microsoft Defender for Office 365 P1 functionalities in addition to post-breach investigation, hunting capabilities, automation, and attack simulation training.

Each of these email messaging security products provide functionalities across three main components:

- Prevent/detect
- Investigate
- Respond

The Exchange Online Protection functionalities for all three security components are described in the following table.

SAMPLE

Table 3: Exchange Online Protection functionalities

Prevent/Detect functionalities	Investigate	Respond

▪ Prevents and detects the following threats:
  o Spam
  o Phishing
  o Malware
  o Bulk mail
▪ Spoof intelligence
▪ Quarantine
▪ False positives and false negative reporting by admin submissions and user-reported messages
▪ Allow and block entries in the Tenant Allow/Block List for:
  o Domains and email addresses
  o Spoof
  o URLs
  o Files
	▪ Audit log search
	▪ Message Trace
	▪ Email security reports
		▪ Zero-hour auto purge (ZAP)
		▪ Refinement and testing of entries in the Tenant Allow/Block List

SAMPLE

The Defender for Office 365 P1 functionalities for all three security components are described in the following table.

Table 4: Defender for Office 365 P1 functionalities

Prevent/Detect functionalities	Investigate	Respond
▪ Safe Attachments in email ▪ Safe Attachments for Microsoft SharePoint, Microsoft OneDrive, and Microsoft Teams ▪ Safe Links in email, Office clients, and Teams ▪ Advanced anti-phishing thresholds in anti-phishing policies ▪ User, domain, and mailbox intelligence impersonation protection in anti-phishing policies	▪ SIEM integration API for detections ▪ Real-time detections ▪ URL trace ▪ Specific Microsoft Defender for Office 365 reports	▪ ZAP ▪ Refinement and testing of entries in the Tenant Allow/Block List

▪ Alerts and SIEM integration API for alerts		

The Defender for Office 365 P2 functionalities for all three security components are described in the following table.

Table 5: Defender for Office 365 P2 functionalities

Prevent/Detect functionalities	Investigate	Respond
▪ Attack simulation training	▪ Threat Explorer ▪ Threat Trackers ▪ Campaign Views	▪ Automated Investigation and Response (AIR) ▪ AIR from Threat Explorer ▪ AIR for compromised users ▪ SIEM Integration API for Automated Investigations

SAMPLE

How threat protection works in Microsoft Defender for Office 365

The filtering process for Defender for Office 365 protection includes four phases: edge protection, sender intelligence, content filtering, and post-delivery protection. If an email message passes all four phases, it will be delivered to the recipient mailbox.

Phase 1: Edge protection

Edge protection is the entry location where the email message is processed, and includes the following functionalities:

- Network throttling. Protects Microsoft 365 datacenter infrastructure from denial-of-service attacks. Network throttling limits the number of messages that a sender can submit at a specific point of time.
- IP reputation and throttling. Recognizes IP addresses that belong to malicious senders and blocks messages being sent from those IP addresses. Furthermore, if a specific IP sends a large number of email messages in a short period of time, those email messages will be throttled.
- Domain reputation. Recognizes domain names used by malicious senders, and blocks email messages sent from those senders.
- Directory-based edge filtering. Blocks SMTP harvest attacks where the attackers try to guess an email address, by adding many usernames to the organization's valid SMTP domain name.
- Backscatter detection. Prevents attacks that contain multiple invalid non-delivery reports (NDRs).

- **Enhanced filtering for connectors**. Protects authentication data in hybrid routing scenarios, when the authentication data is transferred through another server or device before it reaches Office 365.

Phase 2: Sender intelligence

Sender intelligence protects users from spam, bulk, impersonation, unauthorized spoofing, and phishing email messages. Sender intelligence includes the following functionalities.

- **Account compromise detection**. Includes triggers and alerts that are activated when an anomalous behavior for an account is detected, which might indicate that the account is compromised. In this scenario, the user account might be blocked so that it cannot send email messages until the threat is analyzed and resolved.
- **Email Authentication**. Ensures that senders are authenticated and authorized, which prevents spoofing attacks. Email authentication includes the following components:
  - **SPF**. Authenticates the sender's email server by verifying that the sender's email servers are listed in the public DNS TXT records, also called SPF records. If the sender's organization doesn't have SPF DNS records, then email messages sent by this organization might be rejected.
  - **DKIM**. Authenticates the sender by adding an encrypted digital signature to the outbound email message header.
  - **DMARC**. Works in coordination with SPF and DKIM by ensuring that the recipient's email infrastructure trusts email messages sent from the sender's email infrastructure.
  - **ARC**. Authenticates senders who performed an email message change for a justified reason. While this change might invalidate the SPF, DKIM, and DMARC authentication methods, it will help ensure that the sender is authenticated.
- **Spoof intelligence**. Detects and blocks malicious senders who send spam and phishing email messages pretending that those email messages originate from well-known external SMTP domains. Furthermore, it includes intra-organizational spoof intelligence, which detects and blocks spoof attempts from an internal organization domain.
- **Cross-domain spoof intelligence**. Detects and blocks spoof attempts from a domain outside the organization.
- **Bulk filtering**. Allows messaging administrators to define a bulk complaint level (BCL), which indicates whether the message was sent from a bulk sender. Bulk filtering decides whether to allow an email message to be delivered based on the BCL.
- **Mailbox intelligence**. Monitors sender's email behaviors and detects any malicious or impersonation activities.
- **Mailbox intelligence impersonation**. Identifies user impersonation based on the user's email behavior.
- **User impersonation**. Provides messaging administrators with the possibility to create a list of protected email addresses that are likely to be targeted with impersonation attacks. If an email message has a sender value that is similar to the protected email address, for example b0b@contoso.com instead of bob@contoso.com, the email message is marked or tagged.

SAMPLE

- **Domain impersonation**. Protects organizations from impersonation attacks, when an email message is sent from a domain that is similar to the organization's domain, for example john@cont0so.com, instead of john@contoso.com.

Phase 3: Content filtering

Content filtering analyzes the content of the email message, and includes the following functionalities:

- **Transport rules** (also known as mail flow rules or Exchange transport rules). Provide messaging administrators with the ability to perform actions on email messages, based on various criteria such as the content of the message.
- **Microsoft Defender Antivirus**. Contains multiple antivirus engines that detect all known malware in attachments.
- **Type blocking**. Blocks attachment file types, regardless of the filename extension. Messaging admins can modify the list of the attachment file types that need to be blocked.
- **Attachment reputation blocking**. Blocks a file that has a reputation of containing malware, where the file is blocked not only in Exchange Online, but across all Office 365 apps.
- **Heuristic clustering**. Performs heuristic analysis on a file that is suspicious of containing malware. If a suspicious attachment is found, the file will be sandboxed.
- **Machine learning models**. Performs machine learning analysis on the header, body content, and URLs of a message to detect phishing attempts.
- **URL reputation blocking**. Blocks malicious URL links based on their reputation.
- **Content heuristics**. Uses machine learning models to detect suspicious messages based on structure and word frequency within the body of the message.
- **Safe Attachments**. Performs sandboxing and dynamic analysis of every attachment to detect threats that haven't been encountered previously.
- **Linked content detonation**. Activated every time an email message contains a URL link pointing to a file and performs asynchronous sandboxing of the file at the time of delivery.
- **URL Detonation**. Activated every time anti-phishing analysis finds a message or URL to be suspicious. URL detonation sandboxes the URLs in the message at the time of delivery.

SAMPLE

Phase 4: Post-delivery protection

Post-delivery protection is the last phase of the Defender for Office 365 protection filtering process and is performed after the email message is already delivered in the user's mailbox.

- **Safe Links**. Performs time-of-click protection, where every URL in the email message is wrapped to point to Microsoft Safe Links servers. When a recipient selects the URL in the email message, the Safe Link functionality checks the URL link reputation before the user is redirected to the target site. Furthermore, the URL is asynchronously sandboxed to update its reputation.
- **ZAP for phishing**. Retroactively detects and neutralizes malicious phishing messages that have already been delivered to Exchange Online mailboxes.

- **ZAP for malware**. Retroactively acts on malware email messages that have already been delivered to Exchange Online mailboxes. When detected, malware is neutralized by the ZAP for malware functionality.
- **ZAP for spam**. Retroactively acts on spam email messages that have already been delivered to Exchange Online mailboxes. When detected, the spam email message is neutralized by the ZAP for spam functionality.
- **Campaign Views**. Provides messaging administrators with a high-level overview of an attack by using anti-phishing, anti-spam, and anti-malware data across Office 365 to identify campaigns. Messaging and security administrators can use the information provided by the Campaign Views functionality to investigate attacks and identify the targets, the level of the impact, and the flows of the attack.
- **Report Message add-ins**. Enables users to report false positives (for example, non-spam email that is marked as spam) or false negatives (for example spam email that is marked as non-spam) to Microsoft for further analysis.
- **Safe Links for Office clients**. Provides Safe Links protection for links located in supported Office apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel.
- **Safe Attachments for OneDrive, SharePoint, and Teams.** Provides protection against malicious files located in OneDrive, SharePoint, and Teams.
- **URL detonation**. Performs sandboxing on URL links that point to files in email that has already been delivered. If the sandboxing results show that there is no threat, the file pointed to by the URL can be accessed by the users.

SAMPLE

What is Microsoft Defender for Identity?

Microsoft Defender for Identity is a cloud-based identity security solution that detects different types of identity attacks and protects organizations from such attacks. Defender for Identity analyzes identity data located both in on-premises Active Directory and in the cloud, and provides security administrators with a solution for:

- **Preventing breaches**, by analyzing identity security postures.
- **Detecting threats**, by performing real-time analytics and data intelligence.
- **Investigating suspicious activities**, by analyzing incident information.
- **Responding to attacks**, with automatic response to compromised identities.

Defender for Identity performs monitoring on domain controllers by capturing and parsing network traffic. Data monitoring is performed by so-called sensors that can be installed on the Active Directory domain controllers, Active Directory Federation Server (AD FS) servers, or Active Directory Certificate Server (AD CS) servers. Furthermore, Defender for Identity can perform monitoring of third-party identity providers. The captured data is then analyzed for attacks and threats.

