AVANAN

A **Check Point** Company

16 May 2025

AVANAN

Administration Guide

CHECK POINT™

Important Information

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Patent Notice

Avanan is protected by the following patents in the United States and elsewhere. This page is intended to serve as notice under 35 U.S.C. § 287(a):
US10,372,931, US10,498,835, US10,509,917, US11,647,047, US11,736,496, US11,936,662

Revision History

Date	Description
16 May 2025	Updated *"Automatic Ingestion of End User Reports" on page 362*.
13 May 2025	Updates to: ■ Updated *"Security Awareness Training - End User Experience" on page 503*. ■ Added *"Supported Languages for Phishing Simulations" on page 505* *"Supported Languages for Training Modules" on page 506*.
22 April 2025	Updates to: ■ Updated *"Quarantine Restore Requests" on page 433* and *"Phishing Reports Dashboard" on page 362*. ■ and • Added *"Limiting End User Portal Access to Specific Users" on page 432* and *"Including Blocklisted Emails in the End User Portal" on page 433*. • Updated *"Configuring Daily Quarantine Report (Digest)" on page 424* and *"Authentication for Email Notifications" on page 448*.
09 April 2025	Updates to: ■ Updated and removed *"Security Awareness Training" on page 477*. ■ Added *"Customizing the From address for Email Notifications" on page 227*. ■ Updated *"Manual Integration with Office 365 Mail - Required Permissions" on page 544*. ■ Added *"Approving User" on page 56*.
28 March 2025	Updated *"Customizing Security Awareness Training Policy" on page 477*
21 March 2025	Added *"Security Awareness Training Domains" on page 483*.
13 March 2025	Updates to: ■ Added *"DKIM Management" on page 473*. ■ Added *"Use of Azure AD Graph APIs" on page 56*. ■ Updated *"Emails Falsely Quarantined by Microsoft" on page 139*.

Date	Description
26 February 2025	Added *"Configuring the SPF Record" on page 471* and *"Defining the SPF Record" on page 472*.
10 February 2025	Updates to: ■ Added *"Automatic Handling of Quarantined Restore Requests" on page 434*. ■ Added *"Graymail Dedicated Folder" on page 185*.
24 January 2025	Updates to: ■ Updated *"Security Awareness Training" on page 477* ■ Added *"Users" on page 494*. ■ Added *"Monitoring Phishing Simulations" on page 494*. ■ Added *"Monitoring User Awareness Training Progress" on page 497*. ■ Added the Claim value column *"Required Permissions" on page 49*.
09 January 2025	Updated *"Slack" on page 269*.
2 January 2025	Updates to: ■ *"Anti-Malware Exceptions" on page 317*. ■ *"End-User Portal (Email Security Portal)" on page 428*.
31 December 2024	■ Updated *"Encrypting Outgoing Emails" on page 215*. ■ Added information about *"Customizing the Analytics Dashboard using Infinity AI Copilot" on page 338*. ■ Added information about *"SPF Management" on page 468*.
24 December 2024	Added *"Appendix G: Permitted IP Addresses to access the Avanan Azure Application" on page 630*.
17 December 2024	Updates to : ■ Added *"Authorizing Training Module Access for the Organization" on page 480*. ■ Added *"Required Permissions for Microsoft Login Authorization" on page 482*. ■ Added *"Overriding Microsoft False Detections as Spam (Send to Junk)" on page 108*. ■ Updated *"Supported Smart Banners" on page 233*
27 November 2024	Updated the Required Permissions for Office 365 Mail.

Date	Description
21 November 2024	Initial release of the document in Check Point format.

Table of Contents

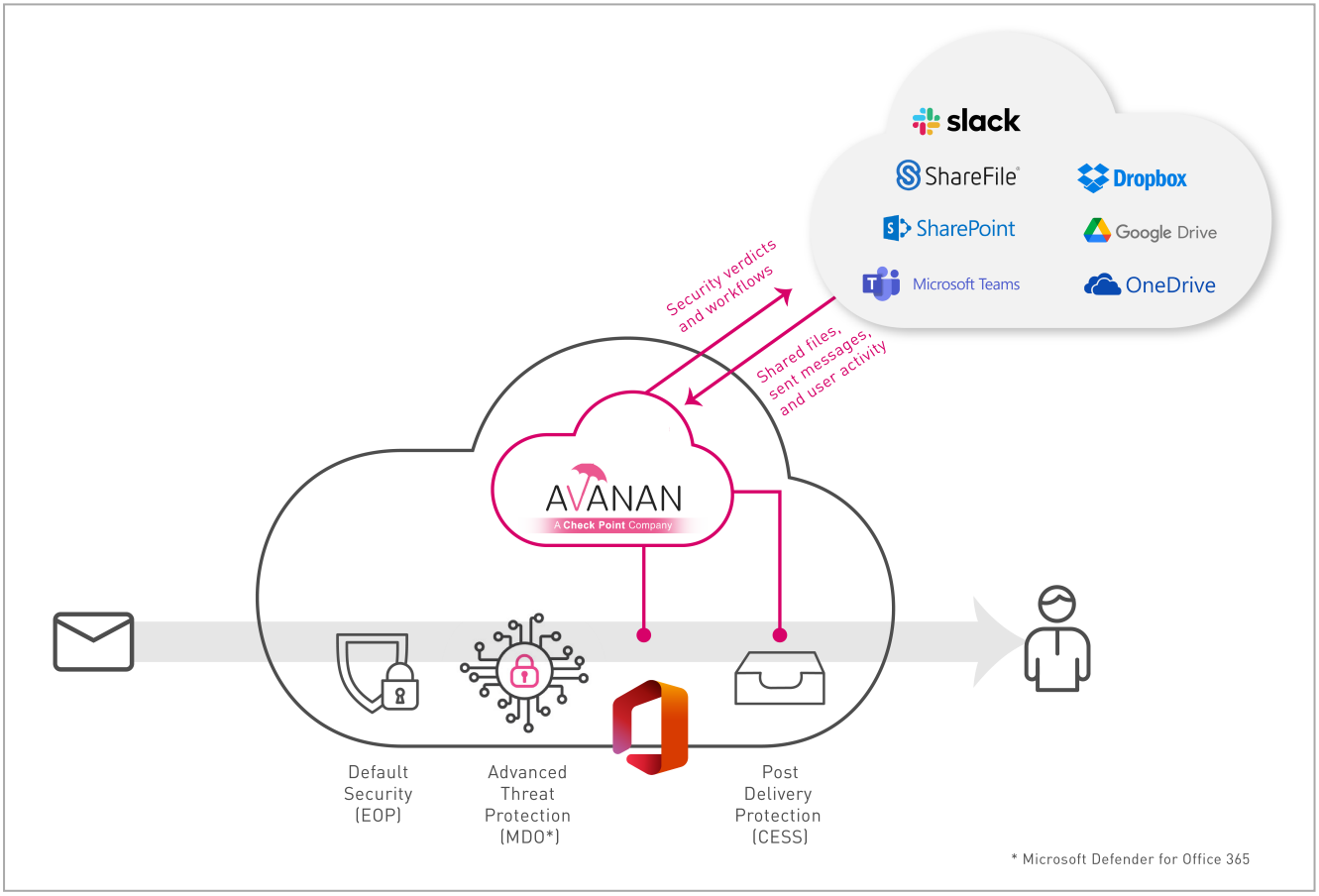
Introduction to Avanan

Overview

Check Point's Avanan is an API-based inline protection service that protects your SaaS applications from advanced threats, such as:

- Zero-Day Threat
- Phishing
- Account Takeover
- Data Leakage
- SaaS Shadow IT Discovery

How It Works



Email Protection

When an email is sent, Avanan intercepts and sends the email to Check Point's ThreatCloud for analysis before the email is delivered to the recipient. If the verdict is malicious, then the email is handled according to the configured workflow (for example, quarantine). Otherwise, the email is delivered to the recipient.

Avanan also inspects internal and outgoing traffic, both for data leakage and for phishing and malware. Emails can be removed and modified post-delivery if needed.

Supported Applications

- Microsoft Exchange Online (Office 365 Mail)
- Gmail

File Sharing Applications

When you upload a file to the application, Avanan inspects it for malware and against the organization's DLP policy. Files with detected threats are quarantined or vaulted.

Supported Applications

- Microsoft OneDrive
- Microsoft SharePoint
- Google Drive
- Citrix ShareFile
- DropBox
- Box

Messaging Applications

Avanan inspects every message for malware, DLP and phishing indicators. It also inspects every uploaded file for malware and DLP.

Supported Applications

- Microsoft Teams
- Slack

BEC/Compromised Accounts (Account Takeover)

Avanan inspects the behavior of users inside the Microsoft environment – their login patterns, correspondence patterns, and many more – to determine if an account has been compromised before any damage is done. The account is then automatically blocked by the system, or manually blocked by an administrator.

About this Guide

This guide describes how to protect cloud email and collaboration suites using Avanan.

Learn how to:

- Activate the protection for supported SaaS applications.
- Configure security policies and settings for each of the protected applications.
- Review security events and act on them.
- Generate reports and integrate with external SIEM platforms.

Getting Started

Avanan's automatic deployment is a process that enables security administrators to deploy instantly and fine-tune security policies.

During deployment of Avanan, configuration changes are added to the protected SaaS applications.

To get started with Avanan:

1. Access the Avanan Administrator Portal
2. License the product
3. Activate the required SaaS applications
4. Configure security policies
5. Review security events and act on them

Accessing the Avanan Administrator Portal

Contact your Avanan representative to get an account for the Avanan Administrator Portal.

Regional Data Residency

Avanan Administrator Portal supports data residency in these regions (countries):

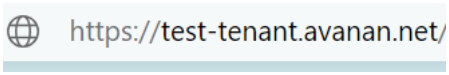
Region	Supported Data Residency
Americas	United States
	Canada
EMEA (Europe, Middle East and Africa)	Ireland
	United Arab Emirates
APAC (Asia Pacific)	India
	Australia
United Kingdom	United Kingdom

You can select the data residency when creating an account in the Avanan Administrator Portal. After you choose the data residency region, your data is stored and processed only within the boundaries of the selected country.

Portal Identifier of Avanan Tenant

Portal identifier is the starting URL of the Avanan Administrator Portal excluding *avanan.net*.

For example, if the URL is *test-tenant.avanan.net*, then *test-tenant* is the **portal identifier**.



Licensing the Product

When you access the Avanan Administrator Portal for the first time, you get a free 14-day trial. During the trial period you can access all the features for unlimited number of users. After the trial period expires, you must purchase a software license to use the product.

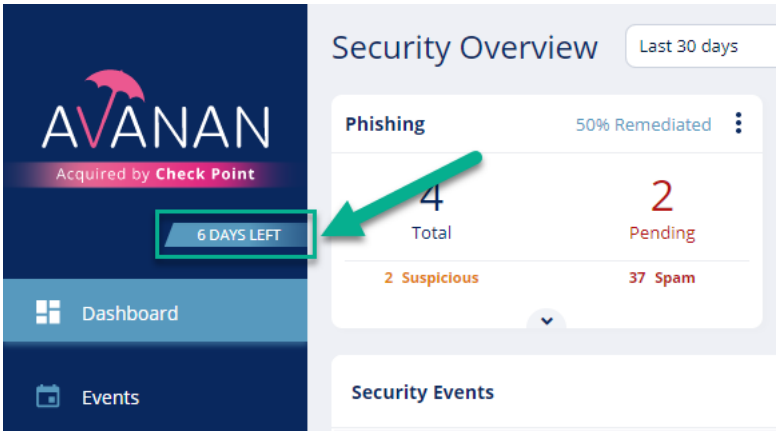
Trial

Trial Period

By default, the trial is for 14 days. During the trial period you can access all the features for unlimited number of users.

You are in **Trial** mode unless the account has a valid Avanan license.

You can see the number of days left in the trial period on the top left corner in the Avanan Administrator Portal.

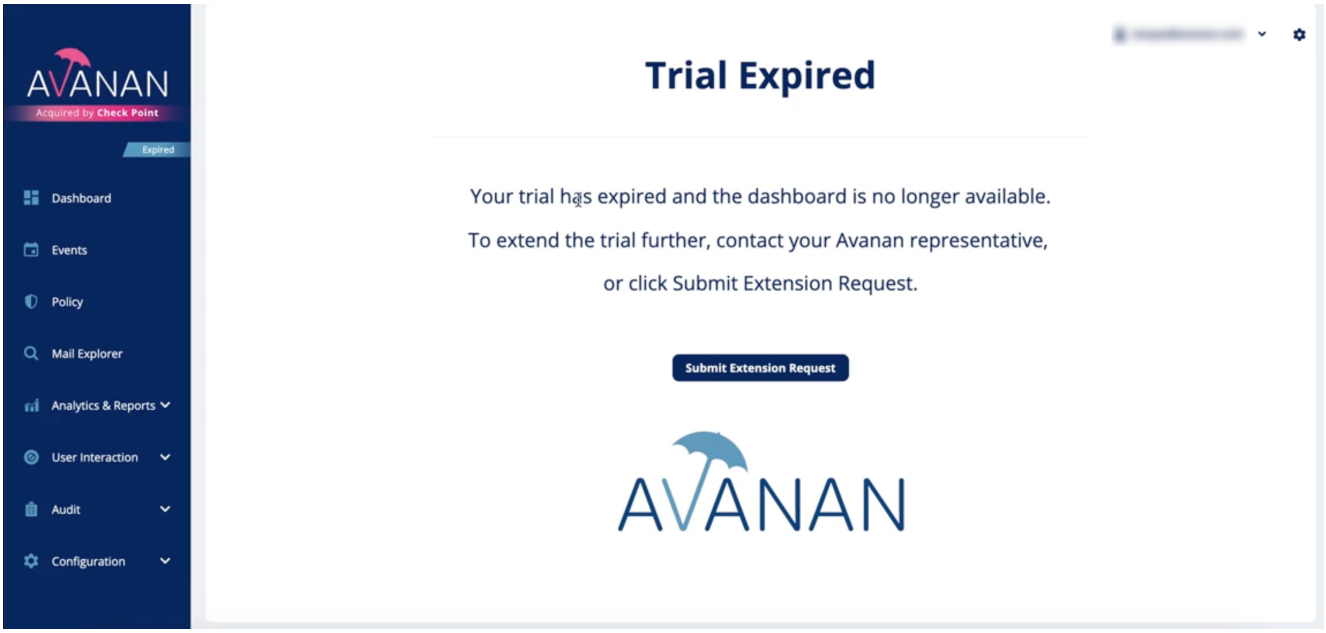


To extend the trial period beyond 14 days, contact your Avanan representative.

Trial Expiry

After the trial expires, you will not be able to access the Avanan menus and functions.

During this time, the emails continue to flow through the Avanan platform but they are not inspected and always delivered to the end-user.



To regain access to Avanan, do one of these:

- To extend the trial period, click **Submit Extension Request** and a Avanan representative will review the request.
- Contact your Avanan representative.

License Packages and Add-Ons

Avanan is available in different license packages with optional add-ons.

Packages

Avanan packages have different coverage and security.

- **Coverage** - Select to purchase security packages for **Email Only** or **Email and Collaboration**.
  - **Email Only** - Includes security for Microsoft 365 Mail and Google Gmail.
  - **Email and Collaboration** - Includes security for emails (Microsoft 365 and Gmail) and other collaboration applications (OneDrive, SharePoint, and so on).
- **Security** - Select one of these levels of protection.
  - **Basic Protect** - Includes phishing protection, account takeover protection, and protection against known malicious URLs and files.
  - **Advanced Protect** - Includes **Basic Protect** plus protection against unknown malicious URLs (URL Emulation) and unknown malicious files (Sandbox and CDR).
  - **Complete Protect** - Includes **Advanced Protect** plus Data Loss Prevention (DLP).

Features Available	Basic Protect	Advanced Protect	Complete Protect
Anti-Phishing for incoming and internal emails	✓	✓	✓
Known malware prevention (Anti-Virus)	✓	✓	✓
Malicious URL prevention (URL Protection)	✓	✓	✓
URL Click-Time Protection (URL Rewriting)	✓	✓	✓
Account takeover prevention (Anomalies)	✓	✓	✓
Unauthorized applications detection (Shadow IT)	✓	✓	✓
Complete known malware and zero-day malware prevention (Sandboxing)	–	✓	✓
Attachment sanitization (CDR;Threat Extraction)	–	✓	✓
Data Loss Prevention (DLP)	–	–	✓

Add-ons

Regardless of the selected package, you can purchase these add-ons:

- **Archiving** - Stores emails for up to 10 years. It allows you to filter emails and export large batches of emails for disaster recovery and legal use cases. See *"Email Archiving" on page 253*.
- **Incident Response as a Service (IRaaS)** - Check Point expert analysts respond to all your end-user restore requests and phishing reports. See *"Incident Response as a Service (IRaaS)" on page 454*.
- **DMARC Management** - Supports the maintenance of a restrictive DMARC policy, ensuring you and your customers are protected from impersonation attacks and your business emails always reach their external destination. See *"DMARC Management" on page 458*.

Managing Licenses

Protected and Licensed Users

Under **Policy**, you can create policy rules for each protected SaaS application. You can apply a rule to all users or a specific group of users that you define.

- Avanan protects only active user accounts with valid Microsoft / Google licenses and at least one associated mailbox.
- For every user account with a Microsoft/Google/other license to any protected SaaS application, Avanan consumes a license from the quota.
- If Microsoft and Google SaaS applications are protected from the same Avanan account (tenant) in the Infinity Portal, and if the same user has a Google account and a Microsoft account associated with different email addresses, then Avanan consumes two licenses for that user.
- To restrict the list of protected users, see *"Limiting license consumption and security inspection to a specific group" on the next page*.
- Specific Microsoft entities:
  - Avanan protects group mailboxes, unlicensed shared mailboxes, and other aliases. However, it does not count them for licensing purpose. Do not purchase licenses for these mailboxes.

    Notes:
    - To protect licensed shared mailboxes (shared mailboxes that Microsoft bills for), Avanan consumes a license.
    - Avanan supports these groups for group filtering:
      - Assigned Membership:
        - Microsoft 365 Group
        - Mail-enabled Security Group
        - Distribution List
      - Dynamic Membership:
        - Microsoft 365 Group
  - Avanan does not protect Microsoft Public folders, Mail contacts and Mail users.
  - At the moment, users with licenses only for Microsoft Teams will be protected but will not show up as consuming licenses. However, you must purchase licenses for these users.
- Specific Google entities:

- Avanan does not protect email addresses of Google Groups.

  When a malicious email is sent to the email address of a Google Group, Avanan blocks the email from reaching the group members' mailboxes, as they are protected. However, when you open the group's web page, the email is accessible.

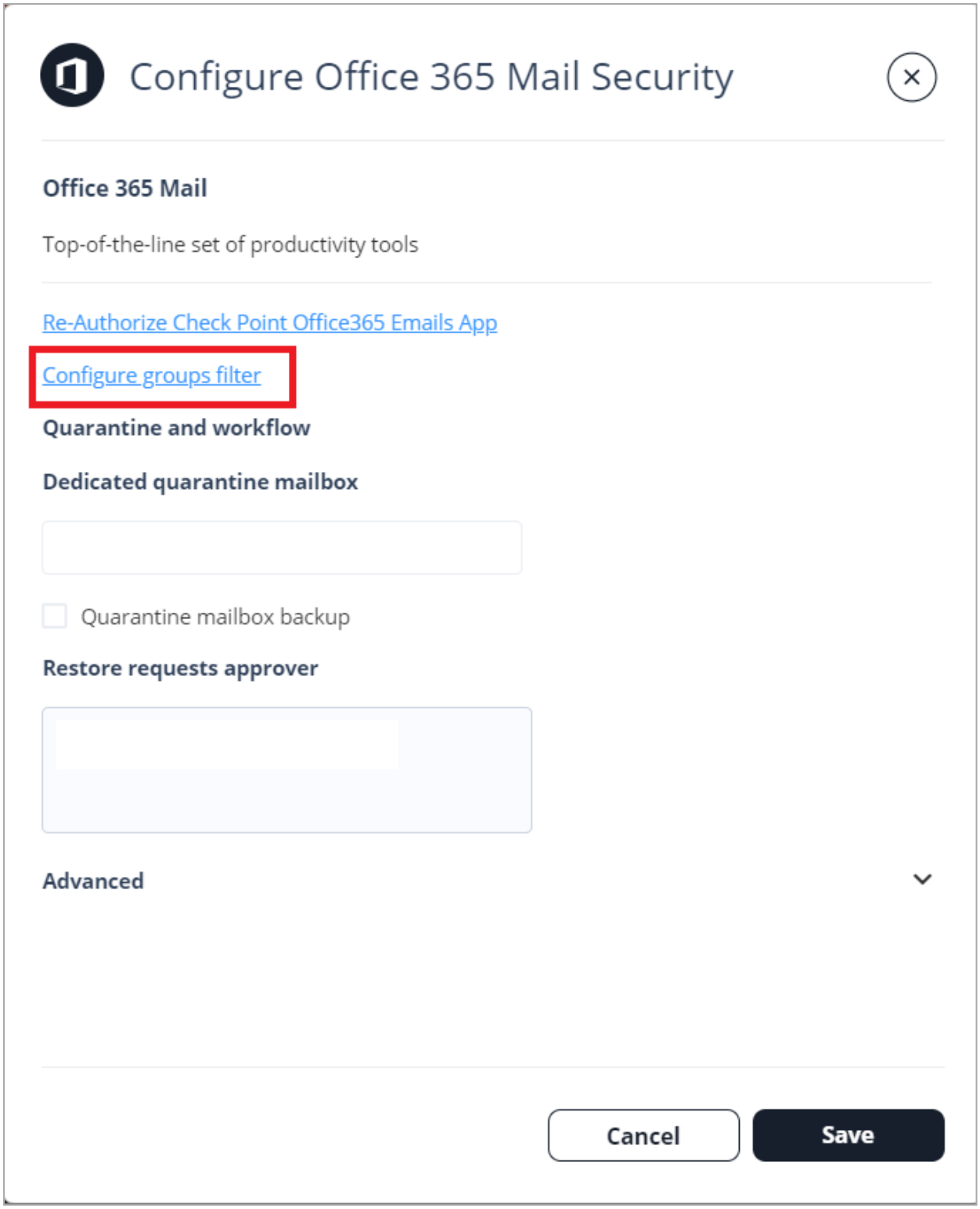
- Avanan sync users every 24 hours with Microsoft and Google accounts. So, deleting or adding a user might take up to 24 hours to affect the license count.

Limiting license consumption and security inspection to a specific group

After activating the SaaS application, Avanan inspects emails, messages and files for the selected users in the Microsoft 365/Google account.

To limit the license consumption and security inspection to a specific group after activating the SaaS application:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Office 365 Mail or Gmail.
3. In the pop-up that opens, click **Configure groups filter**.



4. Select a group selection.

a. **All organization** - Licenses will be assigned automatically to your user mailboxes.

b. **Specific group** - Enter the name of the group in Office 365 or Google Workspace containing the user mailboxes or groups of user mailboxes you wish to protect with Avanan.

5. Click **OK**.

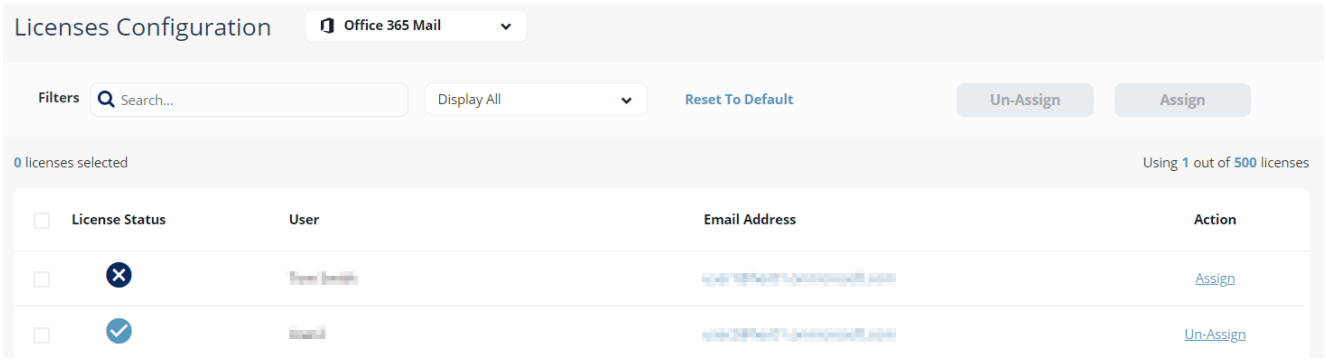
Manual changes to license assignment

After configuring the licenses for a specific group or the entire organization, you can assign or remove licenses to specific user mailboxes if required.

To assign or remove licenses to specific user mailboxes, go to **System Settings > Licenses**.

Note - This menu is not available in the trial mode and when the purchased license is of a pay-as-you-go type.

The **Licenses Configuration** screen shows the usage status of your licenses and the individual licensing status of user mailboxes.



The **License Status** column shows if a license covers the user mailbox. To add or remove the license to a user mailbox, click **Assign**/**Un-Assign**.

Note - You can select multiple user mailboxes and assign or un-assign a license. The license assignment might take up to four hours to become effective.

Activating SaaS Applications

After activating your Check Point's Avanan portal and having logged into the system, you can start activating your SaaS applications and monitor the security events.

Workflow:

Step	Description
1	The **Getting Started** wizard appears after activating Avanan.
2	Start activating the SaaS application(s) required.
3	Navigate to **Overview** and begin monitoring.

To begin the workflow:

1. In the **Getting Started** wizard, click **Let's Get Started**.

   The **SaaS Applications** screens appears.

2. Select the SaaS application you want to activate.

   Activations are done through OAuth and require admin-level authentication and authorization. Make sure you have the admin-level credentials available for the SaaS application you want to activate.

Notes:

- The procedure to activate the SaaS application varies according to the application you select.
- When a SaaS application is activated, it automatically starts the **Monitor only** mode. There is no change to the end-user's experience and no action or remediation is taken. However, you can already see events generated from the Avanan portal.

Minimum License Requirements to Activate SaaS Applications

Avanan need these licenses to protect the SaaS applications:

- **Microsoft 365 - Mail, OneDrive, and SharePoint**

Minimum License Required	Other Supported Licenses	Licenses Not Supported
Business Basic (formerly Business Essential) **Note** - Integration with Microsoft Encryption requires Office 365 E3 or Office 365 E5 licenses.	• Business Premium (formerly Business) • Business Standard (formerly Business Premium) • Exchange Online Kiosk • Exchange Online Plan 1 • Exchange Online Plan 2 • Office 365 A1 • Office 365 A3 • Office 365 A5 • Office 365 E1 • Office 365 E3 • Office 365 E5 • Microsoft 365 F1 • Microsoft 365 F3	Microsoft 365 Developer Program

- **Microsoft 365 - Teams**

Minimum License Required	Other Supported Licenses	Licenses Not Supported

• Office 365 E5/A5/G5
• Microsoft 365 E5/A5/G5
• Microsoft 365 E5/A5/F5/G5 Compliance and Microsoft 365 F5 Security & Compliance
• Microsoft 365 E5/A5/F5/G5 Information Protection and Governance or Microsoft 365 E5 Compliance add-on, when either of them is added to one of the these E3 licenses:
  ◦ Enterprise Mobility + Security E3
  ◦ Office 365 E3
  ◦ Microsoft 365 E3
	–	–

- **Google Workspace - Gmail and Google Drive**

Minimum License Required	Other Supported Licenses	Licenses Not Supported
• Gmail - Supports all licenses except Essentials editions • Google Drive - Business Standard **Notes**: • You must have an additional Google Workspace license to integrate with Avanan. • If "Comprehensive mail storage" is enabled, **Protect (Inline)** mode is not supported.	• Business Starter (only for Gmail) • Business Standard • Business Plus • Enterprise • Frontline • Google Workspace for Education Fundamentals • Google Workspace for Education Standard • Teaching and Learning Upgrade • Google Workspace for Education Plus • Google Workspace for Nonprofits	• Business Starter (only for Google Drive) • G Suite legacy • Google Apps

- **Box**

Minimum License Required	Other Supported Licenses	Licenses Not Supported
Enterprise	–	• Starter • Business • Business Plus

- **Dropbox**

Minimum License Required	Other Supported Licenses	Licenses Not Supported
Business Plus	Enterprise	• Basic • Plus • Essentials • Business

- **Slack**

Minimum License Required	Other Supported Licenses	Licenses Not Supported
Enterprise Grid	–	• Free • Pro • Business Plus

For Office 365 Government environments, Avanan supports **Office 365 GCC**. To enable login events, after the onboarding process is complete, contact *Avanan Support*.

Note - Avanan does not support **Office 365 GCC High**.

After activating your Avanan portal and having logged into the system, you can start activating your SaaS applications and monitor security events.

Workflow:

Step	Description
1	Getting Started Wizard opens after activating Avanan.
2	Start activating the SaaS application(s) required.
3	Navigate to **Overview** and begin monitoring.

To begin the Getting Started wizard:

1. Click **Let's Get Started**.

   The **SaaS Applications** screens opens.

2. Select the SaaS application you want to **activate**.

   Activations are done through OAuth and require admin-level authentication and authorization. Make sure you have the admin-level credentials available for the SaaS you select to activate.

Notes:

- The procedure to activate the SaaS application varies according to the application you select.
- When a SaaS application is activated, it automatically starts the **Monitor only** mode. There is no change to the end-user's experience and no action or remediation is taken. However, you can already see events generated from the Avanan portal.

Activating Office 365 Mail

To protect Office 365 Mail, Avanan uses **Avanan Cloud Security Platform - Emails V2** enterprise application that is automatically added to your Microsoft Azure cloud platform.

As a prerequisite to activate Office 365, make sure you have these:

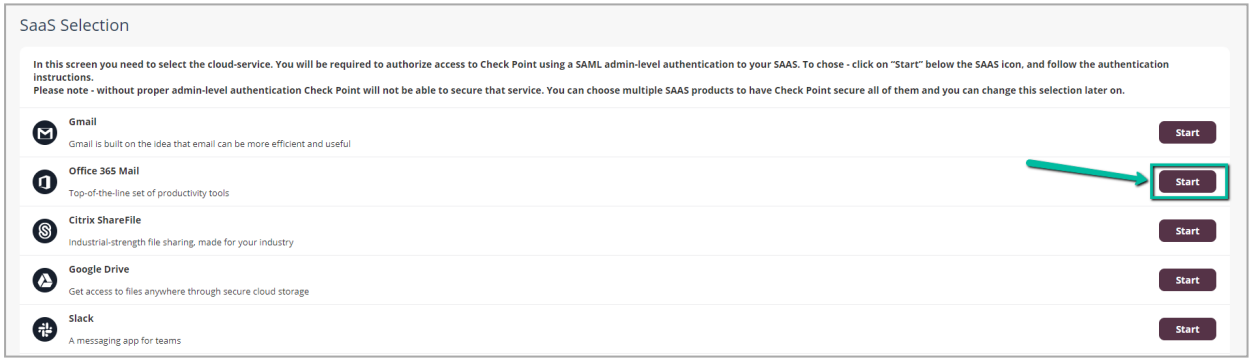
- You are a user with Privileged Role Administrator role or higher permissions, or you have the credentials of such a user.
- You have the minimum supported SaaS license. See *"Minimum License Requirements to Activate SaaS Applications" on page 43*.
- If some mailboxes are on an on-premises Exchange server, see *"Appendix F: Activating Office 365 Mail in Hybrid Environments" on page 627*.

To activate Office 365 Mail:

1. From the **Getting Started Wizard** click **Start** for Office 365 Mail.

   or

   Navigate to **Security Settings > SaaS Applications** and click **Start** for Office 365 Mail.



2. Select the mode of operation for Office 365.

   - **Automatic mode**

     Avanan performs the necessary configurations to your Microsoft 365 environment and operates in **Monitor only** mode. For more information, see *"Automatic Mode Onboarding - Microsoft 365 Footprint" on page 56*.

   - **Manual mode**

     You must manually perform the necessary configurations in the Office 365 Admin Exchange Center before you bind the application to your Office 365 email account and every time you add or edit the security policy associated with Office 365 emails. For more information, see *"Appendix A: Avanan Manual Integration with Office 365" on page 543*.

Note - Avanan recommends using **Automatic mode**, allowing better maintenance, management, and smoother user experience. Before using the **Manual mode**, contact *Avanan Support* to help resolve any issues raised with the **Automatic mode** for onboarding.

3. Enable the **I Accept Terms Of Service** checkbox.
4. If you need to limit the license consumption and protection to a specific group of users or to connect multiple Avanan tenants to the same Microsoft 365 account:
   a. Enable the **Restrict inspection to a specific group (Groups Filter)** checkbox and click **OK**.
   b. In the **Office 365 Authorization** window that appears, sign in with a user with Privileged Role Administrator role or higher permissions.

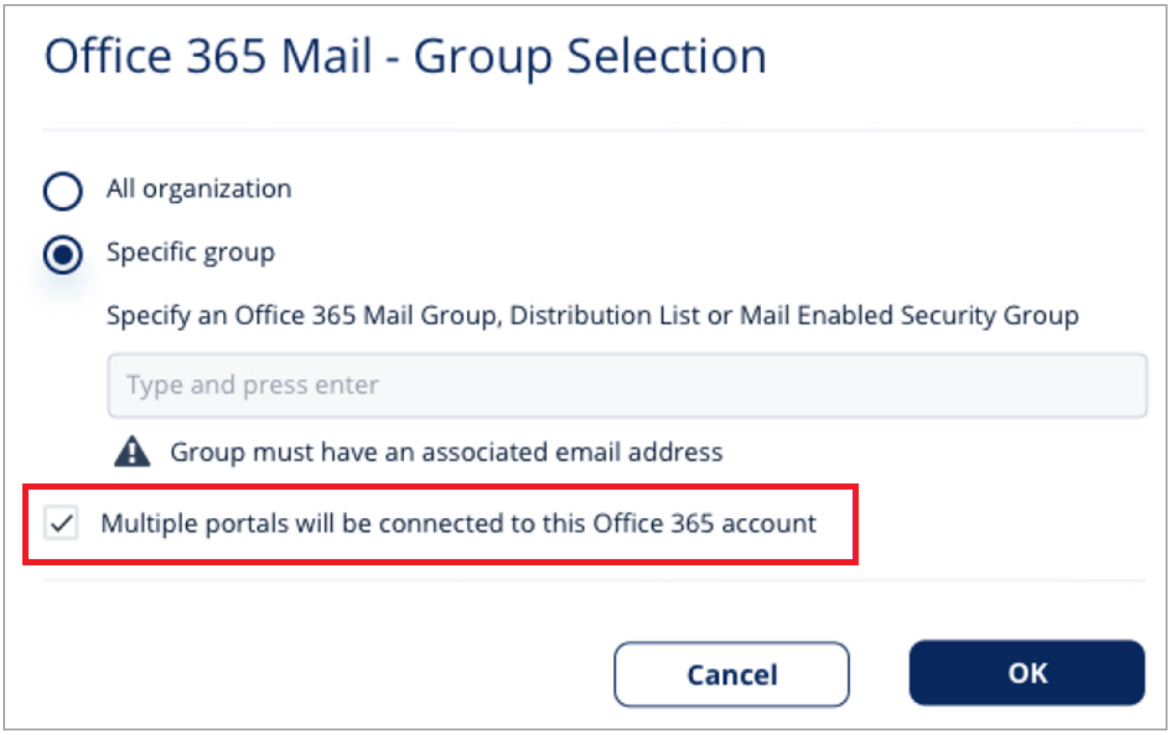
      In the authorization screen, click **Accept** to grant permissions for **Avanan Cloud Security Platform - Emails V2** application.

      To view the permitted IP addresses to access this application, see *"Appendix G: Permitted IP Addresses to access the Avanan Azure Application" on page 630*.
   c. In the **Office 365 Mail - Group Selection** pop-up, select **Specific group**.
   d. Enter the group name you need to protect with Avanan.

      Notes:
      - The group name must have an associated email address.
      - Avanan supports these groups for group filtering:
        - Assigned Membership:
          - Microsoft 365 Group
          - Mail-enabled Security Group
          - Distribution List
        - Dynamic Membership:
          - Microsoft 365 Group

e. If you need to connect multiple Avanan tenants to the same Microsoft 365 account, enable the **Multiple portals will be connected to this Office 365 account** checkbox.

Caution - Before you enable the checkbox, see *"Connecting Multiple Portals to the Same Microsoft 365 Account" on page 74*.



f. Click **OK**.

Now, the Office 365 Mail SaaS is enabled and monitoring begins immediately.

Note - After activating Office 365 Mail, Avanan performs retroactive scan of its content. For more information, see *"Onboarding Next Steps" on page 94*.

Note - By default, **Monitor only** mode is assigned for all the SaaS applications you connect to. This allows you to immediately see the value that Avanan brings as it recognizes security incidents that occurred before on your SaaS platform. To configure email protection, see *"Threat Detection Policy" on page 150*.

Required Roles and Permissions

Avanan need these roles and permissions to secure all users and remediate all threats.

Required Permissions

Avanan require the following permissions from Microsoft.

Permissions required from Microsoft 365	Claim Value	Functions performed by Avanan
Create groups	Group.Create	Creating groups while onboarding as part of setting up protection.
Manage Exchange As Application	Exchange.ManageAsApp	Used to run PowerShell commands on Exchange elements on behalf of the Check Point application.
Manage all users' identities	User.ManageIdentities.All	Used to block compromised accounts.
Read and write directory data	Directory.ReadWrite.All	Used for these: ■ Read users, groups, and other directory data during onboarding. ■ Read updates from Active Directory to influence policy assignments and create a shared mailbox to receive reported phishing emails.
Read and write domains	Domain.ReadWrite.All	In addition to **Read Domains**, creates a Check Point sub domain while onboarding and uses its certificate to deliver emails back to Microsoft.

Permissions required from Microsoft 365	Claim Value	Functions performed by Avanan
Read activity data for your organization	ActivityFeed.Read	Used for these: ■ Getting user login events, Microsoft Defender events and others to present login activities and detect compromised accounts (Anomalies). ■ Getting Microsoft detection information to present for every email.
Read all audit log data	AuditLog.Read.All	Used for retrospective audit of login events to detect compromised accounts (Anomalies).
Read all applications	Application.Read.All	■ Used to read application parameters required for onboarding and off-boarding of the application.
Read all directory RBAC settings	RoleManagement.Read.Directory	Used to collect users and their roles to scope policies, enforce them, and generate user-specific reports.

Permissions required from Microsoft 365	Claim Value	Functions performed by Avanan
Read and write all directory RBAC settings	RoleManagement.ReadWrite.Directory	Used for these: ■ In addition to **Read all directory RBAC settings**, assigns a role to the Check Point application while onboarding, so that it can run PowerShell commands.
Read all hidden memberships	Member.Read.Hidden	Used to collect hidden group members to support policy assignment, policy enforcement, and user-based reporting.
Read all groups	Group.Read.All	Used for mapping users to groups to properly assign policies to users.
Read contacts in all mailboxes	Contacts.Read	Used to protect contacts and scope policies for users.
Read domains	Domain.Read.All	Collect protected domains to: ■ Secure domains. ■ Skip inspection and avoid returning emails from other domains to Microsoft. ■ Allow DMARC Management for these domains. ■ Automatically apply branding to the Security Awareness Training end user experience.

Permissions required from Microsoft 365	Claim Value	Functions performed by Avanan
Read all users' full profiles	User.Read.All	Used to collect all users for the purposes of protection and policy scoping.
Read and write all user mailbox settings	MailboxSettings.ReadWrite	Used for these: ■ Read mailbox rules to detect compromised accounts. ■ Add a mailbox rule as part of the Greymail workflow.
Read and write mail in all mailboxes	Mail.ReadWrite	Used for these: ■ Enforcing Detect and Remediate policy rules, where emails are quarantined or modified post-delivery. ■ Allowing administrators to quarantine emails that are already in the users' mailboxes. ■ Allowing administrators to restore emails to users' mailboxes. ■ Baselining communication patterns as part of **Learning Mode**.
Use Exchange Web Services with full access to all mailboxes	full_access_as_app	Used to send notifications to end user mailboxes and restore quarantined emails to end user mailboxes.

Permissions required from Microsoft 365	Claim Value	Functions performed by Avanan
Send mail as any user		Used to send notifications to end users in scenarios where Microsoft does not support other delivery methods.
Read and write all group memberships	GroupMember.ReadWrite.All	In addition to **Read all groups**, when changing the users that are protected inline, a group created by Avanan gets automatically adjusted to include the new inline users.
Read all published labels and label policies for an organization	InformationProtectionPolicy.Read.All	Read Microsoft Sensitivity Labels to use them as part of the Check Point DLP policy.

Required Application Roles

Avanan need these roles during onboarding:

- Exchange Administrator
- Privileged Authentication Administrator

Exchange Administrator

Avanan uses the **Exchange Administrator** role to perform these tasks in several methods including running PowerShell commands.

- **Initial onboarding** - To configure *"Mail Flow Rules" on page 57*, *"Connectors" on page 65*, and additional elements for incoming, internal, and outgoing mail flow, as required to enforce the configured DLP, Threat Detection, and Click-Time Protection policies. For more information, see *"Automatic Mode Onboarding - Microsoft 365 Footprint" on page 56*.
- **Unified Quarantine** - Filter information about emails quarantined by Microsoft and, if required, restore them from the Microsoft quarantine.

- **Track Microsoft Spam Policy** - To determine what Microsoft would have done with every email, Avanan checks for updates in your configured Microsoft policy for every *"Spam confidence level (SCL)" on page 143*.
- **Integration with Microsoft Encryption** - To enable the integration with Microsoft Encryption to support DLP policy rules with the **Email is allowed. Encrypted by Microsoft** workflow. For more information, see *"DLP Policy for Outgoing Emails" on page 190*.
- **Automated maintenance** - To enhance troubleshooting capabilities and support infrastructure growth.
- To support new features in the future.

Privileged Authentication Administrator

Avanan uses the **Privileged Authentication Administrator** role to block users and reset their passwords if they are detected as compromised. See *"Remediating Compromised Accounts" on page 386*.

Reducing the Assigned Microsoft Application Role

- Avanan uses the **Privileged Authentication Administrator** role to block accounts that are detected as compromised. This role allows to block every compromised account, even if it is a **Global Administrator**. For more information, see *"Remediating Compromised Accounts" on page 386*.
- After successfully *"Activating Office 365 Mail" on page 47*, administrators can reduce the **Privileged Authentication Administrator** role to any of the roles described in this Microsoft article.
- Once you do that, Avanan will only be able to block compromised accounts that the selected role can reset their password (see this Microsoft article).

  Notes:
  - When reducing the application role, make sure to apply the lesser role first (see this Microsoft article) and then remove the more privileged role (see this Microsoft article).
  - If you have connected Avanan to Office 365 Mail prior to December 09, 2024, your application might be assigned with the **Global Administrator** role. You can manually reduce this role to **Exchange Administrator**, **Privileged Authentication Administrator** or a lesser role.

Instructions to reduce the assigned Microsoft application roles:

1. Add the new roles to the Avanan application.
2. Wait 30 minutes to allow the new roles to populate properly .
3. Remove the old roles from the Avanan application.

Microsoft 365 Mail - Approving User

As part of activating Office 365 Mail protection, you need a user with the **Privileged Role Administrator** role or higher to approve the required permissions for the application.

Use of Azure AD Graph APIs

As part of the integration with Microsoft, Avanan uses some Azure AD Graph APIs.

Since Microsoft is about to deprecate these APIs, you may receive notifications stating that a service principal (Avanan) uses an API scheduled for deprecation.

Avanan is actively migrating the remaining API calls from Azure AD Graph APIs to the newer Microsoft Graph APIs.

Avanan completes the migration before the end of June 2025.

For now, you can disregard these alerts from Microsoft.

Automatic Mode Onboarding - Microsoft 365 Footprint

While onboarding, if you choose to activate Office 365 Mail using the **Automatic mode** of operation, Avanan adds the **Avanan Cloud Security Platform - Emails V2** enterprise application to your Microsoft Azure and makes these changes to your Microsoft 365 environment.

- *"Mail Flow Rules" on the next page*
- *"Connectors" on page 65*
- *"Connection Filters" on page 69*
- *"Journal Rules" on page 70*
- *"Groups" on page 71*
- *"Distribution Lists" on page 72*
- *"Spoofed Senders Allow List" on page 72*
- *"Trusted ARC Sealers" on page 72*
- *"Reported Phishing Emails" on page 73*
- *"Delegated Token" on page 73*
- *"PowerShell Scripts" on page 73*

Approving User

Avanan uses the user who approves the Office 365 Mail application (see *"Activating Office 365 Mail" on page 47*) to keep the delegation token fresh.

This token ensures that, if you disconnect Avanan from your Office 365 Mail application, the system properly removes all related components from your Azure environment.

As a result, you may observe multiple login attempts by this user from Avanan IP addresses, along with token refresh activity.

Mail Flow Rules

To support **Prevent (Inline)** protection mode for policies, Avanan creates Mail Flow rules. These rules allow Avanan to scan and perform remediation before the email is delivered to the recipient's mailbox.

Avanan creates these Mail Flow rules.

- *"Avanan - Protect Outgoing Rule" below*
- *"Avanan - Protect Rule" on page 59*
- *"Avanan - Whitelist Rule" on page 60*
- *"Avanan - Junk Filter Low Rule" on page 62*
- *"Avanan- Junk Filter Rule" on page 63*
- *"Avanan - Protect Internal" on page 65*

Note - This is added only if inline policy is enabled for Internal Traffic.

Avanan - Protect Outgoing Rule

When is this rule applied?	What does this rule do?	Exceptions
■ Email is sent *Outside the organization*. ■ Email is received from a *avanan_inline_outgoing@[portal domain]* group member.	■ Routes the email using *"Avanan DLP Outbound Connector" on page 68*. ■ Sets the message header *X-CLOUD-SEC-AV-Info* with the *[portal],office365_emails,sent,inline* value. ■ Stops processing more rules.	Sender IP address belongs to one of the relevant IP addresses for **Avanan - Protect Outgoing** rule. See *"IP Addresses for Avanan - Protect Outgoing Rule" on the next page*.

Note - [portal] refers to the unique identifier of your Avanan tenant.

IP Addresses for Avanan - Protect Outgoing Rule

Avanan tenants residing in the United States

- 35.174.145.124
- 3.214.204.181
- 44.211.178.96/28
- 3.101.216.128/28
- 3.101.216.144/28
- 44.211.178.112/28

Avanan tenants residing in Europe

- 52.17.62.50
- 52.212.19.177
- 3.252.108.160/28
- 13.39.103.0/28
- 13.39.103.16/28
- 3.252.108.176/28

Avanan tenants residing in Australia

- 3.27.51.160/28
- 3.27.51.176/28
- 3.27.51.178/28
- 3.105.224.60
- 13.211.69.231
- 18.143.136.64/28
- 18.143.136.80/28

Avanan tenants residing in Canada

- 15.222.110.90
- 52.60.189.48
- 3.101.216.128/28
- 3.101.216.144/28

- 3.99.253.64/28
- 3.99.253.80/28

Avanan tenants residing in United Arab Emirates (UAE) *

- 3.29.194.128/28
- 3.29.194.144/28

* These regions are relevant only for tenants created using the Avanan MSP portal.

Avanan - Protect Rule

When is this rule applied?	What does this rule do?	Exceptions
■ Email is received from *Outside the organization*. ■ Email is sent *Inside the organization*. ■ Email is sent to *avanan_inline_incoming@[portal domain]* group member.	■ Routes the email using *"Avanan Outbound Connector" on page 68*. ■ Sets the message header *X-CLOUD-SEC-AV-Info* with the *[portal],office365_emails,inline* value. ■ Stops processing more rules.	Sender IP address belongs to one of the relevant IP addresses for the **Avanan - Protect** rule. See *"IP Addresses for Avanan - Protect Rule" below*.

Notes - [portal] refers to the unique identifier of your Avanan tenant.

IP Addresses for Avanan - Protect Rule

- **Avanan tenants residing in the United States**
  - 35.174.145.124
  - 44.211.178.96/28
  - 3.101.216.128/28
- **Avanan tenants residing in Europe**
  - 52.212.19.177
  - 3.252.108.160/28

- 13.39.103.0/28

- **Infinity Portal tenants residing in Australia**
  - 13.211.69.231
  - 18.143.136.64/28
  - 3.27.51.160/28
- **Avanan tenants residing in Canada**
  - 15.222.110.90
  - 3.101.216.128/28
  - 3.99.253.64/28
- **Avanan tenants residing in India**
  - 43.205.150.240/29
  - 18.143.136.64/28
  - 43.205.150.240/29
- **Avanan tenants residing in United Arab Emirates (UAE) ***
  - 3.29.194.128/28
  - 3.29.194.144/28

  * These regions are relevant only for tenants created using the Avanan MSP portal.
- **Avanan tenants residing in United Kingdom**
  - 13.42.61.32
  - 13.42.61.32/28
  - 13.39.103.0/28

Avanan - Whitelist Rule

When is this rule applied?	What does this rule do?	Exceptions
Sender IP address belongs to one of the relevant IP addresses for the **Avanan - Whitelist** rule. See *"IP Addresses for Avanan - Whitelist Rule" on the next page*.	Sets the Spam Confidence Level (SCL) to -1.	If the message header *X-CLOUD-SEC-AV-SCL* matches the following patterns: *true*.

IP Addresses for Avanan - Whitelist Rule

- Avanan tenants residing in the United States
    - 35.174.145.124
    - 44.211.178.96/28
    - 3.101.216.128/28
- Avanan tenants residing in Europe
    - 52.212.19.177
    - 3.252.108.160/28
    - 13.39.103.0/28
- Infinity Portal tenants residing in Australia
    - 13.211.69.231
    - 18.143.136.64/28
    - 3.27.51.160/28
- Avanan tenants residing in Canada
    - 15.222.110.90
    - 3.101.216.128/28
    - 3.99.253.64/28
- Avanan tenants residing in India
    - 43.205.150.240/29
    - 18.143.136.64/28
    - 43.205.150.240/29
- Avanan tenants residing in United Arab Emirates (UAE) *
    - 3.29.194.128/28
    - 3.29.194.144/28

    * These regions are relevant only for tenants created using the Avanan MSP portal.
- Avanan tenants residing in United Kingdom

- 13.42.61.32
- 13.42.61.32/28
- 13.39.103.0/28

Avanan - Junk Filter Low Rule

This rule is used to mark Microsoft that the email was detected as spam by Avanan and should be delivered to the Junk folder.

When is this rule applied?	What does this rule do?
■ Sender IP address belongs to one of the relevant IP addresses for the **Avanan - Junk Filter Low** rule. See *"IP Addresses for Avanan - Junk Filter Low Rule" below*. ■ *X-CLOUD-SEC-AV-SPAM-LOW* header matches the following patterns: *true*	Sets the Spam Confidence Level (SCL) to 6.

IP Addresses for Avanan - Junk Filter Low Rule

■ **Avanan tenants residing in the United States**

- 35.174.145.124
- 44.211.178.96/28
- 3.101.216.128/28

■ **Avanan tenants residing in Europe**

- 52.212.19.177
- 3.252.108.160/28
- 13.39.103.0/28

■ **Infinity Portal tenants residing in Australia**

- 13.211.69.231
- 18.143.136.64/28
- 3.27.51.160/28

■ **Avanan tenants residing in Canada**

- 15.222.110.90
- 3.101.216.128/28

- 3.99.253.64/28

- **Avanan tenants residing in India**
  - 43.205.150.240/29
  - 18.143.136.64/28
  - 43.205.150.240/29

- **Avanan tenants residing in United Arab Emirates (UAE) ***
  - 3.29.194.128/28
  - 3.29.194.144/28

  * These regions are relevant only for tenants created using the Avanan MSP portal.

- **Avanan tenants residing in United Kingdom**
  - 13.42.61.32
  - 13.42.61.32/28
  - 13.39.103.0/28

Avanan- Junk Filter Rule

This rule is used to mark Microsoft that the email was detected as spam by Avanan and should be delivered to the Junk folder.

When is this rule applied?	What does this rule do?
■ Sender IP address belongs to one of the relevant IP addresses for the **Avanan - Junk Filter** rule. See *"IP Addresses for Avanan - Junk Filter Rule" below*. ■ *X-CLOUD-SEC-AV-SPAM-HIGH* header matches the following patterns: *true*	Sets the Spam Confidence Level (SCL) to 9.

IP Addresses for Avanan - Junk Filter Rule

- **Avanan tenants residing in the United States**
  - 35.174.145.124
  - 44.211.178.96/28
  - 3.101.216.128/28

- **Avanan tenants residing in Europe**
    - 52.212.19.177
    - 3.252.108.160/28
    - 13.39.103.0/28
- **Infinity Portal tenants residing in Australia**
    - 13.211.69.231
    - 18.143.136.64/28
    - 3.27.51.160/28
- **Avanan tenants residing in Canada**
    - 15.222.110.90
    - 3.101.216.128/28
    - 3.99.253.64/28
- **Avanan tenants residing in India**
    - 43.205.150.240/29
    - 18.143.136.64/28
    - 43.205.150.240/29
- **Avanan tenants residing in United Arab Emirates (UAE) ***
    - 3.29.194.128/28
    - 3.29.194.144/28

    * These regions are relevant only for tenants created using the Avanan MSP portal.
- **Avanan tenants residing in United Kingdom**
    - 13.42.61.32
    - 13.42.61.32/28
    - 13.39.103.0/28

Avanan - Protect Internal

When is this rule applied?	What does this rule do?	Exceptions
■ Recipient is inside the organization and is a member of the inline group. See, *"Avanan Inline Incoming Group" on page 71*. ■ Sender is inside the organization.	■ Routes the email using Outbound DLP Avanan Connector. ■ Adds *X-CLOUD-SEC-AV-Info* to the header with *[portal],office365_emails,internal,inline* value.	■ If the SCL is greater than or equal to 5. ■ Sender IP address belongs to one of the relevant IP addresses for the Avanan - Protect rule. See *"IP Addresses for Avanan - Protect Rule" on page 59*.

Notes - [portal] refers to the unique identifier of your Avanan tenant.

Connectors

To support **Prevent (Inline)** protection mode for policies, Avanan creates connectors. These connectors allow Avanan to scan and perform remediation before the email is delivered to the recipient's mailbox.

Avanan creates these connectors.

- *"Avanan Inbound Connector" below*
- *"Avanan DLP Inbound Connector" on page 67*
- *"Avanan Outbound Connector" on page 68*
- *"Avanan DLP Outbound Connector" on page 68*
- *"Avanan Journaling Outbound Connector" on page 69*

Avanan Inbound Connector

Mail flow scenario:

- From: Partner organization
- To: Office 365

Identify your partner organization by:

Identify the partner organization by verifying that the messages are coming from one of the relevant IP addresses for **Avanan Inbound** Connector. See *"IP Addresses for Avanan Inbound Connector" on the next page*.

Security restrictions:

- Reject messages if they aren't encrypted using Transport Layer Security (TLS).

IP Addresses for Avanan Inbound Connector

- **Avanan tenants residing in the United States**
  - 35.174.145.124
  - 44.211.178.96/28
  - 3.101.216.128/28
- **Avanan tenants residing in Europe**
  - 52.212.19.177
  - 3.252.108.160/28
  - 13.39.103.0/28
- **Infinity Portal tenants residing in Australia**
  - 13.211.69.231
  - 18.143.136.64/28
  - 3.27.51.160/28
- **Avanan tenants residing in Canada**
  - 15.222.110.90
  - 3.101.216.128/28
  - 3.99.253.64/28
- **Avanan tenants residing in India**
  - 43.205.150.240/29
  - 18.143.136.64/28
  - 43.205.150.240/29
- **Avanan tenants residing in United Arab Emirates (UAE) ***
  - 3.29.194.128/28
  - 3.29.194.144/28

  * These regions are relevant only for tenants created using the Avanan MSP portal.
- **Avanan tenants residing in United Kingdom**

- 13.42.61.32
- 13.42.61.32/28
- 13.39.103.0/28

Avanan DLP Inbound Connector

Mail flow scenario:

- From: Your organization's email server
- To: Office 365

Identify incoming emails are sent from your email by:

- Identify the incoming messages from your email server by verifying that the sender's IP address is one of the relevant IP addresses for **Avanan DLP Inbound** Connector. See *"IP Addresses for Avanan DLP Inbound Connector" below*.
- Sender's email address is an accepted domain for your organization.

IP Addresses for Avanan DLP Inbound Connector

- **Avanan tenants residing in the United States**
  - 3.101.216.144/28
  - 44.211.178.112/28
  - 3.214.204.181
- **Avanan tenants residing in Europe**
  - 52.17.62.50
  - 3.252.108.176/28
  - 13.39.103.16/28
- **Avanan tenants residing in Australia**
  - 3.27.51.178/28
  - 18.143.136.80/28
  - 3.105.224.60
- **Avanan tenants residing in Canada**
  - 52.60.189.48
  - 3.101.216.144/28

- 3.99.253.80/28

- **Avanan tenants residing in India**
  - 43.204.62.184
  - 18.143.136.80/28
  - 43.205.150.248/29
- **Avanan tenants residing in United Arab Emirates (UAE)**
  - 3.29.194.144/28
- **Avanan tenants residing in United kingdom**
  - 13.42.61.47
  - 13.42.61.47/28
  - 13.39.103.23/28

Avanan Outbound Connector

Mail flow scenario:

- From: Office 365
- To: Partner organization

Use of connector:

Use only when I have a transport rule set up that redirects messages to this connector.

Routing:

Route email messages through these smart hosts: *[portal]-host.avanan.net*

Security restrictions:

- Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

Avanan DLP Outbound Connector

Mail flow scenario:

- From: Office 365
- To: Your organization's email server

Use of connector:

- Use only when I have a transport rule set up that redirects messages to this connector.

Routing:

Route email messages through these smart hosts: *[portal]-dlp.avanan.net*

Security restrictions:

- Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

Avanan Journaling Outbound Connector

Mail flow scenario:

- From: Office 365
- To: Your organization's email server

Use of connector:

Use only for email sent to these domains: *[portal]-mail.avanan.net*

Routing:

Route email messages through these smart hosts: *[portal]-host.avanan.net*

Security restrictions:

- Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

Connection Filters

Avanan creates Connection Filters to prevent the blocking of emails sent to users.

Connection filter name: Connection filter policy (Default)

Avanan tenants residing in the United States

- 35.174.145.124
- 3.214.204.181
- 44.211.178.96/28
- 3.101.216.128/28
- 3.101.216.144/28
- 44.211.178.112/28

Avanan tenants residing in Europe

- 52.17.62.50
- 52.212.19.177
- 3.252.108.160/28

- 13.39.103.0/28
- 13.39.103.16/28
- 3.252.108.176/28

Avanan tenants residing in Australia

- 3.27.51.160/28
- 3.27.51.176/28
- 3.27.51.178/28
- 3.105.224.60
- 13.211.69.231
- 18.143.136.64/28
- 18.143.136.80/28

Avanan tenants residing in Canada

- 15.222.110.90
- 52.60.189.48
- 3.101.216.128/28
- 3.101.216.144/28
- 3.99.253.64/28
- 3.99.253.80/28

Avanan tenants residing in United Arab Emirates (UAE) *

- 3.29.194.128/28
- 3.29.194.144/28

* These regions are relevant only for tenants created using the Avanan MSP portal.

Journal Rules

Avanan creates a Journal rule that configures Microsoft 365 to send a copy of all scoped emails to the journaling mailbox used by Avanan for inspection.

Avanan uses this Journal rule only for policies in **Detect** and **Detect and Remediate** protection modes.

Journal rule name: Avanan - Monitor

Journal Reports

Avanan configures the Journal rule to send the Journal reports to *[portal]@[portal]-mail.avanan.net*

It also configures a mailbox for undeliverable journal reports, if the mailbox was not configured yet for the Avanan tenant.

Avanan sends the undeliverable journal reports to these mailboxes when they are not deliverable to the email address specified in the journal rule:

Avanan Tenant Region	Undeliverable Journal Report Mailbox
United States	*[portal name]@mt-prod-3-journal-error.avanan.net*
Europe	*[portal name]@mt-prod-av-1-journal-error.avanan.net*
Canada	*[portal name]@mt-prod-av-ca-2-journal-error.avanan.net*

Groups

Avanan creates groups to protect the specific users and groups selected in the policies for **Prevent (Inline)** protection mode.

When administrators configure **Scope** for a policy in **Prevent (Inline)** protection mode, it gets updated to the relevant group so that only those specific users are protected inline.

Avanan creates these groups:

- avanan_inline_incoming
- avanan_inline_outgoing

Avanan Inline Incoming Group

This group allows Avanan to protect only the incoming emails sent to users protected by an incoming policy in **Prevent (Inline)** protection mode.

Group name: avanan_inline_incoming

Group email address: avanan_inline_incoming@[portal domain]

Avanan Inline Outgoing Group

This group allows Avanan to protect only the outgoing emails sent by users protected by an outgoing policy in **Prevent (Inline)** protection mode.

Group name: avanan_inline_outcoming

Group email address: avanan_inline_outcoming@[portal domain]

Distribution Lists

Avanan creates a distribution list to support the protection of group mailboxes for policies in **Prevent (Inline)** protection mode.

Distribution list name: avanan_inline_groups

Spoofed Senders Allow List

To route emails from protected users and send emails on behalf of the protected domain, Avanan adds spoofed sender exceptions to Tenant Allow/Block List in Microsoft 365.

For example, Avanan adds these infrastructure values for Avanan tenants residing in the United States region.

User	Sending Infrastructure	Spoof Type	Action
*	us.cloud-sec-av.com	Internal	Allow
*	us.cloud-sec-av.com	External	Allow

Sending infrastructure for Avanan tenants residing in different regions:

Region	Country	Sending Infrastructure
Americas	USA	us.cloud-sec-av.com
	Canada	ca.cloud-sec-av.com
EMEA (Europe, Middle East and Africa)	Ireland	eu.cloud-sec-av.com
	United Arab Emirates	mec.cloud-sec-av.com
APAC (Asia Pacific)	Australia	au.cloud-sec-av.com
	India	aps.cloud-sec-av.com
United Kingdom	-	euw2.cloud-sec-av.com

Trusted ARC Sealers

To ensure email authentication remains valid even after routing emails, Avanan adds a Avanan domain to the list of Authentication Received Chain (ARC) trusted sealers.

Avanan adds this to the list of trusted ARC sealers: **avanan.net**

Reported Phishing Emails

To present all phishing reported emails from end users using the *"Microsoft Report Message Add-in" on page 366*, reports must be configured to be sent to Microsoft and to an internal phishing reporting mailbox.

If your Microsoft 365 account is configured to send reported emails to an internal mailbox, Avanan monitors that internal mailbox for phishing reports, and the configuration does not change.

If your Microsoft 365 account is not configured to send emails to an internal mailbox, the system creates a shared mailbox with **report-phishing-checkpoint@<your domain>** email address and configures it to receive these reports.

Note - The system creates only a shared mailbox and it does not consume a Microsoft license from your account.

Delegated Token

To complete the required actions during automatic onboarding, such as creating groups and assigning a **Global Admin** role to the Avanan application, Avanan uses a delegated token from the authorizing user who approved the permissions.

If you choose to disconnect Avanan from Microsoft 365, Avanan executes the reverse actions, including deleting groups and disassociating roles. To do that, the Avanan Azure application must periodically refresh and maintain a valid delegated token.

The system initiates the refresh action on behalf of the authorizing user, and you can observe these activities in your Microsoft 365 audit log:

- Periodic logins by the Avanan application on behalf of the user to refresh the token.
- Failed login attempts in case the user no longer exists or the password has changed.

  Note - These failed logins do not affect security or email delivery. However, when disconnecting Avanan from Microsoft 365, manual actions are necessary to eliminate its footprint.
  To resolve this issue, re-authorize the Microsoft 365 application with the same or another Microsoft administrator credentials.
  1. Click **Security Settings** > **SaaS Applications**.
  2. Click **Configure** for Office 365 Mail.
  3. Click **Re-Authorize Avanan Office 365 Email App**.
  4. Follow the onscreen instructions and authorize the Microsoft 365 application.

PowerShell Scripts

Avanan uses PowerShell scripts to perform various tasks in the Microsoft 365 environment, such as:

- Create / edit / delete Mail Flow rules, Connectors, Journal rules, Connection Filter, and Distribution List.
- Configuring a mailbox for undeliverable *"Journal Reports" on page 71* (if the mailbox was not configured yet for the tenant).

  This mailbox will be used to receive *"Journal Reports" on page 71* when they are not deliverable to the email address specified in the Journal rule.
- Reading the Hosted Content Filter Policy to get the tenant's policy actions.
- Allowing Avanan domain, so emails will not be blocked when going through Avanan's security engines.
- In case a policy that triggers Microsoft Encryption is created, a script will read the IRM Encryption to configure an Encryption rule.
- Creating a new shared mailbox and configuring the system to forward reported phishing emails to the mailbox using the *"Microsoft Report Message Add-in" on page 366*.

  Note - If the Microsoft account is already configured to forward reported phishing emails to an internal mailbox, this configuration will not be performed.

Connecting Multiple Portals to the Same Microsoft 365 Account

Sometimes, administrators need to connect multiple Avanan tenants to the same Microsoft 365 account.

This might be needed to apply strict categorization of users, where administrators of one tenant do not read emails, files, and messages of users in other tenants.

Use Case

- Large global organization with different branch offices managed by different administrators.
- MSPs hosting multiple small customers on the MSP's Microsoft 365 account.

Limitations

- If you activated the Office 365 Mail SaaS application in the past not following the procedure below, you cannot connect additional tenants to it.
  - To connect multiple Avanan tenants to the same Microsoft 365 account, you must disconnect the existing Office 365 Mail SaaS application from the tenant and connect it again. See *"Deactivating Office 365 Mail" on page 78* and *"Connecting Multiple Avanan Tenants" on the next page*.
- By default, Avanan does not support connecting tenants from different regions (see *"Regional Data Residency" on page 35*) to the same Microsoft 365 account. If you need this option to be enabled, contact *Avanan Support*.

- Each tenant must be restricted to a specific group of users (user group). These user groups must be mutually exclusive and no user can be a member of two such groups.
- Currently, Microsoft Teams can be enabled only for one tenant when connecting multiple Avanan tenants to the same Microsoft 365 account.

Connecting Multiple Avanan Tenants

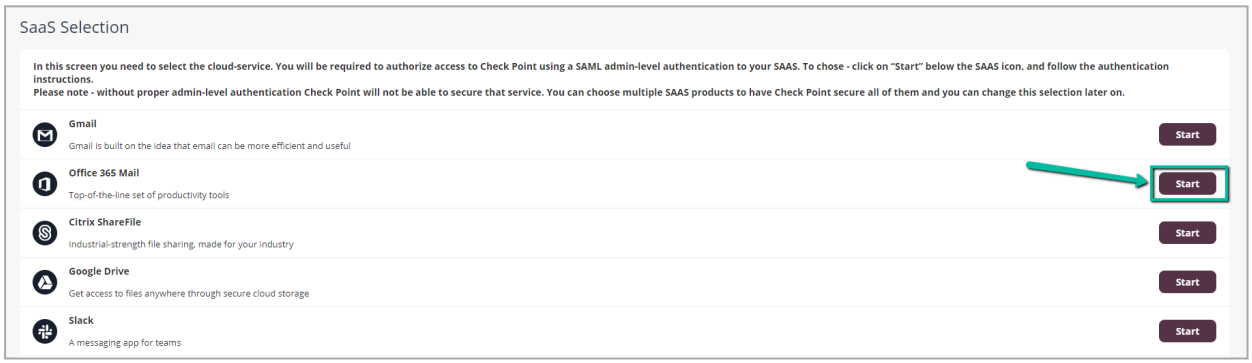
To connect multiple Avanan tenants to the same Microsoft 365 account:

Note - Before connecting the tenants, see the *"Limitations" on the previous page*.

1. From the **Getting Started Wizard** click **Start** for Office 365 Mail.

   or

   Navigate to **Security Settings > SaaS Applications** and click **Start** for Office 365 Mail.



2. Select the mode of operation for Office 365.

   - **Automatic mode**

     Avanan performs the necessary configurations to your Microsoft 365 environment and operates in **Monitor only** mode. For more information, see *"Automatic Mode Onboarding - Microsoft 365 Footprint" on page 56*.

   - **Manual mode**

     You must manually perform the necessary configurations in the Office 365 Admin Exchange Center before you bind the application to your Office 365 email account and every time you add or edit the security policy associated with Office 365 emails. For more information, see *"Appendix A: Avanan Manual Integration with Office 365" on page 543*.

   Note - Avanan recommends using **Automatic mode**, allowing better maintenance, management, and smoother user experience. Before using the **Manual mode**, contact *Avanan Support* to help resolve any issues raised with the **Automatic mode** for onboarding.

3. Enable the **I Accept Terms Of Service** checkbox.

4. If you need to limit the license consumption and protection to a specific group of users or to connect multiple Avanan tenants to the same Microsoft 365 account:

   a. Enable the **Restrict inspection to a specific group (Groups Filter)** checkbox and click **OK**.

   b. In the **Office 365 Authorization** window that appears, sign in with a user with Privileged Role Administrator role or higher permissions.

      In the authorization screen, click **Accept** to grant permissions for **Avanan Cloud Security Platform - Emails V2** application.

      To view the permitted IP addresses to access this application, see *"Appendix G: Permitted IP Addresses to access the Avanan Azure Application" on page 630*.

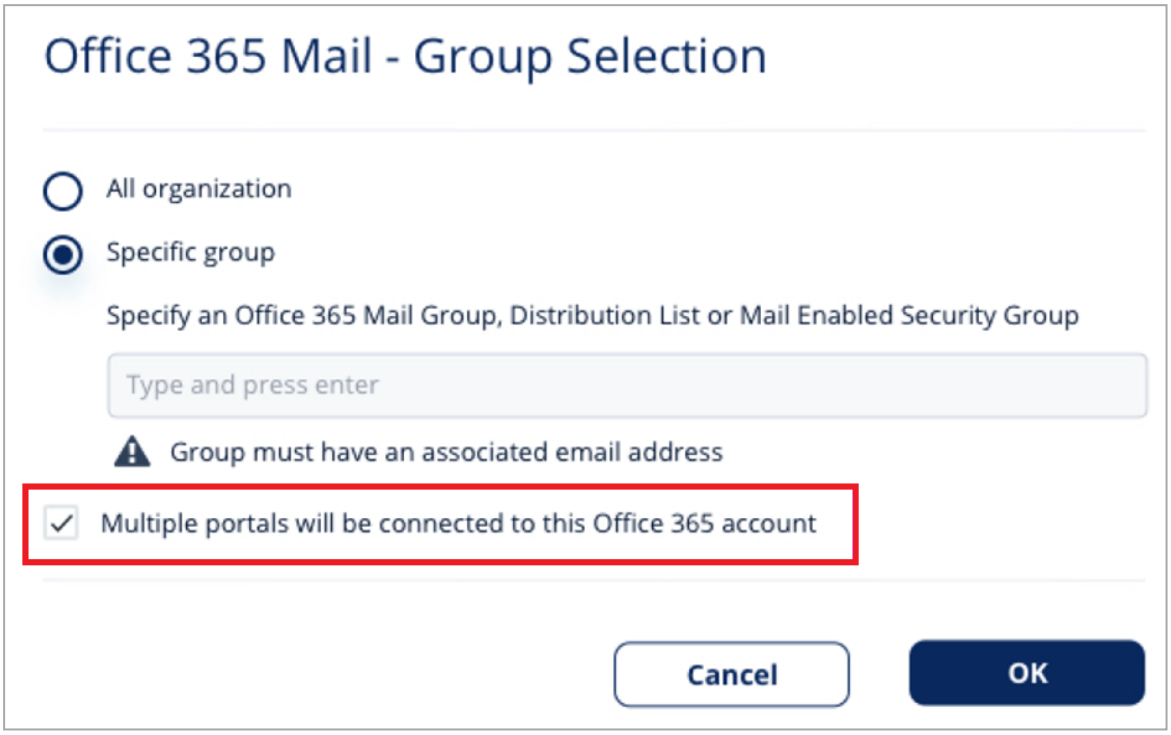
   c. In the **Office 365 Mail - Group Selection** pop-up, select **Specific group**.

   d. Enter the group name you need to protect with Avanan.

      Notes:
      - The group name must have an associated email address.
      - Avanan supports these groups for group filtering:
        - Assigned Membership:
          - Microsoft 365 Group
          - Mail-enabled Security Group
          - Distribution List
        - Dynamic Membership:
          - Microsoft 365 Group

e. If you need to connect multiple Avanan tenants to the same Microsoft 365 account, enable the **Multiple portals will be connected to this Office 365 account** checkbox.

Caution - Before you enable the checkbox, see *"Connecting Multiple Portals to the Same Microsoft 365 Account" on page 74*.



f. Click **OK**.

Now, the Office 365 Mail SaaS is enabled and monitoring begins immediately.

Note - After activating Office 365 Mail, Avanan performs retroactive scan of its content. For more information, see *"Onboarding Next Steps" on page 94*.

Connecting Multiple Tenants to the same Microsoft 365 Account - Microsoft 365 Footprint

As part of the connection to Microsoft 365, Avanan creates Mail Flow rules, Connectors, Journaling Rules and Groups.

As part of the automatic connection of multiple Avanan tenants to the same Microsoft 365 account, these artifacts will be created separately for each tenant, and their names will include a suffix that serves as a **portal identifier**.

These artifacts will appear in your Microsoft 365 account once for every connected tenant:

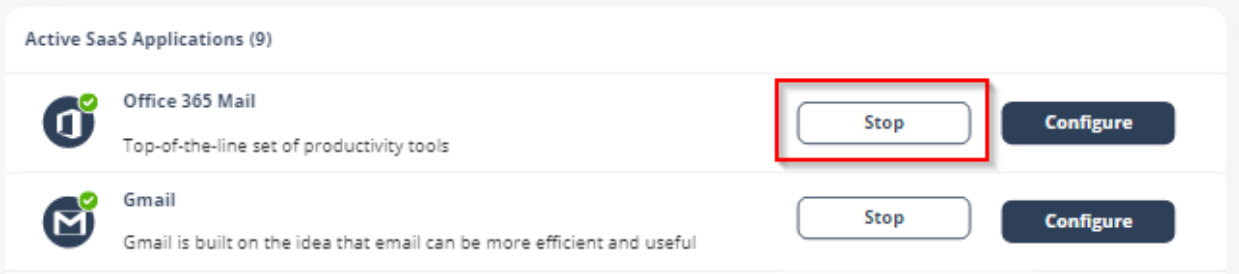
- Mail Flow Rules:
  - Avanan Protect – [portal identifier]
  - Avanan Protect Outgoing – [portal identifier]
- Connectors

    - Avanan Journaling Outbound – [portal identifier]
    - Avanan Outbound – [portal identifier]
    - Avanan DLP Outbound – [portal identifier]
- Journal rule
    - Avanan – Monitor – [portal identifier]
- Groups – a Microsoft group is created for every portal
    - avanan_inline_incoming_[portal identifier]
    - avanan_inline_outgoing_[portal identifier]
- Distribution list
    - avanan_inline_groups_[portal identifier]

For more information about portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.

Deactivating Office 365 Mail

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Office 365 Mail.



3. In the confirmation pop-up, click **Stop**.

Upon deactivation, Avanan will no longer protect your organization's Office 365 mailboxes.

To complete the deactivation process:

- If you receive *Office 365 protection was successfully uninstalled* message, follow these steps.
    1. Sign in to the Microsoft Entra ID (formerly Azure AD) portal as a Global Administrator or a Co-Administrator.

2. In the left menu, select **Enterprise applications**.

   The **All applications** pane opens and displays a list of the applications in your Microsoft Entra ID (formerly Azure AD) tenant.

3. Select the application you want to delete.

4. In the **Manage** section of the left menu, select **Properties**.

5. At the top of the **Properties** pane, select **Delete**, and then select **Yes** to confirm you want to delete the application from your Microsoft Entra ID (formerly Azure AD) tenant.

6. Repeat steps 3-5 for all the applications you want to delete.

7. Review the Reported message destinations settings (Go to **User reported settings** and scroll down to **Reported message destinations**) and choose whether you want to change them.

   Note - When you initially connected Avanan to Microsoft 365, these settings were modified to ensure reported emails appear in the Avanan Administrator Portal. For more information, see *"Reported Phishing Emails" on page 73*.

- If you receive *Avanan was unable to be uninstalled automatically from Office 365* message, follow these steps.

1. **In the Exchange Admin Center**

    a. Sign in to the Exchange Admin Center as the Global Administrator or a Co-Administrator.

    b. In the left menu, select **Mail Flow**, and then **Rules**.

    c. Delete all entries that start with Avanan.

        i. In **Journal Rules**, click on the value shown right after the text "*Send undeliverable journal reports to:*".

        ii. In the dialog box, clear the value (or set a new value as your preference) and click **Save**.

    d. In the left menu, select **Mail Flow**, and then **Connectors**.

    e. Delete all entries that start with Avanan.

    f. In the left menu, select **Protection**, and then **Connection Filter**.

    g. Select the **Default entry** and click **Edit**.

h. In the dialog box that appears, click **Connection filtering**, and remove the IP address relevant to your data region in the **Allowed IP Address** list:

- If your data residency is in the United States:
  - 35.174.145.124
  - 3.214.204.181
- If your data residency is in Europe:
  - 52.212.19.177
  - 52.17.62.50
- If your data residency is in Australia *:
  - 13.211.69.231
  - 3.105.224.60
- If your data residency is in Canada:
  - 15.222.110.90
  - 52.60.189.48
- If your data residency is in India *:
  - 3.109.187.96
  - 43.204.62.184
- If your data residency is in United Arab Emirates *:
  - 3.29.194.128
  - 3.29.194.144
- If your data residency is in United Kingdom *:
  - 13.42.61.32
  - 13.42.61.47

* These regions are relevant only for tenants created using the Avanan MSP portal.

i. Click **Save**.

2. **In the Microsoft Entra ID (formerly Azure AD) portal**

    a. Sign in to the Microsoft Entra ID (formerly Azure AD) portal as the Global Administrator or a Co-Administrator.

    b. In the left menu, select **Enterprise applications**.

    The **All applications** pane opens and displays a list of the applications in your Microsoft Entra ID (formerly Azure AD) tenant.

    c. Select the application you want to delete.

    d. In the **Manage** section of the left menu, select **Properties**.

    e. At the top of the **Properties** pane, select **Delete**, and then select **Yes** to confirm you want to delete the application from your Microsoft Entra ID (formerly Azure AD) tenant.

    f. Repeat steps 2.c - 2.e for all the applications you want to delete.

After a certain period of time your tenant-related data will be deleted. If you want the data to be deleted immediately, contact *Avanan Support*.

Activating Microsoft Teams

Important

- To activate Microsoft Teams, you must have administrator access to Office 365.
- To activate Microsoft Teams, you must have any of these licenses:
    - Office 365 E5/A5/G5
    - Microsoft 365 E5/A5/G5
    - Microsoft 365 E5/A5/F5/G5 Compliance and Microsoft 365 F5 Security & Compliance
    - Microsoft 365 E5/A5/F5/G5 Information Protection and Governance or Microsoft 365 E5 Compliance add-on, when either of them is added to one of the these E3 licenses:
        - Enterprise Mobility + Security E3
        - Office 365 E3
        - Microsoft 365 E3

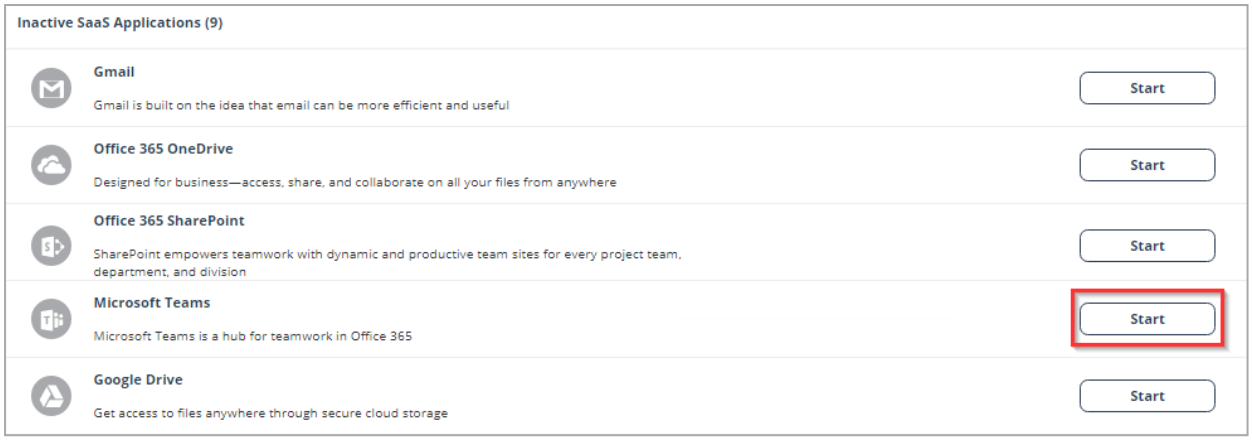
To activate Microsoft Teams:

1. From the **Getting Started Wizard** click **Start** for Microsoft Teams.

    Note - This wizard appears only when you are activating your first SaaS application in the Avanan Administrator Portal.

    or

    Navigate to **Security Settings > SaaS Applications** and click **Start** for Microsoft Teams.



2. Click **Start** in the pop-up screen that appears.
3. In the **Microsoft Sign in** window that opens, sign in with your Microsoft administrator credentials.

   Note - Microsoft performs the authentication, and Avanan does not provide these credentials.

4. In the authorization screen from Microsoft, click **Accept** to grant necessary permissions to Avanan.

   For the list of permissions requested from Microsoft, see *"Required Permissions" on page 257*.

   The Microsoft Teams SaaS is enabled, and monitoring begins immediately.

Activating Office 365 OneDrive

Important - To activate Office 365 OneDrive, make sure you have these:

- You are a user with Microsoft Global Administrator permissions, or you have the credentials of such a user.
- You have the minimum supported SaaS license. See *"Minimum License Requirements to Activate SaaS Applications" on page 43*.

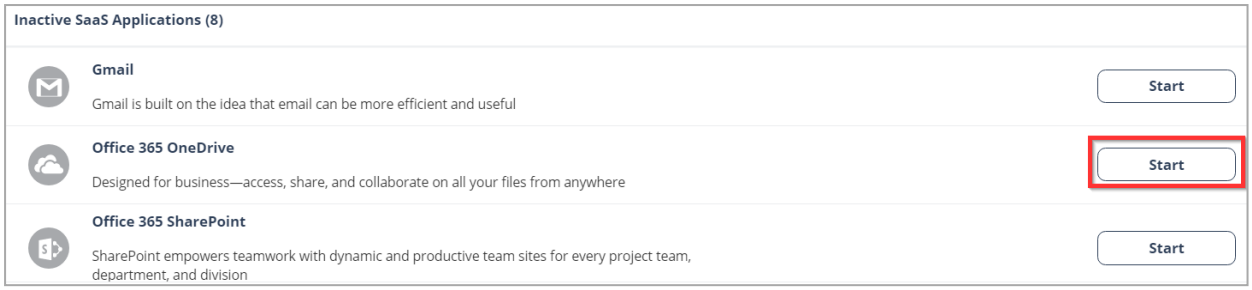
To activate Office 365 OneDrive:

1. From the **Getting Started Wizard** click **Start** for Office 365 OneDrive.

   Note - This wizard appears only when you are activating your first SaaS application in the Avanan Administrator Portal.

   or

   Navigate to **Security Settings > SaaS Applications** and click **Start** for Office 365 OneDrive.



2. Click **Start** in the pop-up screen that appears.
3. In the **Microsoft Sign in** window that opens, sign in with your Microsoft administrator credentials.

   Note - Microsoft performs the authentication, and Avanan does not provide these credentials.

4. In the authorization screen from Microsoft, click **Accept** to grant necessary permissions to Avanan.

   For the list of permissions requested from Microsoft, see *"Required Permissions" on page 275*.

   The Office 365 OneDrive SaaS is enabled, and monitoring begins immediately.

Activating Office 365 SharePoint

Important - To activate Office 365 SharePoint, make sure you have these:

- You are a user with Microsoft Global Administrator permissions, or you have the credentials of such a user.
- You have the minimum supported SaaS license. See *"Minimum License Requirements to Activate SaaS Applications" on page 43*.

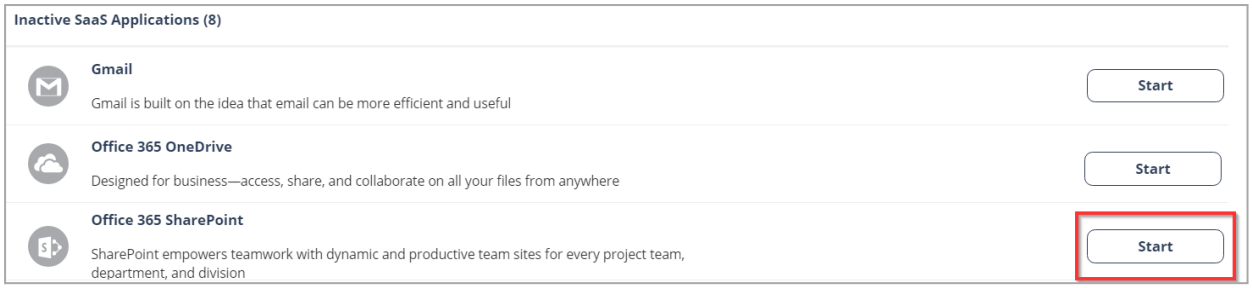
To activate Office 365 SharePoint:

1. From the **Getting Started Wizard** click **Start** for Office 365 SharePoint.

   Note - This wizard appears only when you are activating your first SaaS application in Avanan Administrator Portal.

   or

   Navigate to **Security Settings > SaaS Applications** and click **Start** for Office 365 SharePoint.

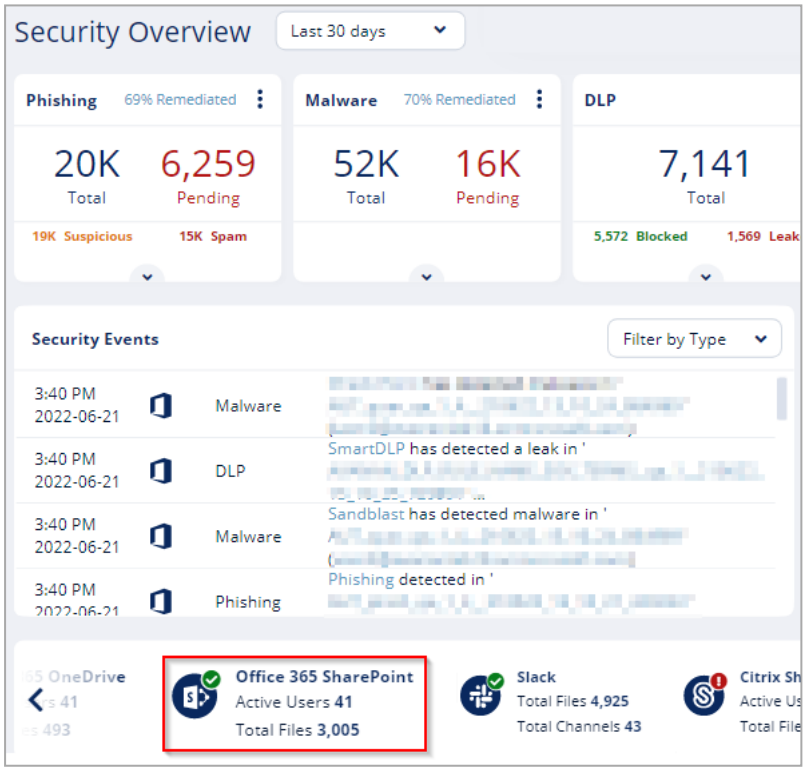


2. Click **Start** in the pop-up screen that appears.
3. In the **Microsoft Sign in** window that opens, sign in with your Microsoft administrator credentials.

   Note - Microsoft performs the authentication, and Avanan does not provide these credentials.
4. In the authorization screen from Microsoft, click **Accept** to grant necessary permissions to Avanan.

   For the list of permissions requested from Microsoft, see *"Required Permissions" on page 285*.

   The Office 365 SharePoint SaaS is enabled, and monitoring begins immediately.



Activating Google Workspace (Gmail and Google Drive)

Prerequisites

To activate Google Workspace, you must have these:

- You have the Administrator access to activate Google Workspace.
- Additional Google Workspace license to integrate with Avanan. (Integration is not supported for clients on the free G-Suite license tiers.)
- You have the minimum supported SaaS license. See *"Minimum License Requirements to Activate SaaS Applications" on page 43*.
- If you use GCDS (Google Cloud Directory Sync) to synchronize your user groups on-premises and in the cloud, before activating Google Workspace, you must create exclusion rules for these user groups.
  - **avanan_inline_policy**
  - **avanan_inline_outgoing_policy**
  - **avanan_monitor_policy**
  - **avanan_monitor_outgoing_policy**

  For more information, see *"User Groups" on page 91*.