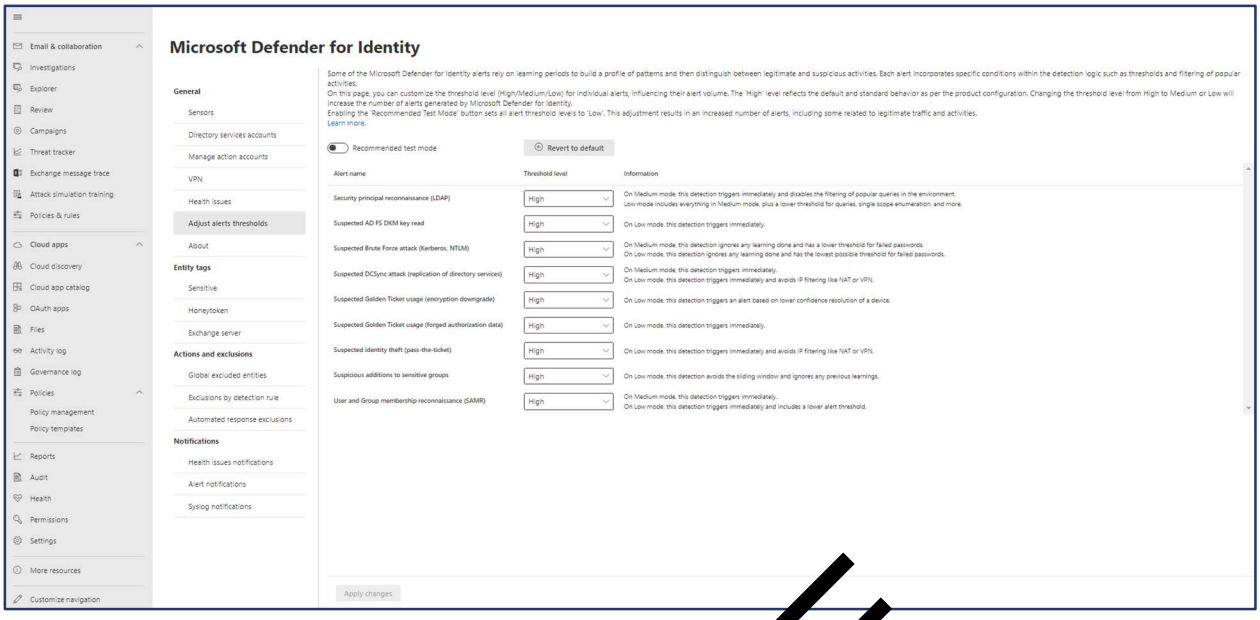


Figure 2: Defender for Identity settings

SAMPLE

Defender for Identity components

Defender for Identity includes the following components:

- **Defender for Identity cloud service**. Runs on Azure infrastructure and is connected to Microsoft's intelligent security graph.
- **Defender for Identity sensor**. Can be directly installed on the following servers:
  - **Domain controllers**: The sensor directly monitors domain controller traffic.
  - **AD FS / AD CS**: The sensor directly monitors network traffic and authentication events.

    Defender for Identity sensor:

    - Captures and inspects domain controller network traffic.
    - Receives Windows Events from the domain controllers.
    - Receives RADIUS accounting information from VPN servers.
    - Retrieves data about users and computers from the Active Directory domain.
    - Performs resolution of network entities (users, groups, and computers).
    - Transfers relevant data to the Defender for Identity cloud service.
- **Microsoft Defender portal**. The Microsoft Defender portal displays the data that is received from Defender for Identity sensors and enables security administrators to monitor, manage, and investigate threats in an organization's network environment. The Microsoft Defender portal:
  - Creates the Defender for Identity workspace.
  - Integrates with other Microsoft security services.
  - Manages Defender for Identity sensor configuration settings.

- Displays data received from Defender for Identity sensors.
- Monitors detected suspicious activities and suspected attacks based on the attack kill chain model.
- Sends notifications when security alerts or health issues are detected.

The following table describes some of the scenarios for threat detection in Defender for Identity.

Table 6: Scenarios for threat detection

Threat	Defender for Identity
Reconnaissance	Identifies rogue users and attackers' attempts to gain information. Attackers search for information about usernames, users' group membership, IP addresses assigned to devices, resources, and more, using various methods.
Compromised credentials	Identifies attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes, and other methods.
Lateral movements	Detects attempts to move laterally inside the network to gain further control of sensitive users, utilizing methods such as Pass the Ticket, Pass the Hash, Overpass the Hash, and more.
Domain dominance	Reviews highlighted attacker behavior if domain dominance is achieved. For example, attackers might run code remotely on the domain controller, or use methods like DC Shadow, malicious domain controller replication, Golden Ticket activities, and more.

SAMPLE

Attack simulation in Microsoft Defender for Office 365

Attack simulation training is a Defender functionality that runs realistic attack scenarios in your organization. Security administrators can use these simulated attacks to identify vulnerable users. After the simulated attack is completed, security administrators can review reports of attack simulation and organize training activities for the users, so that the organization is prepared for a potential real attack. Attack simulation training includes:

- Simulations
- Training
- Reports
- Automations
- Content library

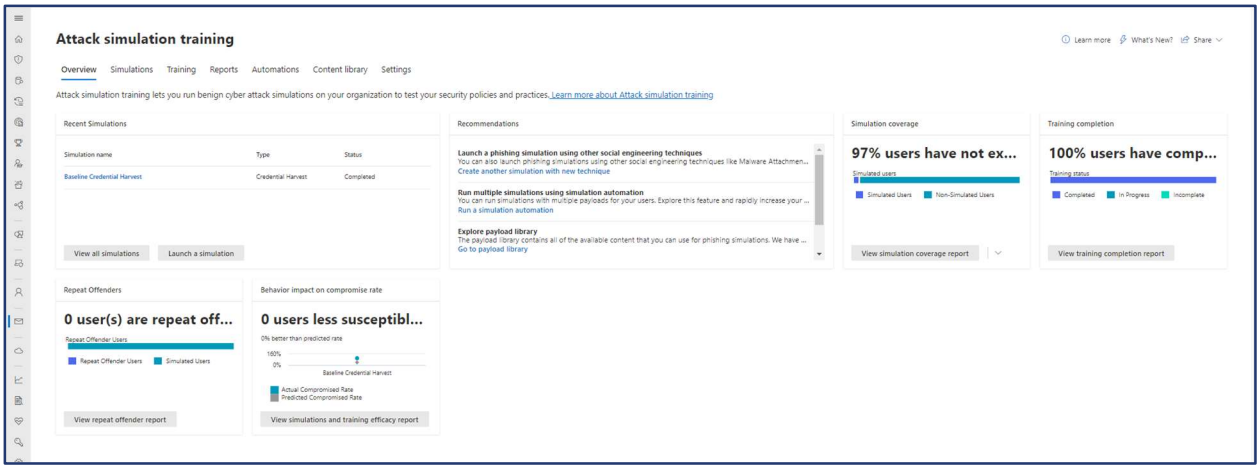


Figure 3: The Attack simulation training dashboard

Simulations

Social engineering is an attack technique that targets human behavior to obtain unauthorized access to sensitive information. This way, social engineering attackers convince users to provide to them sensitive information such as usernames, passwords, or credit card information. To protect users' personal data as well as organizational data, it's important to train users on how to detect social engineering.

Attack simulation training includes the following social engineering attack techniques that security administrators can use to simulate attacks and train users:

- **Credential Harvest**. Includes a malicious email message which contains text that is designed to be very similar to a text that some known party would send, such as a bank, government institution, or cloud service provider. Furthermore, the message also contains a URL link leading to a malicious website that asks the targeted users to provide their usernames and passwords. Attack simulation includes the following steps:
  a. User opens the email.
  b. User selects the link in the email.
  c. User enters their credentials in a form on the malicious website.
- **Malware Attachment**. Includes a malicious email message with an attachment. When the targeted user opens the attachment, a malicious code runs that will cause harm to the user's device or install additional code on a target device to perform further malicious activities. Attack simulation includes the following steps:
  a. User opens the email.
  b. User opens the attachment in the email.
  c. The malicious code from the attachment executes on the user's device.
- **Link in Attachment**. Includes a malicious email message with a URL in an attachment. When the targeted user opens the attachment and then selects the URL link in that attachment, they are led to a malicious website that asks them to provide their usernames and passwords. Attack simulation includes the following steps:

SAMPLE

a. User opens the email payload.
b. User selects the link in the email payload.
c. User enters their credentials in a form on the malicious website.

- **Link to Malware Attachment**. Includes a malicious email message with a URL in an attachment. When the targeted user opens the attachment and then selects the URL link in that attachment, they are led to a file-sharing site that contains a malicious file. When the targeted user opens the malicious file, a malicious code runs that will cause harm to the user's device or will install additional code on a target device to perform further malicious activities. Attack simulation includes the following steps:
  a. User opens the email.
  b. User opens the attachment in the email.
  c. User selects the URL in the attachment.
  d. The malicious code from the attachment runs on the user's device.
- **Drive-by URL**. Includes a malicious email message that contains a URL. When the targeted user selects the URL link in the message, they are redirected to a malicious website that will run background code to gather information about the target or deploy malicious code to the user's device. As in the previous type of attacks, the website will be designed to resemble that of a well-known company. Attack simulation includes the following steps:
  a. User opens the email.
  b. User selects the URL link in the email.
  c. The malicious website runs a code on the user's device.
- **OAuth Consent Grant**. Is based on a Microsoft Azure application that the attacker has created. The application asks the targeted user to grant permissions over some of the user's data by providing a URL link. If the targeted user selects the URL link, the application's consent grant mechanism will be activated, displaying a message; for example, "Contoso Corporation App would like read access to your data." Attack simulation includes the following steps:
  a. User opens the email.
  b. User selects the URL link in the email.
  c. User grants permissions.
- **How-to Guide**. Sends instructions to users on how to accomplish a specific task. The purpose of these instructions is to help guide the recipient into taking a desired action, such as reporting the payload through stylized instructions. Once the action is accomplished, end users would have completed their learning. Attack simulation includes the following steps:
  a. User opens the email.
  b. User reads the email.
  c. User reports the email message as phish.

Creating an attack simulation

To create an attack simulation for training purposes, perform the following steps:

SAMPLE

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in the web browser, enter **https://security.microsoft.com**, and then sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Attack simulation training**.
3. In the **Attack simulation training** dashboard, select **Simulations**, and then select **Launch a simulation**.
4. In the **Select technique** window, select which social engineering technique you'll use for the training purposes, for example, **Credential Harvest**.
5. In the **Name simulation** window, enter the name of the simulation, and, optionally, the description.
6. In the **Select payload and login page** window, select the payload for the simulation technique; for example, **Keep Office 365 password**, or create your own payload.
7. In the **Target users** window, choose between including all users in the organization, or including only specific users and groups.
8. In the **Exclude users** window, select users that you want to exclude from the simulation training.
9. In the **Assign training** window, select the training material that you want to assign to the users after the attack simulation completes, such as Microsoft training experience, or custom training. Furthermore, you can select a training due date for employees, such as 30 days after Simulation ends.
10. In the **Phish landing page** window, select the landing page that will provide further learning instructions to users that will help them identify the phishing email message.
11. In the **Select end user notification** window, select the notification that will be sent to the user, such as training assignment notification and training reminder notification. Furthermore, you will need to select the notification delivery preference, for example, twice a week.
12. In the **Launch details** window, define when to launch the simulation, and when to end the simulation.
13. Finally, in the **Review simulation** window, you can review the simulation information, send a test email for formatting validation, and submit the simulation.
14. When the simulation is launched, users will receive an email with the phishing content, with options to select the content that simulates malicious behavior. Furthermore, users will receive an email with training assignments, where details will be provided on how they will access the training materials and the date by which they need to complete the training.