By default, the Google Chrome browser authenticates the signed-in Chrome user in Google Workspace instead of a selected account. To see if you are signed in to Google Chrome, look for the user name in the browser's top-right corner.

Possible workarounds:

- Perform the Google Workspace activation using a non-Chrome browser.
- Sign out (switch to Guest) any logged-in Chrome user before you continue.

While onboarding Google Workspace (Gmail / Google Drive), Avanan creates a service user (*cloud-sec-av@[domain]*) in the root organizational unit.

Before onboarding, make sure that these settings are selected in your Google Admin console.

- Go to **Authentication Settings** of the root organizational unit and check these settings.
  - The **Allow users to turn on 2-Step Verification** check-box is selected.
  - If the **Only security key** option is selected, do not select the **Don't allow users to generate security codes** option.

Notes:
If the **Authentication Settings** are not supported, onboarding fails. To resolve this issue, do one of these.

- If you want to keep the unsupported **Authentication Settings** of your root organizational unit, move the service user (*cloud-sec-av@[domain]*) to an organizational unit with the supported **Authentication Settings**. Then, start onboarding Gmail or Google Drive again.
- Create a new dedicated organizational unit with the supported **Authentication Settings** and move the service user (*cloud-sec-av@[domain]*) to the organizational unit. Then, start onboarding Gmail or Google Drive again.

Activating Gmail

To activate Gmail:

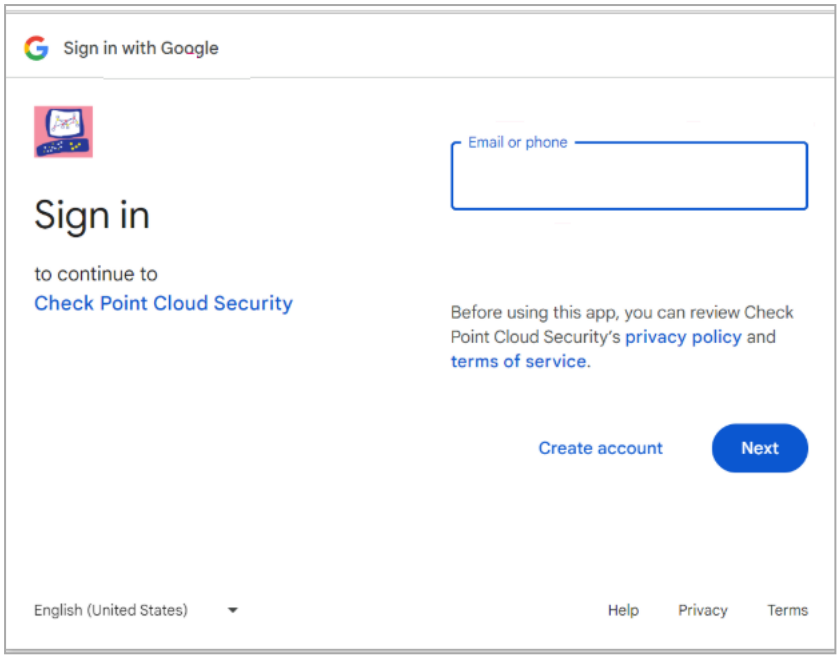
1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Start** for Gmail.

3. Select the mode of operation:
   - **Automatic mode**

     Avanan performs the necessary configurations to your Google Workspace environment and operates in **Monitor only** mode.
   - **Manual mode**

     You must manually configure the necessary settings in the Google Admin Console before linking the application to your Gmail account and every time you add or edit the security policy associated with emails.

   Note - Avanan recommends using **Automatic mode** for better maintenance and management and a smoother user experience. Before using the **Manual mode**, contact *Avanan Support* to help resolve any issues raised with the **Automatic mode** for onboarding.
4. Enable the **I Accept Terms Of Service** checkbox and click **OK**.
5. In the Google Workspace window that appears, sign in with Google administrator credentials.



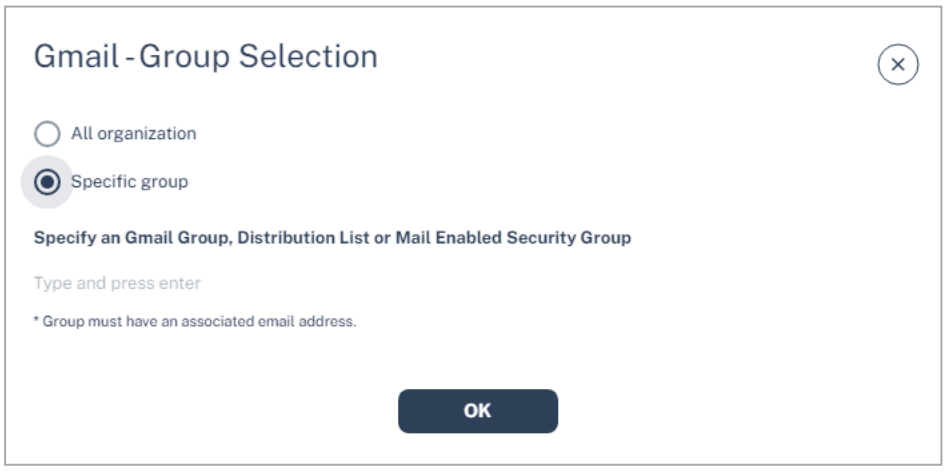
6. After successful authentication, you will be redirected to the **Avanan** application installation page.

   Click **Admin Install**.

7. In the **Admin install** pop-up that appears, click **Continue**.
8. Review the permissions requested by **Avanan** application. Select **Everyone at your organization**, accept the terms of services, and click **Finish**.
9. In the confirmation pop-up that appears after the **Avanan** application completes the installation, click **Done**.

   Gmail - Group Selection pop-up that appears.

10. To protect all users in your organization, select **All Organization** and click **OK**.



11. To protect specific users in your organization, select **Specific group**, enter the group name and click **OK**.

Note - The group name must have an associated email address.

Avanan enables the Gmail SaaS application and starts monitoring for security events.

Activating Google Drive

To activate Google Drive:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Start** for Google Drive.

3. Log in to the Google Workspace Marketplace using your Google administrator credentials.
4. If the **Avanan Cloud Security** app is already installed from Google Workspace Marketplace, after successful authentication, Avanan starts scanning the Google Drive of users.

   If not, continue from steps 3 in *"Activating Gmail" on page 87*.

Note - After activating Google Drive, Avanan performs retroactive scan of its content. For more information, see *"Onboarding Next Steps" on page 94*.

For more details about automatic configuration on Google Workspace, see *"Google Workspace Footprint" below*.

Google Workspace Footprint

After *"Activating Google Workspace (Gmail and Google Drive)" on page 85*, Avanan automatically creates a **Super Admin**, host (mail route), inbound gateway, SMTP relay service, two user groups, and four content compliance rules.

Super Admin

While installing the **Avanan Cloud Security** app, a new **Super Admin** user account is created in your Google Admin console.

The **Super Admin** user has an email address in the *cloud-sec-av@[domain]* format and is sometimes referred to as the **Avanan Service User**.

This user requires a Gmail license. For more details about the **Super Admin** role, see Pre-built administrator roles.

What is the Super Admin User Used For?

Avanan uses Super Admin user to perform tasks that cannot be accomplished with the Google APIs.

Avanan uses Super Admin user to do these tasks:

- To connect with Google Workspace and create *"User Groups" on the next page*, *"Host" on the next page*, *"Inbound Gateway" on page 92*, *"SMTP Relay Service" on page 92*, and *"Content Compliance Rules" on page 92*.
- To enable different artifacts that allow DLP inspection of outgoing emails in **Protect (Inline)** policy mode.
- To do maintenance activities from time to time, primarily to optimize support case handling.
- To take actions on files uploaded to Google Drive that do not have an owner. For more information, see *"Google Drive Permissions Changes" on page 93*.
- To support new features in the future.

Super Admin Security

The password of the **Super Admin** contains 43 random characters, a mix of lower case letters, upper case letters, and digits. The password is safely stored in AWS Key Management Service (AWS KMS).

Also, Avanan recommends to enable Multi-Factor Authentication (MFA) to enhance security for this account.

Changing the Google Application Role

After successfully onboarding the Google Workspace SaaS application to Avanan, the administrator can change the role assigned to the Avanan application. To do that:

1. Sign in to your Google Admin console with an account with super administrator privileges.
2. Create a custom admin role. For more information, see Google Documentation.
3. Assign these privileges to the role:
    a. In the **Admin console** privileges:
        i. Assign **Settings** privilege to **Gmail**.
        ii. Assign **Groups** privilege.
    b. In the **Admin API** privilege, assign **Groups** privilege.
4. Search for the **Cloud-Sec-AV Service Admin** role and do these:

a. Unassign the **Super Admin** role. For more information, see Google Documentation.

b. Assign the custom admin role created in step 2. For more information, see Google Documentation.

User Groups

After activating Google Workspace, Avanan automatically creates these user groups.

- **avanan_inline_policy**
- **avanan_monitor_policy**

You can view these user groups under **Groups** in your Google Admin console.

Note - If you use GCDS (Google Cloud Directory Sync) to synchronize your user groups on-premises and in the cloud, the synchronization triggers the deletion of these Avanan groups. Though this will not impact the email delivery, Avanan cannot scan the emails, and no security events get generated.

Before activating Google Workspace, you must create exclusion rules for these user groups. Select the exclusion type as **Group Email Address**, match type as **Exact Match**, and the group email address should be in the *groupname@[domain]* format.

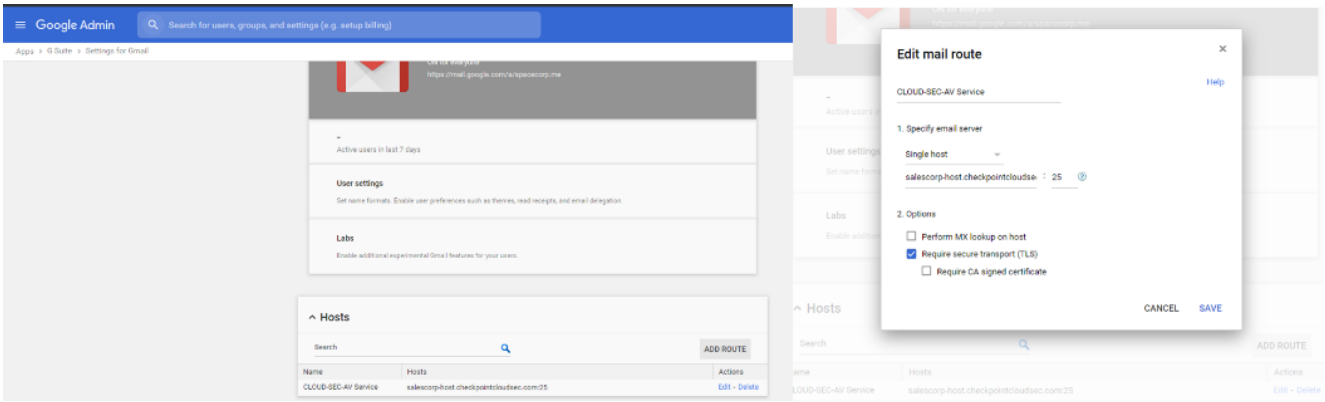
For example, the group email addresses should be **avanan_inline_policy@mycompany.com** and **avanan_monitor_policy@mycompany.com**, where mycompany is the name of your company.

Note - If you have activated Google Workspace without creating exclusion rules, contact *Avanan Support*.

Host

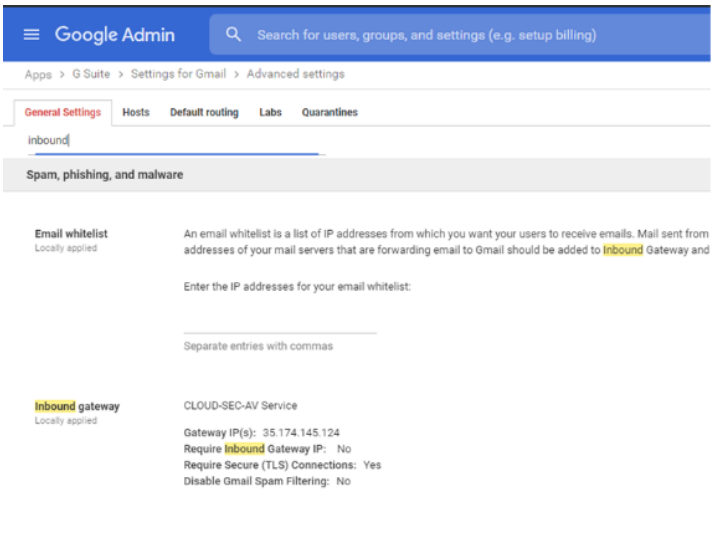
Avanan automatically creates a host (aka mail route) in your Google Admin console. You can see the host from the Google Admin Console under *Apps > G Suite > Settings* for *Gmail > Hosts*.

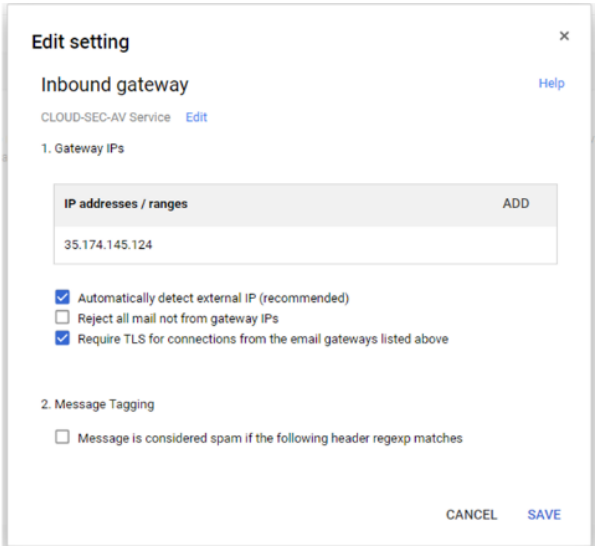
Note - By default, the **Required mail to be transmitted via a secure (TLS) connection (Recommended)** checkbox is selected. To disable it, contact *Avanan Support*.



Inbound Gateway

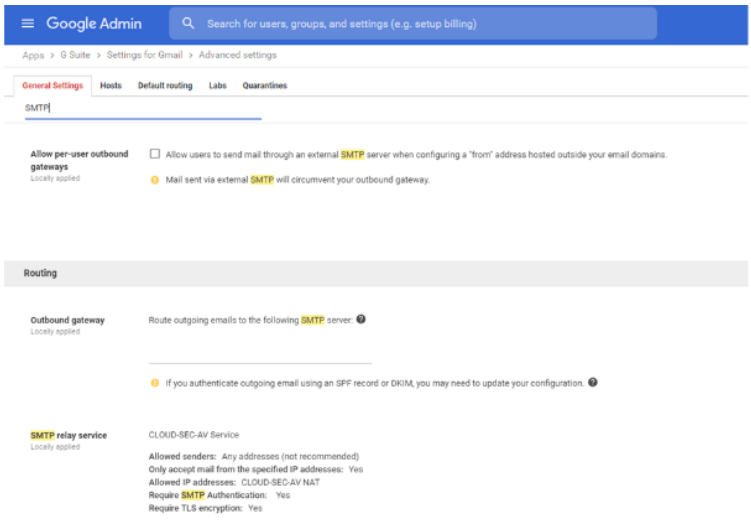
Avanan automatically creates an Inbound gateway. You can see the inbound gateway from the Google Admin console under *Apps > G Suite > Settings for Gmail > Advanced Settings*.

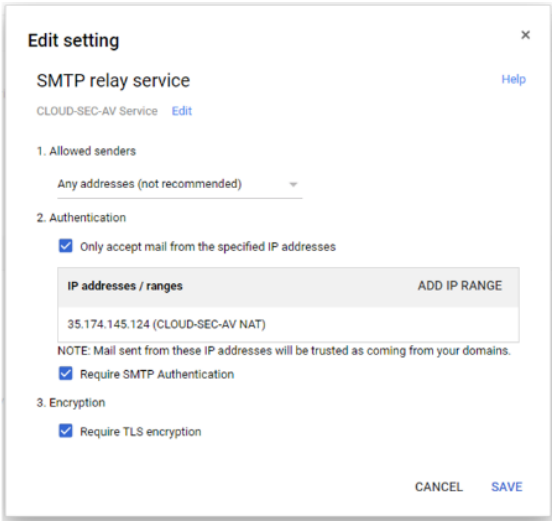




SMTP Relay Service

Avanan automatically creates an SMTP relay service. You can see the SMTP relay service from your Google Admin console under *Apps > G Suite > Settings for Gmail > Advanced Settings*.





Content Compliance Rules

Avanan automatically creates three Content Compliance Rules. You can review the content compliance rules from your Google Admin console under *Apps > G Suite > Settings for Gmail > Advanced Settings*. The rules are called:

- **[tenantname]_monitor_ei**
- **[tenantname]_monitor_ii**

- **[tenantname]_monitor_eo**
- **[tenantname]_inline_ei**

where ei stands for incoming traffic, ii stands for internal traffic, and eo stands for outgoing traffic.

Note - The **[tenantname]_inline_ei** rule gets created when the **Protect (Inline)** mode is enabled. If you remove the **Protect (Inline)** mode for users in Avanan, the Content Compliance Rule remains in the Google Admin console but the content of the user group **avanan_inline_rule** gets updated to reflect that no users are protected in this mode.

Google Drive Permissions Changes

Depending on the Google Drive policy configured by the administrator, Avanan takes action (quarantine, remove permissions) on the files uploaded to Google Drive.

Avanan uses different users to take these actions depending on whether the Drive containing the file has an owner.

- If Google Drive has an owner, Avanan takes the action on behalf of the owner.
- If Google Drive does not have an owner, Avanan follows this procedure:
  1. Avanan adds the *"Super Admin" on page 89* user as an owner of the Drive.
  2. Avanan uses the Super Admin user to take the necessary action on the file.
  3. Avanan removes the Super Admin user from being the owner of the Drive.

Activating Slack

Important

- Discovery API support is required to scan messages. The *Enterprise Grid* plan supports this.
- To activate Slack, the onboarding user must have administrator access to the relevant workspace.
- You must have the minimum supported SaaS license. See *"Minimum License Requirements to Activate SaaS Applications" on page 43*.
- The onboarding user must be part of the relevant workspace.

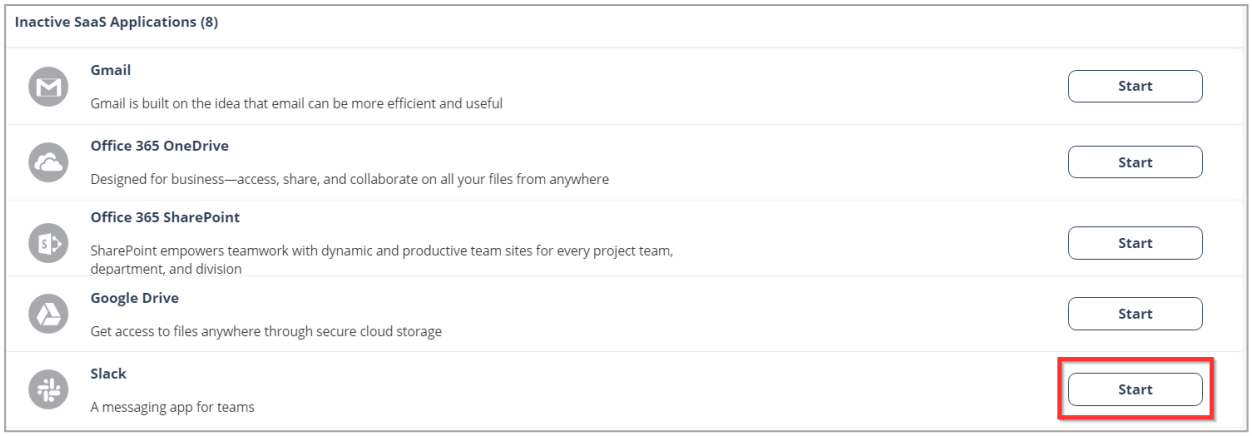
To activate Slack:

1. From the **Getting Started Wizard** click **Start** for Slack.

   Note - This wizard appears only when you are activating your first SaaS application in the Avanan Administrator Portal.

   or

   Navigate to **Security Settings > SaaS Applications** and click **Start** for Slack.

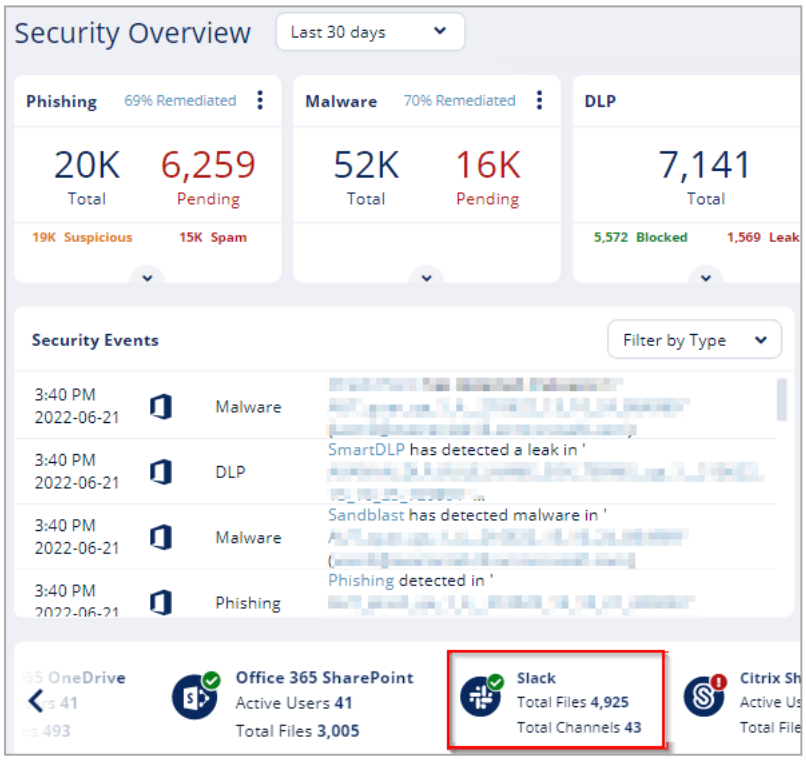


2. Click **Start** in the pop-up screen that appears.
3. In the **Slack Sign in** window that opens, sign in with your Slack administrator credentials.

   Note - Slack performs the authentication, and Avanan does not provide these credentials.

4. In the authorization screen from Slack, click **Accept** to grant necessary permissions to Avanan.

   The Slack SaaS is enabled, and monitoring begins immediately.



Onboarding Next Steps

Learning Mode

After activating Office 365 Mail or Gmail, Avanan performs several calibration processes for the Anti-Phishing engine.

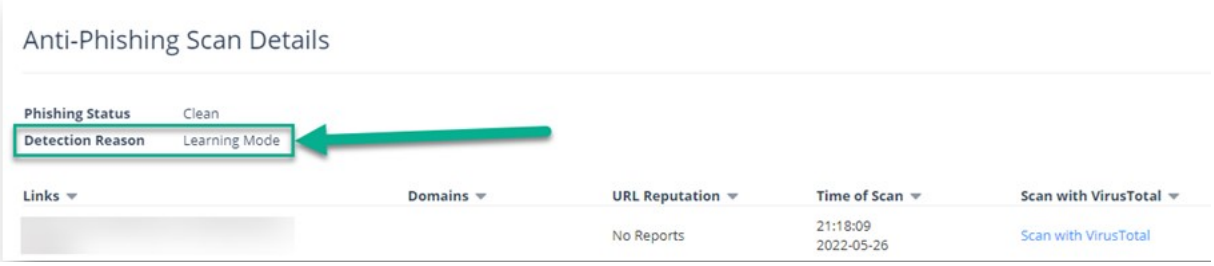
The processes include:

- Scanning 13 months of email metadata (sender, recipient, subject, time) in users' mailboxes to determine the communication patterns.
- Automatic identification of MTAs placed before Microsoft or Google. It could affect SPF checks and other aspects of detection.

While these processes are running, Avanan will be in **Learning Mode**. You can see a banner at the top of the dashboard. Also you can see the progress of the **Learning Mode** in **Overview** tab.

Note - To complete these processes, it takes a couple of minutes to 72 hours, depending on the number of protected mailboxes and the volume of their emails.

In **Learning Mode**, no email will be flagged as phishing or spam. All Anti-Phishing scans return **Phishing Status** as **Clean** and the **Detection Reason** as **Learning Mode**.



All other security engines work as usual in the **Learning Mode** and flag the malware, DLP, Shadow IT, and anomalies.

Avanan automatically exits **Learning Mode** after the calibration processes are complete.

Note - If a **Prevent (Inline)** policy rule is added, **Learning Mode** automatically stops.

While in **Learning Mode**, and at times for a while after it is completed, Anti-Phishing engine automatically adjusts these parameters to fine tune the detection accuracy:

- Upstream MTAs - In **Learning Mode**, Avanan automatically detects and adds MTAs to the list. It does not delete MTAs added manually by administrators. See *"Upstream Message Transfer Agents (MTAs)" on page 102*.
- *"Phishing Confidence Level (Threshold)" on page 97*

  Note - If administrators configured the phishing confidence level to a value different from the default value, Avanan does not change this value.

Live Scanning

After activating the SaaS application, Avanan starts scanning all the files and emails for any threats in real-time.

The **Overview** page shows the security events found, if any. At the bottom of the overview screen, you can see the status of active scans of your SaaS applications. Depending on the amount of data, this stage may take time.

Note - The number of active users may exceed the number of licensed users in the SaaS and does not necessarily reflect the number of Avanan licenses required.

Click **Active users** to review the list of users. This opens a query in the **Custom Queries** under **Analytics** tab.

For example, in Office 365, **Shared Mailboxes** do not require a separate license in Avanan but are counted as active users.

Note - By default, after activating a SaaS application, policy gets created for threats (phishing and malware). For DLP, there is no default policy.

Configuring Security Engines

Avanan uses these Security Engines:

- *"Anti-Phishing (Smart-Phish)" below*
- *"Anti-Malware (Check Point SandBlast)" on page 109*
- *"Data Loss Prevention (SmartDLP)" on page 110*
- *"Click-Time Protection" on page 120*
- *"URL Reputation" on page 134*

Anti-Phishing (Smart-Phish)

The Anti-Phishing (Smart-Phish) security engine detects phishing, suspected phishing, and spam emails. It analyzes various components of an email, such as attachments, links, sender reputation, domain analysis, OCR, URLs behind QR code, and many more.

The Anti-Phishing engine detects phishing in emails in all languages. Language-based detections are supported for languages, as mentioned in *"Appendix D: Supported Languages for Anti-Phishing" on page 618*.

Phishing Confidence Level (Threshold)

The Anti-Phishing algorithm returns a verdict on each email analyzed with confidence that may go from Lowest to Highest.

Any email categorized as phishing with a confidence level equal to or greater than the phishing confidence level (threshold) generates a **Phishing** event and triggers the relevant workflow.

Any email categorized as phishing with a confidence level below the defined phishing confidence level (threshold) generates a **Suspected Phishing** event and triggers the relevant workflow.

For example, if the phishing confidence level (threshold) is High and if the Anti-Phishing engine categorized an email as phishing with phishing confidence level (threshold) as Medium, it triggers the **Suspected Phishing** workflow.

By default, the phishing confidence level (threshold) is set to **High**.

To configure the phishing confidence level (threshold):

1. Access the Avanan Administrator Portal.
2. Go to **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.

4. Under **Phishing confidence level**, select the required threshold.
5. Click **Save**.

Nickname Impersonation

Protection Against Executive Spoofing

Executive spoofing is a scam in which cyber criminals impersonate the names and emails of company executives to try and fool an internal employee into disclosing sensitive information or executing a payment.

Anti-Phishing has a setting that allows Avanan Administrator Portal administrators to automatically block such spoofing attempts.

Configuring Nickname Impersonation

When Anti-Phishing security engine detects nickname impersonation, administrators can configure the Avanan Administrator Portal to trigger the **Phishing** or **Suspected Phishing** workflow.

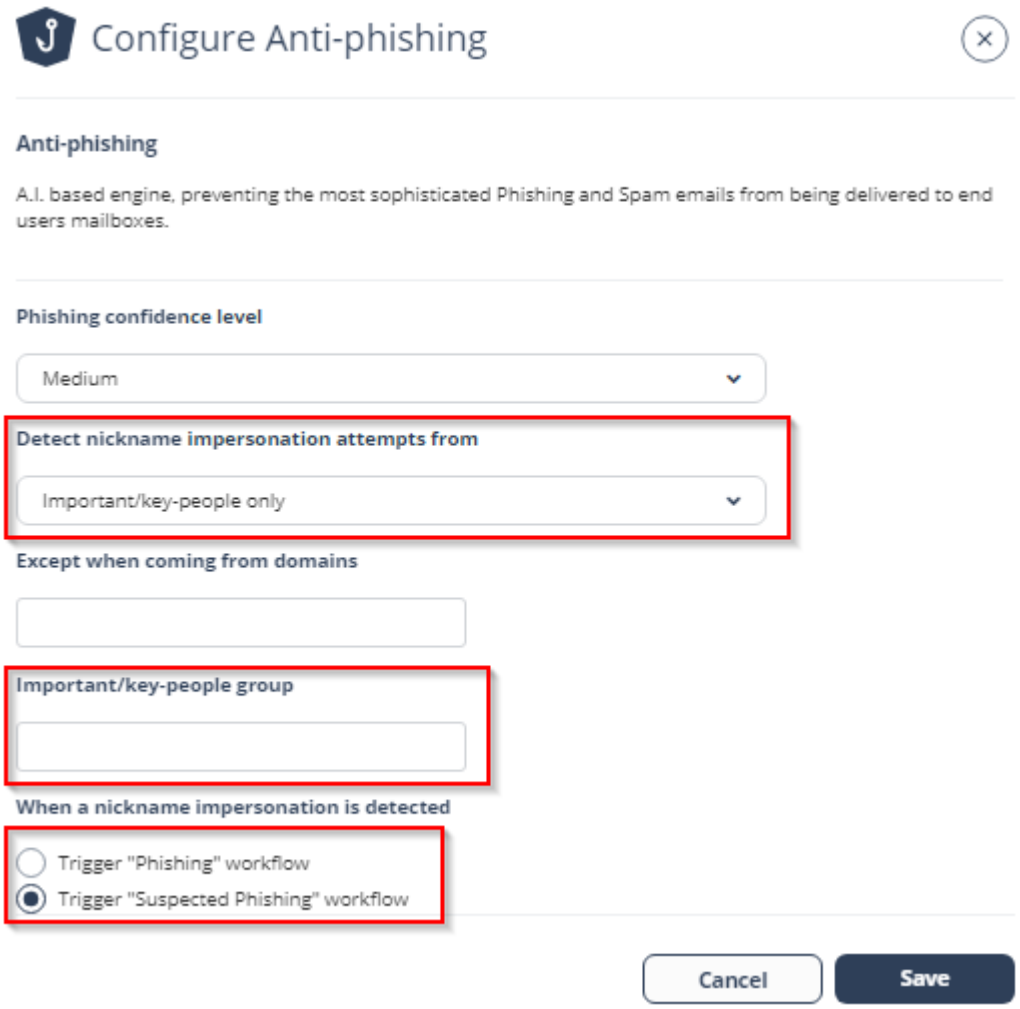
To configure nickname impersonation:

1. Navigate to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Smart-Phish**.
3. Select the scope of users:
   - Important/key people

     Note - By default, Anti-Phishing references the job title of the user to determine the seniority. Examples of senior titles are CEO, CFO, etc. Alternatively, you can define your own senior users by creating a security group (in Office 365 or Gmail) for senior-level users, and entering the exact name of the security group in the designated field. This field is case sensitive.

   - All internal users

4. Select the **Phishing** or **Suspected Phishing** workflow for detections.



Best Practices for Detecting Nickname Impersonation

- It is recommended to start protecting a small group of senior-level people first and then expand it to other people and/or use the **Suspected Phishing** workflow.
- If you wish to extend nickname impersonation workflows for all internal users, it is recommended to use the **Suspected Phishing** workflow to avoid false positive detections.
- Protected users must be informed to not use their personal email addresses, as these will be detected as impersonations.

Note - Anti-Phishing always looks for nickname impersonations for all users.

Handling False Positives

Many commonly used services like Salesforce or ServiceNow sends legitimate emails on behalf of other users. The Anti-Phishing engine detects these emails as nickname impersonations. Therefore, it's important to ensure that this configuration is not generating false positive phishing/suspected phishing detections.

To monitor detections, create *"Custom Queries" on page 379* that filters the detections containing nickname impersonations.

Note - Since Impersonation detection takes priority, sometimes an Allow-List rule will be overridden due to an SPF failure. If you need to ensure that an email is not overridden by an SPF failure or suspected impersonation, edit the Allow-List rule to *Ignore SPF check*.

Ensure to add legitimate services to **Allow-List** that appear in the query by navigating to **Security Settings > Exceptions > Anti-Phishing**.

For more details, contact *Avanan Support*.

Phishing Simulation Solutions

Many organizations use phishing simulation solutions to educate their employees on how to detect and report phishing attacks. These solutions send fake phishing emails to employees to try and trick them into performing actions, opening attachments or clicking on phishing URLs.

Avanan automatically detects such emails from commonly-used phishing simulation solutions and does not mark them as phishing. Phishing reports from users regarding these emails will be automatically declined.

Avanan detects phishing simulation solutions from the following:

Phishing Simulation Solutions
ActiveTrail
BenchMark
CybeReady
Hoxhunt
HubSpot
Infosec IQ
KnowBe4
MailChimp

Phishing Simulation Solutions
MailGun
MailJet
MimeCast
Phished
PhishMe
ProofPoint
SendGrid
SendInBlue
Sophos Phish Threat V2
TargetHero
TerraNova
ZoHo

If you use a different phishing simulation solution:

- To avoid detection of phishing simulation emails, add an Anti-Phishing Allow-List rule based on the solution's IP address.

  For information about adding an Allow-List, see *"Anti-Phishing Exceptions" on page 313*.

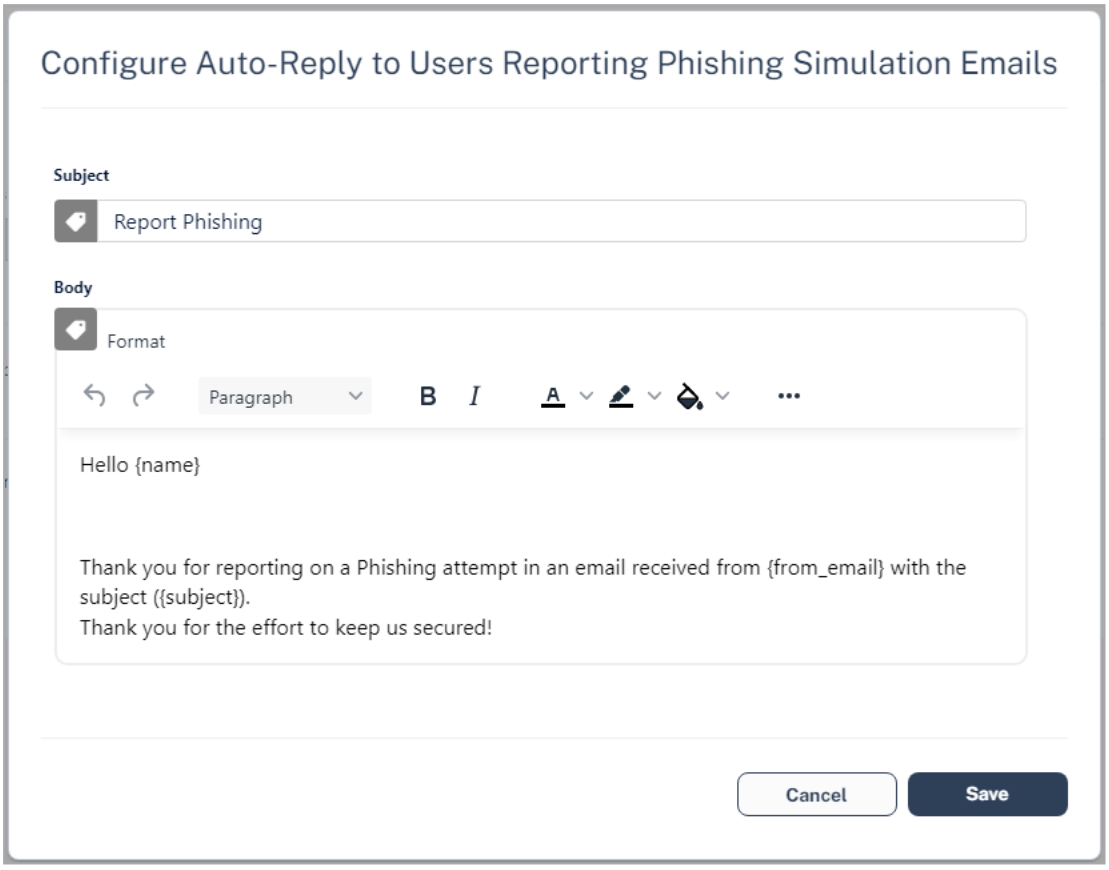
- To request for supporting the phishing simulation solution, contact *Avanan Support*.
- To automatically decline end-users' phishing reports regarding phishing simulation emails, contact *Avanan Support*.

To configure the Avanan Administrator Portal to automatically send feedback to users who reported phishing training emails as phishing:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **User Interaction** > **Phishing Reports**.
3. In the **Phishing simulation emails** section, select the **Notify user** checkbox.
4. (Optional) To change the default text in the feedback:

a. Click the ⚙ icon next to **Notify user** checkbox.

The **Configure Auto-Reply to Users Reporting Phishing Simulation Emails** pop-up appears.



b. Make the necessary changes and click **Save**.

5. Click **Save and Apply**.

Note - When a user reports a phishing simulation email, Avanan automatically declines the associated phishing report.

For Office 365, to see user reported phishing reports from phishing simulation solutions, see *"Automatic Ingestion of End User Reports" on page 362*.

Upstream Message Transfer Agents (MTAs)

During *"Learning Mode" on page 94*, to improve the accuracy of the Anti-Phishing engine, Avanan automatically detects MTAs that process emails before they reach Microsoft/Google.

If there are other MTAs that are not detected by Avanan, you can add them manually.

To add MTAs manually:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.

3. Click **Configure** for **Smart-Phish**.
4. Scroll-down to **SMTP host/s acting as Mail Transfer Agent/s (MTA)** and enter the full DNS names or IP addresses of MTAs separated by comma.
5. Click **Save**.

Blocking Emails that Fail DMARC

Some organizations configure their DMARC (Domain-based Message Authentication, Reporting and Conformance) record to quarantine or reject emails that fail DMARC checks. Most organizations choose to enforce this rejection for incoming emails with Microsoft/Google.

If you wish to enforce it with Avanan, you may configure to trigger the **Suspected Phishing** or **Phishing** workflow for emails that fail DMARC checks.

By default, **No extra action** is selected for DMARC failed emails in the Anti-Phishing security engine.

To configure the workflow for DMARC failed emails with Quarantine or Reject action:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings > Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll-down to **When emails fail DMARC with action reject/quarantine** section and select one of these.
   - **No extra action** - Enforces no extra action.
   - **Trigger 'Suspected Phishing' workflow** - Enforces the **Suspected Phishing** workflow configured in the threat detection policy. See *"Configuring a Threat Detection Policy Rule" on page 150* and *"Suspected Phishing Workflow" on page 164*.
   - **Trigger 'Phishing' workflow** - Enforces the **Phishing** workflow configured in the threat detection policy. See *"Configuring a Threat Detection Policy Rule" on page 150* and *"Phishing Workflow" on page 162*.
5. Click **Save**.

Warning - If incoming emails go through a secure email gateway (SEG) before reaching Microsoft/Google, then Microsoft/Google might flag these emails as DMARC violation because the email comes in from the SEG, whose IP might not be authorized in the SPF/DMARC records.
In such cases, selecting to trigger **Suspected Phishing** or **Phishing** workflow might result in a high number of false positives and might impact email delivery. Make sure the DMARC record is configured properly before selecting these workflows.

Impersonation of your Partners

Avanan lists all your partners in the *"Partner Risk Assessment (Compromised Partners)" on page 309* dashboard.

When a sender from a newly registered domain sends an email to your organization, the Anti-Phishing engine checks if the sender domain resembles your partner domain(s). By default, if such a domain similarity is detected, it is considered an indicator in the AI-based Anti-Phishing security engine. It might or might not yield a Phishing verdict.

Partner Impersonation Attacks - Workflow

Administrators can select to override the AI-based verdict of the Anti-Phishing security engine and trigger a specific workflow when such a similarity is detected.

To configure a specific workflow for emails from domains that resemble a partner domain:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll-down to **When the sender domain resembles the domain of a partner** section and select one of these workflows.
   - Consider as an indicator in the standard Anti-Phishing inspection (Default)
   - Trigger Suspected Phishing workflow
   - Trigger Phishing workflow
5. Click **Save**.

Handling Secured (Encrypted) Emails

Administrators can select how to manage incoming encrypted emails for end users, including Microsoft RPMSG and Microsoft 365 Message Encryption and so on.

To view the content of the encrypted emails, the end users must click the link provided in the email and authenticate.

To configure workflow for secured (encrypted) emails:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll down to the **Secured encrypted emails** section and select a workflow.

- Do not trigger any phishing workflow
- Trigger Suspected Phishing workflow for recurring first time senders
- Trigger Suspected Phishing workflow for first time senders
- Trigger Suspected Phishing workflow
- Trigger Phishing workflow for recurring first time senders
- Trigger Phishing workflow for first time senders
- Trigger Phishing workflow

Note - Recurring first-time senders are senders identified as sending multiple emails where they are considered first-time senders, across all the Avanan customers.

5. Click **Save**.

Preventing Email Bomb Attacks

An Email Bomb is a social engineering attack that overwhelms inboxes with unwanted emails. Usually, subscription confirmations to newsletters the users never signed up for.

Users targeted by these attacks lose access to their business emails, and the attackers may even use this as a distraction while performing malicious activities on the user's behalf.

To prevent such attacks, administrators must configure these in Avanan:

- Conditions for detecting and handling an ongoing Email Bomb attack.
- Workflow to be triggered when such an attack is detected.

Identifying an Email Bomb Attack

Avanan identifies an Email Bomb attack when the number of emails from new senders exceeds a defined threshold in a common attack timeframe.

Note - The attack timeframe is dynamic and changes depending on the Avanan security analyst's judgement. It is usually a couple of hours.

To configure the Email Bomb attack threshold:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll down to **Email Bomb – Threshold** and enter the threshold value.
5. Click **Save**.

Once the number of emails from new senders in the common attack timeframe exceeds the threshold, Avanan treats all subsequent emails from any new sender as part of the attack. This continues until the attack timeframe passes without the number of emails from new senders going over the threshold.

For example, if an administrator configured the Email Bomb threshold as 50, Avanan counts emails 51 and above as part of the attack.

Handling Emails of an Email Bomb Attack

By default, when Avanan detects an Email Bomb attack, it individually evaluates every email part of the attack for Spam and Phishing. Administrators can configure a dedicated workflow for these emails.

To configure the workflow for Email Bomb attack:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll down to **Email Bomb – Workflow** and select the required workflow.
    - Evaluate each email separately for spam/phishing
    - Trigger Spam workflow
    - Trigger Suspected Phishing workflow
    - Trigger Phishing workflow
5. Click **Save**.

Spam Protection Settings

Spam Confidence Level

Any email categorized as spam with a confidence level equal to or greater than the spam confidence level (threshold) generates a **Spam** event and triggers the relevant workflow.

To configure the spam confidence level (threshold):

1. Access the Avanan Administrator Portal.
2. Click **Security Settings** > **Security Engines**.
3. Click **Configure** for **Smart-Phish**.
4. Scroll down to the **Spam confidence level** section and select the required threshold.

- Lowest
- Low
- Medium
- High
- Highest

Note - Low confidence levels could result in a high number of false positives.