SAMPLE

Managing and monitoring attack simulations

Security administrators can manage and monitor attack simulations by opening the **Attack simulation training** dashboard and selecting an appropriate tab within the dashboard. The tabs include:

- **Simulations**. Contains the following information:
  - The list of all simulations
  - Scheduled attack simulations

    - Attack simulations in progress
    - Completed attack simulations
    - Failed attack simulations
    - Cancelled attack simulations
- **Training**. Contains the following information:
    - The list of all training campaigns
    - Scheduled training campaigns
    - Training campaigns in progress
    - Completed training campaigns
    - Failed training campaigns
- **Reports**. Contains the following information:
    - Simulation coverage percentage
    - Training competition percentage
    - Repeat offenders
    - Behavior impact on compromise rate
- **Automations**. Used for creating automated flows with specific techniques and payloads whenever a condition is met, such as a specific sender name or sender email.
- **Content library**. Includes multiple types of payloads, i.e., phishing emails and webpages that are used to launch simulations. Security administrators can choose from these payloads to customize the user training experience.
- **Settings**. Defines the threshold for the number of simulations in a row that a user has compromised, and the number of days for which a training module will not be reassigned to a user who has completed the training.

SAMPLE

Lesson 3: Using Microsoft Defender for message security

Messaging and security administrators can use Defender to protect their organizations from various types of threats. Defender includes multiple tools for security settings and configurations, and monitoring tools for analyzing events caused by different types of threats. It also includes several predefined configurations.

By completing this lesson, you'll achieve the knowledge and skills to:

- Explain the preset security policies in Exchange Online Protection and Microsoft Defender for Office 365.
- Manage and configure anti-spam protection.
- Manage and configure anti-malware protection.
- Manage and configure spoofing protection.
- Manage and configure phishing protection.

- Configure Safe Attachments.
- Configure Safe Links.
- Configure connection filtering.
- Configure outbound spam protection.
- Configure quarantine and quarantine policies.

Preset security policies in Exchange Online Protection and Microsoft Defender for Office 365

To help security administrators protect their organizational identities, data, and apps, Microsoft 365 provides several predefined security policies in Exchange Online Protection and Defender for Office 365. Preset security policies are defined with the recommended settings by Microsoft. Furthermore, preset security policies are not static. Microsoft regularly updates them based on existing security threats. In some organizations, security administrators might choose to apply the preset security policies, whereas in other organizations, security administrators might choose to customize some of the preset security policy settings based on the organization's business requirements.

Microsoft 365 includes the following preset security policies:

- **Standard preset security policy**. Includes a baseline profile of security settings for protection against spam, phishing, and malware threats. Standard preset security settings are suitable for most of the recipients in the organization.
- **Strict preset security policy**. Includes a more aggressive profile of security settings against spam, phishing, and malware threats in both Exchange Online Protection and Defender for Office 365. Security administrators might choose to assign strict preset security settings to selected users who work with sensitive information.
- **Built-in protection preset security policy**. Enabled only in tenants where the Defender for Office 365 subscription is included and applied to all users in the organization. Built-in preset security policy includes protection against malicious links and attachments.

SAMPLE

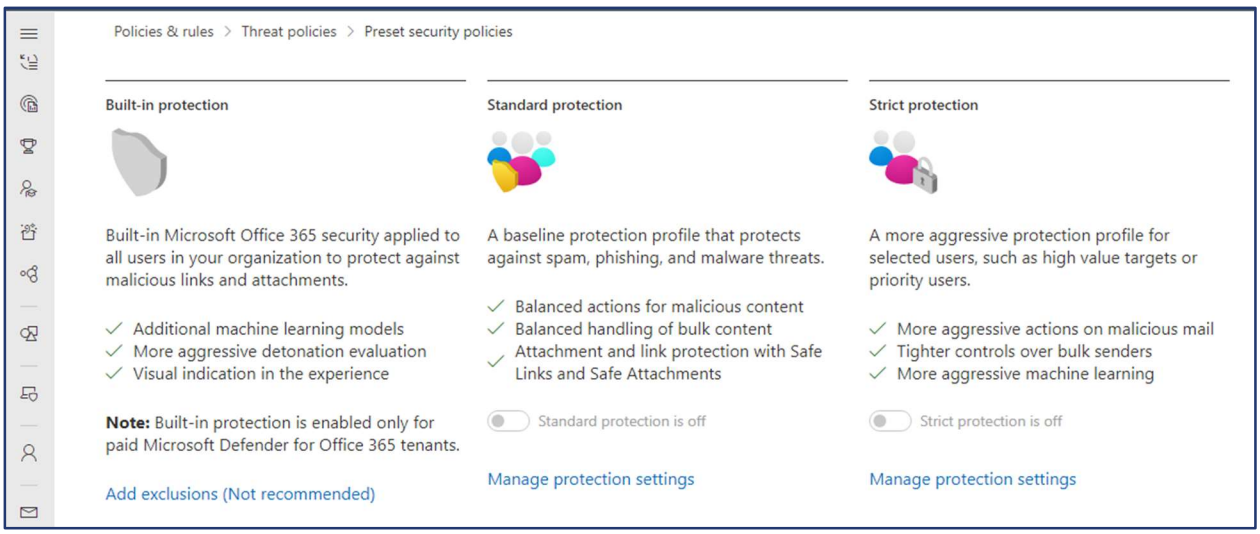


Figure 4: Preset security policies

The following table provides a comparison between Standard and Strict policy security settings.

Table 7: Standard vs. Strict policy security settings

Protection functionality	Standard preset security policy	Strict preset security policy
Anti-malware policy	No difference	No difference
Anti-spam policy: BCL met or exceeded **detection action** (***BulkSpamAction***)	**Move message to Junk Email folder** (MoveToJmf)	**Quarantine message** (Quarantine)
Anti-spam policy: Bulk email threshold (***BulkThreshold***)	**6**	**5**
Anti-spam policy: Spam **detection action** (***SpamAction***)	**Move message to Junk Email folder** (MoveToJmf)	**Quarantine message** (Quarantine)
Anti-phishing policy: If the message is detected as spoof by spoof intelligence (***AuthenticationFailAction***)	**Move message to Junk Email folder** (MoveToJmf)	**Quarantine message** (Quarantine)
Anti-phishing policy:	Selected ($true)	Not selected ($false)

SAMPLE

Show first contact safety tip (***EnableFirstContactSafetyTips***)		
Anti-phishing policy: If mailbox intelligence detects an impersonated user (***MailboxIntelligenceProtectionAction***)	**Move message to Junk Email folder** (MoveToJmf)	**Quarantine message** (Quarantine)
Anti-phishing policy: Phishing email threshold (***PhishThresholdLevel***)	**3 - More aggressive** (3)	**4 - Most aggressive** (4)
Safe Attachments policy	No difference	No difference
Safe Links policy	No difference	No difference

The following table provides a comparison between Built-in protection, Standard, and Strict policy security settings.

Table 8: Built-in protection, Standard, and Strict policy security settings

Protection functionality	**Built-in preset security policy**	**Standard and Strict preset security policy**
Safe Attachments policy	No difference	No difference
Safe Links policy: Let users select through to the original URL (***AllowClickThrough***)	Selected ($true)	Not selected ($false)
Safe Links policy: Do not rewrite URLs, do checks via Safe Links API only (***DisableURLRewrite***)	Selected ($true)	Not selected ($false)
Safe Links policy: Apply Safe Links to email messages sent within the organization (***EnableForInternalSenders***)	Not selected ($false)	Selected ($true)

SAMPLE

Configuration analyzer tool

Exchange Online Protection also includes the *Configuration analyzer* tool, which helps messaging administrators identify potential issues in a configuration. Based on the analysis, Configuration analyzer can suggest a standard recommendation or strict recommendation. For example, if the messaging administrator has configured the Bulk email threshold setting to 7, then a standard recommendation will suggest a setting of 6, whereas a strict recommendation will suggest a setting of 5. Configuration analyzer includes the **Apply recommendation** option, which messaging administrators can select to apply the recommended setting, instead of applying it manually.

Managing preset security policies

To manage preset security policies, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and then, from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com** and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies** and then select **Preset security policies**.
4. In the Preset security policies window, note that you cannot edit Built-in protection, except to create exclusions for users, groups, and domains.

> **Caution**: Creating exclusions in Built-in protection is not recommended.

5. In the Preset security policies window, you can choose to enable and configure Standard protection and Strict protection.

To enable preset Standard or Strict security policies, perform the following steps:

1. In the Preset security policies window, under **Standard protection** or under **Strict protection**, select **Manage protection settings**.
2. In the Apply Exchange Online Protection window, choose from the following settings:
   - Whether to apply Exchange Online Protection to:
     - Include all recipients
     - Include specific recipients, groups and domains
     - Exclude specific recipients, groups, and domains
   - Whether to not apply Exchange Online Protection
   - Whether to apply Defender for Office 365 Protection to:
     - The same recipients as Exchange Online Protection
     - Include all recipients, include specific recipients, groups, and domains
     - Exclude specific recipients, groups, and domains
   - Whether to not apply Defender for Office 365 Protection
3. In the **Impersonation protection** section, choose:

SAMPLE

- Which custom users and domains to protect
- Which trusted email addresses and domains will not be flagged as impersonation

4. In the Policy mode window, select if you want the policy to be turned on or off after completing the wizard.
5. In the Review and confirm your changes window, select **Confirm** to apply the policy.

When multiple policies apply to a recipient, the security settings will apply in the following order:

1. The Strict preset security policy
2. The Standard preset security policy
3. Defender for Office 365 evaluation policies
4. Custom policies based on the priority of the policy (a lower number indicates a higher priority)
5. The Built-in protection preset security policy for Safe Links and Safe Attachments; the default policies for anti-malware, anti-spam, and anti-phishing

SAMPLE

Managing and configuring anti-spam protection

Exchange Online Protection includes multiple technologies for anti-spam protection that are activated by default in every subscription that contains Exchange Online, for example:

- Exchange Online Plan 1
- Exchange Online Plan 2
- Office 365
- Microsoft 365
- Subscriptions that include stand-alone Exchange Online Protection.

Every email message that Exchange Online Protection receives goes through a filtering process. Depending on the results of the filtering, Exchange Online Protection takes the appropriate action. One of the actions is assigning an SCL value in each message's X-header. The SCL can take different values, and the higher the value, the higher the possibility that the email message is spam.

The following table describes SCL values and their definitions.

Table 9: SCL values and their definitions

SCL	Definition	Default action
-1	The message skipped spam filtering. For example, the message is from a safe sender, was sent to a safe recipient, or is from an email source server on the IP Allow List.	Deliver the message to recipient Inbox folders.
0, 1	Spam filtering determined the message wasn't spam.	Deliver the message to recipient Inbox folders.