5. Click **Save**.

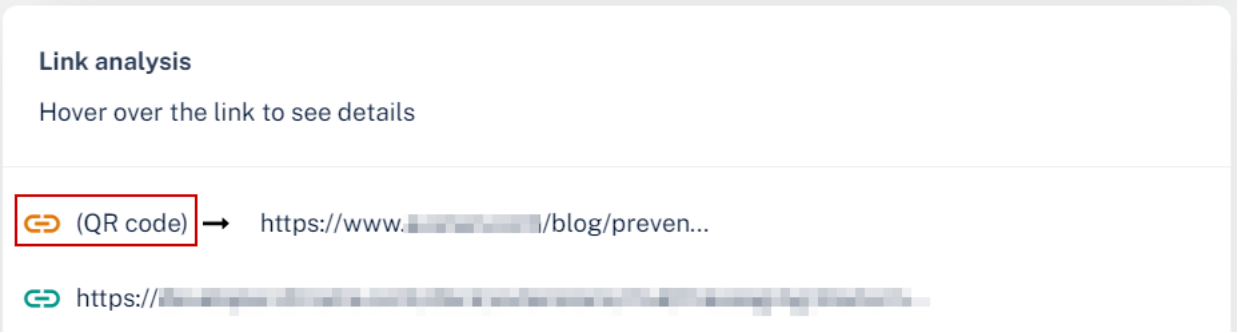
Trusted Senders - End-User Spam Allow-List

See *"Trusted Senders - End-User Allow-List" on page 327*.

Detecting Malicious QR Codes

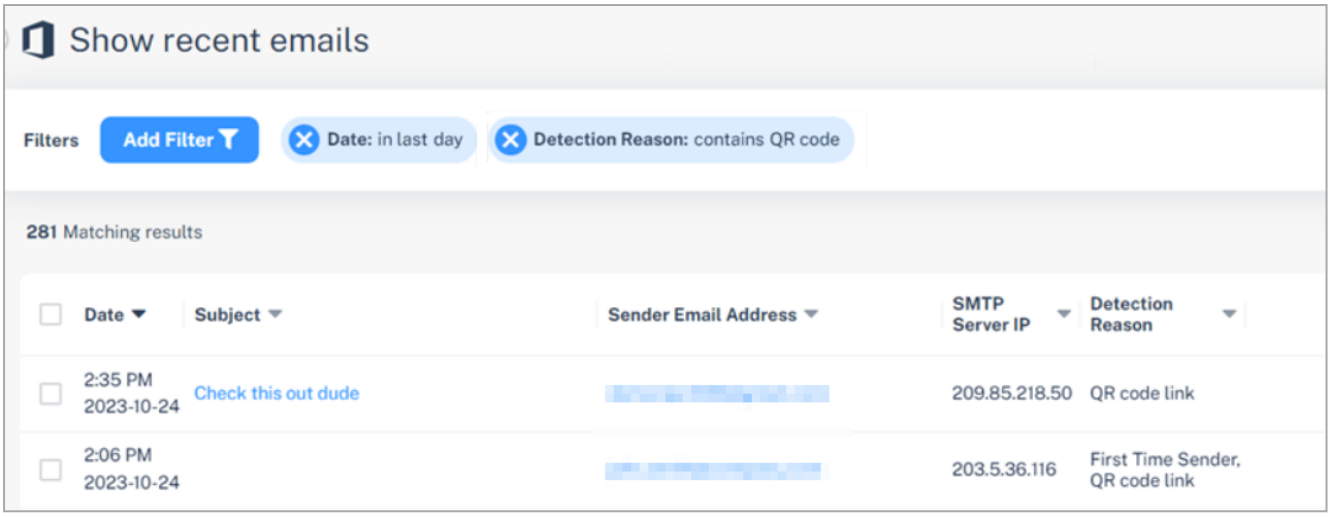
The Anti-Phishing security engine analyzes the links behind the QR codes and reports the malicious links, if any.

To view the links behind QR codes, open the **Email Profile** page and scroll down to the **Link analysis** section.



Filtering Emails Containing QR Codes

Using the **Detection reason** as QR in **Custom Queries**, the administrators can filter emails with malicious QR code. For more information, see *"Custom Queries" on page 379*.



Overriding Microsoft False Detections as Spam (Send to Junk)

Administrators can configure Avanan to manage the phishing emails that Microsoft / Google flags as spam and intend to send them to the user's Junk folder, while Avanan classifies the emails as clean. To do this:

1. Go to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Anti-phishing**.
3. Scroll down to the **Emails flagged as Spam by Microsoft / Google but Clean by Avanan** section and select one of these.
    - **Treat as Clean emails** - The system treats the phishing email that Microsoft detected as clean, applies the workflow, and delivers the email to the user's mailbox.
    - **Treat as Spam emails (leave SCL score as is)** - The system treats the phishing email that Microsoft detected as spam and sends it to the user's Junk folder. However, the email profile page in Avanan shows that Avanan classifies the email as clean.
4. Click **Save**.

Note - This workflow is applicable only to the emails inspected and enforced by a **Prevent (Inline)** policy.

Anti-Phishing Exceptions

See *"Anti-Phishing Exceptions" on page 313*.

Anti-Malware (Check Point SandBlast)

The Anti-Malware security engine determines if an email attachment or a shared file contains malware.

It uses Avanan's ThreatCloud to detect files containing known malware (Anti-Virus) and Avanan's advanced sandbox (Threat Emulation) to detect the evasive zero-day malware.

Engines Enabled

Under **Engines Enabled**, you can see the security engines available based on the license.

It could include **Anti-Virus** (known malware detection) or **Threat Emulation & Antivirus** (advanced sandbox).

To see the **Engines Enabled** for your tenant, go to **Security Settings**> **Security Engines** and click **Configure** for Anti-Malware.

Malware Emulation Operating Systems

Sandboxing attachments and shared files is crucial for detecting advanced zero-day unknown malware hidden in them.

During sandboxing, the Check Point Anti-Malware (Check Point SandBlast) (Threat Emulation) engine opens the file in a secured virtual machine and baits it to trigger its malicious behavior.

A dedicated team in Check Point constantly perfects the engine and the preferences of the virtual machines on which files are emulated. Specifically, this team selects the operating systems of those machines.

Administrators can choose not to follow the Check Point best practices and to select the operating systems on their own. To do that, contact *Avanan Support*.

Note - Changing the default operating systems for emulation is not recommended and can damage the malware detection rate.

Anti-Malware Inspection - File Size Limit

The Anti-Malware security engine inspects files attached to an email or shared via supported file sharing/messaging applications for malware only if it is less than 50 MB.

Anti-Malware Exceptions

See *"Anti-Malware Exceptions" on page 317*.

Data Loss Prevention (SmartDLP)

Overview

Avanan's Data Loss Prevention (SmartDLP) engine safeguards the organization's data from breaches or unauthorized sharing. It scans emails, attachments, shared files, and text messages, even extracting text from images using OCR. The DLP engine identifies patterns that should not be shared with unauthorized people or destinations.

The DLP engine enables you to create universal policies across multiple cloud applications to control how files are shared amongst internal and external users. DLP identifies and marks files containing confidential, financial, and personally identifiable information, including credit card numbers, social security numbers, bank routing numbers, or data protected under HIPAA, etc.

Notes:

- The DLP engine scans and detects sensitive information in both the email subject and body content.
- DLP is not available for Avanan accounts residing in the United Arab Emirates (UAE) region. If required, you can request to enable DLP. However, sensitive data analysis will be performed in the United Kingdom (UK) and not within the borders of the UAE. If you wish to enable DLP, contact *Avanan Support*.

DLP Policies

This chapter discusses defining the DLP categories, Data Types and other DLP security engine settings.

To enforce your organization’s DLP standards, you need to define DLP policies for different protected SaaS applications.

To configure DLP policy, see the relevant SaaS application:

- Email *"Data Loss Prevention (DLP) Policy" on page 188*
- File Storage SaaS applications
  - *"Configuring DLP Policy for OneDrive" on page 283*
  - *"Configuring DLP Policy for SharePoint" on page 290*
  - *"Configuring DLP Policy for Google Drive" on page 297*
- Messaging SaaS applications
  - *"Configuring DLP Policy for Microsoft Teams" on page 264*
  - *"Configuring DLP Policy for Slack" on page 273*

DLP Categories

DLP categories are containers of multiple data types used in different DLP policies to describe data sharing that can be considered as a DLP violation and should trigger a DLP workflow.

For example, the PII DLP category includes the **Passport Number** DLP Data Type.

Managing DLP Categories

You can configure all the available DLP categories and manage them under **Security Settings > Security Engines > DLP**.

Editing DLP Categories

To edit the list of DLP Data Types each category contains:

1. Access the Avanan Administrator Portal.
2. Click **Security Settings > Security Engines**.
3. Click **Configure** for SmartDLP.
4. Scroll down to **Detection Types** and find the relevant DLP category.
5. Add or remove data types from the category.

   Note - To exclude Universal Air Travel Plan (UATP) card numbers from detecting as credit card numbers, under PCI detection type, enable the **Exclude UATP cards from the Credit Card data types** checkbox.
6. Click **Save**.

For more information about the default DLP Data Types and their DLP categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.

DLP Data Types

DLP Data Types describe the content the DLP engine tries to detect. Every time the engine detects a data type, it adds 1 to the hit count of every DLP category containing this data type.

Managing DLP Data Types

To view and manage the available Data Types, go to **Security Settings > DLP Data Types**.

Custom DLP Data Types

Avanan allows you to create custom DLP Data Types. These Data Types provide organizations the flexibility to add any DLP data type to each of the DLP categories.

Note - You must add the custom DLP Data Type to a DLP category before it is enforced. To add the custom DLP Data Type to a DLP category, see *"DLP Categories" above*.

Creating Custom DLP Data Types

Regular Expression DLP Data Types

Data Types based on regular expressions are data types that will add a hit count to their parent category every time a string in the inspected email/file/message is matched against the defined Regular Expression.

To create a regular expression Data Type:

1. Click **Security Settings > DLP Data Types**.
2. Click **Create Data Type**.

   Create Custom DLP Data Type section appears.
3. Enter the required **Name** and **Description** for the Data Type.
4. Under **Match type**, select **Regular Expression** and enter the required regular expressions.

   Note - Avanan supports Regular Expression 2 syntax. For more information about the syntax, see this article.
5. Click **Save**.

Dictionary DLP Data Types

A dictionary is a list of custom strings. These Data Types add a hit count to their parent category every time a string in the inspected email/file/message matches one of the strings in the dictionary.

To create a Dictionary DLP Data Type:

1. Click **Security Settings > DLP Data Types**.
2. Click **Create Data Type**.

   Create Custom DLP Data Type section appears.
3. Enter the required **Name** and **Description** for the Data Type.
4. Under **Match type**, select **Dictionary** and add the required keywords:
   - To add a keyword to the dictionary, enter the required keyword and click **Add Keyword**.

- To import keywords to the dictionary from a CSV file:
  a. Click **Import dictionary**.
  b. Under **Upload Dictionary File**, select the required CSV file.
  c. To override the existing keywords, enable the **Override all existing words** checkbox.

  Note - To export the keywords in the dictionary to a CSV file, click **Export dictionary**.

5. Click **Save**.

Compound DLP Data Types

Compound DLP Data Types are parent DLP Data Types that contain other child DLP Data Types, divided into two groups:

- **Triggers** – DLP Data Types that **must match** otherwise, the parent DLP Data Type will not match
- **Children** – DLP Data Types that **could match** and add to the parent DLP Data Type hit count.

In addition, each Compound DLP Data Type has a **Minimum Match Type Count** of its own so that the number of matches across all contained data types must be above it for the parent DLP Data Type to match.

For example, you can create a compound DLP Data Type named **MyCompany Internal Documents** the following way:

1. Triggers
   a. A string “MyCompany”
   b. A string “Confidential”
2. Children
   a. Source Code
   b. Bank Swift routing numbers
3. Minimum Match Type Count = 4

Example scenarios:

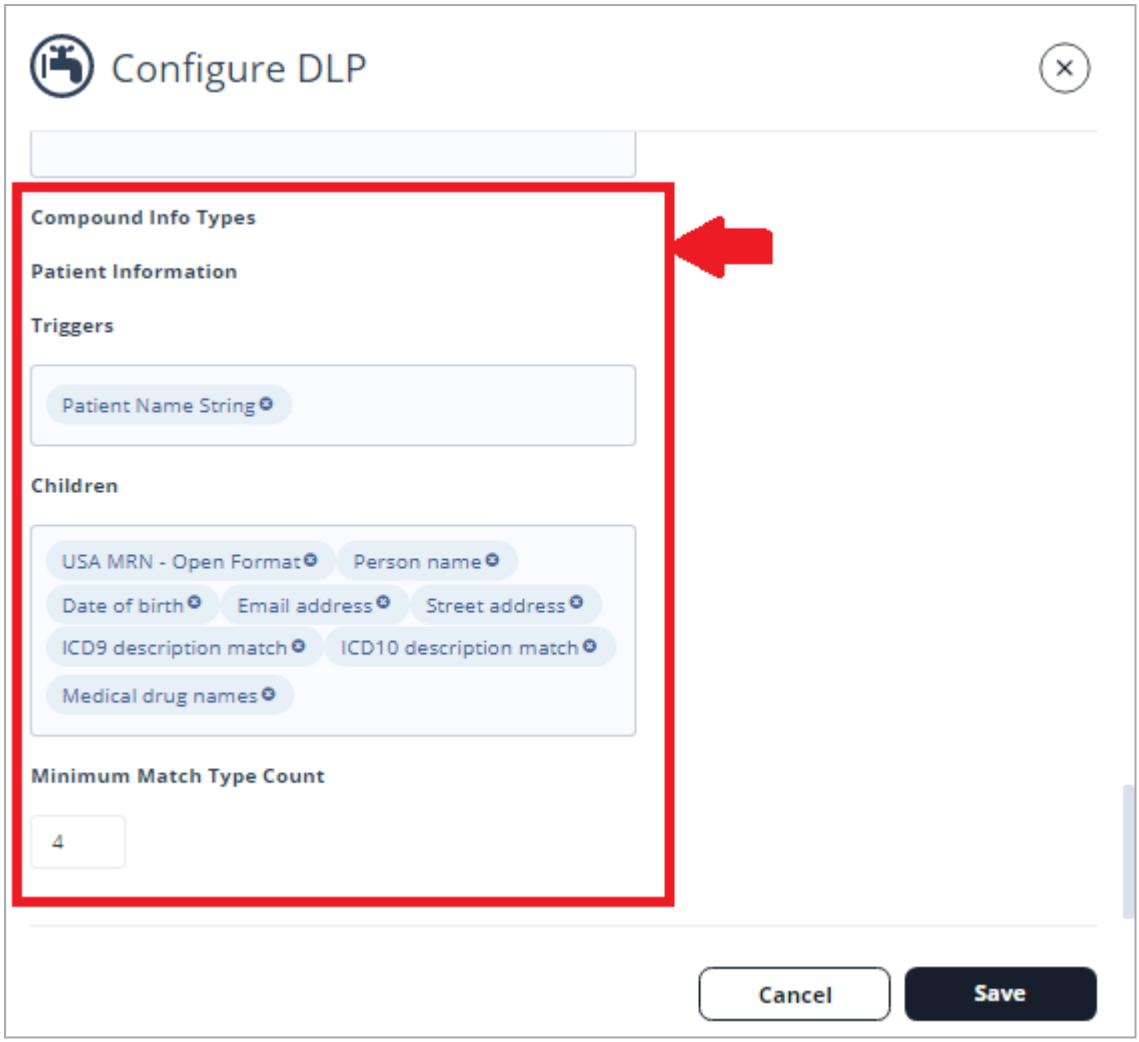
Scenario	Findings				Match?	Reason
	“My Company”	"Confidential"	Source Code	Bank SWIFT Routing Numbers		
Only Triggers	2	3	0	0	Yes	All triggers plus match count above the threshold
Some Triggers	3	0	2	2	No	One of the triggers not matched
Not enough matches	1	1	1	0	No	Match count below the threshold
Triggers and Children	1	1	2	2	Yes	All triggers plus match count above the threshold

Creating a Compound DLP Data Type

Avanan allows you to define a custom Compound DLP Data Type.

To create a compound DLP Data Type:

1. Click **Security Settings > Security Engines**.
2. Click **Configure** for SmartDLP.
3. Scroll down and find **Patient Information** below **Compound Info Types**.



4. Edit the **Triggers**, **Children**, and **Minimum Match Type Count**.
5. Add Patient Information to one of the DLP Categories so that it can be used in the DLP policy rules. For more details, see *"DLP Categories" on page 111*.
6. Click **Save**.

Other Custom Data Types

If you need a different custom data type, open a support ticket or contact *Avanan Support*.

Edit, Clone, or Delete Custom DLP Data Types

To edit a custom DLP Data Type:

1. Click **Security Settings > DLP Data Types**.
2. Select a custom DLP Data Type.
3. Click on the vertical ellipses icon (in the top right corner of the selected custom DLP Data Type), and then select **Edit**.
4. Make the required changes to the DLP Data Type and click **Save**.

To clone a custom DLP Data Type:

1. Click **Security Settings > DLP Data Types**.
2. Select a custom DLP Data Type.
3. Click on the vertical ellipses icon (in the top right corner of the selected custom DLP Data Type), and then select **Clone**.
4. Make the required changes to the DLP Data Type and click **Save**.

To delete a custom DLP Data Type:

1. Click **Security Settings > DLP Data Types**.
2. Select a custom DLP Data Type.
3. Click on the vertical ellipses icon (in the top right corner of the selected custom DLP Data Type), and then select **Delete**.
4. Click **OK**.

Configuring Advanced Data Type Parameters

To refine the definitions of a DLP category or to handle cases of false-positive detections, you can control how to match a DLP Data Type in an email/file/message.

Match Hit Count Settings

By default, a DLP Data Type's hit count increases every time a string in the email/file/message matches with the DLP Data Type's definitions. If the same matched string appears multiple times in the email/file/message, the hit count increases accordingly.

To configure Avanan to ignore duplications of the same string when calculating the hit count, enable the **Unique detections only** box in the **Configure DLP** window.

Occurrence Threshold

By default, if a DLP Data Type is matched X times, the hit count of the DLP Category containing this DLP Data Type increases by X.

Setting the occurrence threshold for the DLP Data Type to Y means that:

- If the DLP Data Type matches < Y times, the hit count of the containing DLP Category will not be increased at all.
- If the DLP Data Type matches >= Y times, the hit count of the containing DLP Category will be increased by the total number of matches.

To configure **Occurrence Threshold**, open a support ticket or contact *Avanan Support*.

Likelihood Adjustment

By default, the DLP engine returns a specific likelihood level (*"Minimal Likelihood" on page 119*) to a DLP Category.

If you want to determine if one of the DLP Data Types is matched, the likelihood will automatically increase or decrease. You can configure the **Likelihood Adjustment** value for every DLP Data Type with positive or negative values accordingly.

To configure **Likelihood Adjustment**, open a support ticket or contact *Avanan Support*.

Hot/Cold Words

Every DLP Data Type is searched across the entire email/file/message by default.

You can define the scope of the search so that it happens in the vicinity of certain words and/or not in the vicinity of others.

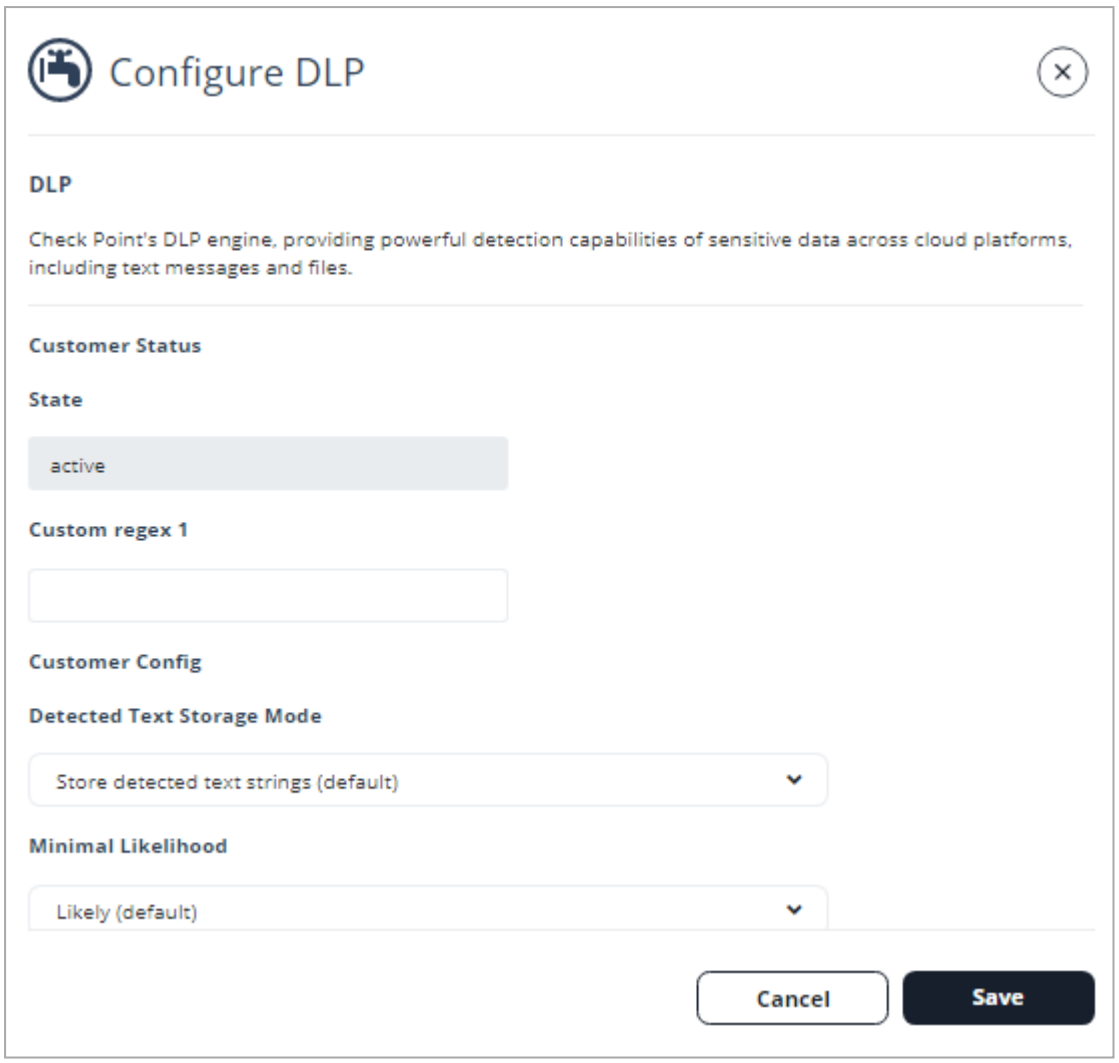
To configure **Hot/Cold Words**, open a support ticket or contact *Avanan Support*.

Configuring DLP Engine Settings

To configure DLP engine settings:

1. Click **Security Settings > Security Engines**.
2. Click **Configure** for SmartDLP.

3. Configure the different configuration options and click **Save**.



Storage of Detected Strings

When the DLP engine matches strings to a DLP Data Type, Avanan stores these strings and displays them for administrators with sufficient permissions when they investigate the security events.

Since these strings are considered sensitive and private end-user data, you can select how they are stored and presented in the system called **Detected Text Storage Mode**.

To update Detected Text Storage Mode:

1. Click **Security Settings > Security Engines**.
2. Click **Configure** for SmartDLP.
3. Scroll down to **Detected Text Storage Mode** and select one of these options.

- **Store detected text strings (default)**: This is the default option, and the detected data is saved and displayed on the security events for the forensic process.
- **Obfuscate detected text prior to storage**: Detected data is saved and displayed on the security events obfuscated. The original data is discarded and cannot be accessed.
- **Do not store detected text**: No detected data is stored or displayed on the security events.

4. Click **Save**.

Minimal Likelihood

Whenever the DLP engine detects a possible data leak, it assigns the detection a **Likelihood** level. **Likelihood** levels are mostly affected by context around the detected strings.

For example, when a Social Security Number (SSN) is discovered, the DLP engine also checks for the presence of relevant strings close to the discovered pattern, i.e., "SSN" or "Social Security."

Likelihood scale:

- Very Unlikely
- Unlikely
- Possible
- Likely
- Very Likely

DLP Exceptions

See *"DLP Exceptions" on page 322*.

DLP - Supported File Types

Avanan detects DLP violations in a large list of file types, including EML, HTML, PDF, Microsoft Office files, images, and many more.

For more information, see *"Appendix H: Supported File Types for DLP" on page 632*.

DLP Inspection - File Size Limit

The DLP security engine inspects the email, its attachments and files that are less than 50 MB only.

Note - At times, the DLP security engine might inspect the archived files larger than 50 MB.

Forensics

DLP detections are recorded as events for forensic and auditing purposes. The events include what type of sensitive information was potentially leaked (PII, HIPAA, etc.).

You can see events from **Events**.

Date & Time	State	Severity	SaaS	Type	Description	Actions Taken
1:50 PM 2022-02-09	Remediated			DLP	DLP has detected PCI, PII leak in ' [redacted] ([redacted] 's mailbox)	Email quarantined
10:55 PM 2022-02-03	Remediated			DLP	DLP has detected PCI, PII leak in ' [redacted] ([redacted] 's mailbox)	Email quarantined
10:50 PM 2022-02-03	Detected			DLP	DLP has detected PCI, PII leak in ' Personal Information' ([redacted] 's mailbox)	
9:09 PM 2022-02-02	Remediated			DLP	DLP has detected PCI, PII leak in ' [redacted] ([redacted] 's mailbox)	Email quarantined
11:09 PM 2021-11-29	Detected			DLP	DLP has detected PII, PCI leak in ' [redacted] ([redacted] 's mailbox)	

Click-Time Protection

Check Point's virtual inline technology provides phishing protection for emails after they have been scanned by Microsoft servers, but before they reach the user's mailbox.

New attacks became more sophisticated and are able to generate phishing campaigns such that the phishing website they link to does not have any known bad reputation, sometimes for hours and days after the emails are sent.

Click-Time Protection replaces links in the email's body and attachments. The replaced links point to the Check Point inspection services, so that every time a user clicks on a link, the website behind the link is inspected to ensure it is not a phishing website.

Click-Time Protection uses these security engines for inspection.

- **URL Reputation** - Checks if the URL is known to be malicious or holds any malicious references.
- **URL Emulation** - Emulates the website to detect zero-day phishing websites.

Benefits

- **Most Up-to-Date Intelligence** - Inspecting links when the user clicks on the URL allows Check Point to inspect the URL based on the latest inspection intelligence and software capabilities.
- **Protection against zero-day phishing websites** - Inspecting links when the user clicks on the URL allows Check Point to follow the user into the website. Click-Time Protection then emulates the website to expose hidden Phishing indicators. So the Phishing websites that are not known to be malicious are also flagged.

- **Pointing out the users that clicked the malicious URL** - Click-Time Protection forensics allows administrators to detect the users that require further education and training to avoid clicking on malicious links.

Note - Click-Time Protection is available only for Office 365 Mail and Gmail.

Interaction with Microsoft ATP

Avanan supports link rewriting even when Microsoft Safe Links is enabled.

When both Avanan Click-Time Protection and Microsoft Safe Links are active, the Avanan rewritten link is embedded within the Microsoft rewritten link.

The format of the rewritten link is as follows:

<Safe Links rewritten URL prefix> <Avanan rewritten URL prefix> <Original URL> <Avanan rewritten URL suffix> <Microsoft Safe Links suffix>.

This integration provides the protection of both Avanan and Microsoft without you requiring to disable either one:

- Both Avanan and Microsoft inspects the original link upon email receipt.
- When a user clicks the URL, both Avanan and Microsoft inspects the website or file linked and can block access if it is identified as malicious.

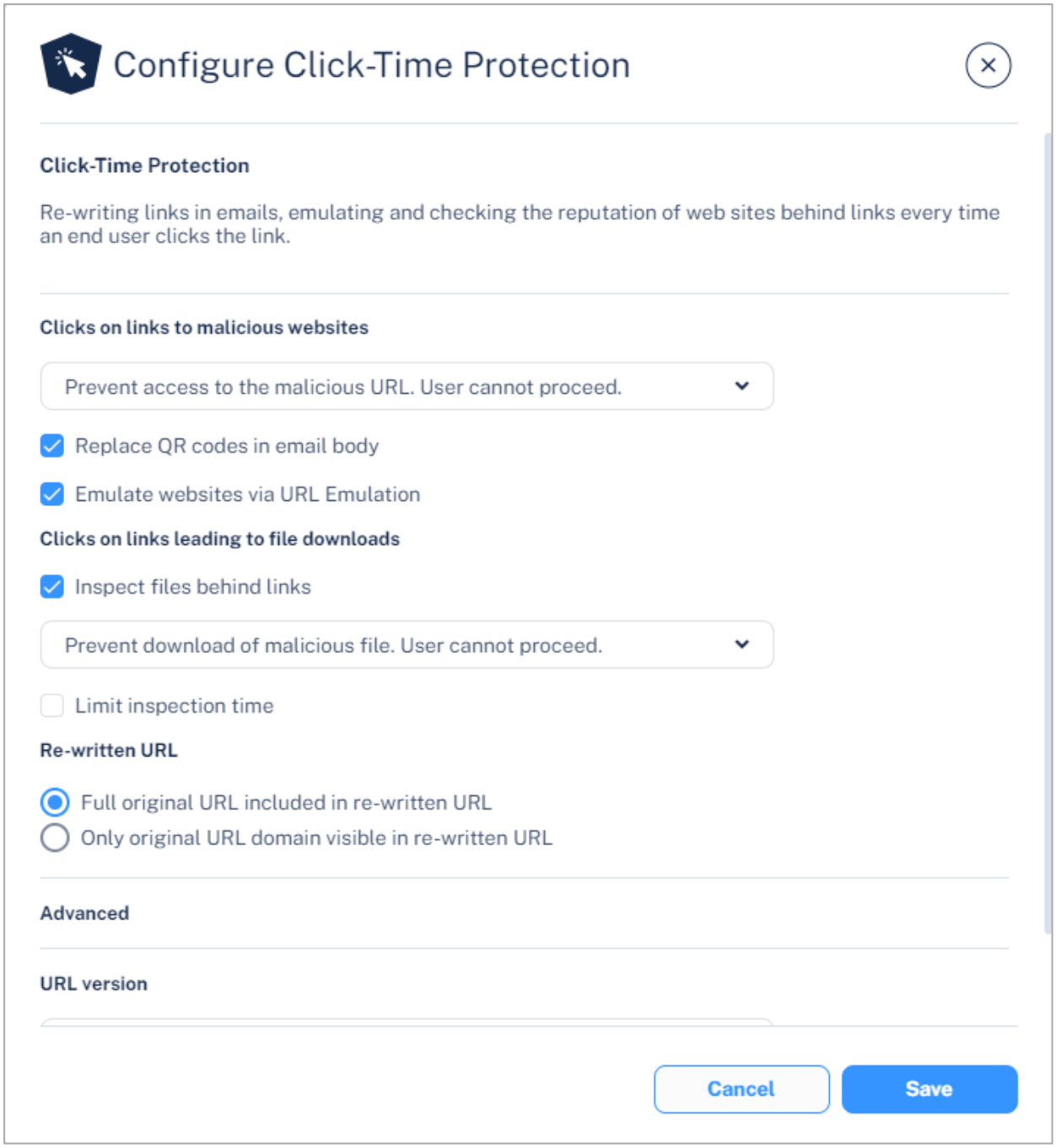
When clicking on re-written links, the end user experiences the following:

Microsoft Verdict	Avanan Verdict	User Experience
Clean	Clean	Redirect to the original URL.
Malicious	Malicious or Clean	Microsoft block page.
Clean	Malicious	Avanan block page. See *"Click-Time Protection - End-User Experience" on page 127*.

Configuring Click-Time Protection Engine

To configure Click-Time Protection engine:

1. Navigate to **Security Settings > Security Engines**.
2. Click **Configure** for **Click-Time Protection**.



3. In the **Click on links to malicious websites** section, select the required option to handle the malicious websites.
    - Prevent access to the malicious URL. User has option to proceed.
    - Prevent access to the malicious URL. User cannot proceed.
    - Do nothing
4. To replace the QR code in the body of the email to redirect to the rewritten link, select the **Replace QR codes in email body** checkbox.

Note - For the rewritten QR codes, the structure will be the same as V2 version even if you select to use V1 version. For more information, see *"Rewritten Avanan URL" on the next page*.

5. To emulate websites behind links to detect phishing websites with no bad reputation, select the **Emulate websites via URL Emulation** checkbox.

   Note - If the **Emulate websites via URL Emulation** was disabled, and if the administrator enables it, it could take up to 20 minutes for the URL Emulation to start working.

6. To inspect files behind links, do these in the **Clicks on links leading to file downloads** section:

   a. Select the **Inspect files behind links** checkbox.

   b. Select a workflow:

      - Prevent download of malicious file. User has option to proceed and download.
      - Prevent download of malicious file. User cannot proceed.
      - Do nothing

   c. To allow the download of files if the file inspection exceeds a specific time, do these:

      i. Select the **Limit inspection time** checkbox.

      ii. In the **Allow download if inspection takes more than (seconds)** field, enter the time in seconds.

   For more information, see *"Protection Against Malicious Files Behind Links" on page 127*.

7. Under **Advanced**, select the required URL version (**V1** or **V2**).

   For more information about URL version, see *"Rewritten Avanan URL" on the next page*.

   Note - Avanan recommends using **V2** version.

8. Click **Save**.

   Notes:
   - To start rewriting the links, you must configure a Click-Time Protection policy. To configure Click-Time Protection policy, see *"Click-Time Protection Policy" on page 223*.
   - To create Allow-List or Block-List for Click-Time Protection, see *"Click-Time Protection Exceptions" on page 324*.

Rewritten Avanan URL

The format of the rewritten Avanan URL is *<click-time domain>_<original url>_<encrypted blob>*. While configuring the **Click-Time Protection** engine, administrators can choose the *<click-time domain>* from these versions:

- V1: https://avanan.url-protection.com/v1/
- V2: https://url.avanan.click/v2/

In the *<click-time domain>* V2 version, the original URL is surrounded by underscores, making it easier to identify the original (rewritten) URL. Also, the URL is shorter and the domain is different from V1 version.

Notes:

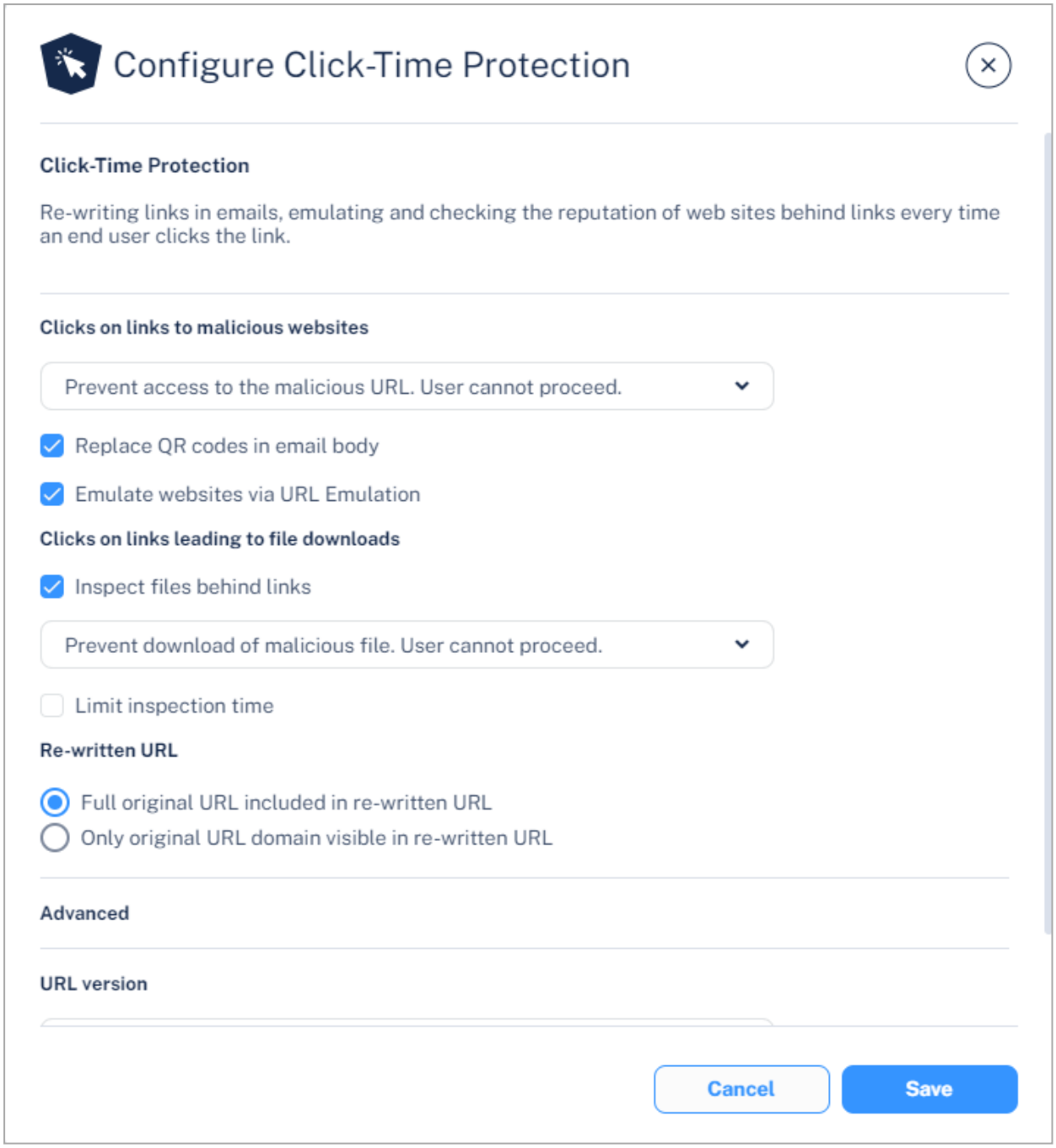
- Avanan recommends using V2 version.
- For rewritten QR codes, the structure will be the same as V2 version even if you select to use V1 version.
- If a **Click-Time Protection** policy is configured and the **Protect (Inline) Internal Traffic** option is enabled in the **Threat Detection** policy, the system rewrites links in emails sent to members of the same organization. See *"Threat Detection Policy for Internal Emails" on page 154*

Hiding Original URL Full Path

By default, the rewritten URL includes the full path of the original URL, improving readability and predictability for end users. However, if administrators do not want to show the full path, they can configure the Click-Time Protection security engine to rewrite the URL to include only the domain of the original link, obfuscating the remaining path.

To obfuscate the full path of the original URL:

1. Navigate to **Security Settings > Security Engines**.
2. Click **Configure** for **Click-Time Protection**.



3. In the **Re-written URL** field, select one of these:
   - **Full original URL included in re-written URL**
   - **Only original URL domain visible in re-written URL**

Note - Obfuscating the original URL is only supported when the version of the re-written link is v2.

Re-written URL Containing an Obfuscated Original URL

For example, if the original link is `https://www.acme.org/lorem/ipsum/dolor.aspx`, the re-written link:

- **Without obfuscation** - `https://url.avanan.click/v2/___ https://www.acme.org/lorem/ipsum/dolor.aspx{}.YXAzOnByb2...{_}`
- **With obfuscation** - `https://url.avanan.click/v2/___ https://www.acme.org/Nsyjwsfqrjidljsjyn.fxuC___.YXAzOnByb2...`

Note -The obfuscation may increase the length of the rewritten link by approximately 2-3 characters compared to the link without obfuscation.

Validity of Rewritten URL

- Avanan inspects the website behind the rewritten URL only when you have a valid license.
- Rewritten URLs remain valid indefinitely, even when you do not have a valid license or when you delete the Avanan portal.
- After the license expires, Avanan redirects the rewritten URL to the original URL without inspection.
- Avanan handles the rewritten URLs as described above regardless of the identity of the user that clicks the URL - internal user, external user, or unidentified user.

  Therefore, even if the email is forwarded to a user in your organization that is not protected by Check Point, this user's click is also secured by Check Point.

Replacing Links Inside Attachments - Supported File Types

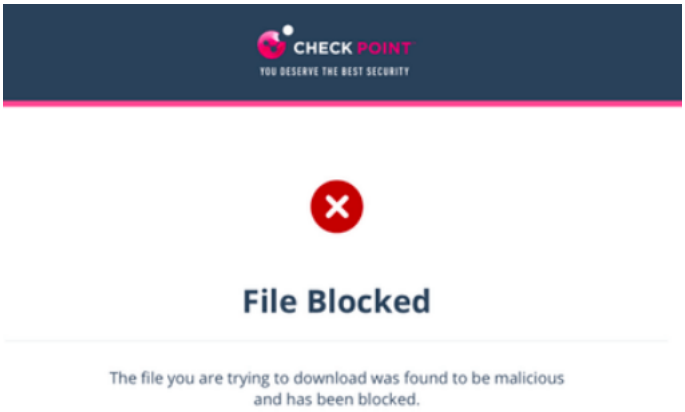
If you configured the *"Click-Time Protection Policy" on page 223* to replace links inside the attachments, the links get replaced for these file types:

File Type	File Extensions
Adobe FDF	FDF
Adobe PDF (all versions)	PDF
Microsoft Excel 2007 and later	XLSX, XLSB, XLSM, XLTX, XLTM, XLAM
Microsoft Excel 2007 Binary	XLSB
Microsoft Excel 97 - 2003	XLS
Microsoft PowerPoint 2007 and later	PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM
Microsoft PowerPoint 97 - 2003	PPT, PPS, POT, PPA
Microsoft Word 2007 and later	DOCX, DOCM, DOTX, DOTM
Microsoft Word 97 - 2003	DOC, DOT

Protection Against Malicious Files Behind Links

The Anti-Malware security engine emulates the files behind direct download links before delivering them to end users. To prevent attacks in which the file behind the link is altered after the email is sent, this inspection will also take place when users click on such links after they are re-written by Click-Time Protection.

If the file behind the link is found to be malicious, and the Click-Time Protection security engine is configured to block it, access to the file will be blocked.



To configure the workflow in the Click-Time Protection security engine, see *"Configuring Click-Time Protection Engine" on page 121*.

Click-Time Protection - End-User Experience

After *"Configuring Click-Time Protection Engine" on page 121* and *"Click-Time Protection Policy" on page 223*, Avanan replaces all URLs in the incoming emails and their attachments with a Avanan URL.

The URL also provides a tool-tip with the original URL, indicating that the link is protected by Avanan.

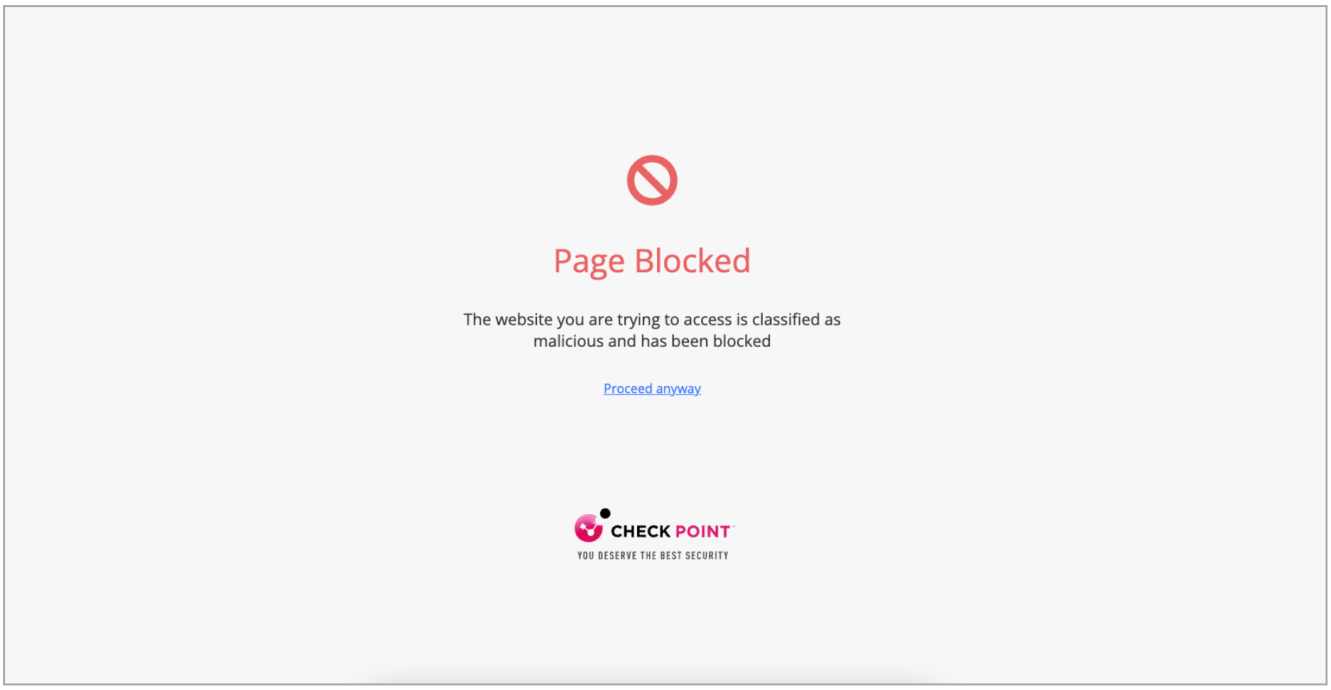
Note - Formatted tool tips are available on Microsoft Outlook for Mac, Outlook Web Access, and many other clients. Some clients, such as Outlook for Windows, limit the ability to present tool tips and will present the raw rewritten URL.

Clicks on Malicious Websites - User Experience

When a user click on the URL of a website, Avanan checks the target URL.

- If the URL is not found to be malicious, the user will be redirected to the original URL.
- If the URL is found to be malicious, the user will be forwarded to a warning page.

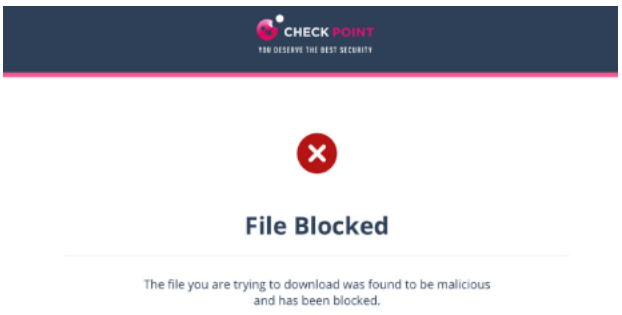
- If the workflow for malicious URLs is to **Prevent access to the malicious URL. User has option to proceed** in the Click-Time Protection security engine, an additional **Proceed anyway** link will be available in the warning page.



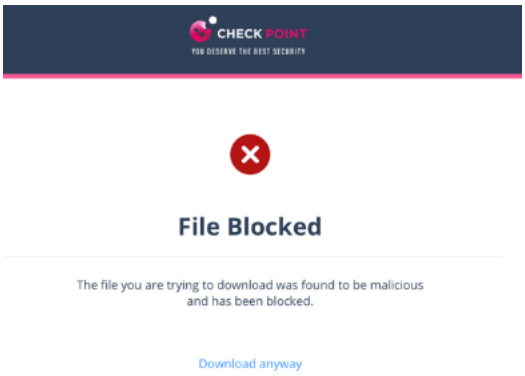
Clicks on Direct Download Links - User Experience

When a user clicks a direct download link, the Anti-Malware security engine emulates the file.

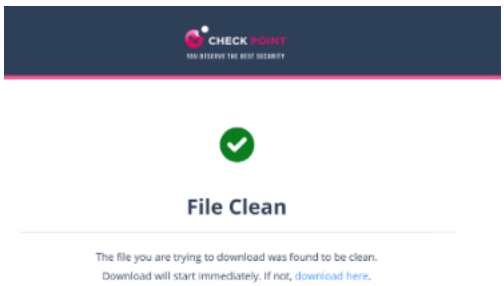
- If the file is detected as malicious:
  - If the configured workflow is **Prevent download of malicious file. User cannot proceed**, it blocks the file and shows the warning page.



- If the configured workflow is **Prevent download of malicious file. User has the option to proceed and download**, it blocks the file and shows the warning page. However, the user can click **Download anyway** to download the file.

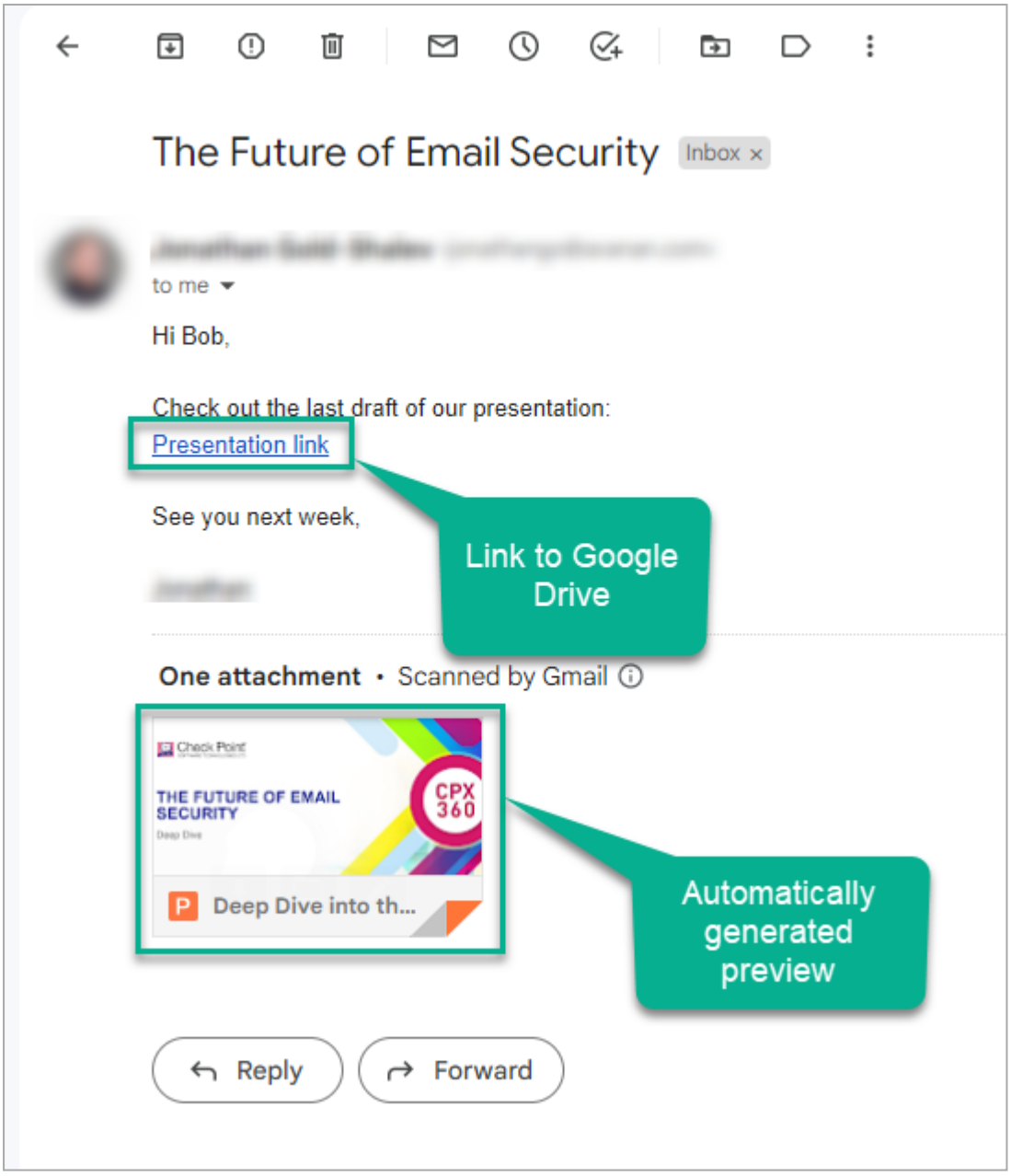


- If the file is detected as clean, it shows the notification and downloads the file.



Google Drive Preview Links

By default, in the Gmail interface, when there is a link to a file in Google Drive, the email shows the file preview as if it was attached to the email.



But, when Avanan rewrites the link, the system does not show the file preview.

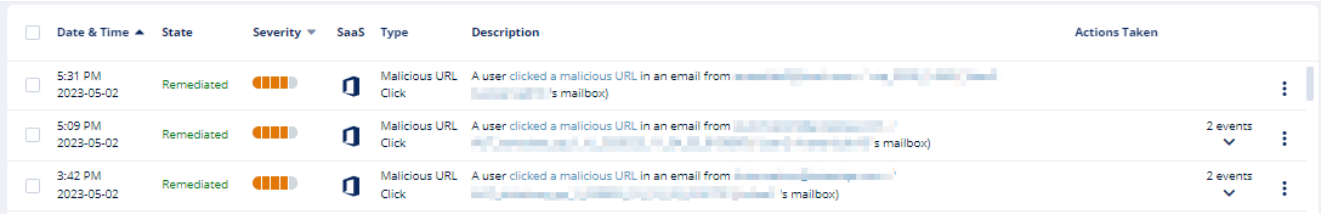
Forensics

Each stage of the Click-Time Protection process is recorded for forensic and auditing purposes, from the original URL replacement to the result of the time-of-click scan.

Click-Time Protection processes the events as **Malicious Url Click** and **Proceed to Malicious Url**.

- **Malicious Url Click** event is recorded when a user clicks on the rewritten URL and is redirected to the warning page or block page.
- **Proceed to Malicious Url** event is recorded when the user clicks *Proceed anyway* in the warning page. See *"Configuring Click-Time Protection Engine" on page 121*.

For multiple recipients, each URL click would generate an event. Events are aggregated by default.



Viewing Emails with the Replaced Links

You can view these details in the **Emails with Modified Attachments** page.

- Emails with attachments, where the links in the attachments were replaced. See *"Click-Time Protection" on page 120*.
- Emails with attachments that were cleaned. See *"Attachment Cleaning (Threat Extraction)" on page 174*.

Note - The page does not show emails where links in the email body were replaced.

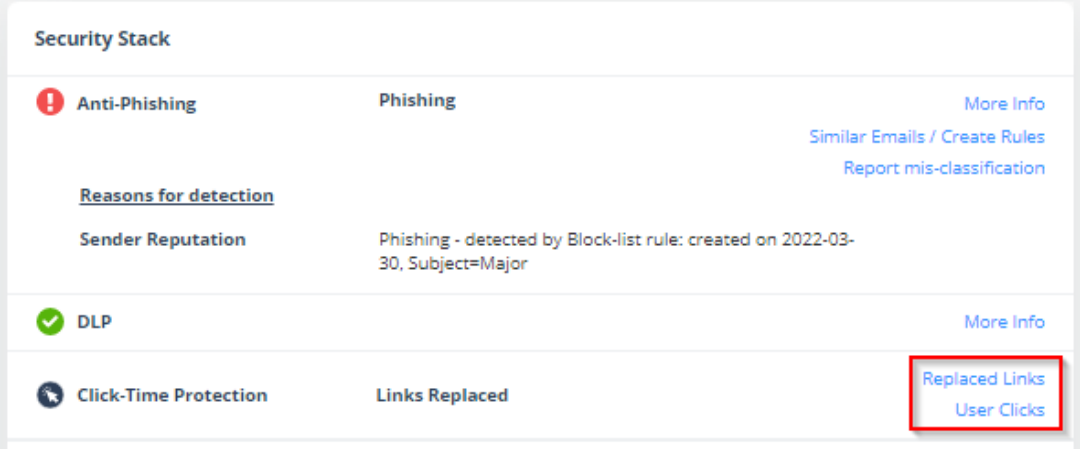
Sending the Unmodified Emails to End Users

To send the original email to the end-user, do one of these.

- From the **Modified Attachments** page.
  1. Go to **User Interaction** > **Modified Attachments**.
  2. To send a original email, click the ⋮ icon for the email from the last column of the request table and select **Send Original**.
  3. To send multiple emails at a time, select the emails and click **Send Original** from the top-right corner of the page.
  4. Click **OK**.
- From the Email profile page.
  1. Open the email profile page.
  2. In the **Email Profile** section, click **Send** for **Send Original Email**.
  3. Click **OK**.

Viewing Replaced Links and User Clicks

- From the **Email Profile** page
  - Under **Security Stack**, for **Click-Time Protection**, administrators can view:
    - **Replaced Links** - All the links replaced by Click-Time Protection engine in the email body and its attachments
    - **User Clicks** – All the clicks performed by users (for clean and malicious websites)



  - Under **Email Attachments**, attachments with replaced links will be marked with a small icon.
- From the **Attachment Info** page, under **Security Stack**, administrators can see all the **Replaced Links** in the attachment.

  The list of **User Clicks** on links inside the attachments and in the email body is available only on the **Email Profile** page and not on the **Attachment info** page.

Determining which User Clicked a Link

Identification of the user that clicked a link is based on a cookie Avanan adds to the clicking user's browser.

Identification procedure:

1. When a user clicks on a replaced link in an email sent to only one email address (click number 1), Avanan adds a cookie to the user's browser.
2. If the user clicks (click number 2) on another replaced link in an email using the same browser within 30 days of the previous click, and the email is sent to the same email address, the user's identity will be linked to that browser.

3. Click number 2 and all future clicks on replaced links (that are opened on the same browser) within the next 365 days will be attributed to the user, regardless of the number of email recipients.
4. After 365 days from click number 1, the cookie is removed from the browser, and the procedure restarts.

Example: Every row in this table describes a click on a replaced link by John Smith:

Date	Email recipients	John Smith's browser	Reported clicked user	Why the user is reported as the clicked user?
01 January 2023	John Smith	Cookie is added	Undetermined	One click is not enough to determine the user as John Smith.
02 January 2023	John Smith Mary Brown James Wilson	Cookie is still valid	Undetermined	Waiting for another click from this browser on links in emails with a single recipient.
03 January 2023 (or any date before 30 January 2023)	John Smith	Cookie is still valid	John Smith	John Smith clicked the replaced link (click number 2) in an email (sent only to one person) using the same browser within 30 days from the previous click. So, John Smith is reported as the clicked user.
20 February 2023 (or any date before 01 January 2024)	John Smith Mary Brown James Wilson	Cookie is still valid	John Smith	As the cookie is still valid, John Smith is reported as the clicked user though the email is sent to multiple users.

Date	Email recipients	John Smith's browser	Reported clicked user	Why the user is reported as the clicked user?
01 January 2024	John Smith	New cookie is added	Undetermined	Now, as 365 days are complete from the first click (click number 1), the old cookie is removed, a new cookie is added, and the user identification procedure starts again.

URL Reputation

URL Reputation security engine uses Check Point's ThreatCloud to detect and prevent access to malicious URLs. It allows administrators to add exceptions for domains and URLs that need to be allowed or blocked, regardless of whether they are malicious or not.

To add URL Reputation exceptions, see *"URL Reputation Exceptions" on page 325*.

Email Protection

When a user shares an email or file through the SaaS application, Avanan gets notified through API. The security engine then scans the data for threats and malicious content, and determines if it is necessary to quarantine, clean, remove, and more.

To scan the data for threats, Avanan uses a full-blown Check Point security stack. This includes zero-day threats protection and malware prevention, data leak prevention, and the ability to reveal shadow IT scenarios. Avanan is designed to protect from real SaaS threats.

Overview

Avanan offers the industry's most complete cloud security solution with defense-in-depth capabilities to make your SaaS and IaaS safe and compliant. It protects your users and files in any cloud environment, from Office 365 to Gmail, Amazon Web Services to Azure.

Avanan offers three modes of protection for email outlined below:

1. **Monitor only**
2. **Detect and Remediate**
3. **Protect (Inline)**

Monitor only mode provides visibility into the cloud-hosted email leveraging publicly available API's and a journal entry from the SaaS email provider. Scan results are provided from 60+ best of breed security tools. In this mode, manual and automated query based quarantines are available after delivery to the user mailbox.

1. Incoming email passes through email provider's spam filter. Emails are sorted accordingly,
    a. Rejected
    b. Accepted, Moved to Junk
    c. Accepted, Moved to Inbox
2. Manual and automated query based quarantines are available after delivery to the user mailbox.

Detect and Remediate mode provides an increased level of protection that scans email via journaling leveraging the same SaaS email provider API's. This mode adds an automated policy action to quarantine malware, phishing attacks etc. based on the results of the best of breed security stack. In this mode user notifications and release workflows are available.

1. Incoming email arrives in respective mailbox folder.
2. Avanan detects new emails and scans (10 seconds - 5 minutes).

3. If malicious, Avanan takes automatic action, otherwise, leaves the email alone.
4. Optional user notifications and release workflows are available.

Protect (Inline) mode provides the highest level of protection and scans emails prior to delivery to the end user's mailbox. Leveraging the same SaaS email provider API's and implementing mail flow rules Avanan can scan email with a best of breed security stack to protect end users from malware, data leaks, phishing attacks and more. Scanning and quarantining takes place before email is delivered to the user's mailbox. This mode insures that threats are detected and remediated before the user has access to the email.

1. Incoming email heads to the mail flow.
2. Avanan redirects the mail for scanning (10 seconds - 5 minutes).
3. If malicious, Avanan takes action, otherwise, returns email to the mail flow.
4. User notifications and release workflows are defined in policy.

Office 365 Mail

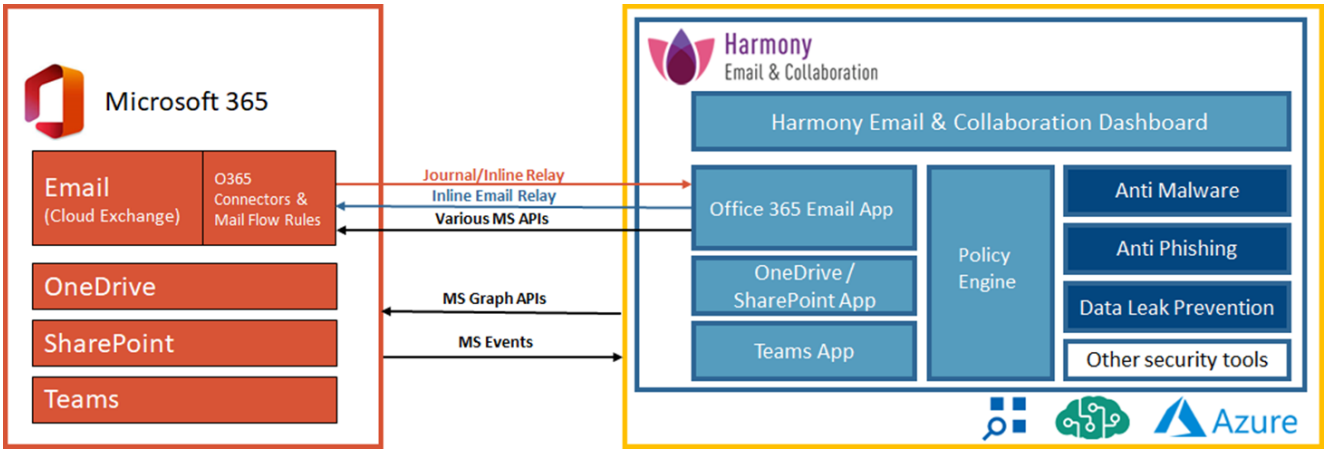
Overview

Microsoft offers a wide variety of SaaS solutions, each with its own infrastructure and integration protocols. Using Avanan's native application programming interface (API), Avanan connects the security tools directly to Microsoft's infrastructure and provides a full suite of security solutions for data within enterprise Microsoft SaaS applications.

How it Works

Avanan integrates with the following Office 365 services:

- Email (Cloud Exchange),
- OneDrive (File storage and sharing),
- SharePoint (Collaboration), and
- Teams (Collaboration).



Office 365 Mail Security Settings

Quarantine Settings

For details about quarantine, see *"Managing Quarantine" on page 421*.

Notification Templates and Senders

The content for notifications sent to internal and external end users are controlled through the Office 365 Mail configuration page.

To configure the notification templates:

1. Navigate to **Security Settings > SaaS Applications > Office 365 Mail**.
2. Click **Configure** for Office 365 Mail.
3. Scroll down to the end and expand **Advanced**.
4. Select the template and make the changes.

Note - Some notifications can be customized from the policy. For more details, see *"Configuring a Threat Detection Policy Rule" on page 150* and *"Data Loss Prevention (DLP) Policy" on page 188* and *"Click-Time Protection Policy" on page 223*.

Available configurable templates

- Quarantine notification `From`
- Quarantine notification `Reply-To`
- Quarantine notification subject
- Quarantine notification body
- Phishing quarantine notification body
- Quarantined notification (admin restore request)
- Restore request subject
- Restore request body
- Decline message subject
- Decline message body
- Threat extracted message format
- Threat extracted attachment name template
- Phishing quarantine notification subject
- Phishing quarantine notification body (admin restore request)
- Phishing decline message subject

- Phishing decline message body
- Spam quarantine notification body
- Spam quarantine notification subject
- DLP quarantined notification body (admin restore request) - Outbound
- DLP quarantined notification body (admin can restore)
- DLP quarantined notification body (user can restore) - Outbound
- DLP restoration notification body - Outbound
- Restore notification subject
- Added header key
- Added header value
- Sender (Envelope From) to use in an alert sent to quarantine inbox
- Email to use as `Reply-To` in an alert sent to quarantine inbox
- Report Phishing approve subject
- Report Phishing approve body
- Report Phishing decline subject
- Report Phishing decline body
- Outgoing spam quarantine notification body
- Outgoing phishing quarantine notification body
- Outgoing phishing quarantine notification body (admin restore request)
- Outgoing quarantine notification body
- Outgoing quarantined notification (admin restore request)
- DLP quarantined notification body (admin restore request) - Inbound
- DLP quarantined notification body (user can restore) - Inbound
- DLP restoration notification body - Inbound
- DLP alert subject to external sender - Inbound
- DLP alert body to external sender - Inbound

Protecting Microsoft 365 Groups

When an email is sent to a Microsoft 365 Group, every member in the group receives the email and the email will also be available in the mailbox assigned with the Microsoft 365 Group.

When a malicious email is sent to a Microsoft 365 Group, Avanan detects and quarantines the malicious email from every group member's individual mailbox.

However, the malicious email gets quarantined from the Microsoft 365 Group mailbox only when the policy is set to **Prevent (Inline)** mode.

Note - Avanan supports to protect these groups:

- Microsoft 365 Groups
- Mail-enabled Security Groups
- Distribution groups

Adding a New Domain to Microsoft 365

At times, organizations might add new domains to their Microsoft 365 account.

To provide continuous protection for the users in these domains using Avanan, these users must not have policies with **Protect (Inline)** protection mode for the first 48 hours after the transition.

To do that:

- For all the existing policies (Threat Detection, DLP and Click-Time Protection) that are in **Protect (Inline)** protection mode, change the scope to exclude the users from the new domain.
- For the users in the new domain, assign new policies with **Detect and Remediate** protection mode.

Note - After 48 hours from the transition, you can change the policy scope so that it protects all domains in the **Protect (Inline)** protection mode.

If you have any queries about how to apply these changes in the configuration, contact *Avanan Support*.

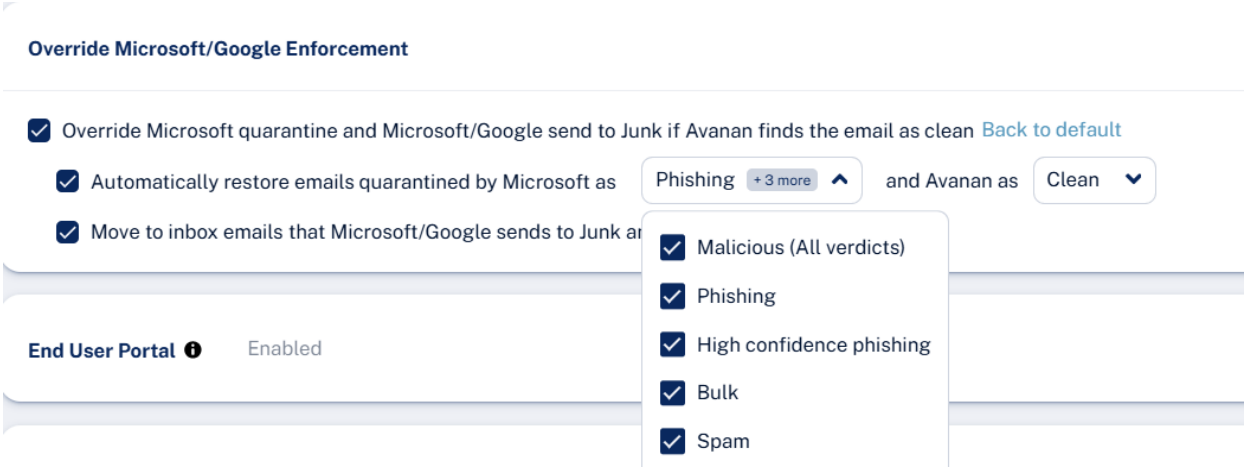
Overriding Microsoft's False Positive Detections

Emails Falsely Quarantined by Microsoft

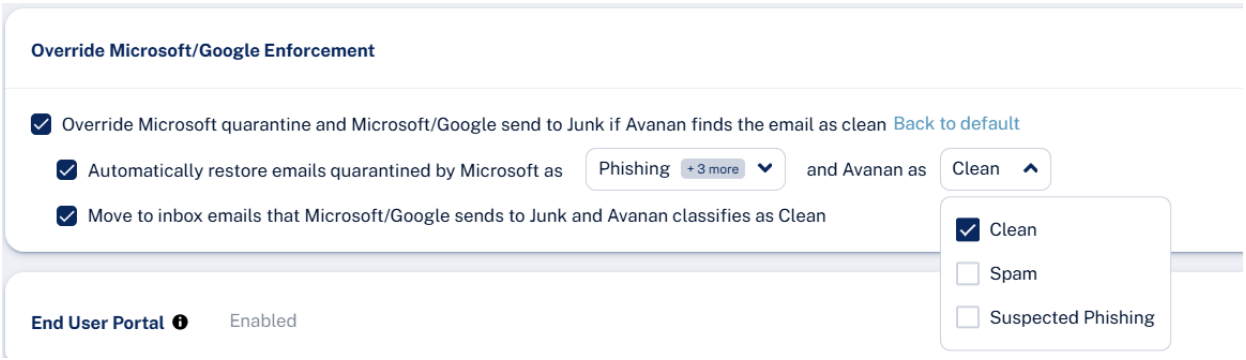
Administrators can configure Avanan to automatically release emails quarantined by Microsoft, if Avanan classifies them as Clean / Spam / Suspected Phishing. To do that:

1. Go to **Security Settings** > **User Interaction** > **Quarantine**.
2. In the **Override Microsoft Enforcement** section, select the **Override Microsoft quarantine/send to Junk if Avanan finds the email as clean** checkbox and click **customize** next to it.
3. Select the **Automatically restore emails quarantined by Microsoft and Avanan** checkbox.

4. From the list, select the required classification of emails to restore from the Microsoft quarantine.
    - Malicious (All verdicts)
    - Phishing
    - High confidence phishing
    - Bulk
    - Spam



5. From the list, select the preferred Avanan verdicts.
    - Clean
    - Spam
    - Suspected Phishing



6. (Optional) To move emails that Microsoft marks as junk to the user's inbox when Avanan classifies them as clean, select the **Move to Inbox for emails that Microsoft sends to Junk and Avanan classifies as Clean** checkbox.
7. Click **Save and Apply**.

Notes:

- These emails do not appear in the Daily Quarantine Report (Digest) or the End-User Quarantine Portal (Email Security Portal).
- The policy workflow do not apply to these emails as the released email is the original email. The email will be sent directly to the user's mailbox.

For information about how the emails are enforced, see *"Enforcement Flow" on page 144*.

Emails Falsely Sent to Junk by Microsoft

Administrators can configure Avanan to manage phishing emails that Microsoft / Google falsely flags as spam.

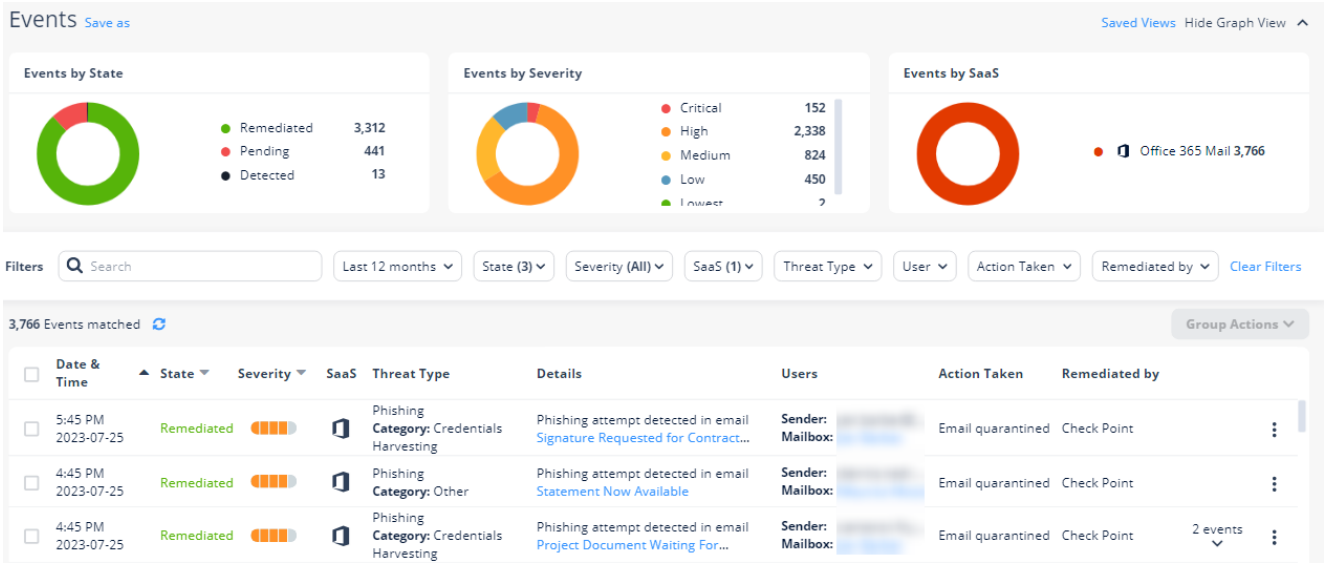
For more information, see *"Overriding Microsoft False Detections as Spam (Send to Junk)" on page 108*.

If you only want to apply it to emails allow-listed by Avanan, refer to the *"Overriding Microsoft / Google sending emails to Junk folder" on page 316*.

Viewing Office 365 Mail Security Events

Avanan records the Office 365 Mail detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.



Viewing Security Events for Microsoft Quarantined Emails

To view security events for Microsoft quarantined emails:

1. Go to **Events** from the left navigation panel.
2. Select the time frame to view the security events.
3. In the **Threat Type** filter, select the relevant threat type:
   - **Malware** for emails Microsoft quarantined because of a malware detection or a block-listed file type.
   - **Phishing** for emails Microsoft quarantined because of a High Confidence Phishing detection or a Transport Rule.
   - **Suspected Phishing** for emails Microsoft quarantined because of a phishing detection.
   - **Spam** for emails Microsoft quarantined because of High Confidence Spam, Spam, or Bulk detections.
4. In the **Action Taken** filter, select **Email quarantined**.
5. In the **Remediated by** filter, select **Microsoft**.

The **Events** page shows all the security events for Microsoft quarantined emails. To take action on these security events, see *"Taking Actions on Events" on page 356*.

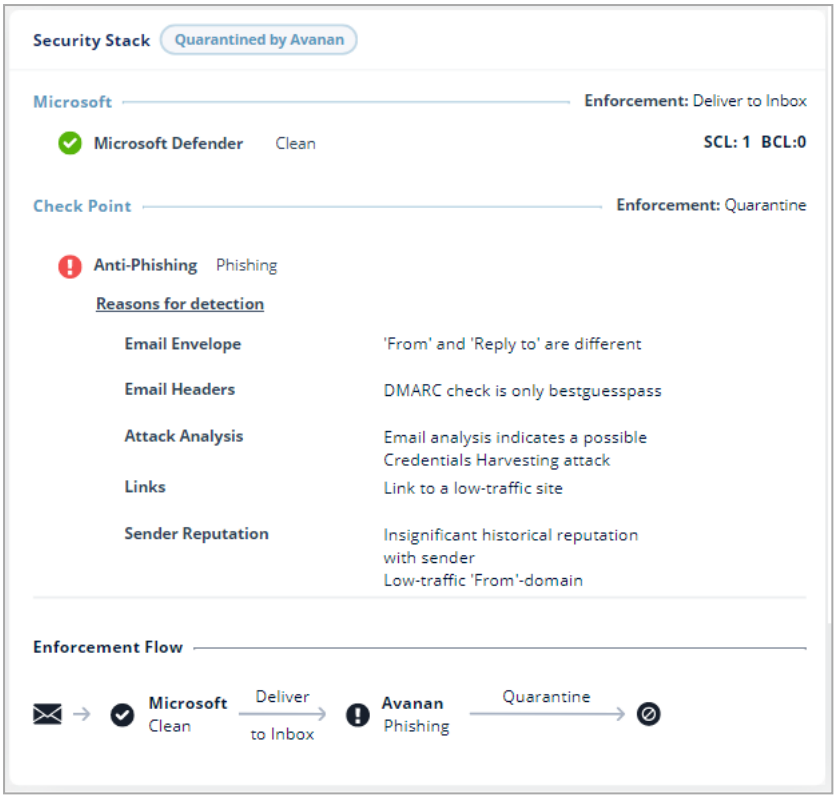
Note - Avanan synchronizes Microsoft quarantined emails hourly due to limitations in how Microsoft's API exposes quarantined emails. During each synchronization, the system retrieves emails received in the hour preceding the last full hour. For example, a sync at 13:30 PM fetches emails received between 11:30 AM and 12:30 PM. As a result, Microsoft quarantined emails appear in the portal at least one hour after receipt.

Visibility into Microsoft Defender Verdict and Enforcement

Avanan provides visibility to how Microsoft Defender classified the emails and which enforcement action it intended to perform on it.

You can view the Microsoft Defender's visibility for an email in the **Security Stack** section of the email profile page.

Note - Microsoft Defender's visibility is available only for incoming and internal emails.



Spam confidence level (SCL)

Microsoft assigns a spam confidence level (SCL) to inbound messages that go through spam filtering and are assigned a spam score. That score is mapped to an individual spam confidence level (SCL) that's added to the email. A higher SCL indicates a message is more likely to be spam.

SCL Value	Description
-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.
0, 1	Spam filtering determined the message wasn't spam.
5, 6	Spam filtering marked the message as spam.
8, 9	Spam filtering marked the message as high confidence spam.

For more information, see Spam confidence level (SCL).

Bulk complaint level (BCL)

Microsoft assigns a bulk complaint level (BCL) to inbound messages from bulk mailers. A higher BCL indicates a bulk message is more likely to generate complaints (and is therefore more likely to be spam).

BCL Value	Description
0	The message isn't from a bulk sender.
1, 2, 3	The message is from a bulk sender that generates few complaints.
4, 5, 6, 7*	The message is from a bulk sender that generates a mixed number of complaints.
8, 9	The message is from a bulk sender that generates a high number of complaints.

* This is the default threshold value used in anti-spam policies.

For more information, see Bulk complaint level (BCL).

Phishing confidence level (PCL)

The phishing confidence level (PCL) indicates the likelihood that a message is a phishing message based on its content.

PCL Value	Description
1, 2, 3	The message content isn't likely to be phishing.
4, 5, 6, 7, 8	The message content is likely to be phishing.

For more information, see Phishing confidence level (PCL).

Enforcement Flow

The **Enforcement Flow** shows the enforcement action taken by Microsoft and Avanan on an email. You can view the **Enforcement Flow** for an email in the **Security Stack** section of the email profile page.

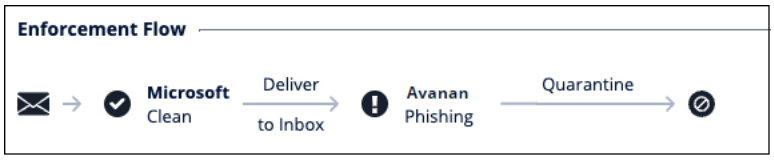
Note - The **Enforcement Flow** does not include manual actions taken on the email.

Depending on the **Protection mode** selected in the threat detection policy, the **Enforcement Flow** would be different.

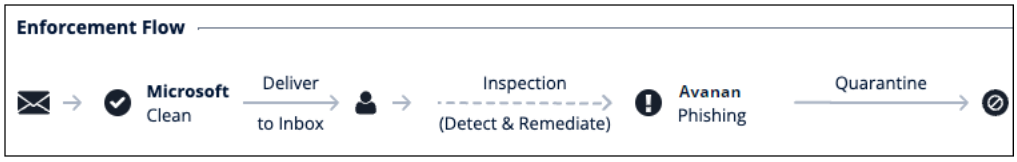
- Example of an email inspected by a policy in **Prevent (Inline)** protection mode.

  Microsoft finds the email **Clean** and intends to deliver it to the user's mailbox; Avanan scans the email, finds it Malicious, and quarantines it before it gets to the user's mailbox since it's inspected by a **Prevent (Inline)** policy.

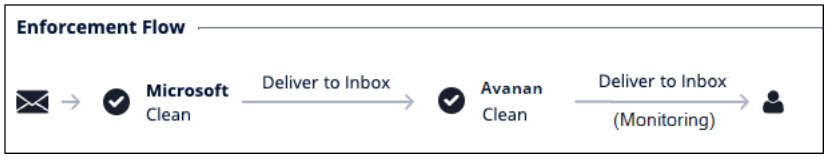
- Microsoft finds the email **Clean** and intends to deliver it to the user's mailbox. Enforcement: **Deliver to Inbox**.
- Avanan scans the email and finds it malicious. Avanan quarantines the email before it gets delivered to the user's mailbox and quarantines it. Enforcement: **Quarantine**.



- Example of an email inspected by a policy in **Detect & Remediate** protection mode.
  - Microsoft finds the email **Clean** and delivers it to the user's mailbox. Enforcement: **Deliver to Inbox**.
  - Avanan scans the email and finds it malicious. Avanan pulls the email from the user's mailbox and quarantines it. Enforcement: **Quarantine**.



- Example of an email inspected by a policy in **Detect** protection mode.
  - Microsoft finds the email **Clean** and delivers it to the user's mailbox. Enforcement: **Deliver to Inbox**.
  - Avanan only scans the email and does not perform any enforcement as the policy protection is in **Detect** mode. Enforcement: **Deliver to Inbox (Monitoring)**.



- When Avanan is configured to automatically restore emails quarantined by Microsoft 365 for being High Confidence Phishing, and if Avanan classifies them as Clean.
  - Microsoft finds the email **High Confidence Phishing** and quarantines it.
  - Avanan scans the email and finds it clean. Avanan restores the email to the user's inbox.

  For information about how to configure Avanan to automatically restore emails quarantined by Microsoft 365 for being High Confidence Phishing, see *"Overriding Microsoft's False Positive Detections " on page 139*.

Google Gmail

Overview

Google offers a lot of APIs for Gmail and Google Drive. Avanan initiates the security by fetching all emails, attachments, files, and folders metadata in a *bootstrap* process. The *bootstrap* ensures the customer's dedicated virtual appliance has the same cloud state.

How it Works

Gmail offers file sharing and file collaboration tools that allow employees and outside collaborators to share files. Avanan adds additional layers of security, privacy, and compliance not offered by Google.

- Malware detection with Anti-Virus and Advanced Persistent Threat detection
- Data Leakage Prevention
- Revocable Encryption (for files leaving the environment)
- File sanitization

Required Permissions

The cloud state used for Gmail by Avanan is composed of the following entities:

- Users
- Emails
- Attachments
- Labels used in emails

Once the cloud state is saved, Avanan starts monitoring the changes for each user. To track each change for each user in the cloud, Avanan uses the following channels:

- Subscribe each user to Google Push Notifications for new messages (https://developers.google.com/gmail/api/guides/push)
- Fallback to polling each user history of changes, each minute if Push Notifications fails (https://developers.google.com/gmail/api/guides/sync)

Avanan uses the following resources for Gmail from the APIs:

- Messages
- Labels
- History of changes
- Attachments

Avanan require the following permissions from Gmail.

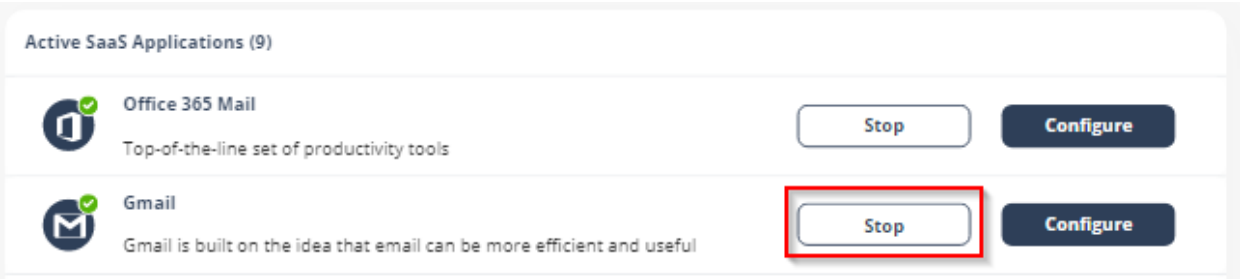
Permissions Required by Gmail
View and manage Emails
View users on your domain
Insert mail into your mailbox
Manage mailbox labels
View and modify but not delete your email
View your emails messages and settings
Manage your basic mail settings
View and manage Pub/Sub topics and subscriptions
View your email address
View your basic profile info

Activating Gmail

For details about the procedure to activate Gmail, see *"Activating Gmail" on page 87*.

Deactivating Gmail

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Gmail.



3. In the confirmation pop-up, click **Stop**.

Upon deactivation, Avanan will no longer protect your organization's Gmail mailboxes.

To complete the deactivation process:

- If you receive *Google Workspace protection was successfully uninstalled* message, remove the Avanan apps.

For the procedure to remove the Marketplace app, see Uninstall a Google Workspace Marketplace app.

- If you receive *Avanan was unable to be uninstalled automatically from Google Workspace* message, follow these steps.

  1. Delete Avanan settings on Google Workspace:
     - Inbound gateway
     - SMTP relay service
     - Hosts
     - Groups
     - Service Admin User
  2. Remove the Avanan apps.

     For the procedure to remove the Marketplace app, see Uninstall a Google Workspace Marketplace app.

After a certain period of time your tenant-related data will be deleted. If you want the data to be deleted immediately, contact *Avanan Support*.

Gmail Security Settings

Quarantine Settings

For details about quarantine, see *"Managing Quarantine" on page 421*.

Notification Templates and Senders

The content for notifications sent to internal and external end users are controlled through the Gmail configuration page.

To configure the notification templates:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Gmail.
3. Scroll-down to the end and expand **Advanced**.
4. Select the template and make the required changes.

Note - Some notifications can be customized from the policy. For more details, see *"Configuring a Threat Detection Policy Rule" on page 150* and *"Data Loss Prevention (DLP) Policy" on page 188* and *"Click-Time Protection Policy" on page 223*.

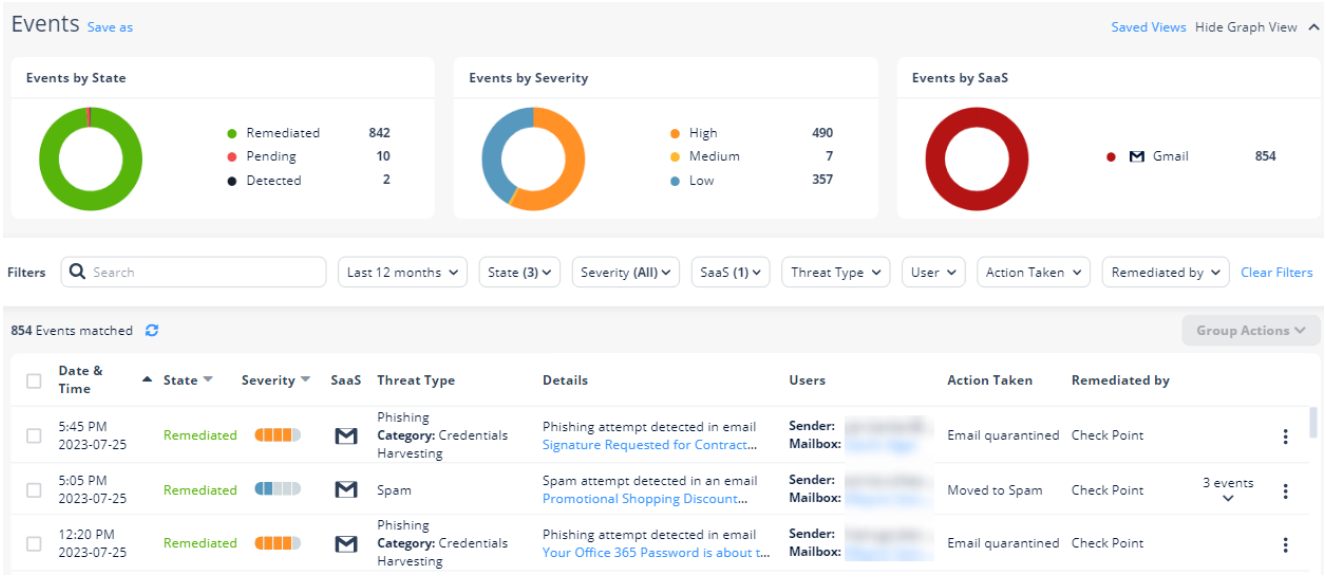
Available configurable templates

- Quarantine notification subject
- Quarantine notification body
- Quarantined notification (admin restore request):
- Restore request subject
- Restore request body
- Decline message subject
- Decline message body
- Threat extracted message format
- Threat extracted attachment name template
- Phishing quarantine notification subject
- Phishing quarantine notification body
- Phishing decline message subject
- Phishing decline message body
- Spam quarantine notification body
- Spam quarantine notification subject
- Report Phishing approve subject
- Report Phishing approve body
- Report Phishing decline subject
- Report Phishing decline body

Viewing Gmail Security Events

Avanan records the Gmail detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.