5, 6	Spam filtering marked the message as Spam.	Default anti-spam policy, new anti-spam policies, and Standard preset security policy: Deliver the message to recipient Junk Email folders.
7, 8, 9	Spam filtering marked the message as High confidence spam.	Default anti-spam policy and new anti-spam policies: Deliver the message to recipient Junk Email folders.

Note: For more information, refer to Create safe sender lists in EOP.

Similar to SCL, the BCL is a value that is assigned to an email message's X-header. The higher the BCL, the higher the possibility that an email message is bulk.

The following table describes BCL values and their definitions.

Table 10: BCL values and definitions

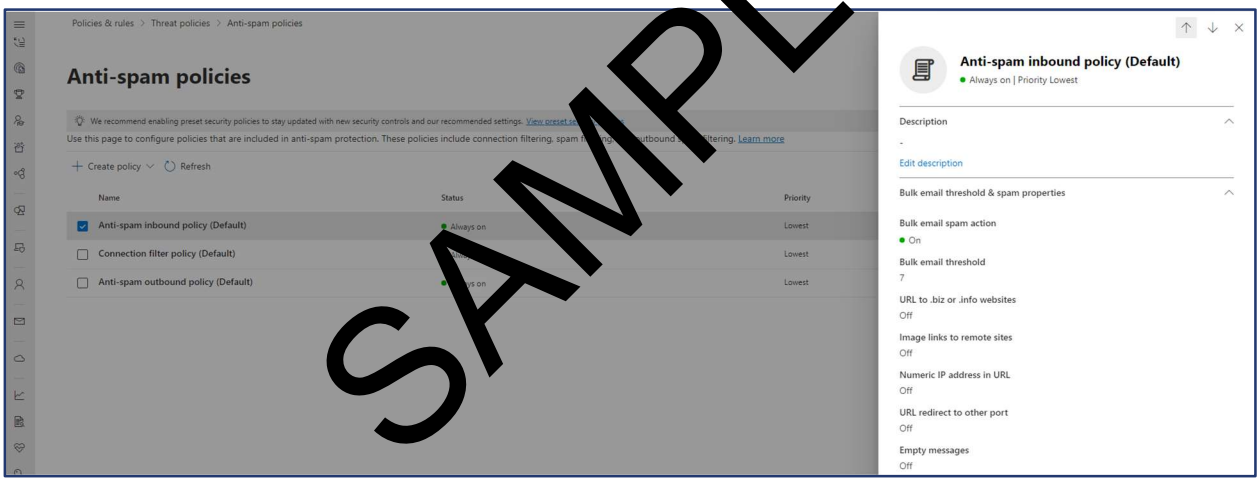
BCL	Definition	Default action
0	The message isn't from a bulk sender.	Deliver the message to recipient Inbox folders.
1, 2, 3	The message is from a bulk sender that generates few complaints.	Deliver the message to recipient Inbox folders.
4, 5, 6, 7	The message is from a bulk sender that generates a mixed number of complaints.	Default anti-spam policy and new anti-spam policies: 7. Deliver the message to recipient Junk Email folders. Standard preset security policy: 6. Deliver the message to recipient Junk Email folders. Strict preset security policy: 5. Quarantine the message.
8, 9	The message is from a bulk sender that generates a high number of complaints.	Default anti-spam policy, new anti-spam policies, and Standard preset security policy: Deliver the message

SAMPLE

		to recipient Junk Email folders. Strict preset security policy: Quarantine the message.

To protect organizations from different types of unsolicited email messages, Exchange Online Protection introduces the following email classification:

- **Spam.** An email message is classified as spam if it has received a spam-confidence level (SCL) of 5 or 6.
- **High confidence spam**. An email message is classified as high confidence spam if it has an SCL of 7, 8, or 9.
- **Phishing**. Email messages classified as phishing are quarantined or sent to the **Junk** email folder.
- **High confidence phishing**. Email messages classified as high confidence phishing are always quarantined and cannot be released by users.
- **Bulk**. An email message is classified as bulk if it meets or exceeds the configured BCL threshold.



SAMPLE

Figure 5: Anti-spam inbound policy settings

Managing anti-spam policies

Messaging administrators can use anti-spam policies to manage anti-spam settings. To access anti-spam policies, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Anti-spam**.
4. In the Anti-spam policies window, review the default anti-spam policies:

- **Anti-spam inbound policy (Default)**
- **Connection filter policy (Default)**
- **Anti-spam outbound policy (Default)**

5. In the Anti-spam policies window, you can create customized anti-spam polices by selecting **Create policy**, and then selecting **Inbound**. The new policy settings include:
   - **Name** and, optionally, **Description**.
   - **Include Users, Groups, and Domains in the policy** . Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied only to those recipients that match *all* of the specified recipient filters, i.e., users and groups and domains.
   - **Exclude Users, Groups, and Domains in the policy** . Same as when including, note that the policy is applied only to those recipients that match all the specified recipient filters, i.e., users and groups and domains.
   - **Bulk email threshold & spam properties**. In this window, you can configure the bulk email threshold, which, by default, has the value **7**.

     You may choose to increase the spam score of an email message if it contains the following type of links or URLs:

     - Image links to remote websites
     - Numeric IP address in URL
     - URL redirect to other port
     - Links to website with top level domain of .biz or .info.

     Furthermore, you may choose to mark messages as spam if they include the following properties:

     - Empty messages
     - Embedded tags in HTML
     - JavaScript or VBScript in HTML
     - Form tags in HTML
     - Frame or iframe tags in HTML
     - Web bugs in HTML
     - Object tags in HTML
     - Sensitive words
     - SPF record: hard fail
     - Sender ID filtering hard fail
     - Backscatter
     - Contain specific languages, or originate from specific countries

     Moreover, you may configure test mode options, such as adding default X-header text to the email message if some of the criteria are met.

SAMPLE

- **Actions**. In the Actions window, you can set the action for the anti-spam policy if the messages are marked as belonging one of the following categories:
  - Spam
  - High confidence spam
  - Phishing
  - High confidence phishing
  - BCL met or exceeded

  The actions on email messages that are marked by Exchange Online Protection with these categories include:

  - **Move message to Junk Email folder**
  - **Add X-header**
  - **Prepend subject line with text**
  - **Redirect message to email address**
  - **Delete message**
  - **Quarantine message**. If you choose the **Quarantine message** action, you'll also need to specify a quarantine policy. There are three quarantine policies to choose from:
    - **DefaultFullAccessPolicy**. When you select this policy, users will have permissions to preview the message, release the message from quarantine, delete the message, or block the sender. The users will not receive quarantine notifications.
    - **AdminOnlyAccessPolicy**. When you select this policy, only the security administrators will have permissions to preview the message or release the message from quarantine. The users will not receive quarantine notifications.
    - **DefaultFullAccessWithNotificationPolicy**. When you select this policy, users will have permissions to preview the message, release the message from quarantine, delete the message, or block the sender. The user will also receive quarantine notifications.
  - **Enable safety tips** that give informational messages in Outlook, which inform the recipient about potentially harmful messages.
  - **Zero-hour auto purge** (ZAP), which enables purging messages that contain spam, phishing, or malware from the recipient's inbox.
- **Allow & block list**. In the Allow & block list window, you can add allowed and blocked senders and domains.

Managing and configuring anti-malware protection

Exchange Online Protection includes functionalities that protect organizations from different types of malware. Anti-malware functionality is activated by default in every subscription that contains Exchange Online and also in subscriptions that include standalone Exchange Online Protection.

Major malware threats can include:

SAMPLE

- **Viruses**. Viruses infect apps and data, and spread to other files on the computer's storage, as well as through the network.
- **Spyware**. Spyware performs unauthorized gathering of users' personal data and sends the data to attackers.
- **Ransomware**. Ransomware encrypts the data of the attacked user and demands payment from the user to decrypt the data.

Anti-malware protection in Exchange Online Protection includes the following functionalities:

- **Layered defenses against malware**. Exchange Online Protection uses multiple anti-malware engines that include heuristic detection to protect organizations from malware.
- **Real-time threat response.** Exchange Online Protection provides real-time anti-malware protection by updating security policy rules every two hours.
- **Fast anti-malware definition deployment**. Exchange Online Protection uses anti-malware engines that are deployed right after they are developed.

If Exchange Online Protection finds email message that contain malware, it will quarantine the message. Users by default cannot access or release quarantined email messages that contain malware. Only messaging administrators can access email messages that were quarantined because of containing malware. In some organizations, a SecOps mailbox is used, which is a dedicated mailbox that contains unfiltered messages that are analyzed by security administrators. For that purpose, anti-malware filtering is skipped for SecOps mailboxes.

SAMPLE



Figure 6: Anti-malware policy settings

Managing anti-malware policies

Messaging administrators can manage anti-malware settings through anti-malware policies. To access anti-malware policies, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Anti-malware**.
4. In the Anti-malware window, review the default anti-spam policy: **Default (Default)**
5. In the Anti-malware window, you can create customized anti-malware policies by selecting **Create**. The new policy settings include:
    - **Name** and, optionally, **Description**.
    - **Include Users, Groups, and Domains** in the policy. Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied only to those recipients that match *all* of the specified recipient filters, i.e., users and groups and domains.
    - **Exclude Users, Groups, and Domains** from the policy. Same as when including, note that the policy is applied only to those recipients that match all the specified recipient filters, i.e., users and groups and domains.
    - **Protection settings**. In the Protection settings window, you can configure the following settings:
        - **Enable the common attachment filter**, which rejects or quarantines common attachment file types that might include malware, such as .exe, .bat, .cmd, and many others. You can also customize the list of file types by adding and removing different file types. Furthermore, you can define the action that Exchange Online Protection will perform when it discovers that a specified attachment type is found in the email message, such as rejecting the message with a non-delivery recipient (NDR) or quarantining the message.
        - **Enable zero-hour auto purge for malware**, which quarantines email messages that contain malware, but which have already been delivered into Exchange Online mailboxes.
        - **Quarantine policy**. By default, the quarantine policy is configured as **AdminOnlyAccessPolicy**, which allows only messaging administrators to access the quarantined messages.
        - **Notifications**. You can choose if you want administrators to be informed regarding undelivered email messages from internal or external senders. You can decide if you want a default notification text to be sent, or you want to customize the notification text.

SAMPLE

Managing and configuring spoofing protection

Spoofing is an attack technique in which attackers send email messages that appear to originate from some known organization, or even from the same organization as the attacked user. Exchange Online Protection includes functionalities that protect organizations from different types of spoofing attacks, such as email authentication, spoof intelligence insight, allowing or blocking spoofed senders, anti-phishing policies, and spoof detections report.

Email authentication

Email authentication (also known as email validation) contains several standards that are designed to protect organizations from spoofing. Exchange Online Protection uses the following standards that work together to verify inbound email:

- **SPF – Sender Policy Framework**. SPF is a standard that requires that organizations publish a TXT SPF record in the public DNS. The SPF record includes IP addresses and domain names of the sender organization's email servers. When the recipient organization's email server receives an email message, it performs a DNS lookup to verify that the sender organization's SPF record is published on a public DNS, and that the sender email server's IP address and domain name match the SPF record data. If the DNS lookup is successful, then the email message is forwarded to other Exchange Online Protection filtering components. However, if DNS lookup fails, then the message might be rejected.

  If the organization's email solution is based only on Exchange Online, the TXT SPF DNS record will have the following format:

  ```
  v=spf1 include:spf.protection.outlook.com -all
  ```

  If the organization's email solution is based only on Exchange hybrid configuration, or on Exchange Online plus an additional email server, the TXT SPF DNS record will have a format like the following example:

  ```
  v=spf1 include:spf.protection.outlook.com ipv4:<IP address of the email server> -all
  ```

- **DKIM - DomainKeys Identified Mail**. DKIM is a standard that provides a digital signature to outbound email messages in the message header. Recipient organizations can use this digital signature to help verify whether incoming email originates from the sender organization and is not spoofed.

  To configure DKIM for Exchange Online, perform the following steps:

  1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
  2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
  3. In the Policies & rules window, select **Threat policies**, select **Email authentication settings**, and then select the **DKIM** tab.
  4. In the DomainKeys Identified Mail (DKIM) window, select the SMTP domain, such as contoso.com, and then select **Create DKIM keys**.
  5. In the Publish CNAMEs window, select **Copy** to copy the CNAME records that will need to be added in the public DNS for the SMTP domain of your organization.
  6. On your organization's public DNS, enter the CNAME records you copied in the previous step.
  7. In the DKIM window, select the toggle button, so that it displays its status as **Enabled**.

SAMPLE

- **DMARC - Domain-based Message Authentication, Reporting, and Conformance** . DMARC is a standard that requires that organizations publish a TXT record in the public DNS. The recipient's organization email server validates the origin of the email messages by authorizing the sender's organization email servers. For example, an organization with a SMTP domain contoso.com may have the following TXT DMARD DNS record:

```
_dmarc.domain  TTL  IN  TXT  "v=DMARC1; p=policy; pct=100"
```

  Parameters in the TXT record include:

  - **domain** is the SMTP domain of the sender's organization, for example contoso.com.
  - **TTL** is Time To Live in seconds.
  - **policy** specifies what action should be performed if DMARC fails. The policy parameter values include **none**, **quarantine**, or **reject**.
  - **pct** defines percentage on email where this rule should be used. In our example, the rule is used for 100% of email.

- **ARC - Authenticated Received Chain**. ARC is a standard that reduces email delivery failures due to modifications applied to the organization's sent email from legitimate services. For example, an organization might send all outgoing email to a third-party service that adds modification on every outgoing email message. This scenario might cause SPF, DKIM, and DMARC verifications to fail, because the message sender's IP address and the message content has been modified. ARC reduces potential SPF, DKIM, and DMARC failures by preserving the original email authentication information.

  In Exchange Online, ARC is implemented by adding the trusted ARC sealer, where Microsoft 365 validates and trusts the authentication results that the ARC sealer provides when an email is delivered to the recipient organization.

  To configure ARC in Exchange Online, perform the following steps:

  1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
  2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
  3. In the Policies & rules window, select **Threat policies**, select **Email authentication settings**, and then select the **ARC** tab.
  4. In the Trusted ARC sealers window, select **Add**.
  5. In the Add trusted ARC sealers window, enter the name of the trusted signing domains, and then select **Save**.

SAMPLE

Spoof intelligence insight and Allow/Block list

Spoof intelligence insight allows messaging administrators to review detected spoofed messages from senders in internal and external domains during the previous seven days. If spoof intelligence insight detects spoofed senders who are legitimately sending unauthenticated email (messages from domains that don't pass SPF, DKIM, or DMARC checks), messaging administrators can

manually allow those legitimate known senders. Messaging administrators can also manually create an Allow list for legitimate spoof senders, or Block list for known unauthorized spoof senders.

Anti-phishing policies

Messaging administrators can configure additional anti-spoofing settings located in the Exchange Online anti-phishing policies.

To configure anti-spoofing settings in Exchange Online, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Anti-Phishing**.
4. In the Anti-phishing window, create a new anti-phishing policy, or edit the existing anti-phishing policy to configure the following anti-spoofing settings:
   - Turn spoof intelligence on or off.
   - Specify the action for blocked spoofed senders, such as rejecting the message, quarantining the message, or moving the message to the recipient's Junk email folder.
   - Turn unauthenticated sender indicators in Outlook on or off.

Spoof detections report

Organizations with a Defender for Office 365 subscription can use the Spoof detection aggregate report, which provides information on users that were allowed or blocked due to spoofing. To monitor spoofing by using the spoof detections report in Defender for Office 365, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, select **Reports**, and then in the Reports window, select **Email & collaboration reports**.
3. In the Email & collaboration reports window, in the **Spoof detection report**, select **View details**.

   The spoof detection report contains information regarding the number of messages with specific status type, such as: Pass, Fail, SoftPass, None, and Other, as well as information such as Date, Spoofed user, Sending infrastructure, Spoof type, Result, Result code, SPF, DKIM, DMARC, and Message count.

SAMPLE

Managing and configuring phishing protection

Phishing is an attack technique in which attackers send email messages that are designed to resemble email messages from well-known organizations, such as banks, government institutions, or cloud service providers. Such email messages ask users to select a link where sensitive information is requested, such as username, password, or credit card number. This way, attackers get unauthorized access to users' data or bank accounts.

Exchange Online includes anti-phishing policies that are enabled by default and protect organizations from phishing attacks.

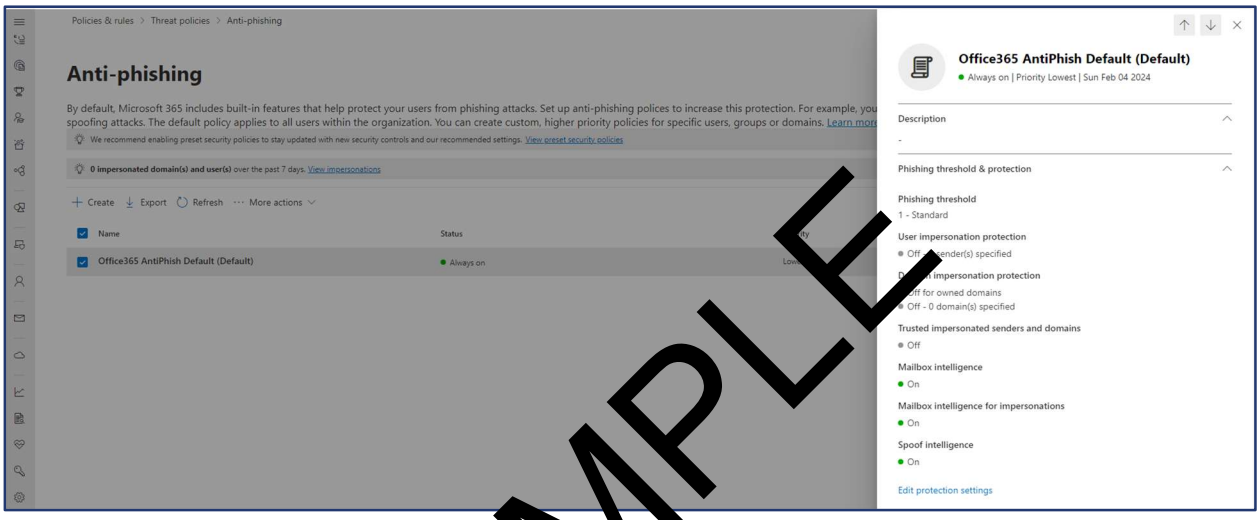


Figure 7: Anti-phishing policy settings

SAMPLE

To configure anti-phishing settings in Exchange Online, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, then select **Anti-Phishing**.
4. In the Anti-phishing window, select **Create** to create a new anti-phishing policy and to configure the following anti-phishing settings:
   - **Policy name** and, optionally, a **Description**.
   - **Include Users, Groups, and Domains** in the policy. Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied only to those recipients that match *all* of the specified recipient filters, i.e., users and groups and domains.
   - **Exclude Users, Groups, and Domains** from the policy. Same as when including users, note that the policy is applied only to those recipients that match *all* the specified recipient filters, i.e., users and groups and domains.
   - **Phishing threshold & protection** includes the following settings:

- **Phishing email threshold**. This setting can have the following values: 1 (Standard), 2 (Aggressive), 3 (More Aggressive), and 4(Most Aggressive).
- **Enable users to protect prevents specific email addresses from being impersonated as message senders**. This setting is recommended to include users that have important roles in the organization and work with sensitive data.
- **Enable domains to protect**. Prevents specific domains in the sender's email address from being impersonated. This setting includes the domain owned by the organization, as well as additional custom domains, such as partner organizations' domains.
- **Enable mailbox intelligence**. Uses artificial intelligence to identify potential impersonation attempts.
- **Enable intelligence for impersonation protection**. Uses enhanced impersonation results based on each user's individual sender map and allows messaging administrators to define specific actions on impersonated messages. Message actions include:
  - Redirect the message to other email addresses
  - Move the message to the recipients' Junk Email folder
  - Quarantine the message
  - Deliver the message and add other addresses to the Bcc line
  - Delete the message before it's delivered

SAMPLE

Configuring Safe Attachments

Safe Attachments is a functionality in subscriptions that include Defender for Office 365. Safe Attachments provides the capability to analyze the attachment in an isolated virtual environment and check for any potential malware threats. This process is also known as *detonation*.