Configuring Email Policy

Threat Detection Policy

Threat Detection policy rules are designed to prevent malicious emails (phishing, spam, malware etc.) from getting to your end-users mailbox or alternatively prevent them from being sent by your end-users to external parties.

Detect and Remediate mode and **Prevent (Inline)** mode offers three separate workflows to manage malware and phishing attacks. In **Detect and Remediate** mode the workflow scans the emails after delivery of email to the user and in **Prevent (Inline)** mode, the workflow scans the emails prior to delivery to the user.

Threat Detection Policy for Incoming Emails

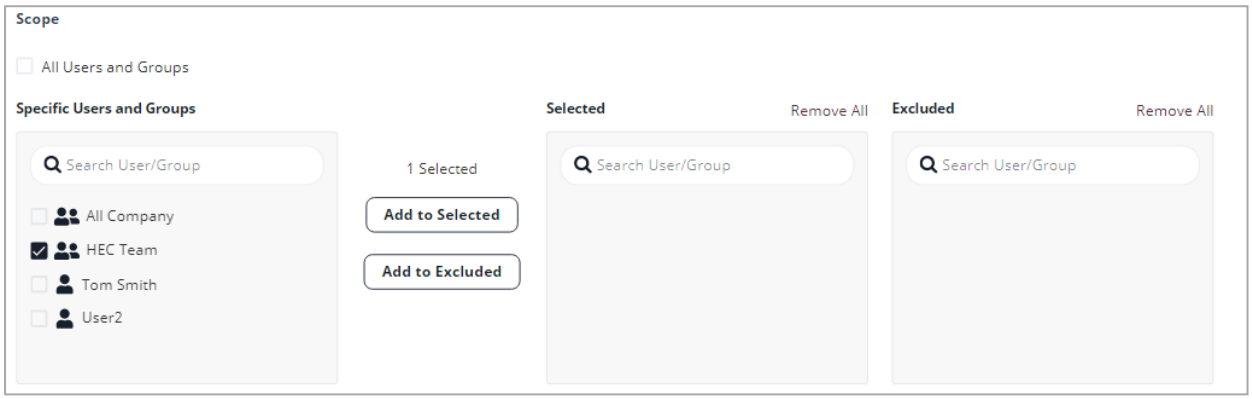
Configuring a Threat Detection Policy Rule

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select the SaaS platform you want to set policy for Office 365 Mail or Gmail.
4. From the **Choose Security** drop-down list, select **Threat Detection** and click **Next**.
5. Select the desired policy protection mode (**Detect**, **Detect and Remediate** or **Prevent (Inline)**).

   If required, you can change the **Rule Name**.

   Note - Avanan protects Microsoft 365 Groups (a service that works with the Microsoft 365) only when the policy mode is set to **Prevent (Inline)**.

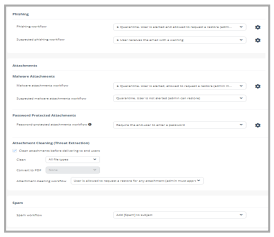
6. Under **Scope**, select the users and groups to which the policy is applicable and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, select **All Users and Groups** checkbox.
   - To apply the policy only to specific users or groups, select the users/groups and click **Add to Selected**.
   - To exclude some of the users or groups from the policy, select the users/groups and click **Add to Excluded**.



For more information about excluded users, see Excluding members of groups from an inline policy.

7. Select the workflows required for the policy.

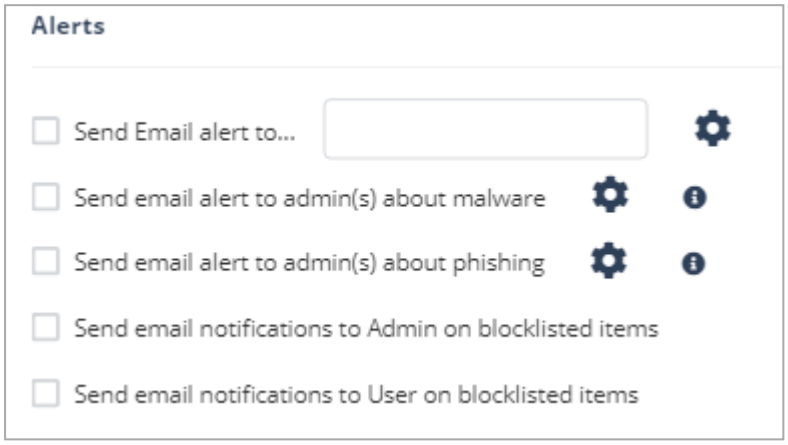
Note - If you select **Detect and Remediate** or **Detect** mode, you may not see some of these additional configuration options that allows you to customize the end user email notifications.



For more information on workflows, see *"Phishing Protection" on page 162*, *"Malware Protection" on page 159*, *"Spam Protection" on page 180*, and *"Password Protected Attachments Protection" on page 165*.

8. Configure **Alerts** to send to the administrators, users, and specific email addresses.
   - To send email alerts about phishing and malware, select **Send email alert to admin(s) about phishing** and **Send email alert to admin(s) about malware**.

- To send email alerts to specific emails, select **Send Email alert to ...** and enter the email address.
- To stop sending alerts to administrators for block-listed items, clear the **Send email notifications to Admin on blocklisted items** checkbox.
- To stop sending alerts to users for block-listed items, clear the **Send email notifications to User on blocklisted items** checkbox.



Notes:

- Even when the alerts are enabled here in the policy, the administrator only receives email alerts for security events when **Send Alerts** option is enabled in *"User Management" on page 508*.
- To customize the email alert templates, click on the gear icon to the right of the alert.

9. After the policy is configured, click **Save and Apply**.

   Note - Policies are based on the order of precedence. Make sure your policies are applied in the proper order. You can adjust the policy order from the order column of **Policy**.

Excluding Members of Microsoft 365 Groups from a Prevent (Inline) Policy

When you exclude a user from a policy in the **Prevent (Inline)** protection mode, this is the expected behavior:

- The excluded user's emails will not be processed by Avanan using the **Prevent (Inline)** protection mode.
- The policy workflow in **Prevent (Inline)** protection mode will not apply to the excluded user.

However, these factors might affect this expected behavior:

1. If the excluded user is a member of a Microsoft 365 group that includes other users protected by a **Prevent (Inline)** policy.
2. If the email is sent to other users who are protected by a **Prevent (Inline)** policy.

Scenarios and Expected Behavior for Excluded Users in Prevent (Inline) Policies:

	Email sent only to the excluded user		Email sent to excluded user and another protected user		Email sent to group	
	Policy protection mode	Workflows applied?	Policy protection mode	Workflows applied?	Policy protection mode	Workflows applied?
Excluded user is part of a protected Microsoft 365 group	Prevent (Inline)	No	Prevent (Inline)	Yes	Prevent (Inline)	Yes
Excluded user is part of another protected group (not Microsoft 365)	Detect	No	Detect	No	Detect	No
Excluded user is not part of any protected group	Detect	No	Detect	No	Detect	No

Example:

Consider a policy in **Prevent (Inline)** protection mode with these settings:

1. The policy applies to all users except John Smith.
2. The policy workflow is configured to quarantine phishing emails.
3. John Smith is part of a Microsoft 365 group with James Wilson.

Scenario 1: A phishing email is sent only to John Smith (excluded user)

Result: The email was inspected and identified as phishing but delivered to John Smith's mailbox since the **Prevent (Inline)** policy was not applied, and the email was not quarantined.

Scenario 2: A phishing email is sent to both John Smith (excluded user) and James Wilson (protected user)

Result: The email was inspected, identified as phishing, and quarantined. John Smith's email was not delivered, though he was excluded from the policy.

Scenario 3: A phishing email is sent to John Smith and James Wilson (both part of a protected Microsoft 365 group)

Result: The email was inspected, identified as phishing, and quarantined. Both John Smith and James Wilson do not receive the email.

Scenario 4: A phishing email is sent to John Smith and James Wilson (both John Smith and James Wilson were part of a different group type

Result: The email was inspected and identified as phishing. The email is delivered to John Smith's mailbox without being quarantined.

Threat Detection Policy for Internal Emails

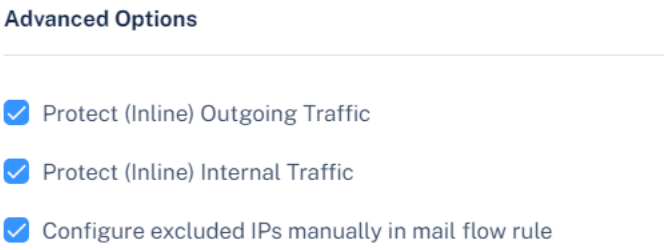
Internal emails refer to emails exchanged between employees of an organization. For internal emails, Avanan applies the threat detection policy workflows of incoming emails.

By default, even if the Threat Detection policy is set to **Prevent (inline)** mode, it only applies to incoming emails. Internal emails are inspected in **Detect and Remediate** protection mode, see *"Fallback Workflows for Internal Traffic" on the next page*.

Inline Protection for Internal Emails (Office 365 Mail)

To enable inline protection for internal emails:

1. Access the Avanan Administrator Portal and click **Policy**.
2. Select **Office 365 Mail** and click on a Threat Detection policy in **Protect (Inline)** protection mode.
3. Go to the **Advanced Options** section and select the **Protect (Inline) Internal Traffic** checkbox.



4. Click **Save and Apply**.

Notes:

- If you enable **Protect (Inline)** protection mode for internal emails in a policy, it applies to all policies in **Protect (Inline)** mode, including the one you are editing.
- In rare cases, as well as when customers onboard Microsoft 365 Mail in Manual Mode, some manual changes are required in your Microsoft 365 environment before enabling inline protection for internal emails. For more information, see *"Inline Protection for Internal Emails (Office 365 Mail) - Manual Configuration Required" below*.

Inline Protection for Internal Emails (Office 365 Mail) - Manual Configuration Required

After selecting the **Protect (Inline) Internal Traffic** checkbox and saving the threat detection policy, a pop up appears stating that some manual configurations are required.

If that happens, follow these two steps:

1. Add a Mail Flow rule named **Avanan - Protect Internal**. For more information, see *"Avanan - Protect Internal" on page 565*
2. Edit the **Avanan DLP Outbound Connector** and check the **Retain internal Exchange email headers** checkbox. For more information, see *"Avanan DLP Outbound Connector" on page 68*.

Only after completing these changes, Avanan protects the internal emails in **Protect (inline)** protection mode.

Fallback Workflows for Internal Traffic

In case Protect (Inline) protection for internal emails is not enabled, internal emails are inspected in **Detect and Remediate** mode.

As they share the policy with incoming emails, workflows defined for inline protection cannot be applied on the internal emails.

Therefore, for every inline workflow defined for incoming emails, these workflows are applied for internal traffic:

Threat Detection Policy Workflow for Incoming Emails	Threat Detection Policy Workflow for Internal Emails	Comments
Quarantine (**Prevent (Inline)** or **Detect and Remediate** protection mode)	Quarantine (**Prevent (Inline)** or **Detect and Remediate** protection mode)	N/A
Email is allowed. Deliver to Junk	Email is allowed. Deliver to Junk	N/A

Threat Detection Policy Workflow for Incoming Emails	Threat Detection Policy Workflow for Internal Emails	Comments
Do nothing	Do nothing	N/A
Email is allowed, Header is added to the email	Do nothing	If you want the fallback workflow as Quarantine, contact *Avanan Support*.
User receives the email with a warning	User receives the email with a warning	N/A
Require end users to enter the password	Require end users to enter the password	Workflow relevant for *"Password Protected Attachments Protection" on page 165*.
Add [SPAM] to subject	Add [SPAM] to subject	N/A
Deliver with Smart Banners	Do nothing	N/A

Threat Detection Policy for Outgoing Emails

Administrators can enable threat detection to prevent malware, phishing, and spam emails from being sent by their organization's users to external parties.

Note - This feature is supported only for Office 365 Mail.

Configuring a Threat Detection Policy Rule

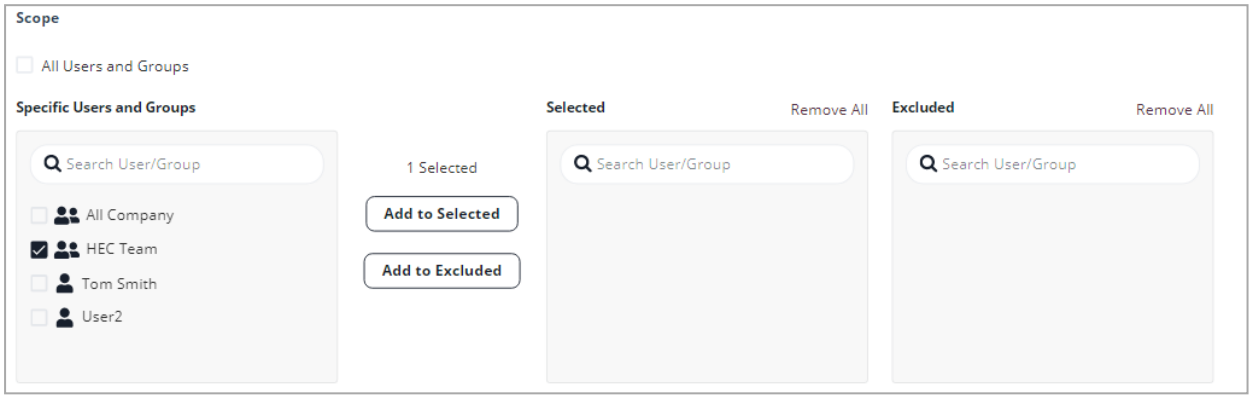
To enable threat detection for outgoing emails:

1. Navigate to **Policy** on the left panel of the Avanan portal.
2. Click on an Office 365 Mail Threat Detection policy rule.

   If you do not have a Office 365 Mail Threat Detection policy rule, create a new policy. See *"Threat Detection Policy for Incoming Emails" on page 150*.
3. Select the desired policy protection mode (**Detect**, **Detect and Remediate** or **Prevent (Inline)**).

   If required, you can change the **Rule Name**.
4. Under **Scope**, select the users and groups to which the policy is applicable and click **Add to Selected**.

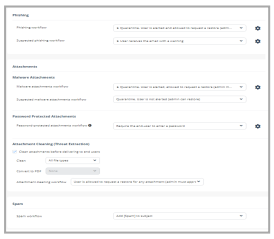
- To apply the policy to all users and groups in your organization, select **All Users and Groups** checkbox.
- To apply the policy only to specific users or groups, select the users/groups and click **Add to Selected**.
- To exclude some of the users or groups from the policy, select the users/groups and click **Add to Excluded**.



For more information about excluded users, see *"Excluding Members of Microsoft 365 Groups from a Prevent (Inline) Policy" on page 152*.

5. Select the workflows required for the policy.

   Note - If you select **Detect and Remediate** or **Detect** mode, you may not see some of these additional configuration options that allows you to customize the end user email notifications.



   For more information on workflows, see *"Phishing Protection" on page 162*, *"Malware Protection" on page 159*, and *"Password Protected Attachments Protection" on page 165*.

6. Scroll down and expand **Advanced Configuration**.
7. Under **Advanced Settings**, enable **Protect (Inline) Outgoing Traffic** checkbox.
8. Click **Save and Apply**.

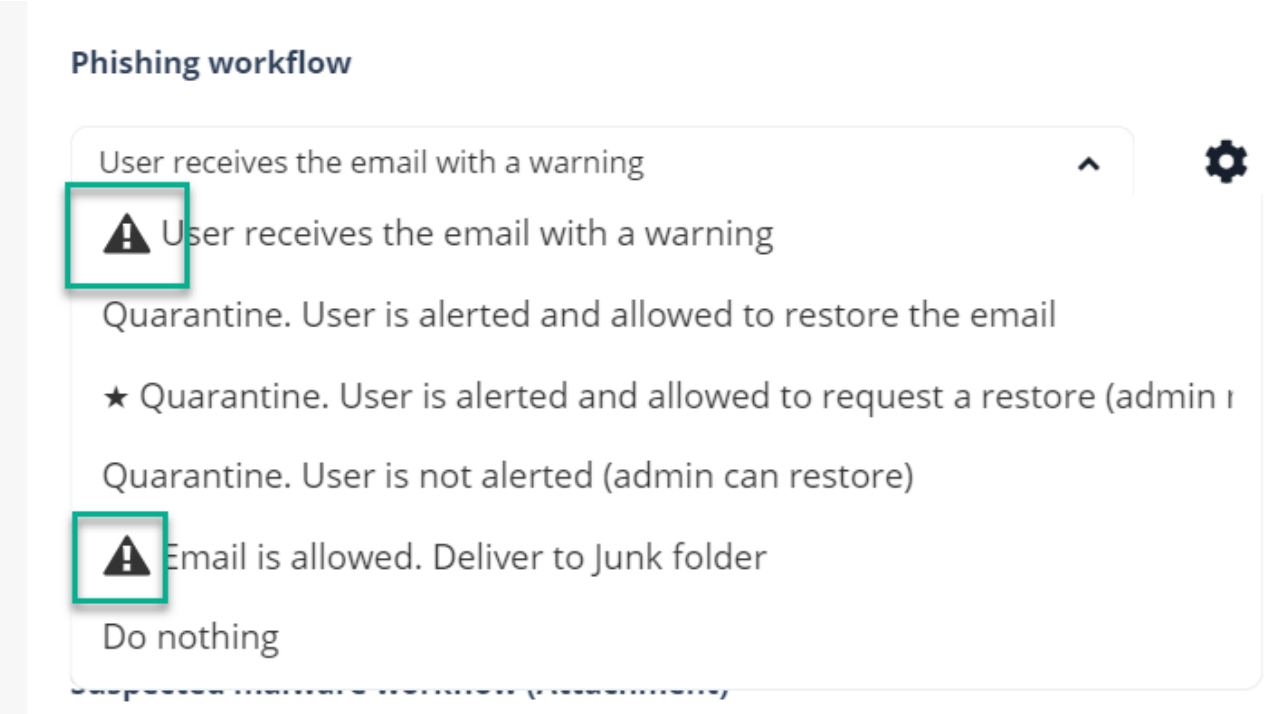
Supported Workflow Actions

As the protected emails are sent from inside the organization to external parties, the threat detection for outgoing emails do not support all the workflows as specified for the incoming emails.

It does not support these workflows:

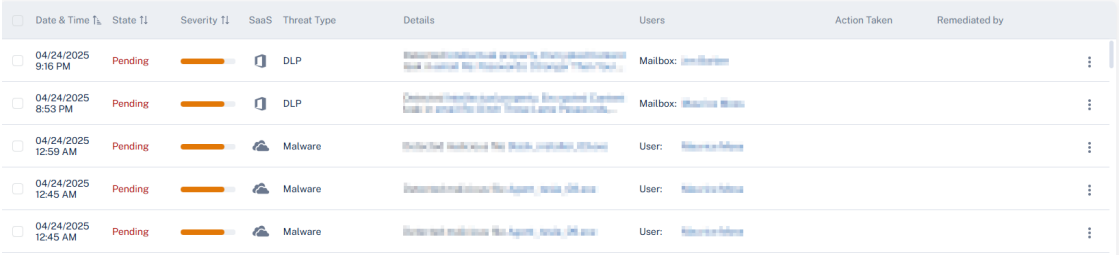
- Delivering the email to the recipient's Junk folder (Email is allowed. Deliver to Junk folder)
- Delivering the email with a warning banner (User receives the email with a warning)
- Delivering the email with a prefix added to the subject (Add [Spam] to subject)

All the workflow actions that are not supported for outgoing emails are marked with a warning symbol.



Notes:

- If the policy rule contains any of the unsupported workflows, the email will be delivered to the external recipient unchanged.
- If the **Do nothing** workflow is configured in the policy and malicious activity is detected, Avanan creates a security event in a **Pending** state. Administrators can review and take appropriate action from the **Events** page.



Prerequisites to Avoid Failing SPF Checks

For Office 365 Mail, if you enable **Protect (Inline) Outgoing Traffic** in the DLP or Threat Detection policy, Avanan gets added to the email delivery chain before reaching external recipients (*Internal email sender > Microsoft 365 > Avanan > Microsoft 365 > External recipient*).

The recipient's email security solution sees the Avanan IP address as part of the delivery chain. If the recipient's email security solution fails to recognize the original IP address, it may consider the Avanan IP address as the IP address from which the email was sent.

If you do not configure the SPF record in your DNS to allow Avanan IP addresses to send emails on behalf of your domain, your emails might fail SPF checks and may be quarantined.

Check Point recommends you add the Avanan IP addresses to your SPF record before you enable **Protect (Inline) Outgoing Traffic** for outgoing emails.

To prevent outgoing emails from failing SPF checks and being quarantined, you must add `include:spfa.cpmails.com` to your SPF record.

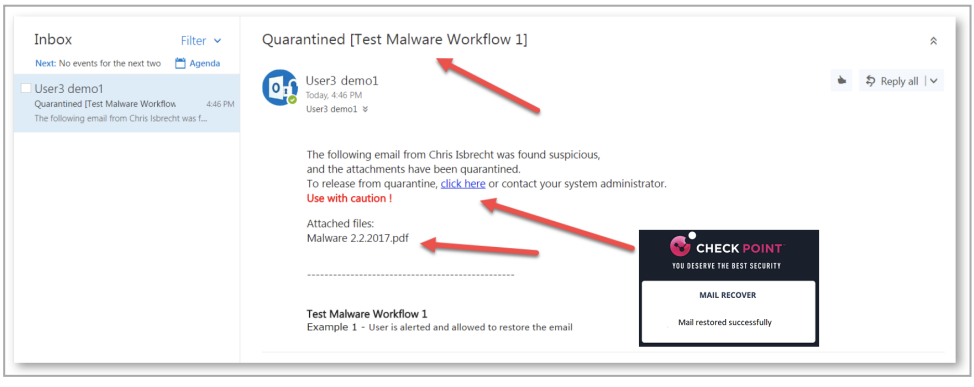
Note - The above statement includes several IP addresses and networks, some outside your Avanan portal's data region. This is done for uniformity and consistency in all Check Point SPF records regardless of your data region. Avanan sends the emails only from one of the IP addresses in your region.

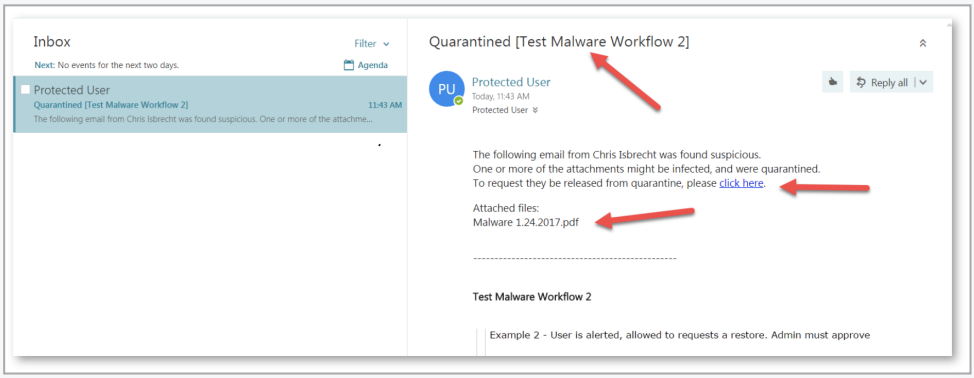
Threat Detection Policy Workflows

Malware Protection

Malware Workflow

The administrators can select any of these workflows for Anti-Malware when malware is detected.

Workflow	Description
Quarantine. User is alerted and allowed to restore the email	Email to the user is scanned and when found malicious, the subject is replaced with a quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, the user has the option to release the quarantined attachment. Using the link in the email, the user can release the attachment. The original email and attachment will be immediately delivered back to the inbox. 

Workflow	Description
Quarantine. User is alerted, allowed to request a restore. Admin must approve	Email to the user is scanned and when found malicious, the subject is replaced with a Quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, using the link in the email, the end-user can request to release the attachment. The administrator is notified via email to the configured **Restore requests approver** email address. The email contains a direct link to the email profile in the Avanan portal. The administrator can do a full security review of the Malware from the Avanan portal and can restore the email or decline the release request. If the request is approved, the original email and attachment will be immediately delivered to the end-user mailbox. 
Quarantine. User is not alerted (admin can restore)	In this mode, the email is automatically quarantined with no user notification.
Email is allowed. Deliver to Junk folder	The detected email is delivered to the recipient's Junk folder.
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Do nothing	The detected email is delivered to the recipients.

For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

Note - To create Allow-List or Block-List for Anti-Malware, see *"Anti-Malware Exceptions" on page 317*.

Suspected Malware Workflow

The administrators can select any of these workflows for Anti-Malware when suspected malware is detected in emails.

Workflow	Description
User receives the email with a warning	The detected email is delivered to the user with a notification inserted in the body of the email.
Email is allowed. Deliver to Junk folder	The detected email is delivered to the recipient's Junk folder.
Quarantine. User is alerted and allowed to request a restore (admin must approve)	Email to the user is scanned and when found malicious, the subject is replaced with a Quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, using the link in the email, the end-user can request to release the attachment. The administrator is notified via email to the configured **Restore requests approver** email address. The email contains a direct link to the email profile in the Avanan portal. The administrator can do a full security review of the Malware from the Avanan portal and can restore the email or decline the release request. If the request is approved, the original email and attachment will be immediately delivered to the end-user mailbox.
Quarantine. User is alerted and allowed to restore the email	Email to the user is scanned and when found malicious, the subject is replaced with a quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, the user has the option to release the quarantined attachment. Using the link in the email, the user can release the attachment. The original email and attachment will be immediately delivered back to the inbox.
Quarantine. User is not alerted (admin can restore)	In this mode, the email is automatically quarantined with no user notification.

Workflow	Description
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Do nothing	The detected email is delivered to the recipients.

Note - To create Allow-List or Block-List for Anti-Malware, see *"Anti-Malware Exceptions" on page 317*.

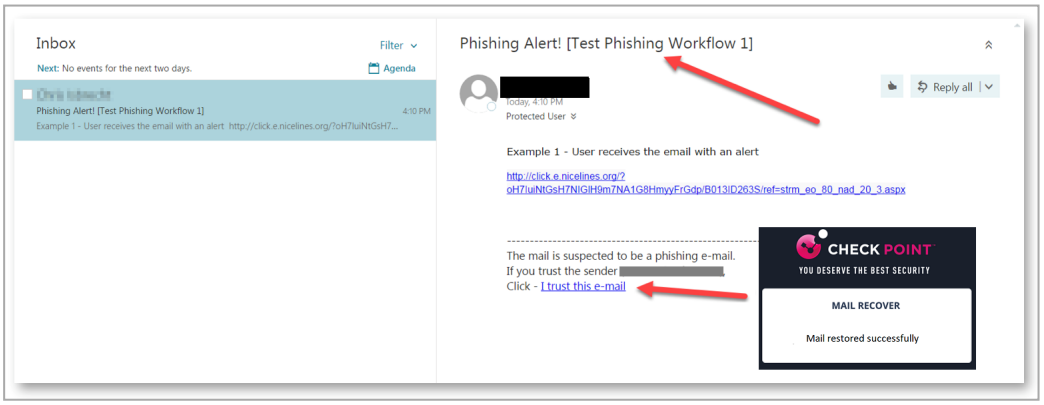
Phishing Protection

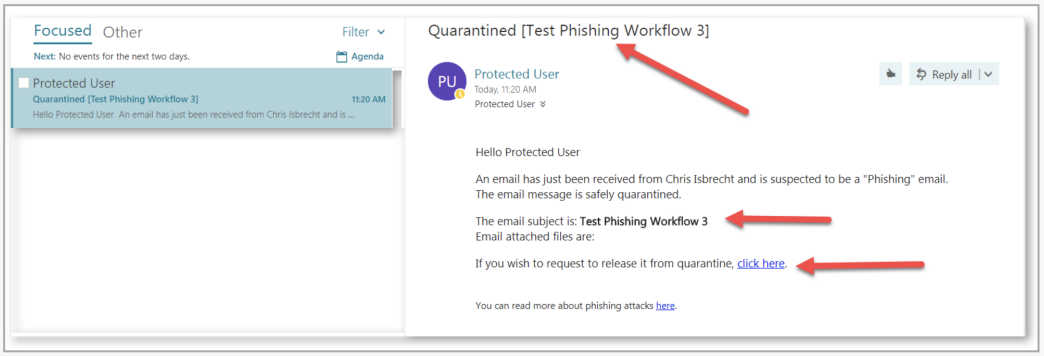
Phishing protection is comprised of the phishing workflows in the policy itself and from the general Anti-Phishing engine settings.

For information about the Anti-Phishing engine settings, see *"Anti-Phishing (Smart-Phish)" on page 97*.

Phishing Workflow

The administrators can select any of these workflows for Anti-Phishing when phishing is detected in emails.

Workflow	Description
User receives the email with a warning	Email to the user is scanned and when found to be suspicious, the email subject is replaced with a Phishing Alert notice and the original subject is provided in brackets. The body of the message includes a customizable message to the user along with a link to remove the warning if a false positive is suspected by the user. 

Workflow	Description
Quarantine. User is alerted and allowed to request a restore (admin must approve)	Email to the user is scanned and when found malicious the subject is replaced with Quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the email if a false positive is suspected. 
Quarantine. User is not alerted (admin can restore)	In this mode, the email is automatically quarantined with no user notification.
Quarantine. User is alerted and allowed to restore the email	Email to the user is scanned and when found malicious, the subject is replaced with a quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, the user has the option to release the quarantined attachment. Using the link in the email, the user can release the attachment. The original email and attachment will be immediately delivered back to the inbox.
Email is allowed. Deliver to Junk folder	The detected email is delivered to the recipient's Junk folder.
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Do nothing	The detected email is delivered to the recipients.

For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

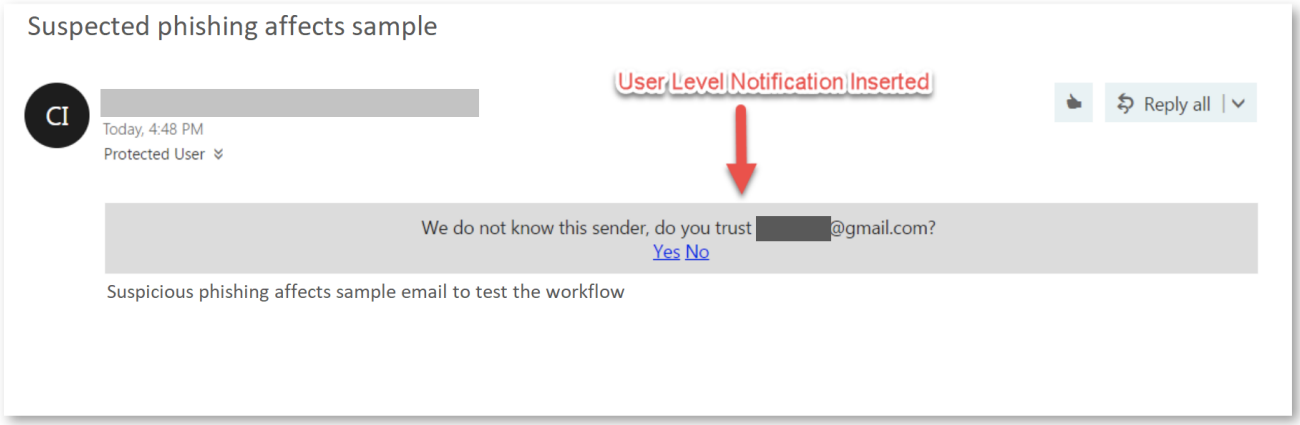
Note - To create Allow-List or Block-List for Anti-Phishing, see *"Anti-Phishing Exceptions" on page 313*.

Suspected Phishing Workflow

The administrators can select any of these workflows for Anti-Phishing when suspected phishing is detected in emails.

Workflow	Description
User receives the email with a warning	The detected email is delivered to the user with a notification inserted in the body of the email.
Quarantine. User is not alerted (admin can restore)	The detected email is automatically quarantined with no user notification.
Quarantine. User is alerted and allowed to request a restore (admin must approve)	Email to the user is scanned and when found malicious the subject is replaced with Quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the email if a false positive is suspected.
Quarantine. User is alerted and allowed to restore the email	Email to the user is scanned and when found malicious, the subject is replaced with a quarantined notice and the original subject is provided in brackets. The body of the message is replaced with a customizable message to the user along with a link to release the file if a false positive is suspected. The attachment is also stripped and noted in the replaced body. In this workflow, the user has the option to release the quarantined attachment. Using the link in the email, the user can release the attachment. The original email and attachment will be immediately delivered back to the inbox.
Email is allowed. Deliver to Junk folder	The detected email is delivered to the recipient's Junk folder.

Workflow	Description
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Do nothing	The detected email is delivered to the recipients.



For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

Password Protected Attachments Protection

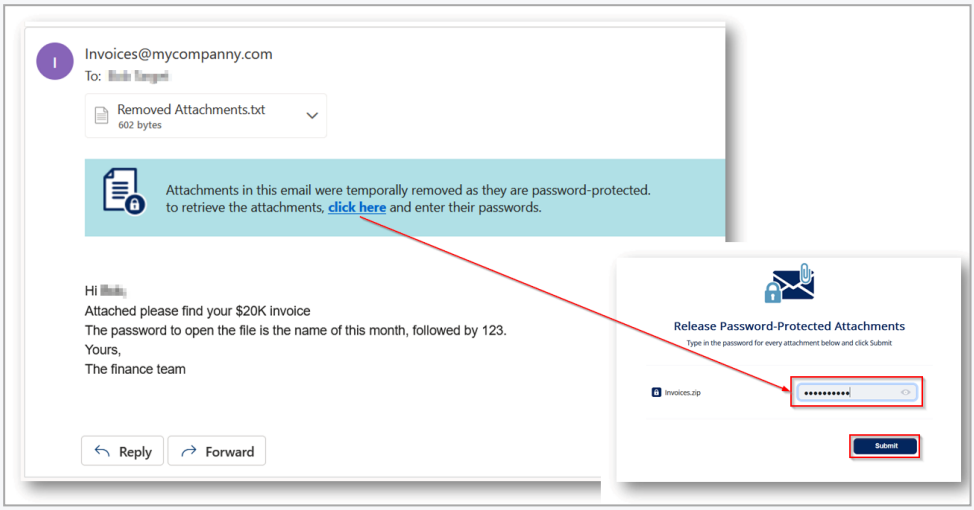
When password-protected attachments are detected, Avanan attempts to extract the password using various techniques such as searching for the password in the email body. If the password is found, Avanan uses the password to decrypt the file and inspect it for malware.

If the password is not found, the administrator can select any one of these workflows:

Password Protected Attachments Workflow

Note - These workflows apply only for the incoming and internal emails.

Workflow	Description
User receives the email with a warning	The detected email is delivered to the user with a notification inserted in the body of the email.

Workflow	Description
Require the end-user to enter a password	The attachment is removed temporarily and a warning banner is added to the email along with a link to enter the password. After the password is entered, the Anti-Malware engine scans the attachment. If the Anti-Malware engine finds the attachment as clean, the original email with the original password-protected attachment gets delivered to the original recipients of the email.  **Notes**: ■ Avanan will not store the passwords entered by the end users. It uses these passwords only for inspection and deletes them after the inspection is complete. ■ If a user tries to release an email which was already released, the system prompts a message that the attachment was already released. ■ Security measures ensure machines do not brute-force password of files (for example, it does not allow to enter password after multiple wrong attempts). • Even if an attacker manages to get the link provided in the warning banner and manages to guess the password, the original password-protected attachments are delivered to the original recipients of the email and not to the mailbox of the person that entered the password.
Quarantine. User is alerted and allowed to restore the email	The email is automatically quarantined and the user is notified about the quarantine. Using the link in the email, the user can release the attachment. The original email and attachment will be immediately delivered back to the inbox.
Quarantine. User is not alerted (admin can restore)	The email is automatically quarantined with no user notification. The administrator can restore the email.

Workflow	Description
Trigger suspected malware workflow	The email follows the workflow configured for Suspected Malware.
Do nothing	The attachment will be considered as clean. **Note** - This workflow flags only the attachment as clean (not malicious). The email can still be found to be malicious for various reasons. For example, if there are other malicious attachments in the email, if the Anti-Phishing engine flagged the email as phishing for other reasons than the attachment being malicious, if there is a DLP violation in the email and more.

To add allow-list for password-protected attachments from specific email addresses or domains, see *"Password-Protected Attachments Allow-List" on page 321*.

For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

Supported File Types

Avanan can detect these file types as password-protected:

File Type	File Extensions
Archives	AR, ARJ, BZ2, CAB, CHM, CRAMFS, CPIO, GZ, IMG, ISO, IZH, QCOW2, RAR, RPM, TAR,TAR.BZ2, TAR.GZ, TAR.XZ, TB2, TBZ, TBZ2, TGZ, TXZ, UDF, WIM, XZ, ZIP, and 7Z.
Adobe PDF (all versions)	PDF
Microsoft Excel 2007 and later	XLSX, XLSB, XLSM, XLTX, XLTM, XLAM
Microsoft Excel 2007 Binary	XLSB
Microsoft Excel 97 - 2003	XLS

File Type	File Extensions
Microsoft PowerPoint 2007 and later	PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM
Microsoft PowerPoint 97 - 2003	PPT, PPS, POT, PPA
Microsoft Word 2007 and later	DOCX, DOCM, DOTX, DOTM
Microsoft Word 97 - 2003	DOC, DOT

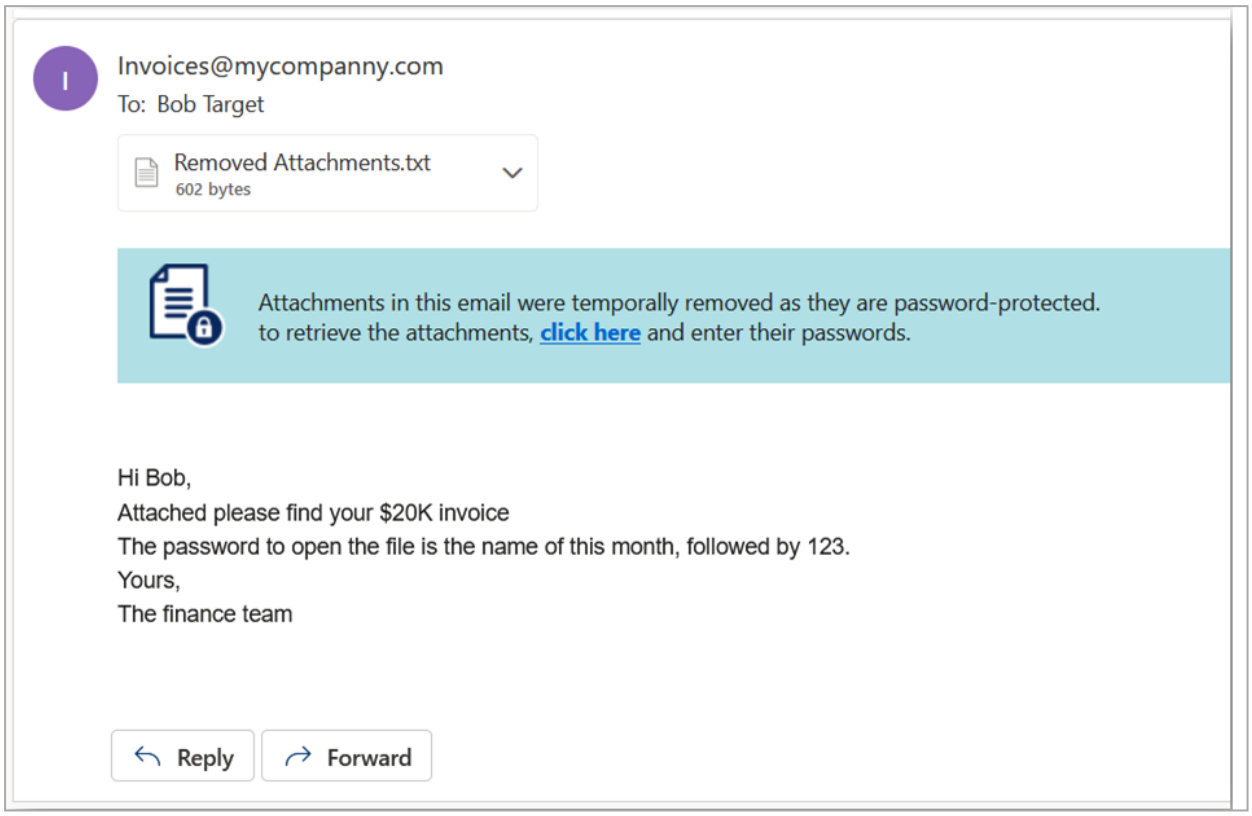
To add allow-list for password-protected attachments from specific email addresses or domains, see *"Password-Protected Attachments Allow-List" on page 321*.

Requesting Passwords from End Users - End-User Experience

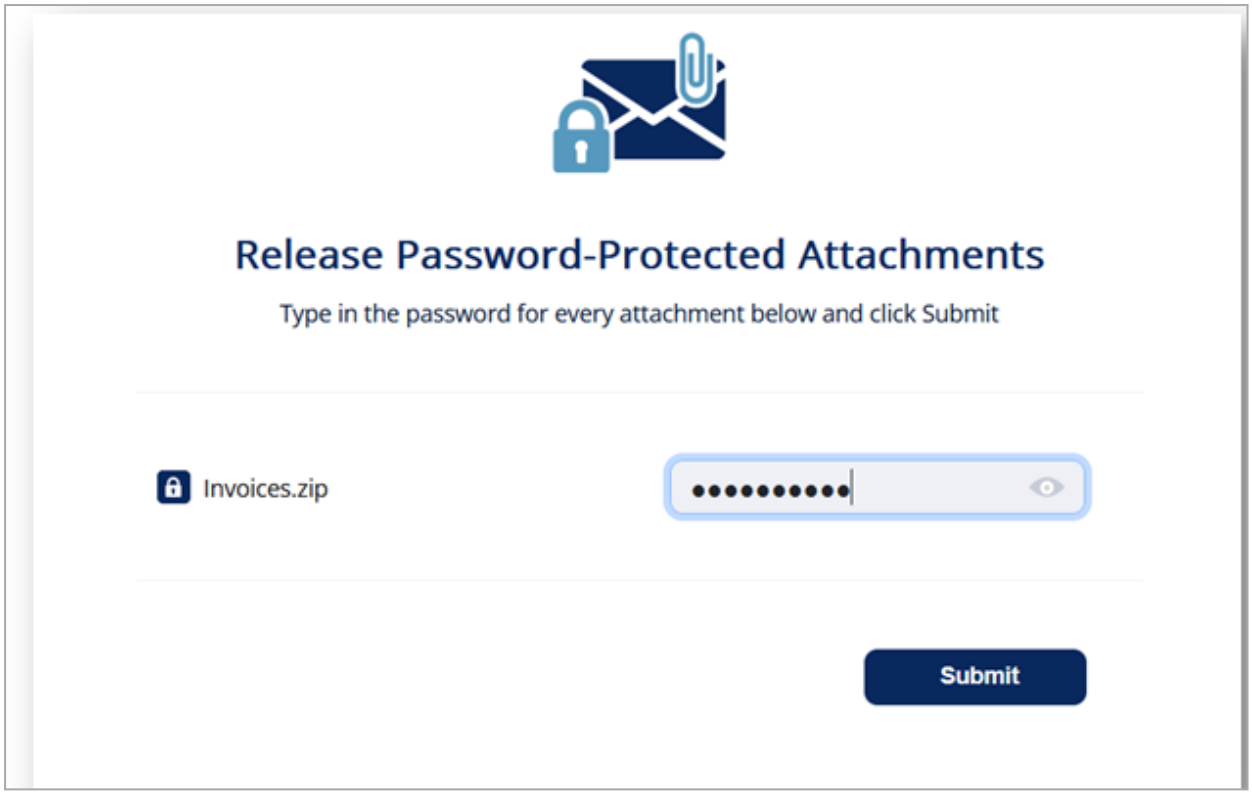
For password protected attachments, if **Require end-user to enter a password** workflow is defined in the policy, the attachment is removed temporarily and a warning banner is added to the email with a link to enter the password.