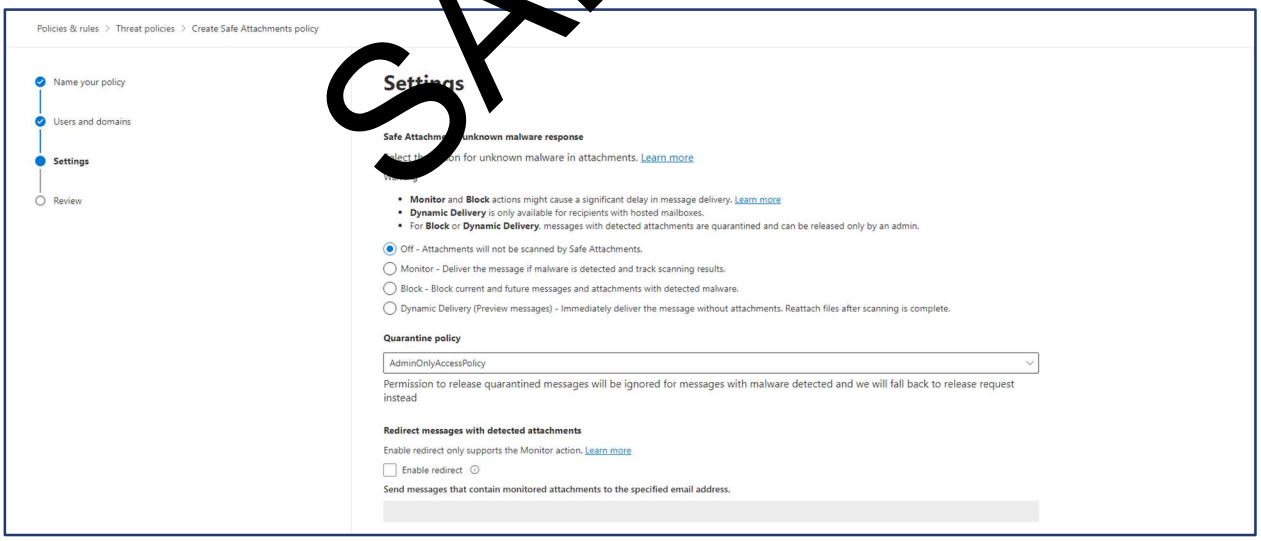


Figure 8: Safe Attachments policy settings

Messaging administrators can manage Safe Attachments settings through policies. To access safe attachment policies, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the left navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Safe Attachments**.
4. In the Safe Attachments window, review the default safe attachment policy: **Built-in protection (Microsoft)**
5. In the Safe Attachments window, select **Create** to create a new safe attachment policy and to configure the following safe attachment settings:
   - **Policy name** and, optionally, a **Description**.
   - **Include Users, Groups, and Domains** in the policy. Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied *only* to those recipients that match all of the specified recipient filters, i.e., users and groups and domains.
   - **Exclude Users, Groups, and Domains** in the policy. Same as when including, note that the policy is applied only to those recipients that match all the specified recipient filters, i.e., users and groups and domains.
6. In the Settings window, define the action for unknown malware response:
   - **Monitor**. This action delivers the email message if malware is detected and tracks the scanning results.
   - **Block**. This action blocks every email message and attachment if malware is detected.
   - **Dynamic Delivery (Preview messages)**. This action delivers the message without an attachment, where the attachment is analyzed in an isolated virtual environment. If the attachment scanning results indicate that there is no malware, the attachment will be reattached to the message which has already been delivered in the user's mailbox.
   - **Quarantine policy**. Defines who will have access to review messages that are quarantined as a result of Safe Attachments malware scanning.
   - **Redirect messages with detected attachments**. This action is available only if the **Monitor** option is selected. If an email message contains malware, it will be forwarded to the specific email address for analysis and investigation.
7. In the Notifications window, choose whether to use the default notification text, or to use customized notification text.

SAMPLE

Configuring Safe Links

Safe Links is a functionality in subscriptions that include Defender for Office 365. Safe Links protects users in organizations from malicious URL links that attackers insert into phishing attacks or other email messages with malicious content. Safe Links protects users when selecting URL links not just in email messages, but also in Teams and Office apps. Whenever users select a URL link, Safe Links will provide URL scanning, rewriting, and verification if the link is safe to be opened or if it needs to be blocked because of malicious content it links to.

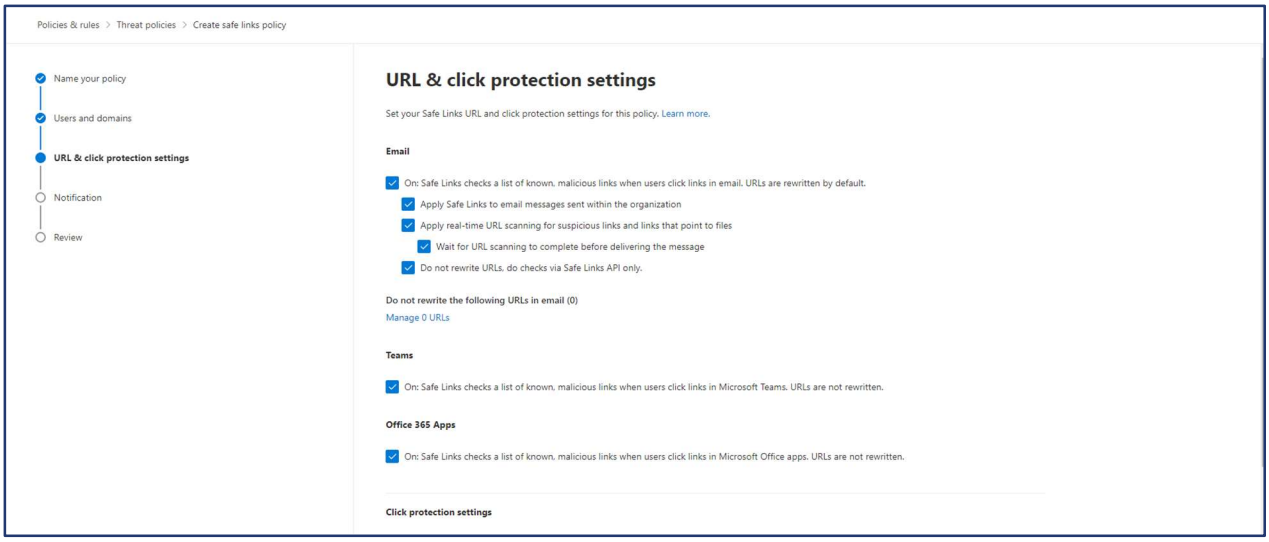


Figure 9: Safe Links policy settings

Messaging administrators can manage Safe Links settings through policies. To access Safe Links policies, perform the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Safe Links**.
4. In the Safe Links window, review the default Safe Links policy:
   - **Built-in protection (Microsoft)**
5. In the Safe Links window, select **Create** to create a new Safe Links policy and to configure the following settings:
   - **Policy name** and, optionally, a **Description**.
   - **Include Users, Groups, and Domains** in the policy. Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied only to those recipients that match *all* of the specified recipient filters, i.e., users and groups and domains.
   - **Exclude Users, Groups, and Domains** from the policy. Same as when including, note that the policy is applied only to those recipients that match all the specified recipient filters, i.e., users and groups and domains.
6. In the URL & click protection settings window, define the following settings for email:
   - **Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.** If this setting is selected, the following options are available:
     - **Apply Safe Links to email messages sent within the organization**
     - **Apply real-time URL scanning for suspicious links and links that point to files** . In addition, for this option you can choose **Wait for URL scanning to complete before delivering the message**

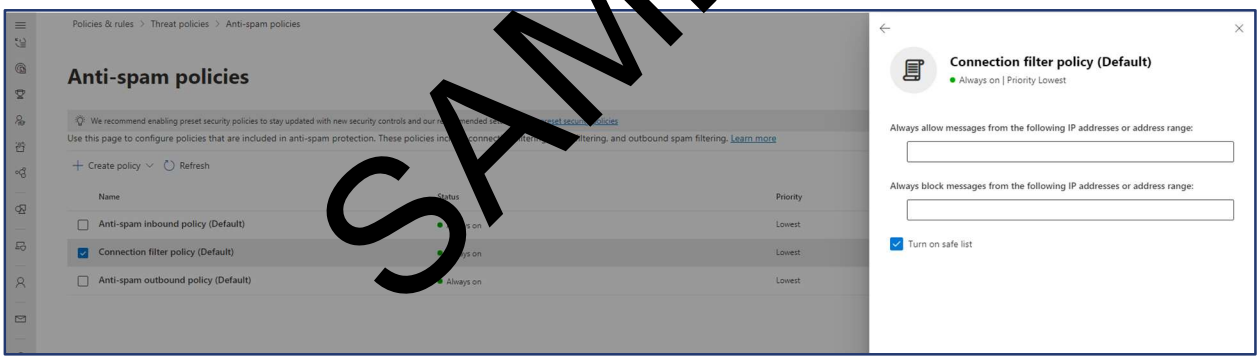
SAMPLE

- **Do not rewrite URLs, do checks via Safe Links API only**
- **Track user clicks**. This setting stores data on user clicks. For this option, you can also choose **Let users click through to the original URL** and **Display the organization branding on notification and warning pages**.

Configuring connection filtering

Connection filtering is an Exchange Online Protection functionality that protects organizations from malicious senders by detecting IP addresses from which harmful email messages might be sent. Connection filtering is available in subscriptions that include Defender for Office 365 and has three main components:

- **IP Allow List**. The IP Allow List includes IP addresses and IP address ranges that are considered safe. Therefore, spam filtering will be skipped for incoming email messages from IP addresses that are on the IP Allow List. However, all incoming email messages will be scanned for malware and high-confidence phishing.
- **IP Block List**. The IP Block List includes IP addresses and IP address ranges that are considered malicious. Therefore, all incoming email messages that are from IP addresses on the IP Block List will be rejected, and no other scanning will occur.
- **Safe list**. The Safe list includes IP addresses and IP address ranges that are considered safe. Microsoft maintains the Safe list. Messaging administrators cannot manage the Safe list but can choose to enable or disable it. All incoming email messages from IP address on the Safe list are skipped from the spam filtering.



SAMPLE

Figure 10: Connection filter policy settings

Messaging administrators can manage connection filtering settings through anti-spam policies by performing the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Anti-spam**.
4. In the Anti-spam policies window, select **Connection filter policy (Default)**.
5. In the Connection filter policy (Default) window, select **Edit connection filter policy**.

6. In the Connection filter policy (Default) window, the IP Allow list is located under **Always allow messages from the following IP addresses or address range** .
7. In the Connection filter policy (Default) window, the IP Block list is located under **Always block messages from the following IP addresses or address range** .
8. In the Connection filter policy (Default) window, select the **Turn on safe list** checkbox to enable the safe list.

Configuring outbound spam protection

Many messaging administrators focus on protecting organizations from inbound spam, but internal users can also be a threat when they unintentionally or intentionally send a large number of emails. By sending a large number of emails, users risk:

- Being considered spam senders by recipient organizations.
- Being listed on various block lists.
- Damaging the reputation of their organization.

Therefore, Exchange Online Protection includes outbound spam protection, which prevents Exchange Online from sending a large number of emails. Furthermore, in scenarios where organizations need to send a large number of emails, such as for marketing campaigns, organizations can choose to use third-party services that are specialized for sending mass email.