To restore the password protected attachments with Require end-user to enter a password workflow:

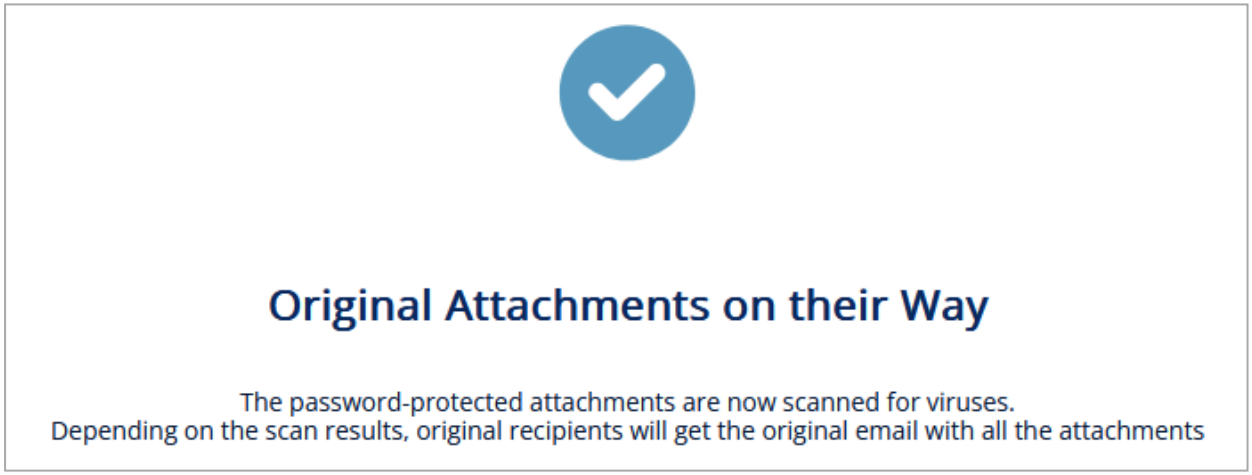
1. Click the link in the warning banner of the email.



2. Enter the password for the attachment and click **Submit**.



After you submit, the Anti-Malware engine scans the attachment for malicious content.



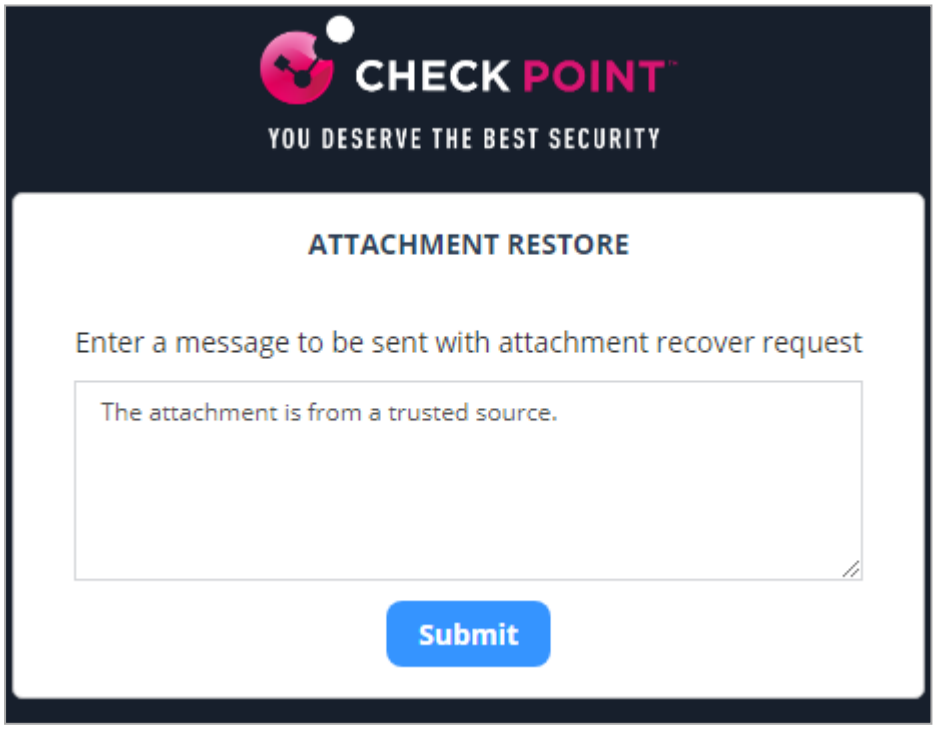
If the Anti-Malware engine finds the attachment as clean, the original email with password-protected attachment gets delivered to the original recipients of the email.

If the email was already released, this message appears:

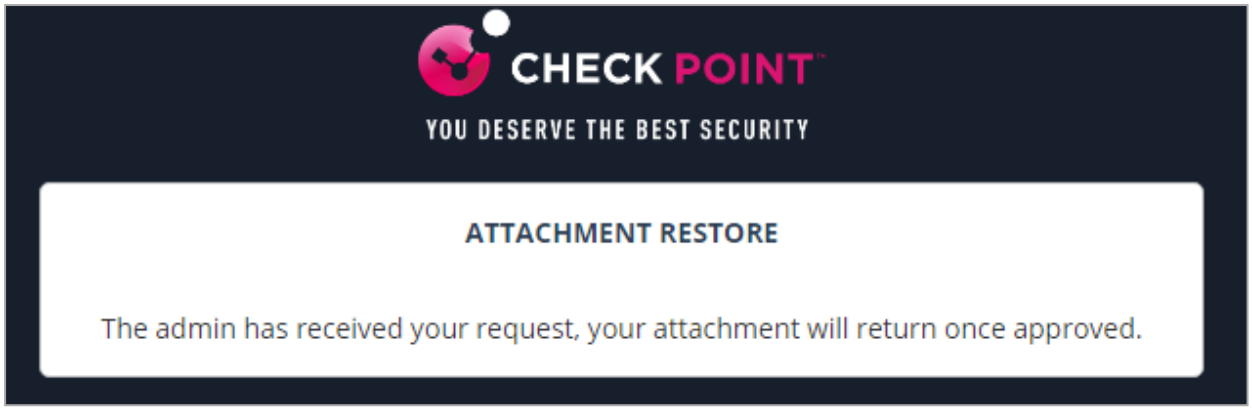
For password protected attachments, if **Quarantine. User is alerted and allowed to restore the email** workflow is defined for the policy, the email body and its attachments are removed. The user receives a notification about the email and its attachments with a link to request to release the email.

To restore the email and its attachments with Quarantine. User is alerted and allowed to restore the email workflow:

1. Click the link provided in the email.
2. If prompted, enter the reason for restoring the attachment, and click **Submit**.



After you submit, the admin receives the request.



After the admin approves, the user receives the original email.

Password Protected Attachments - Administrator Experience

For password protected attachments, if **Quarantine. User is alerted and allowed to restore the email** workflow is defined for the policy, and if the end-user requests to release the email, the administrator is notified about the request.

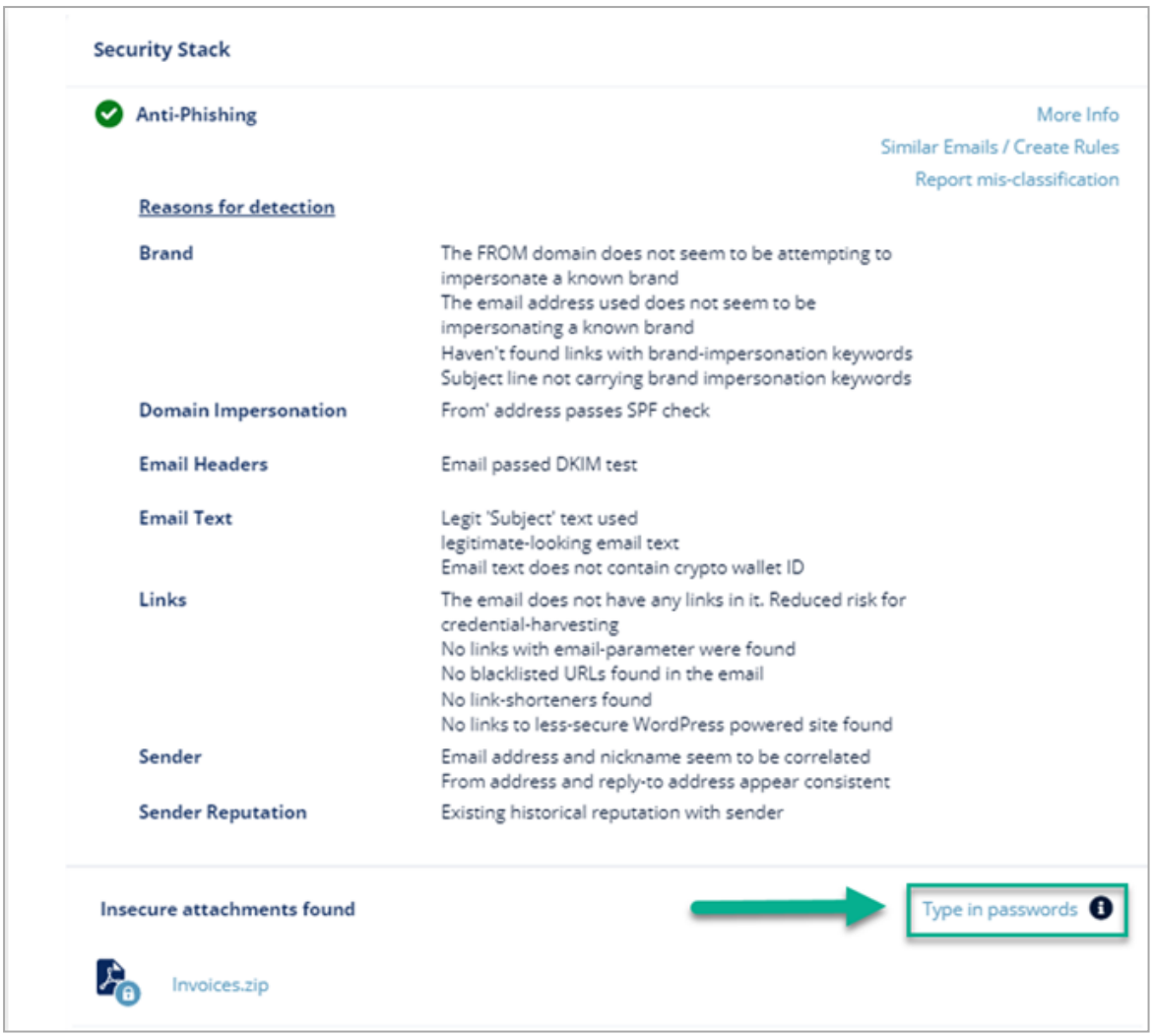
To review the request:

1. Open the security event of the email for which the user requested to release.

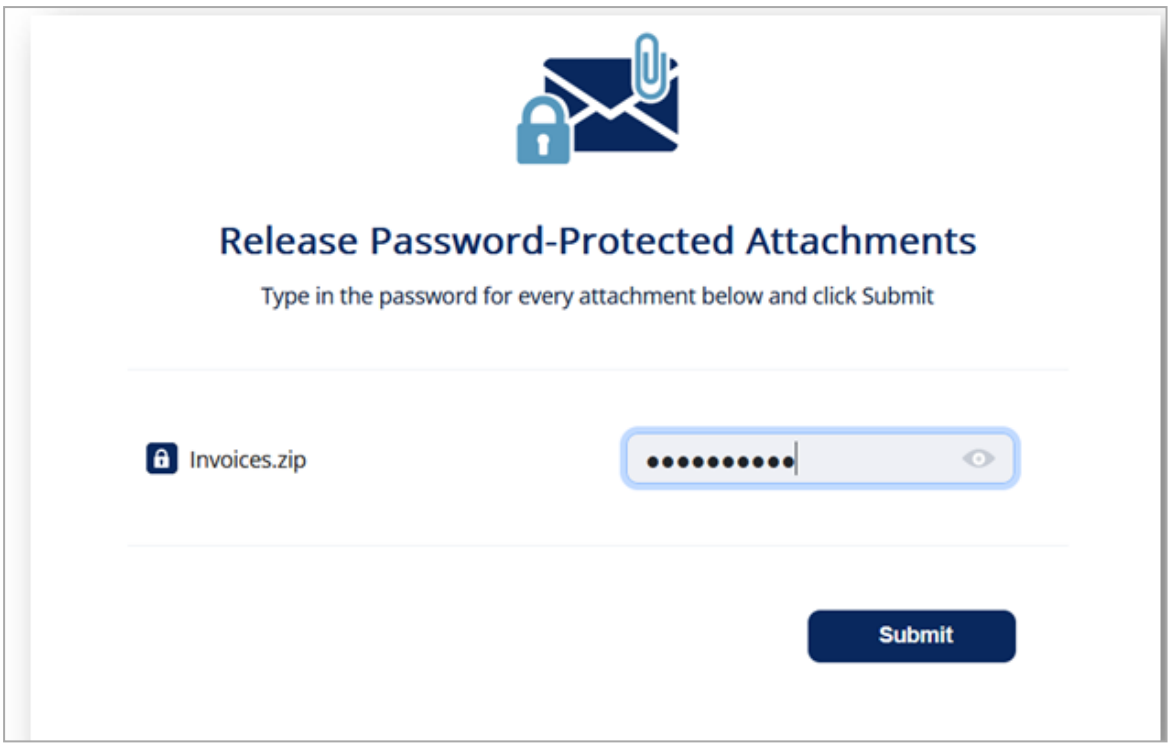
   Under **Security Stack**, the password-protected attachments which are not scanned by Anti-Malware will be marked as **Insecure attachments found**.

2. To inspect the password-protected attachments before restoring the email:

a. Click **Type in passwords** to enter the password for the attachment.



b. Enter the password for the attachment and click **Submit**.



The Anti-Malware engine scans the attachment and gives a verdict. Depending on the verdict decide whether to restore the email or not.

c. To restore the email and its attachments, click **Restore Email**.

3. To release the original email without inspecting the password-protected attachments, click **Restore Email**.

Attachment Cleaning (Threat Extraction)

Attachment Cleaning (Threat Extraction) is a Content Disarm and Reconstruction (CDR) engine that serves as an additional layer of security for email attachments on top of the Anti-Malware engine.

After the Anti-Malware security engine determines an attachment is not malicious, Attachment Cleaning (Threat Extraction) delivers a secure version of the attachment to the end user, removing hyperlinks behind text, macros, and other active content that may contain malware.

Administrators can allow end-users to retrieve the original version of the attachment. This action does not require the help desk's intervention. To configure the attachment cleaning workflow, see *"Configuring Attachment Cleaning (Threat Extraction)" on the next page*.

File Sanitization Modes

Attachment Cleaning (Threat Extraction) can create a safe version of an email attachment in these ways:

- **Clean** - removes macros, embedded objects, and any active content from the attachment while maintaining the file type.

  For example, if a DOC file is cleaned, the end user will get a modified DOC file.

- **Convert** - the file is converted into PDF format, regardless of its original file type, ensuring no active content can ever be a part of it.

  For example, if a DOC file is converted, the end user will get the file in PDF format.

Note - While the **Convert** option is considered to be secure, it has an impact on user experience and productivity. Unless there are strict regulatory or organizational policy requirements, we recommend using the **Clean** option to deliver only PDF files.

Configuring Attachment Cleaning (Threat Extraction)

To configure Attachment Cleaning (Threat Extraction) for Office 365 Mail or Gmail:

1. Click **Policy** on the left panel of the Avanan portal.
2. Open a threat detection policy for Office 365 Mail or Gmail if available, and continue from step 6.

   or

   Click **Add a New Policy Rule**.
3. In the **Choose SaaS** drop-down list, select the SaaS application (Office 365 Mail or Gmail).
4. In the **Choose Security** drop-down list, select **Threat Detection** and click **Next**.
5. Select the **Prevent (Inline)** protection mode.
6. Scroll down to **Attachment Cleaning (Threat Extraction)** section and select the **Clean attachments before delivering to end users** checkbox.
7. In the **Clean** field, select the option required.
   - To clean all the file types, select **All supported file types**.

     Note - When this option is selected, the **Convert** option is disabled.
   - To clean only some file types, select **Only specific file types** and enter the required file types.

     For the supported file types, see *"Supported file types for Attachment Cleaning (Threat Extraction)" on page 177*
   - To exclude some file types from cleaning, select **All supported file types except** and enter the required file types.
   - To stop cleaning the files, select **None**.
8. In the **Convert** field, select the option required.

- To convert all the file types, select **All supported file types**.

  Note - When this option is selected, the **Clean** option is disabled.

- To convert only some file types, select **Only specific file types** and enter the required file types.

  For the supported file types, see *"Supported file types for Attachment Cleaning (Threat Extraction)" on the next page*

- To exclude some file types from converting, select **All supported file types except** and enter the required file types.
- To stop converting the files, select **None**.

9. In the **Attachment cleaning workflow** field, select the workflow. See *"Attachment Cleaning (Threat Extraction) Workflows" below*.
10. Click **Save and Apply**.

Clean Attachments

Threat Extraction cleans an attachment and executes the configured workflow when these conditions are met:

- The attachment is of a supported file type.
- The attachment contains one of the supported active parts for removal.
- The attachment is not detected as malicious (if malicious, the Anti-Malware workflow will take effect).

In addition, Threat Extraction excludes an attachment from cleaning when these conditions are met:

1. Other attachments in the same email are password-protected.
2. The workflow for password-protected attachments is configured as **Require end-user to enter a password**.

When an attachment is not cleaned, its original version is included in the email sent to the end user, and no restoration is required by the user.

Attachment Cleaning (Threat Extraction) Workflows

The administrators can select any of these workflows for attachment cleaning.

Workflow	Description
User is allowed to request a restore for any attachment (admin must approve)	The use is allowed to request for restoring the original attachments. The attachments are restored only after the admin approves.

Workflow	Description
User is allowed to restore benign attachments only	The user can request to restore the attachments. If the attachments are benign, they are restored immediately.
User is allowed to restore any attachment	The user can request to restore the attachments and they are restored immediately.

Supported file types for Attachment Cleaning (Threat Extraction)

File Type	File Extensions
Adobe FDF	FDF
Adobe PDF (all versions)	PDF
Microsoft Excel 2007 and later	XLSX, XLSB, XLSM, XLTX, XLTM, XLAM
Microsoft Excel 2007 Binary	XLSB
Microsoft Excel 97 - 2003	XLS
Microsoft PowerPoint 2007 and later	PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM
Microsoft PowerPoint 97 - 2003	PPT, PPS, POT, PPA
Microsoft Word 2007 and later	DOCX, DOCM, DOTX, DOTM
Microsoft Word 97 - 2003	DOC, DOT

Original Attachments vs Cleaned Attachments

In the Attachment Cleaning process, some components of the attachment are removed or disabled.

By default, these components of the attachment are cleaned and depending on the file type being cleaned, specific components of the attachment may be removed as shown in this table:

Code	File Type	Description
1018	All supported file types	Query to remote database
1019	All supported file types	Files and objects embedded in the documents
1021	All supported file types	Stored data for fast document saving
1026	All supported file types	Microsoft Office macros and PDF JavaScript code

Code	File Type	Description
1034	All supported file types	Links to network or local file paths
1137	PDF	Open other PDF files
1139	PDF	PDF launch action
1141	PDF	Open Uniform Resource Identifier (URI) resources
1142	PDF	Play sound objects
1143	PDF	Play movie files
1150	PDF	Execute JavaScript code
1151	PDF	Submit data to remote locations

To configure Avanan to clean additional part of attachments which are not cleaned by default, contact *Avanan Support*.

Code	File Type	File Part
500	All supported file types	Images embedded in documents
1017	All supported file types	Custom document properties
1025	All supported file types	Links to files that are reviewed by another application
1036	All supported file types	Statistic document properties
1037	All supported file types	Summary document properties
1178	PDF	Embedded 3D Artwork

Viewing Emails with Cleaned Attachments

You can view these details in the **Emails with Modified Attachments** page.

- Emails with attachments, where the links in the attachments were replaced. See *"Click-Time Protection" on page 120*.
- Emails with attachments that were cleaned. See *"Attachment Cleaning (Threat Extraction)" on page 174*.

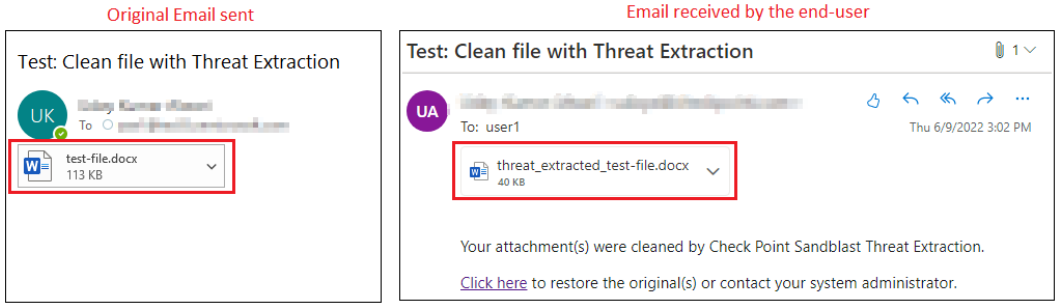
Note - The page does not show emails where links in the email body were replaced.

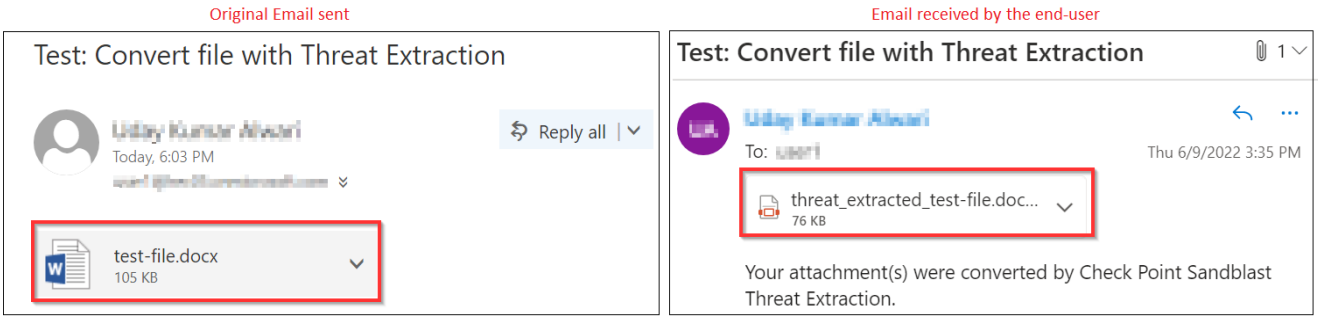
Sending the Unmodified Emails to End Users

To send the original email to the end-user, do one of these.

- From the **Modified Attachments** page.
  1. Go to **User Interaction** > **Modified Attachments**.
  2. To send a original email, click the ⋮ icon for the email from the last column of the request table and select **Send Original**.
  3. To send multiple emails at a time, select the emails and click **Send Original** from the top-right corner of the page.
  4. Click **OK**.
- From the Email profile page.
  1. Open the email profile page.
  2. In the **Email Profile** section, click **Send** for **Send Original Email**.
  3. Click **OK**.

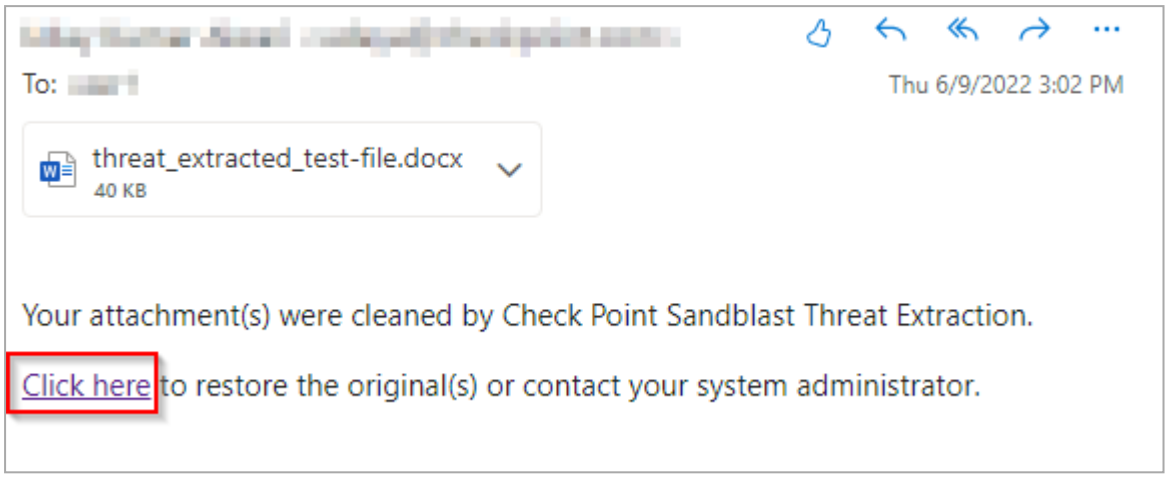
Attachment Cleaning (Threat Extraction) - End-User Experience





To request to restore the original email by the end-user:

1. Click the link below the attachment in the email.



2. If prompted, enter the reason for restoring the attachment, and click **Submit**.

   After you submit, the administrator receives the request.

   After the administrator approves the request, the system delivers the original email to the user's mailbox.

3. If the **Attachment cleaning workflow** is configured such that it does not require administrator's approval to restore the attachment, the original email is delivered to the user immediately.

For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

Spam Protection

Spam Workflows

The administrators can select any of these workflows when spam is detected in emails.

Note - Spam protection workflow is configurable only for Office 365 email and Gmail.

Workflow	Description
Email is allowed. Deliver to Junk folder (Available only for Office 365 Mail)	The Anti-Phishing engine marks the email as Spam by updating the Spam Confidence Level (SCL) to 9 (by setting value of header **X-CLOUD-SEC-AV-SCL** to **True**). The email will be moved to the Spam folder by Office 365 (with the proper Mail Flow rules), based on the configured action for SCL=9 (by default set to deliver the message to the recipients' Junk Email folder). For more information on SCL levels, see SCL.

Workflow	Description
Email is allowed. Move to Spam (Available only for Gmail)	The Anti-Phishing engine delivers the email to the user's Spam folder.
Add [Spam] to subject	The email is delivered to the inbox and the subject is modified to start with '[Spam]' (for example, the email subject 'Are you interested' will be delivered with new subject: '[Spam] Are you interested').
Quarantine. User is alerted and allowed to restore the email	The email is quarantined and the user is allowed to restore the email.
Quarantine. User is not alerted (admin can restore)	The email is quarantined and the admin can restore the email.
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Do nothing	The email is delivered to the end user mailbox.

For more information on who receives the restored emails, see *"Who Receives the Emails Restored from Quarantine" on page 444*.

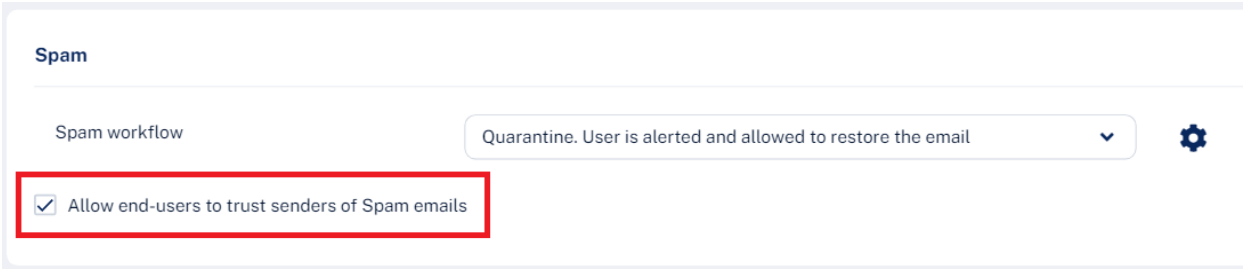
Trusted Senders

Administrators can allow end users to trust senders and domains, so that spam emails sent from these senders are delivered directly to the users' mailbox.

Note - If the emails are classified as phishing or containing malware, they will still be quarantined.

To allow end users to trust senders:

1. Access the Avanan Administrator Portal and click **Policy**.
2. Open an existing Threat Detection policy or create a new one. See *"Threat Detection Policy for Incoming Emails" on page 150*.
3. Scroll down to the **Spam** section and select the **Allow end-users to trust senders of Spam emails** checkbox.

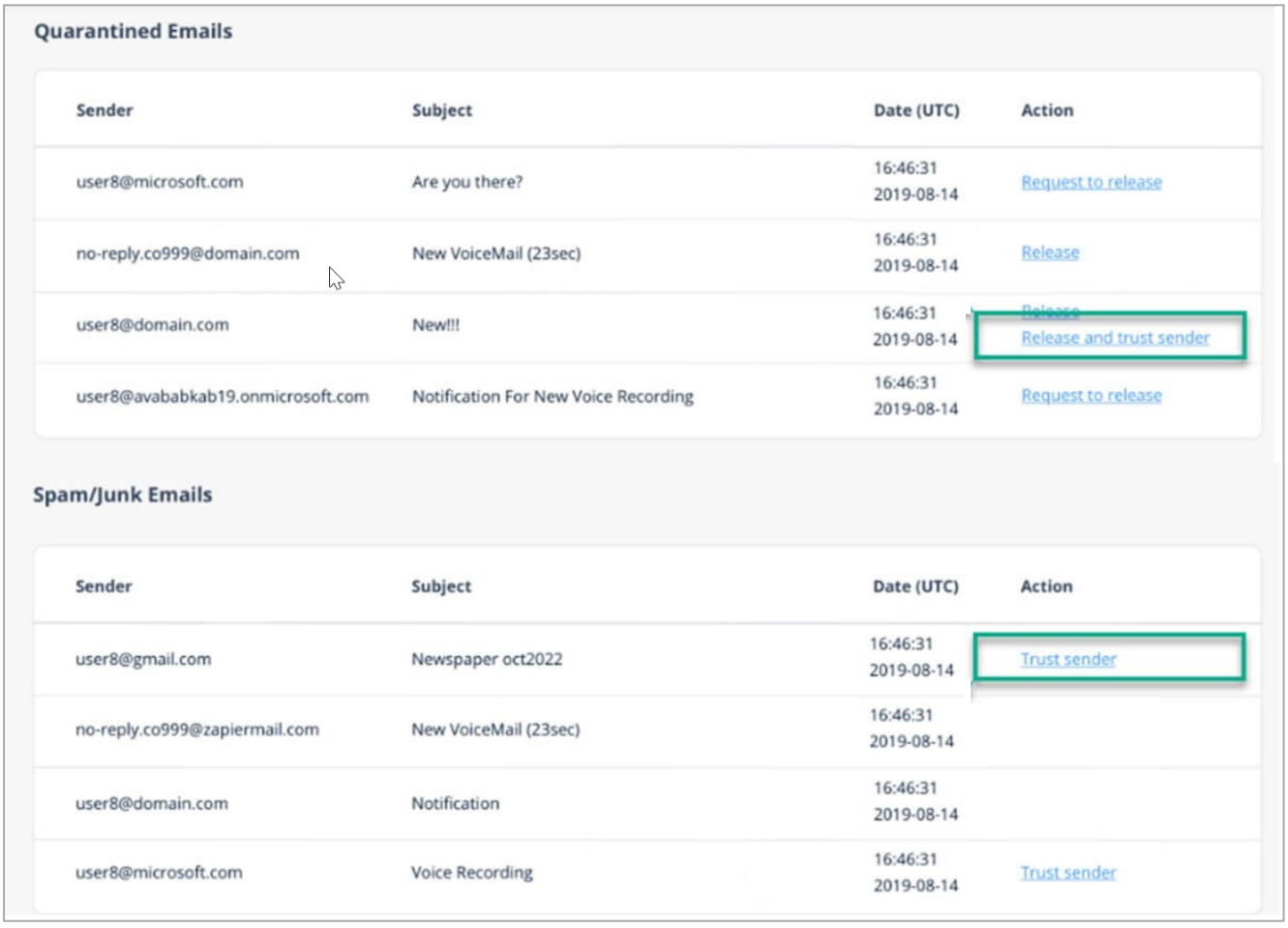


4. Click **Save and Apply**.

For information about how to manage senders trusted by end users, see *"Trusted Senders - End-User Allow-List" on page 327*.

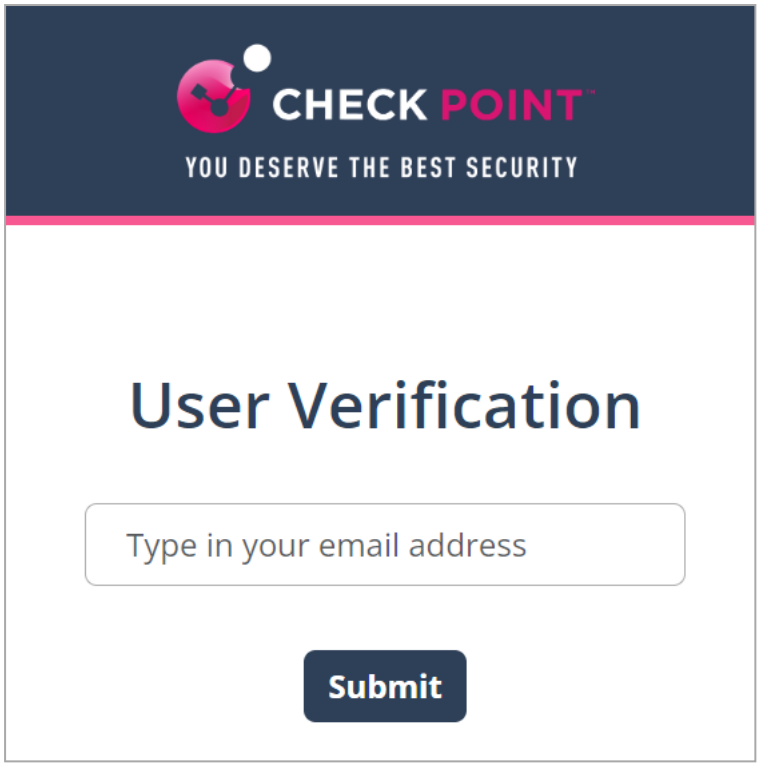
Trusting Senders - End User Experience

When the administrator has configured the policy such that the user is allowed to trust senders, the user will get an option in the to trust senders and their domains.

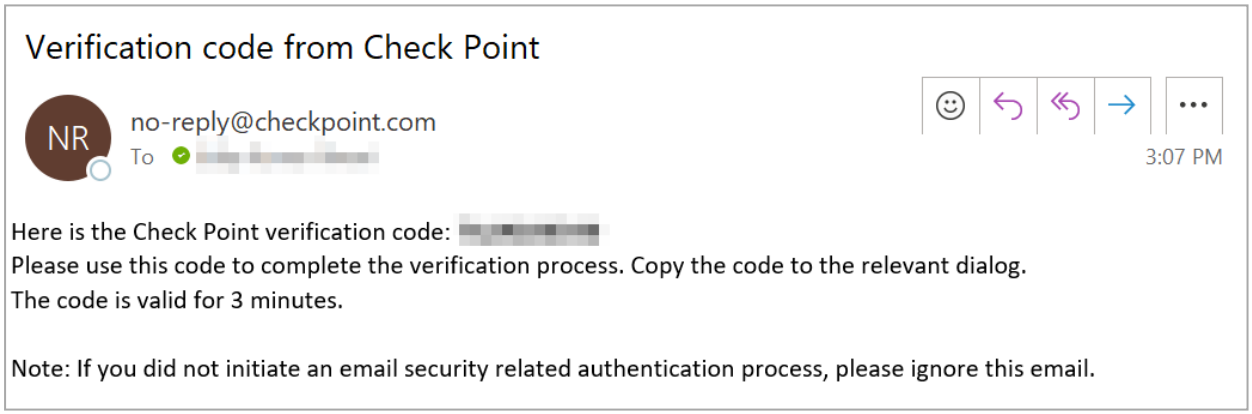


To trust a sender or domain:

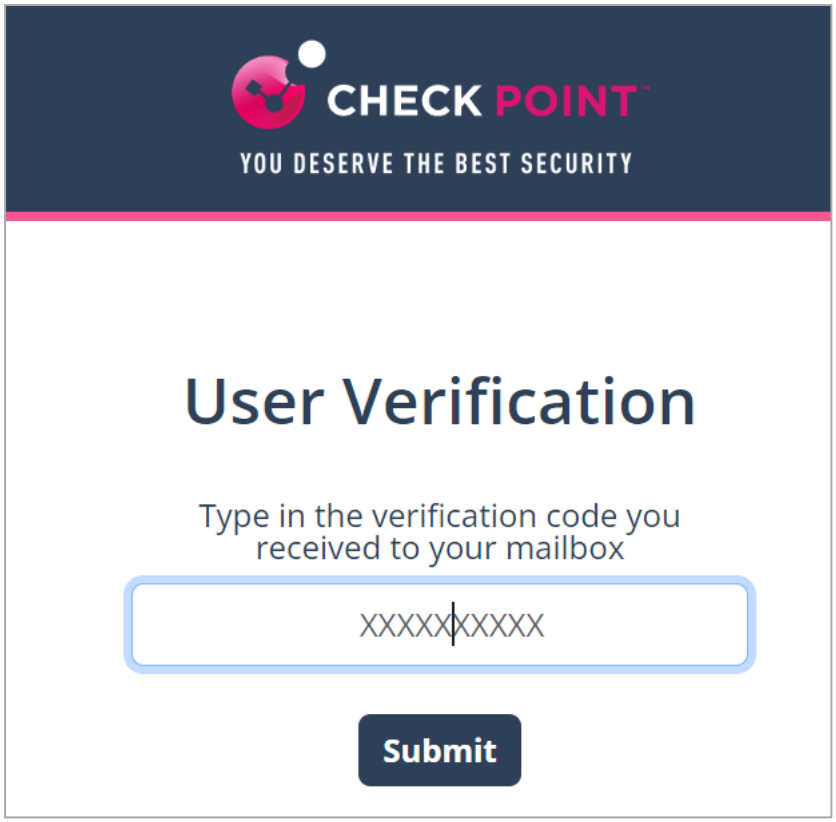
1. Click **Trust sender** in the .
2. Enter your email address and click **Submit**.



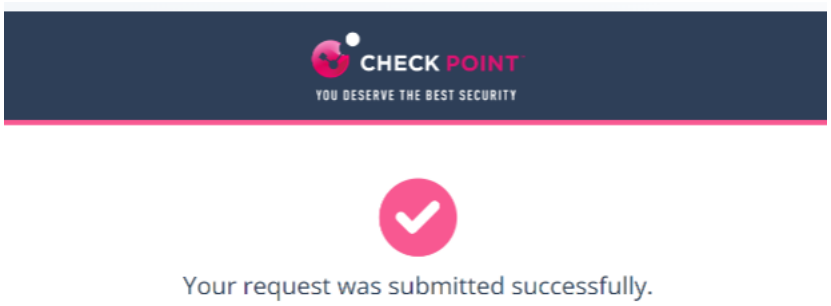
The system sends an email notification with a verification code.



Enter the verification code received from the email and click **Submit**.



After successful verification, the system shows the status.



Once an administrator approves the request, the system adds the sender to the trusted senders list.

Graymail Workflows

Graymails are legitimate but often unwanted emails, such as newsletters and promotional emails, which many users find unnecessary, making it harder to find important messages.

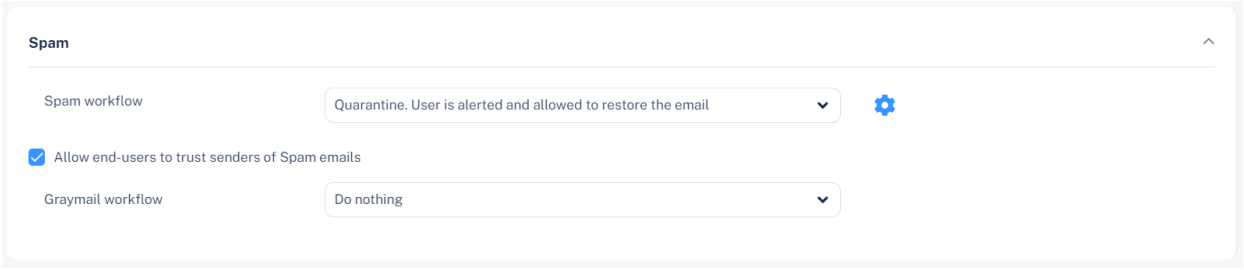
The Graymail workflow moves these unwanted emails to a dedicated folder in the user's mailbox, ensuring a well-maintained inbox and enhancing productivity.

Note - This workflow is supported only for Office 365 Mail.

To configure the graymail workflow and customize the dedicated folder name:

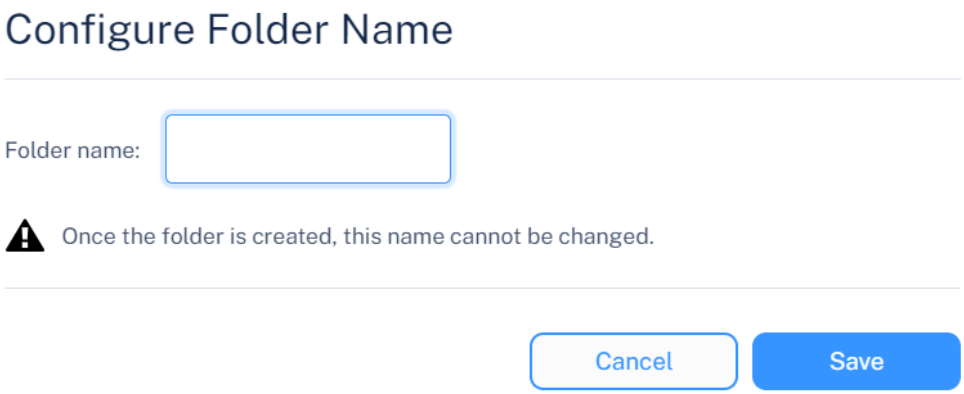
1. Access the Avanan Administrator Portal and click **Policy**.
2. Open an existing Threat Detection policy for Office 365 Mail or create a new one. See *"Threat Detection Policy for Incoming Emails" on page 150*.

   The **Edit Policy Rule** page appears.
3. Go to the **Spam** section.



4. From the **Graymail workflow** list, select the workflow:
   - **Do nothing**
   - **Same as Spam workflow**

     For more information, see *"Spam Workflows" on page 180*.
   - **Email is allowed. Deliver to Promotions folder**.
     - In the **Folder Name** field, enter the folder name. The default folder name is **Promotions**.



     The system creates a dedicated folder in the user's mailbox.
5. Click **Save**.

Graymail Dedicated Folder

When the **Email is allowed. Deliver to Promotions folder** workflow is selected, the system creates a folder with the specified name in each user's inbox assigned to the policy.

If a user deletes the folder, the system recreates it within 24-48 hours. During this period, graymail emails are delivered to the user's inbox.

For new users added to the group associated with the policy, the system creates the folder within 24-48 hours. During this period, graymail emails are delivered to their mailbox.

Notes:

- This option is available only for the **Protect (Inline)** policy mode.
- After the initial configuration, you cannot change the folder name. To modify it, contact *Avanan Support*.