SAMPLE



Figure 11: Anti-spam outbound policy settings

Messaging administrators can manage outbound spam protection settings through anti-spam policies by performing the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Anti-spam**.
4. In the Anti-spam policies window, select and review the **Anti-spam outbound policy (Default)**.
5. In the Anti-spam policies window, to create a new Anti-spam outbound policy, select **Create policy**, and then select **Outbound** to configure the following settings:
    - **Policy name** and, optionally, a **Description**.
    - **Include Users, Groups, and Domains** in the policy. Note that Users, Groups, and Domains are connected with the word And, which means that the policy is applied only to those recipients that match *all* of the specified recipient filters, i.e., users and groups and domains.
    - **Exclude Users, Groups, and Domains** in the policy. Same as when including, note that the policy is applied only to those recipients that match all the specified recipient filters, i.e., users and groups and domains.
6. In the Protection settings window, configure the following settings:
    - **Set an external message limit.**
    - **Set an internal message limit.**
    - **Set a daily message limit.**
    - **Restriction placed on users who reach the message limit**. This setting has the following options:
        - **Restrict the user from sending mail until the following day**
        - **Restrict the user from sending email**
        - **No action, alert only**
    - **Forwarding rules**. This setting controls automatic email forwarding to external recipients, and has the following options:
        - **Automatic**. System-controlled option that disables automatic email forwarding to external recipients.
        - **On**. Automatic external email forwarding isn't disabled by the policy.
        - **Off**. All automatic external email forwarding is disabled by the policy.
    - **Notifications**. This setting has following options:
        - **Send a copy of suspicious outbound messages that exceed these limits to these users and groups**
        - **Notify these users and groups if a sender is blocked due to sending outbound spam**

SAMPLE

Configuring quarantine and quarantine policies

Exchange Online Protection uses quarantine to store messages that could potentially be malicious or spam. For some types of potentially unwanted email messages, such as spam email, messaging administrators can decide whether the message will be delivered to quarantine, or to the user's Junk email folder. However, email messages that contain potentially malicious content are

automatically delivered to quarantine. Furthermore, depending on the type of the potentially unwanted message, administrators can decide if they will allow users to access their quarantine. By default, users can have access to email messages that are stored in quarantine and don't contain malware. Only messaging administrators can have access to email messages that are stored in quarantine and potentially contain malware.

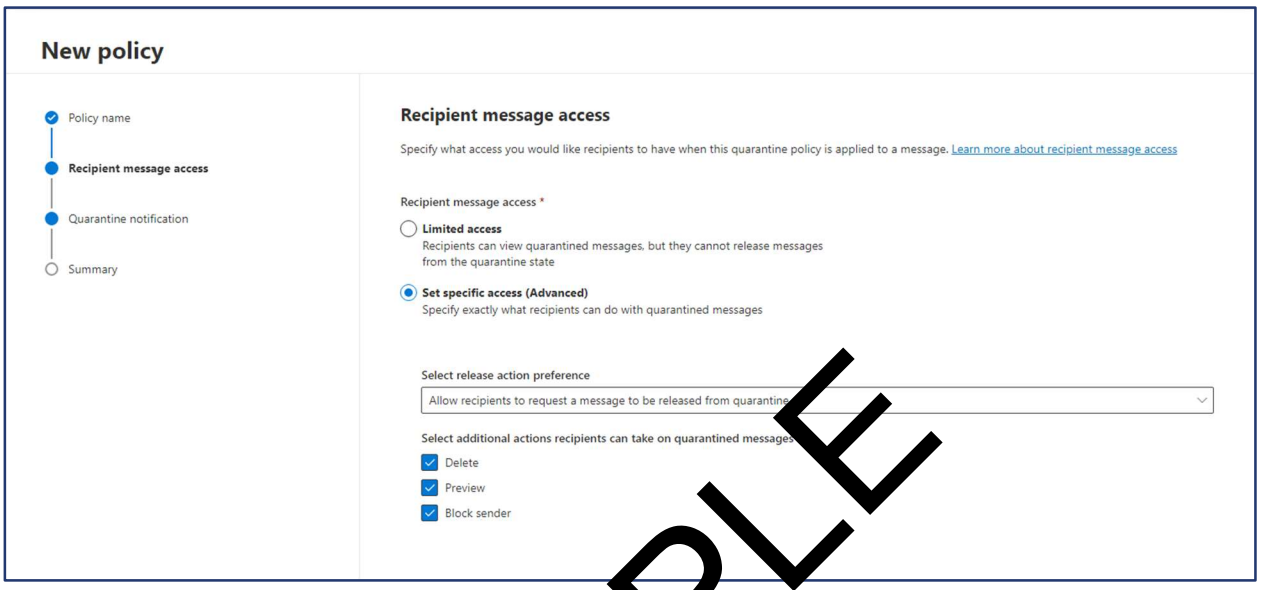


Figure 12: Quarantine policy settings

SAMPLE

Messaging administrators can manage quarantine settings through quarantine policies by performing the following steps:

1. Open Microsoft Defender. Sign in to Microsoft 365 admin center, and from the navigation menu, select **Security**. Alternatively, in a web browser, enter **https://security.microsoft.com**, and sign in with your credentials.
2. In the navigation menu, under **Email & collaboration**, select **Policies & rules**.
3. In the Policies & rules window, select **Threat policies**, and then select **Quarantine policies**.
4. In the Quarantine policy window, review the default quarantine policies:
   - **DefaultFullAccessPolicy**
   - **AdminOnlyAccessPolicy**
   - **DefaultFullAccessWithNotificationPolicy**
5. In Quarantine policy window, to create a new quarantine policy, select **Add custom policy**, and then configure the following setting: **Policy name**.
6. In Recipient message access, configure the following settings:
   - **Limited access**. This setting allows recipients to review their quarantined email messages, but they cannot release them from the quarantine state.
   - **Set specified access (Advanced)**. This setting contains of following options:
     - **Select release action preference**. **Allow recipients to request a message to be released from quarantine** or **Allow recipients to release a message from quarantine**

        - Select additional actions recipients can take on quarantined messages . Delete, Preview, and Block sender.
    - Quarantine notification: Enable or Disable .

Lab A: Implementing message security with preset security policies

Please refer to the online lab to supplement your learning experience with exercises.

Lesson 4: Implementing message encryption in Exchange Online

Email messages that are sent between users have different characteristics in terms of confidentiality. Some email messages contain sensitive or confidential information, such as information about new products or innovations, financial reports, employee information, or legal contracts. Sending email messages with sensitive information to unintended users might cause issues with the organization's reputation, but also might cause financial consequences for the organization. Exchange Online includes message encryption functionalities that help organizations protect sensitive information sent over email, but also to protect email data that is stored in Microsoft datacenters.

By completing this lesson, you'll achieve the knowledge and skills to:

- Explain how message encryption works in Exchange Online.
- Implementing Microsoft Purview Message Encryption.
- Manage message encryption.
- Manage advanced message encryption in Exchange Online.

SAMPLE

How does message encryption work in Exchange Online?

Exchange Online includes multiple technologies that you can use to encrypt and protect your organization's data. Some of these technologies are built into Microsoft 365 datacenters, enabled by default, and cannot be turned off. There are also some functionalities that you can configure and customize to meet specific business requirements. In the following scenarios, encryption technologies include data protection:

- Data in transit:
    - By default, email messages that are sent between mailboxes in Microsoft datacenters are encrypted by using the Transport Layer Security (TLS) protocol.
    - Users can digitally sign and encrypt email messages by using the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol. While S/MIME has been supported from the

earliest versions of Exchange Server, it is also supported in Exchange Online. For this functionality to be implemented, each user must be provided with a *key pair* – a private key and a public key. These keys are generated by the Public Key Infrastructure (PKI) service.

  - Users can encrypt email messages by using Microsoft Purview Message Encryption. For this functionality, users just need to select the **Encrypt** option and choose an encryption template to protect the email message.

- **Data at rest**. All the user data in Microsoft datacenters is stored on disks that are encrypted with BitLocker encryption technology.

Microsoft Purview Message Encryption

Microsoft Purview Message Encryption is an Exchange Online messaging encryption functionality that includes policies for encryption, identity, and authorization. Microsoft Purview Message Encryption uses Microsoft Azure Rights Management Services (Azure RMS), which is part of Azure Information Protection (AIP).

An email message can be encrypted with Microsoft Purview Message Encryption in two ways:

- Users that need to send an email message with sensitive content activate the encryption manually in Outlook or Outlook on the web by selecting the **Encrypt** option and choosing the appropriate encryption template from the drop-down menu.
- Messaging administrators create a mail flow rule that activates message encryption based on some criteria; for example, email is sent to a specific recipient or email is sent that contains sensitive information. In such a scenario, users don't activate the encryption manually; however, whenever they send email that matches the mail flow criteria, the message is automatically encrypted by Exchange Online.

The intended recipients decrypt the encrypted message in one of the following ways:

- Recipients whose mailboxes are located in Exchange Online and connected with Microsoft Outlook or Outlook on the web can open the encrypted email the same way as they would open unencrypted email, i.e., there is no additional action needed to open and read the encrypted email. Supported Outlook clients include Outlook desktop, Outlook Mac, Outlook mobile on iOS and Android, and Outlook on the web (formerly known as Outlook Web App).
- Recipients who access their mailbox with a client other than Outlook will be redirected to an encrypted message portal, where they can access encrypted and rights-protected messages sent to them.
- Recipients whose mailbox is located in Gmail or Yahoo will be redirected to an encrypted message portal, where they can authenticate with their Microsoft account, Gmail, or Yahoo credentials. Once the recipients are authenticated, they can access encrypted and rights-protected messages sent to them.

Microsoft Purview Advanced Message Encryption

Microsoft Purview Advanced Message Encryption provides additional protection functionalities and is included in the Microsoft 365 E5 and Office 365 E5 subscriptions. Organizations that have the

SAMPLE

Microsoft 365 E3 and Office 365 E3 subscriptions can include Microsoft Purview Advanced Message Encryption as part of the Microsoft 365 E5 Compliance add-on.

Microsoft Purview Advanced Message Encryption includes the following components:

- Multiple protection templates for email encryption that can address different compliance requirements for the organization.
- Automatic policies that detect predefined sensitive information types.
- Expiring access to email that contains sensitive information.
- Revoking access to email that contains sensitive information.

Implementing message encryption in Exchange Online with Microsoft Purview

Microsoft Purview Message Encryption is enabled by default in organizations' tenants. This means users can start using it right away and encrypt email messages that contain sensitive content. However, messaging administrators should know how to verify if Microsoft Purview Message Encryption is active, and if needed, activate it. Furthermore, organizations might need to configure mail flow rules that encrypt email messages automatically based on factors such as email message content sensitivity.

Implementing Microsoft Purview Message Encryption functionality involves the following steps:

- **Verify if Azure RMS is active**. Microsoft Purview Message Encryption uses features of Azure RMS. By default, Azure RMS is activated in tenants that contain its license. If messaging administrators need to verify if Azure RMS is active, they can:
  a. Install the **AIPService** module by running the following command in Windows PowerShell:

  ```
  Install-Module -Name AIPService
  ```

  b. Connect to the **AIPService** module by running the following command in Windows PowerShell and provide credentials:

  ```
  Connect-AipService
  ```

  c. Run the following command in Windows PowerShell:

  ```
  Get-AipService
  ```

  d. The result of this command should be **Enabled**, which confirms that the Azure RMS service is active. If the result of the command is **Disabled**, run the following command in Windows PowerShell:

  ```
  Enable-AipService
  ```

- **Verify Microsoft Purview Message Encryption configuration** . Messaging administrators can use Exchange Online PowerShell to verify if Microsoft Purview Message Encryption is configured properly:

SAMPLE

a. Install the Exchange Online PowerShell module by running the following command in elevated Windows PowerShell:

```
Install-Module -Name ExchangeOnlineManagement
```

b. Connect to the **ExchangeOnlineManagement** module by running the following command in Windows PowerShell and providing credentials:

```
Connect-ExchangeOnline
```

c. Run the following command in Windows PowerShell:

```
Test-IRMConfiguration -Sender TestUser1@contoso.com -Recipient
TestUser2@contoso.com
```

d. The result of this command should display multiple information ending with **OVERALL RESULT: PASS.**

To create transport rules that encrypt email messages based on their content sensitivity, perform the following steps:

- Open Microsoft Defender**.** Sign in to Microsoft Exchange admin center, and from the navigation menu, select **Exchange**. Alternatively, in a web browser, enter **https://admin.exchange.microsoft.com** , and sign in with your credentials.
- Navigate to the **Rules** dashboard. In Exchange admin center, in the navigation menu, select **Mail flow**, and then select **Rules.**
- In the **Rules** dashboard, you may create a new transport rule that will perform email message encryption, or you may edit an existing transport rule to perform email message encryption:
  - In the **Rules** dashboard, select **Add a rule**, and then from the drop-down menu, select **Apply Office 365 Message Encryption and rights protection to messages** .
  - In the New transport rule window, on the **Set rule conditions** page, enter the name of the rule, and select the criteria for encryption. For example, the criteria for encryption might contain the following conditions:
    - **Apply this rule if:** The subject or body includes any of these words: **Confidential**
    - **Do the following: Modify the message security**, **Apply Office 365 Message Encryption**
    - **Rights protect message** with **Do Not Forward template**

SAMPLE

Managing message encryption

Organizations might need to modify their encryption configuration due to changes in business requirements or changes in security and compliance regulations. Messaging administrators can address these changes by managing Microsoft Purview Message Encryption settings with the following procedures:

- **Reviewing Microsoft Purview Message Encryption settings** . Messaging administrators can review the Microsoft Purview Message Encryption settings by running the following command in Exchange Online PowerShell:

```
Get-OMEConfiguration
```

- **Managing whether social ID accounts can be used to sign in to encrypted message portals.** By default, when recipients of an encrypted email message have mailboxes outside the sender's organization, the recipients can use social IDs, such as a Microsoft account, Google account, or Yahoo account to sign in to the encrypted message portal and review the encrypted message. If organizations don't want to allow the use of social ID accounts for sign-in, they can disable this functionality by running the following command in Exchange Online PowerShell:

```
Set-OMEConfiguration -Identity "OME Configuration" -SocialIdSignIn
$false
```

- **Managing whether one-pass code is generated** . If the recipients of the encrypted email message don't use Outlook, they will receive a link for reviewing the message on a web browser. The link contains a one-time pass code that has a limited time duration. If organizations don't want to allow that one-pass code to be generated, they can disable this functionality by running the following command in Exchange Online PowerShell:

```
Set-OMEConfiguration -Identity "OME Configuration" -OTPEnabled $false
```

- **Managing whether the Encrypt setting in Outlook on the web is available** . By the fault, the **Encrypt** setting is available to all Outlook on the web users. However, if organizations don't want this setting to be accessible in Outlook on the web, they can run the following command in Exchange Online PowerShell:

```
Set-IRMConfiguration -SimplifiedClientAccessEnabled $false
```

- **Managing service-side decryption for iOS mail app** . If the recipients of the encrypted email message use iOS mail app, by default, they will not be able to open the message. Messaging administrators can configure service-side decryption, so that iOS mail app can open and store the decrypted copy of the message. If the message protection is configured to forbid forwarding, iOS mail users will not be able to forward the email message; however, they will be able to copy and print the message. Furthermore, if the encrypted email message contains an attachment, iOS mail users won't be able to open the attachment. To enable service-side decryption for iOS mail app, run the following command in Exchange Online PowerShell:

```
Set-
ActiveSyncOrganizationSettings -AllowRMSSupportForUnenlightenedApps
$true
```

- **Managing service-side decryption of email attachments for web browser mail clients** . If the recipients of the encrypted email message use web browser mail clients, they won't be able to download the encrypted attachment. Messaging administrators can configure service-side decryption so that attachments can be decrypted and downloaded by the user from a web browser mail client. If the message protection is configured to forbid forwarding of the email message, users won't be able to forward the email message with the attachment; however, they will be able to copy and print the attachment. To enable service-side decryption of email attachments for web browser mail clients, run the following command in Exchange Online PowerShell:

SAMPLE

```
Set-IRMConfiguration -DecryptAttachmentForEncryptOnly $true
```

Managing advanced message encryption in Exchange Online

If your organization has a Microsoft 365 subscription that includes Microsoft Purview Advanced Message Encryption, you can perform additional management tasks that will provide further protection capabilities when sending encrypted email messages.

Managing advanced message encryption involves the following procedures:

- **Creating and configuring branded templates for organization's encrypted email messages and the encryption portal.** Organizations that send encrypted email messages can customize the format of the encrypted email messages and the format of the encryption portal. Customizing encrypted email messages includes:
  - **Creating a branding template**. You can create a new branding template by running the following command in Exchange Online PowerShell:

    ```
    New-OMEConfiguration -Identity "Contoso Template"
    ```

  - **Editing introductory text**. You can customize the introductory text that follows the sender's email address by running the following command in Exchange Online PowerShell:

    ```
    Set-OMEConfiguration -Identity "Contoso Template" -IntroductionText
    "has sent you an encrypted message."
    ```

  - **Disclaimer text**. You can customize the disclaimer text displayed at the end of the email message by running the following command in Exchange Online PowerShell:

    ```
    Set-OMEConfiguration -Identity "Contoso Template" -DisclaimerText
    "Contoso Corporation. All rights reserved."
    ```

  - **URL for organization's privacy statement**. You can customize the privacy statement that is available via a URL link by running the following command in Exchange Online PowerShell:

    ```
    Set-OMEConfiguration -Identity "Contoso
    Template" -PrivacyStatementURL
    "https://www.contoso.com/corporateprivacystatement.html"
    ```

  - **Text for the "Read Message" option**. You can customize the text that appears on the "Read Message" option and following the "Read Message" option, by running the following command in Exchange Online PowerShell:

    ```
    Set-OMEConfiguration -Identity "Contoso Template" -Image
    ([System.IO.File]::ReadAllBytes('C:\ContosoBranding\CompanyLogo.png'
    ))
    ```

  - **Organization logo to be inserted in the encrypted email message and encrypted message portal**. You can decide to insert an organization logo in the encrypted email message and

SAMPLE

the encrypted message portal by running the following commands in Exchange Online PowerShell:

```
Set-OMEConfiguration -Identity "Contoso Template" - ReadButtonText
"Read Encrypted Message”
Set-OMEConfiguration -Identity "Contoso Template" - EmailText
"Encrypted Message from Contoso Corporation”
```

- **Background color in the encrypted email message and encrypted message portal.** You can decide to customize the background color for the encrypted email message and the encrypted message portal, where every color corresponds to a hex code value, such as “#f0ffff” for Azure. To do this, run the following command in Exchange Online PowerShell:

```
Set-OMEConfiguration -Identity "Contoso Template" -BackgroundColor "
#f0ffff"
```

- **Edit the Exchange mail flow rule that applies the custom branding.** Previously, you learned how to create a mail flow rule that performs message encryption based on different email message criteria. You can now edit the mail flow rule to include a customized branding template by performing following steps:
  a. In **Exchange admin center**, in the **Rules** dashboard, select the mail flow rule, and then select **Edit**.
  b. In the mail flow window, in the **Do the following** section next to the **Modify the message security** menu, select the drop-down menu and select **Apply custom branding to OME messages**. Select the custom template, select **OK**, and then select **Save**.
- **Set an expiration date for encrypted email messages**. You can configure expiration dates for encrypted email messages that contain sensitive content and are sent to external users. To configure the expiration date, run the following command in Exchange Online PowerShell:

```
Set-OMEConfiguration -Identity "Contoso Template" -
ExternalMailExpiryInDays 14
```

- **Revoke access to email that contains sensitive information**. In some scenarios, senders might need to revoke access to encrypted email messages, so that the recipient no longer has access to those emails. Encrypted email message senders can revoke only those messages that are received by the recipient in the link-based format.
  - **Revoking access to email by using Outlook on the web**. Senders can revoke an email message that was sent by selecting it, and then selecting **Remove external access**. When the recipient tries to open the message, an error message will convey that “The message has been revoked by the sender”.
  - **Revoking access to email by using Exchange Online PowerShell**. Messaging administrators can revoke access to email by performing the following steps:
    - Identify the Message ID in Message Trace in the Microsoft Purview compliance portal, or by using Message Encryption reports in the Microsoft Purview compliance portal. The message ID should be in the following format: xxxxxxxxxxxxxxxxxxxxxxx@xxxxxx.xxxx.prod.outlook.com
    - Verify if the email message is recoverable by running the following command in Exchange Online PowerShell:

SAMPLE

```
Get-OMEMessageStatus -MessageId "<message id>" | ft -a  Subject,
IsRevocable
```

- If the result of the previous command is “True”, revoke the email message by running the following command in Exchange Online PowerShell:

```
Set-OMEMessageRevocation -Revoke $true -MessageId "<messageId>"
```

- Finally, verify if the email message is revoked, by running the following command in Exchange Online PowerShell:

```
Get-OMEMessageStatus -MessageId "<messageId>" | ft -a  Subject,
Revoked"
```

The result of the previous command should be “Revoked: True”

Lab B: Configuring threat policies and Purview Message Encryption

Please refer to the online lab to supplement your learning experience with exercises.

Knowledge check

Check your knowledge by answering these questions:

1. Which organization’s public DNS record should be edited so that mail flow is directed to Exchange Online? Select the correct option.
   - MX record
   - TXT record
   - PTR record
   - CNAME record
2. Which product is used to educate users on how to detect and respond to email-related threats? Select the correct option.
   - Microsoft Entra ID Protection
   - Microsoft Data Loss Prevention
   - Attack simulation training
   - Microsoft Defender for Identity
3. When multiple security policies apply to a recipient, which policy has the highest priority? Select the correct option.
   - The Strict preset security policy
   - The Standard preset security policy
   - Custom policy

SAMPLE

   - The Built-in protection preset security policy
4. Which Spam Confidence Level (SCL) value indicates that the email message is marked as high confidence spam? Select the correct option.
   - -1
   - 0
   - 6
   - 9
5. Which Exchange Online Protection setting provides the ability to reject or quarantine specific file types that might include malware? Select the correct option.
   - Connection filtering
   - Common attachment filter
   - Quarantine policies
   - Anti-phishing
6. Which Exchange Online functionality provides users with the ability to encrypt a message before sending it to the recipients? Select the correct option.
   - Anti-spam protection
   - Microsoft Purview Message Encryption
   - Quarantine policies

> **Note:** To find the answers, refer to the Knowledge check slides in the PowerPoint presentation.

SAMPLE

Learn more

For more information, refer to:

- Exchange Online Protection overview
- What is Microsoft Defender for Identity?
- Microsoft Defender for Office 365 overview
- Message encryption