Deliver to Dedicated Folder - End User Footprint

When the **Email is allowed. Deliver to Promotions folder** workflow is enabled, the following changes apply to the end user:

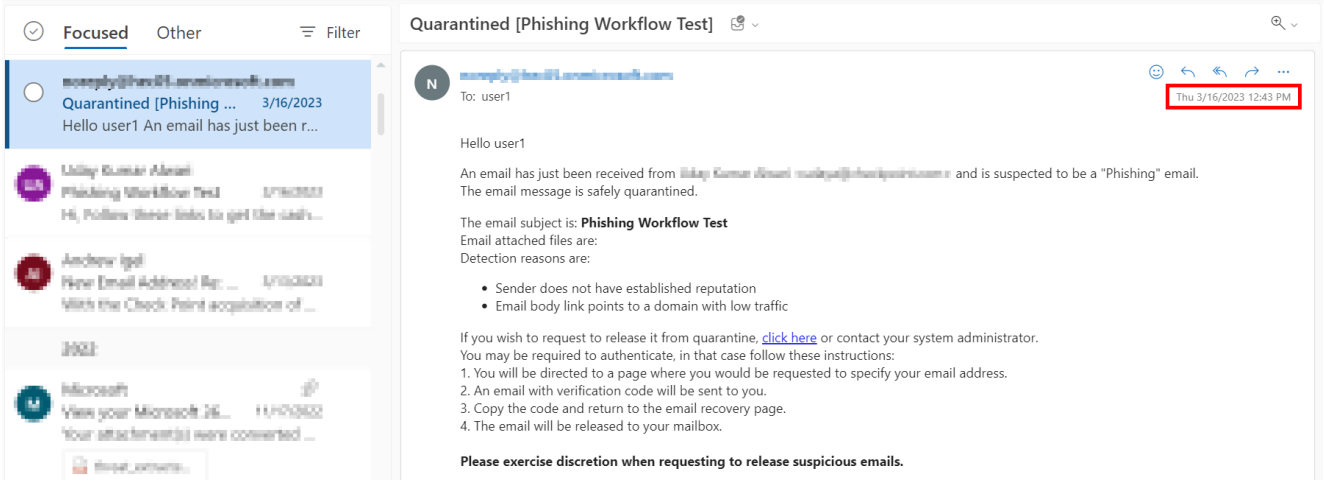
1. The system creates a dedicated folder under the user's mailbox.
2. The system adds *X-CLOUD-SEC-CP-GRAYMAIL* header to all the graymails.
3. The system applies a mailbox rule to each protected user, routing emails with the *X-CLOUD-SEC-CP-GRAYMAIL* header to the new folder.

Quarantined Emails - End-User Experience

After the administrator approves an end-user request to restore an email from quarantine, Avanan performs these actions:

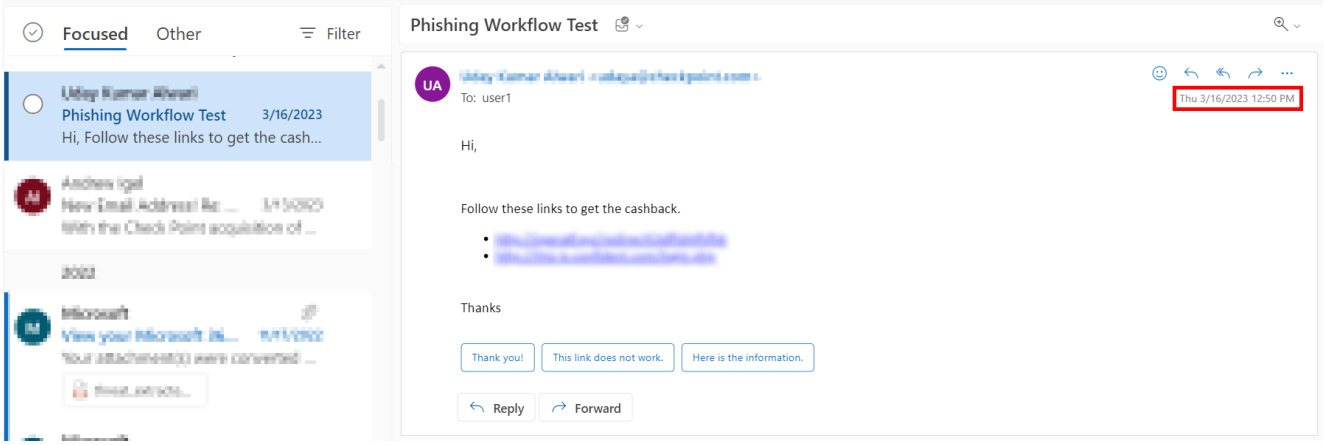
- Removes the quarantine/clean email notifications received for the quarantined email from the end-user mailbox.
- Adds the original email to the end-user mailbox, where the email received time is the restore time of the email from quarantine, but not the original email sent time.

This example shows the initial email received by the end-user.



This example shows the same email received by the end-user after the administrator approved the restore request.

Note - The initial email received by the end-user is removed and the restored email gets delivered as a new email to the end-user mailbox. The email received time is the restore time of the email by the administrator, but not the original email sent time.

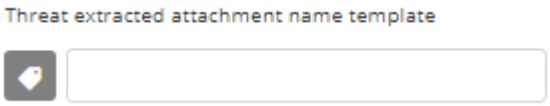


Customizing End-User Experience

Customizing Attachment Cleaning (Threat Extraction) Attachment Name

To customize Attachment Cleaning (Threat Extraction) attachment name:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Office 365 Mail or Gmail.
3. Click **Advanced** and scroll-down to **Threat extracted attachment name template**.
4. Enter the desired attachment name.



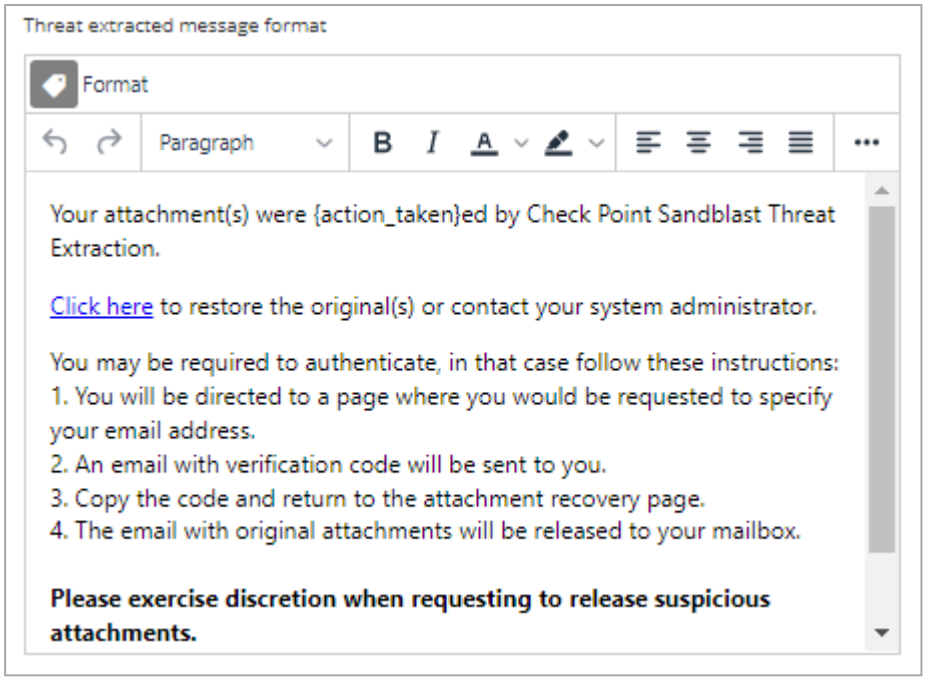
Note - By default, **threat_extracted_{original_name}** is the configured name.

5. Click **Save**.

Customizing Attachment Cleaning (Threat Extraction) Message

To customize Threat extracted message format:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Office 365 Mail or Gmail.
3. Click **Advanced** and scroll-down to **Threat extracted message format**.
4. Configure the desired format for the threat extracted message.



5. Click **Save**.

Data Loss Prevention (DLP) Policy

DLP Policy filters outgoing emails to ensure that sensitive data does not reach unauthorized recipients.

In addition, it can also filter incoming emails to ensure sensitive data is not stored in your organization's mailboxes and/or that it is shared only through authorized delivery methods.

For more details about the DLP security engine, see *"Data Loss Prevention (SmartDLP)" on page 110*.

Notes:

- DLP is not available for Avanan accounts residing in the United Arab Emirates (UAE) region. If required, you can request to enable DLP. However, sensitive data analysis will be performed in the United Kingdom (UK) and not within the borders of the UAE. If you wish to enable DLP, contact *Avanan Support*.
- If an email contains a ZIP file, Avanan recursively scans all files within the archive to detect any DLP violations.

Sync Times with Microsoft

- If you change the policy protection mode from **Monitor Only** or **Detect and Remediate** mode to **Prevent (Inline)** mode, it takes time to start protecting in **Prevent (Inline)** mode. It could take up to an hour, depending on the number of protected users in the Avanan account.

- When adding a user to the scope of a **Prevent (inline)** policy that is not set to **All Users and Groups**, it may take up to 1 hour for emails from this user to be inspected inline.
- When a new user is added to Microsoft 365, administrators can include them in the policy scope within 10 minutes or it might take up to 24 hours.

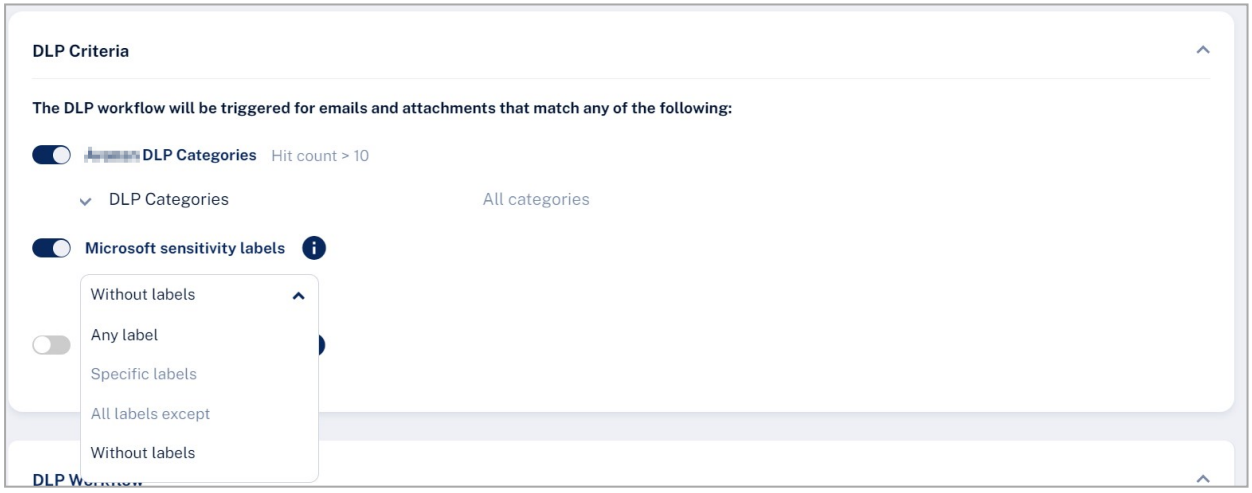
Enhanced DLP Policy using Microsoft Purview Sensitivity Labels

Avanan allows administrators to define Data Loss Prevention (DLP) policies using Microsoft Purview Sensitivity Labels, enabling effective management of sensitive data shared through emails, messages, attachments or files.

- Relevant SaaS Applications: Office 365 Mail, OneDrive, SharePoint, and Microsoft Teams.
- Supported file formats: Emails, DOCX, XLSX, PPTX, PDF.

To define Data Loss Prevention (DLP) policies using Microsoft Purview Sensitivity Labels:

1. Go to **Policy**.
2. Open an existing DLP policy or create a new one.
3. Go to the **DLP Criteria** section.
4. Enable the **Microsoft sensitivity labels** toggle button and from the list, select one of these:



   - **Any label**
   - **Specific labels** and then enter the label name
   - **All labels except** and then enter the label name
   - **Without labels**

Note - After enabling Microsoft sensitivity labels for the first time, an administrator must reauthorize the Avanan application to grant the *InformationProtectionPolicy.Read.All* permission. For more information, see Microsoft Graph permissions reference - Microsoft Graph | Microsoft Learn

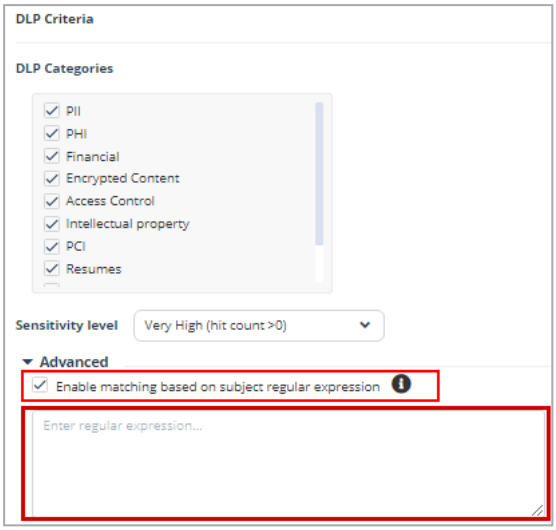
5. To include the email and attachment without labels, select the **Include emails/attachments without labels** checkbox.
6. Click **Save and Apply**.

DLP Policy for Outgoing Emails

To configure DLP policy for outgoing emails:

1. Navigate to **Policy**.
2. Click **Add a New Policy Rule**.
3. Select the desired SaaS application under **Choose SaaS** drop-down.
4. Select **DLP** under **Choose Security** drop-down and click **Next**.
5. Select **Prevent (Inline)** or **Monitor only** protection mode.
6. Select the **Scope** of the policy:
   a. Select email direction as **Outbound** .
   b. Under **Senders**, select the **Specific Users and Groups** the policy applies to.
7. In the **DLP Criteria** section, do these:
   a. Select the required **DLP Categories**.
   b. Select the required **Sensitivity Level**. See *"DLP Policy Sensitivity Level" on page 198*.

c. If you need to add a subject regular expression as the matching criteria to the DLP policy, under **Advanced**, enable the **Enable matching based on subject regular expression** checkbox and enter the regular expression. See *"DLP Subject Regular Expression (Regex)" below*.



8. In the **DLP Workflow** section, select the required workflow. See *"DLP Workflows for Outgoing Emails" on page 193*.

   Note - This option is available only in **Prevent (Inline)** mode.

9. Select the required **Severity**.
10. Select the required **DLP Alerts**. See *"DLP Alerts for Outgoing Emails" on page 194*.
11. Click **Save and Apply**.

    Notes:
    - Applying a **Prevent (Inline)** rule could take up to an hour to take effect, depending on the number of protected users in the Avanan account.
    - If you get **Manual Changes Required** message while creating a **Prevent (Inline)** DLP policy for Gmail, you must make changes in the Google Admin Console. For more information, see *"Appendix B: Manual Steps for Enabling Gmail Prevent (Inline) DLP Policy" on page 578*.

For more details about the DLP security engine, see *"Data Loss Prevention (SmartDLP)" on page 110*.

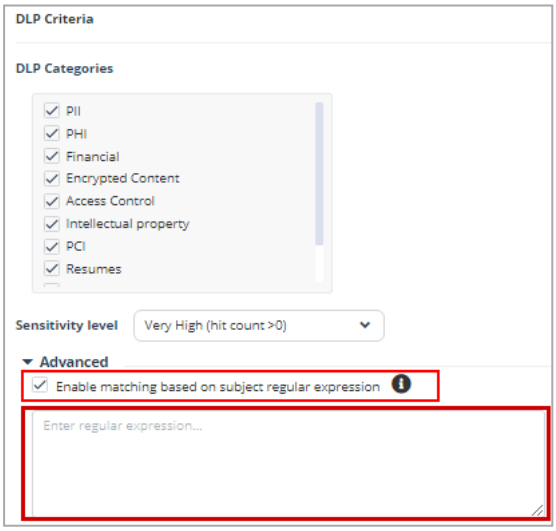
DLP Subject Regular Expression (Regex)

By default, Avanan matches emails to DLP policy rules based on the data types detected in them. However, you can use regular expressions to match emails from the email subject.

This type of matching helps you to detect sensitive emails from the email subject and allows you to trigger specific workflow. Therefore, emails with a defined subject pattern will match the DLP policy rule regardless of the data types they include.

To add a regular expression condition to a DLP policy:

1. Navigate to **Policy**.
2. To add the regular expression to an existing DLP policy, click the policy and continue from step 6.
3. To create a new DLP policy, click **Add a New Policy Rule**.
4. Select the desired SaaS application under **Choose SaaS** drop-down.
5. Select **DLP** under **Choose Security** drop-down and click **Next**.
6. Select **Prevent (Inline)** or **Monitor only** protection mode.
7. Select the **Scope** of the policy:
    a. Select email direction as **Outbound** .
    b. Under **Senders**, select the **Specific Users and Groups** the policy applies to.
8. In the **DLP Criteria** section, do these:
    a. Select the required **DLP Categories**.
    b. Select the required **Sensitivity Level**. See *"DLP Policy Sensitivity Level" on page 198*.
    c. In **Advanced**, select the **Enable matching based on subject regular expression** checkbox.



    d. Enter the regular expression. See *"Subject Regular Expressions Syntax" on the next page*.
9. Click **Save and Apply**.

Subject Regular Expressions Syntax

The **Subject Regular Expression** field allows you to enter values in the *Python Regular Expressions (RE)* syntax.

For example, to create a DLP policy rule to find emails that contains the string **[secure]** in the email subject, add **(?i)\[secure] or \[secure]** where **(?i)** is used to specify that it is case insensitive to the **Subject Regular Expression** field in the policy.

To create a DLP policy rule to find emails that contain either the exact strings **[secure]** or **[encrypt]** in the email subject, you can add either **\[secure\]|\[encrypt\]** or **ex \[secure]|\[encrypt]** to the **Subject Regular Expression** field in the policy.

For more information, see Python regular expressions documentation.

The symbols for the start (**^**) and end (**$**) of a line are not supported.

To create a DLP policy rule that detects emails containing the exact word **sec** in the email body (but not words like **Security** or **Seconds**), regardless of whether it's at the beginning of a sentence or separated by spaces or tabs, you can use the boundary marker **\b**. For example, use **\bsec\b**.

DLP Workflows for Outgoing Emails

Note - The workflows are available only in **Prevent (Inline)** mode.

Workflow	Description
Email is blocked. User is alerted and allowed to request a restore (admin must approve)	Any detected email will not be delivered to the recipient and will be moved to quarantine mailbox. 1. The user receives an email with an alert of the quarantine action. 2. To view the original email, the user must request to restore the email. 3. An administrator must approve the request.
Email is blocked. User is alerted and allowed to restore the email	Any detected email will not be delivered to the recipient and will be moved to quarantine mailbox. 1. The user receives an email with an alert of the quarantine action. 2. The user can restore the original email without any administrator approval.
Email is allowed. Header is added to the email	Any detected email will be delivered to the recipient with additional header that is configured in the policy.
Do nothing	Any detected email will be delivered to the recipient without any changes.

Workflow	Description
Microsoft Encryption Workflows	
Email is blocked and user can resend as encrypted by Microsoft	Any detected email will not be delivered to the recipient and the user can resend the email as Microsoft encrypted email.
Email is allowed. Encrypted by Microsoft	Any detected email will be delivered to the recipient as encrypted by Microsoft and a header will be added to the email. For more information, see *"Microsoft Encryption for Outgoing Emails" on page 216*.
Email is blocked and user can request to resend as encrypted by Microsoft (admin must approve)	Any detected email will not be delivered to the recipient and will be moved to quarantine mailbox. 1. The user receives an email with an alert of the quarantine action. 2. The user can request to resend as Microsoft encrypted email. 3. An administrator must approve the request.
Avanan Email Encryption Workflows	
Email is blocked and user can resend as encrypted by Email Encryption	Any detected email will not be delivered to the recipient and the user can resend the email as Avanan Email Encryption email.
Email is allowed. Encrypted by Email Encryption	Any detected email will be vaulted by Avanan Email Encryption and the recipient receives a email notification. For more information, see *"Encrypting Outgoing Emails" on page 215*.
Email is blocked and user can request to resend as encrypted by Email Encryption (admin must approve)	Any detected email will not be delivered to the recipient and will be moved to quarantine mailbox. 1. The user receives an email with an alert of the quarantine action. 2. The user can request to resend as Avanan Email Encryption email. 3. An administrator must approve the request.

To create Allow-List for DLP, see *"DLP Exceptions" on page 322*.

DLP Alerts for Outgoing Emails

You can configure alerts for outgoing emails detected as violating a DLP policy:

- Send email alert to admins when a DLP policy is violated.
- Send email alert to specific recipients when DLP is detected. It is possible to customize email template using the gear icon next to the action.
- Send email alert to the direct manager when an employee sends (or attempts to send) confidential data that violates a DLP policy.

  Notes:
  - When this option is enabled, the email alerts are sent to the manager even when the email is blocked.
  - This option is available only for Office 365 DLP policies.
- Send email alert to the sender when **DLP Subject Regex** pattern and DLP is detected in the email. For details, see *"DLP Subject Regular Expression (Regex)" on page 191*.
- Send email alert to the sender when **DLP Subject Regex** pattern is not detected but DLP is detected in the email. For details, see *"DLP Subject Regular Expression (Regex)" on page 191*.

Prerequisites to Avoid Failing SPF Checks

For Office 365 Mail, if you enable **Protect (Inline) Outgoing Traffic** in the DLP or Threat Detection policy, Avanan gets added to the email delivery chain before reaching external recipients (*Internal email sender > Microsoft 365 > Avanan > Microsoft 365 > External recipient*).

The recipient's email security solution sees the Avanan IP address as part of the delivery chain. If the recipient's email security solution fails to recognize the original IP address, it may consider the Avanan IP address as the IP address from which the email was sent.

If you do not configure the SPF record in your DNS to allow Avanan IP addresses to send emails on behalf of your domain, your emails might fail SPF checks and may be quarantined.

Check Point recommends you add the Avanan IP addresses to your SPF record before you enable **Protect (Inline) Outgoing Traffic** for outgoing emails.

To prevent outgoing emails from failing SPF checks and being quarantined, you must add `include:spfa.cpmails.com` to your SPF record.

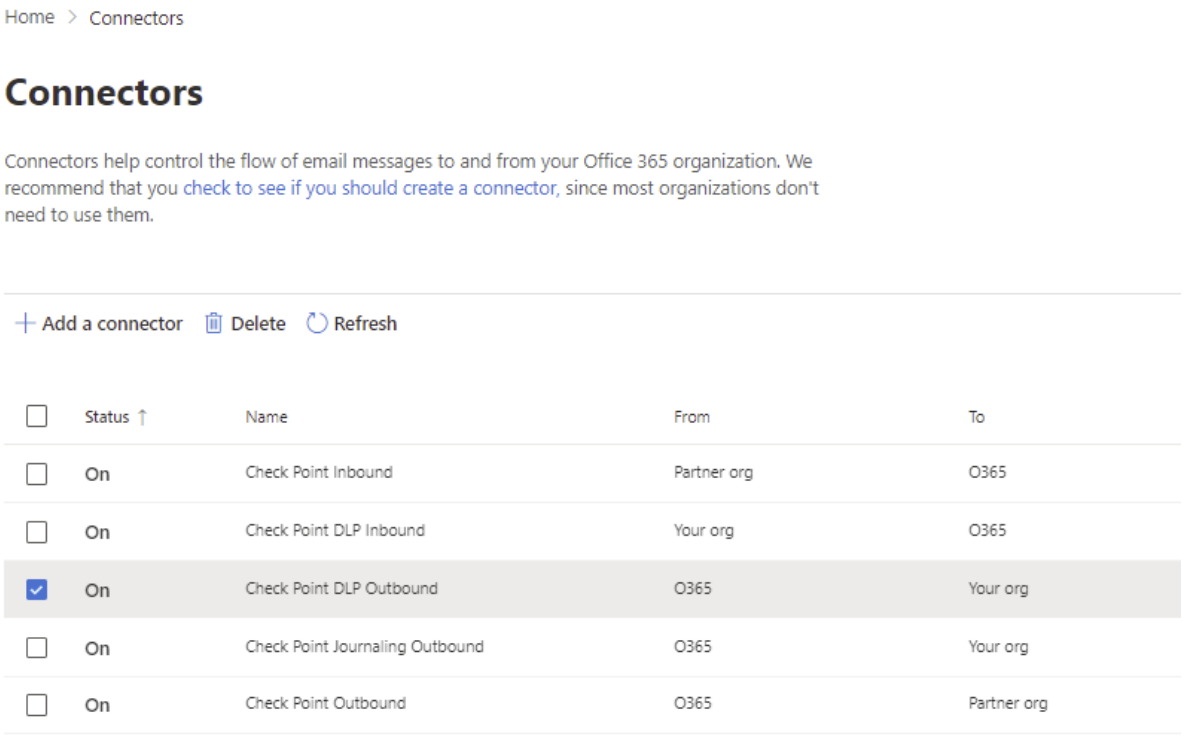
Note - The above statement includes several IP addresses and networks, some outside your Avanan portal's data region. This is done for uniformity and consistency in all Check Point SPF records regardless of your data region. Avanan sends the emails only from one of the IP addresses in your region.

Outgoing Email Protection - Office 365 Footprint for DLP

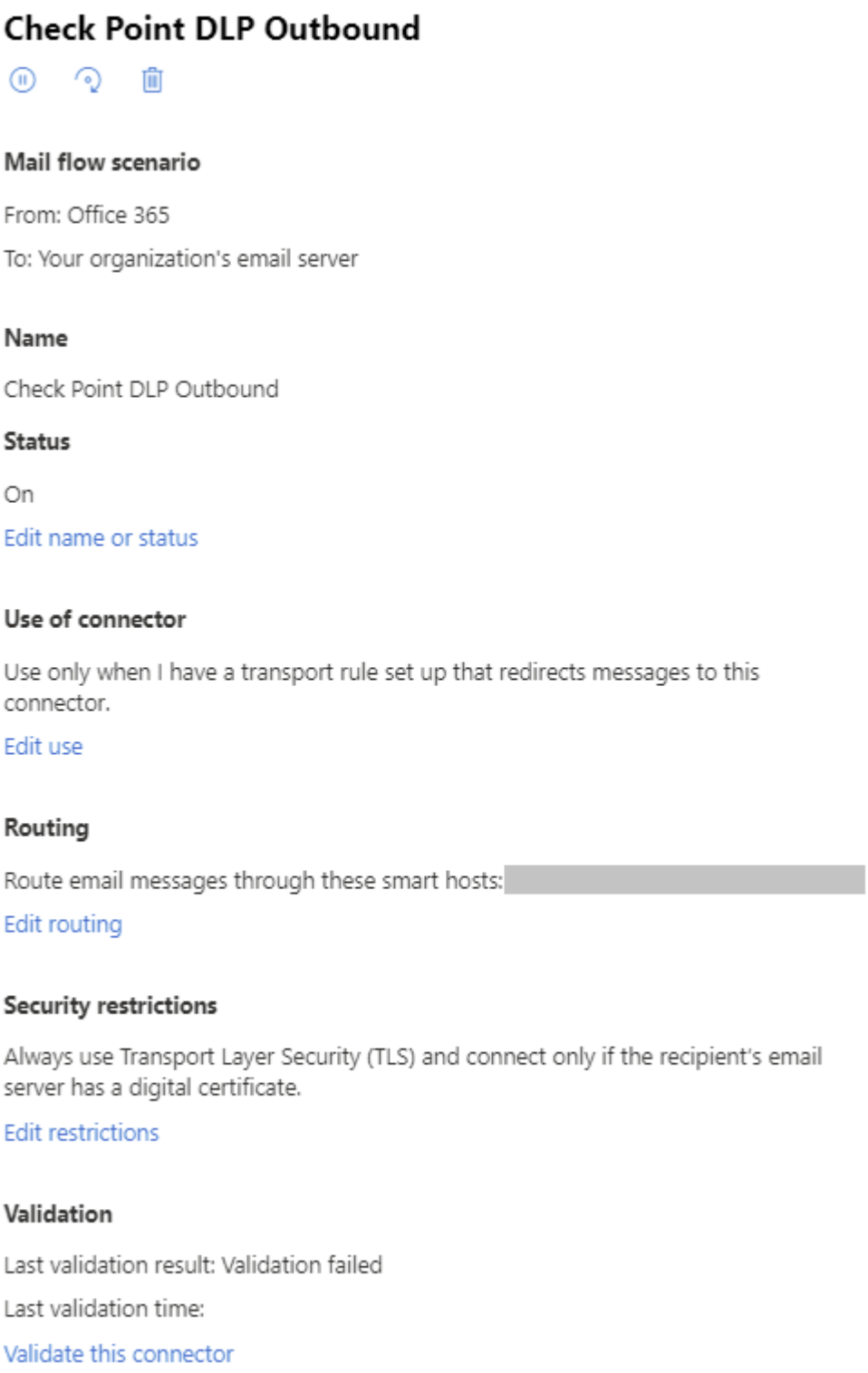
Transport rules

Additional transport rule is created when enabling Inline DLP.

- Rule name: Avanan DLP Outbound
- Rule:



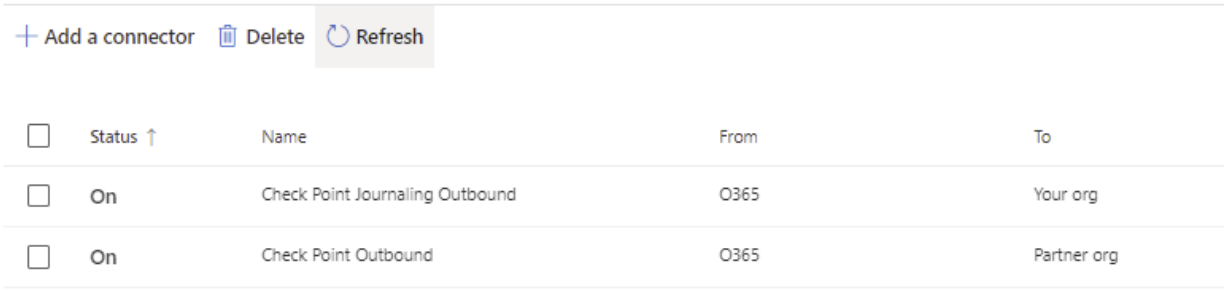
- Rule description:



Connectors

Additional connector will be added, Avanan to Office 365.

- Connector:



DLP Policy Sensitivity Level

The **Sensitivity Level** for a DLP policy is the minimum number of times all the Data Types in the selected categories need to match (hit count) for the policy to trigger the DLP workflow.

You can select these **Sensitivity Level** for every policy rule.

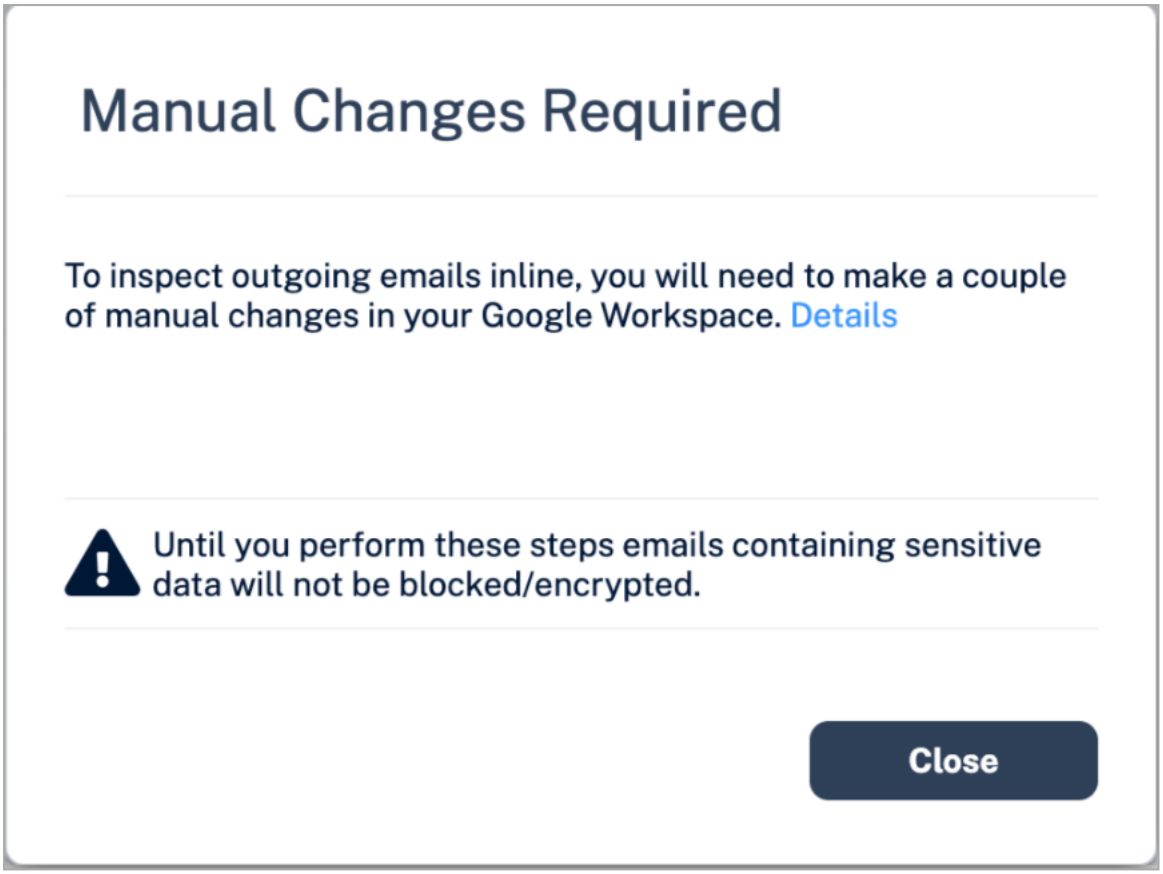
- Very High (hit count > 0)
- High (hit count > 2)
- Medium (hit count > 5)
- Low (hit count > 10)
- Very Low (hit count > 20)
- Custom (and enter the minimum hit count (**Hit count higher than**) required for the policy)

For example, a DLP policy includes only the PII category and you selected the **Sensitivity Level** as **High**.

- If all the Data Types in PII were matched only once - the rule does not trigger the selected DLP workflow.
- If all the Data Types in PII were matched three times - the rule triggers the selected DLP workflow.

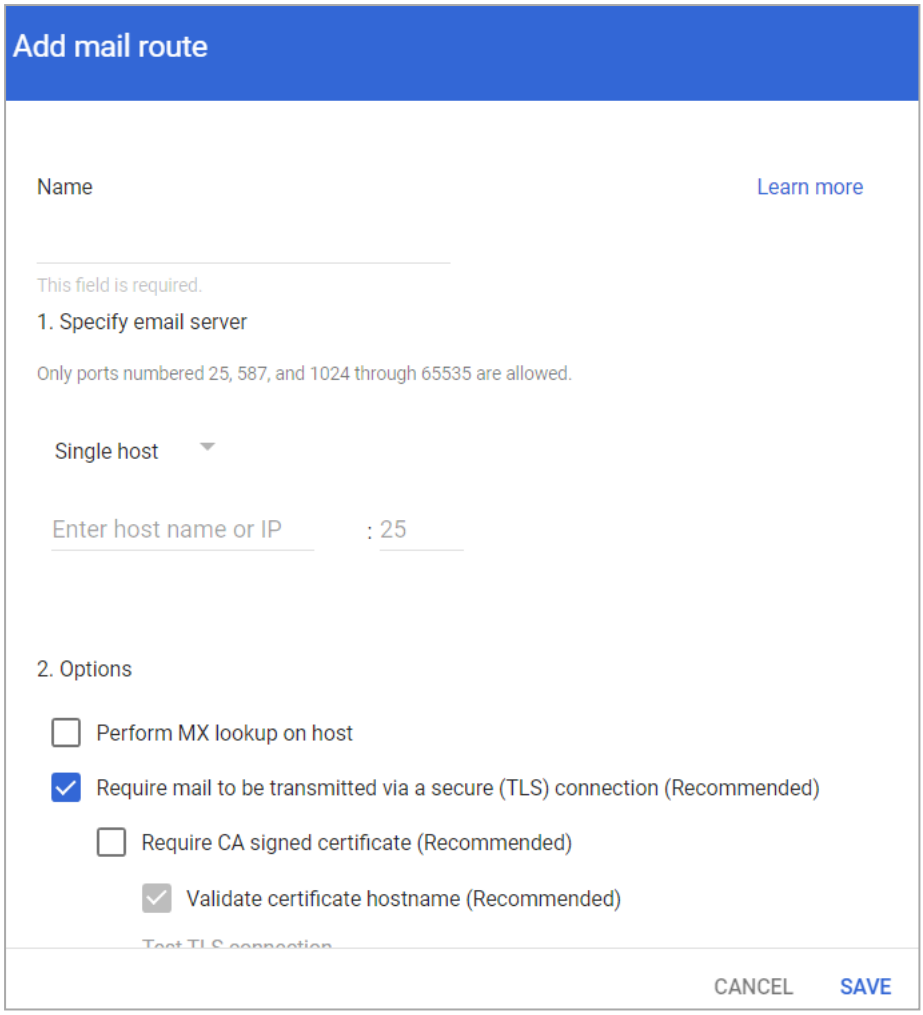
Appendix B: Manual Steps for Enabling Gmail Prevent (Inline) DLP Policy

If you receive the **Manual Changes Required** message while creating a **Prevent (Inline)** DLP policy for Gmail, you must make these changes in the Google Admin Console.



Step 1: Adding a Host

1. Sign in to the Google Admin Console.
2. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
3. Click **Hosts**.
4. Click **Add Route**.
5. Under **Name**, enter **CLOUD-SEC-AV DLP Service**.



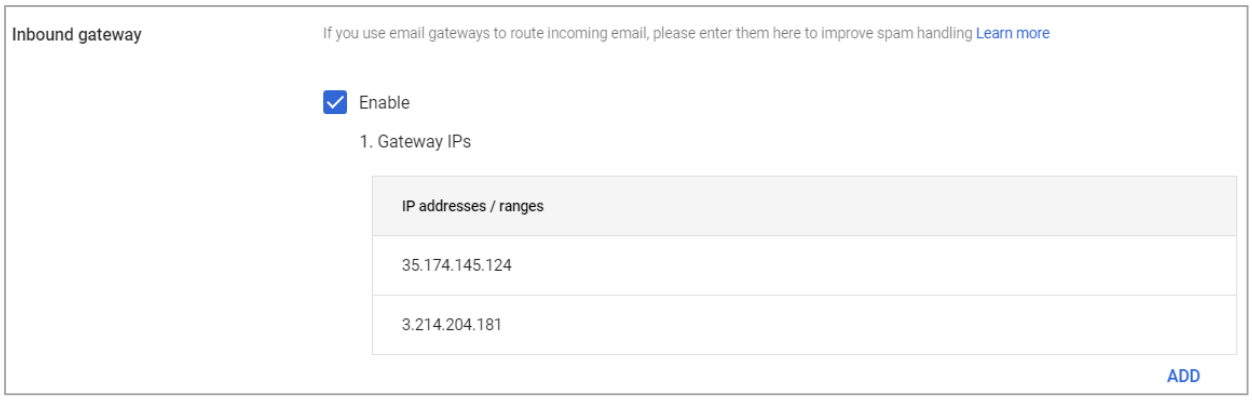
6. Under **Specify email server**, select **Single host**.
7. Enter the host name as **[portal identifier]-dlp.avanan.net**.

   To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.
8. Enter the port number as **25**.
9. Under **Options**, clear the **Require CA signed certificate** checkbox.
10. Click **Save**.

Step 2: Updating Inbound Gateway

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll down and click **Spam, Phishing and Malware**.
3. Click **Inbound gateway**.
4. Select **Enable** and under **Gateway IPs**, click **Add** and enter the IP address or IP address range relevant to your Avanan tenant (account) region.

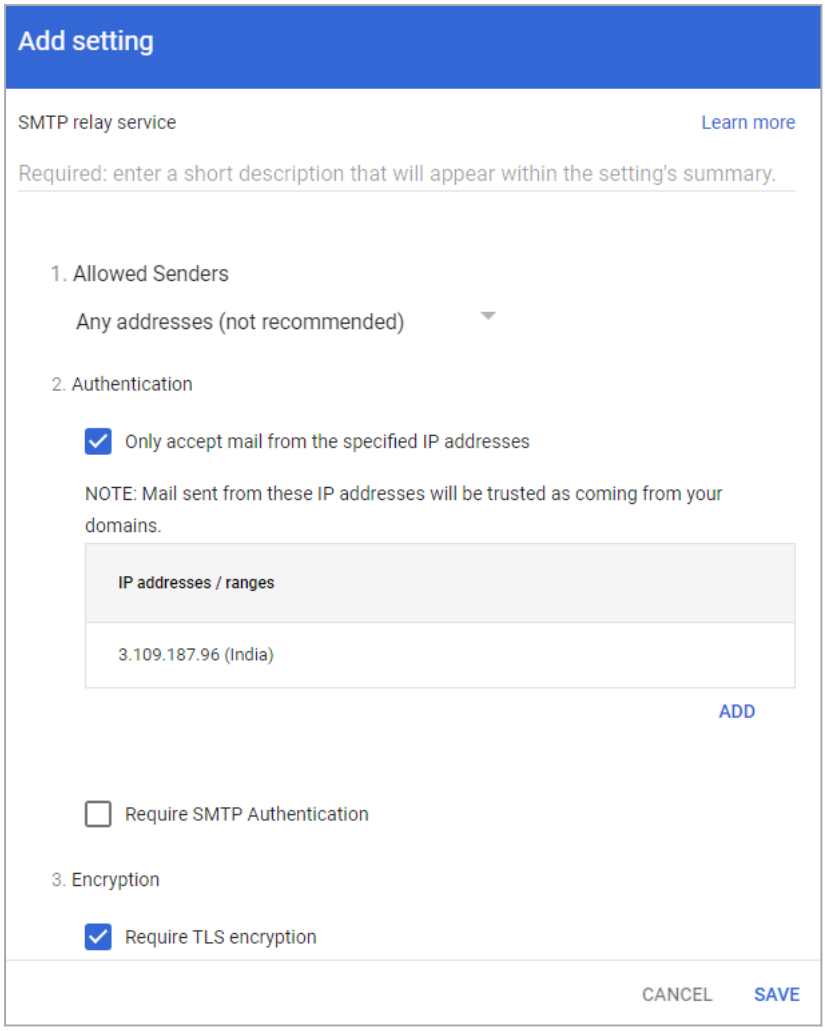
For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 211*.



5. Click **Save**.

Step 3: Adding SMTP Relay Host

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll-down and click **Routing**.
3. Under **SMTP relay service**, click **Add Another Rule**.
4. Enter a description for the rule.



5. In the **Allow Senders** list, select **Any Addresses** checkbox.
6. Under **Authentication**, do these:

a. Select the **Only accept mail from the specified IP addresses** checkbox.

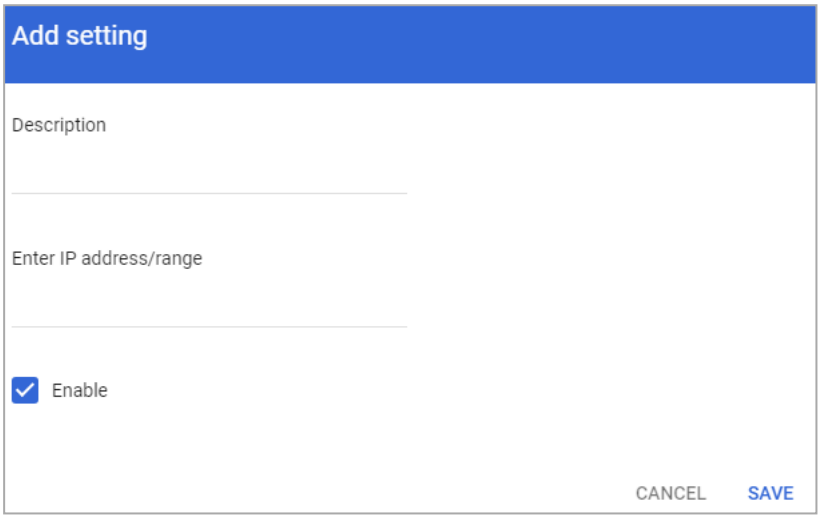
b. Add all the IP addresses relevant to your Avanan tenant (account) region.

For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 211*.

To add an IP address:

i. Click **Add**.

ii. Enter a **Description** for the IP address.



iii. Enter the IP address.

iv. Select the **Enable** checkbox.

v. Click **Save**.

c. Clear the **Require SMTP Authentication** checkbox.

7. Under **Encryption**, select the **Require TLS encryption** checkbox.

8. Click **Save**.

Step 4: Add Groups

You must create two groups.

- avanan_inline_outgoing_policy
- avanan_monitor_outgoing_policy

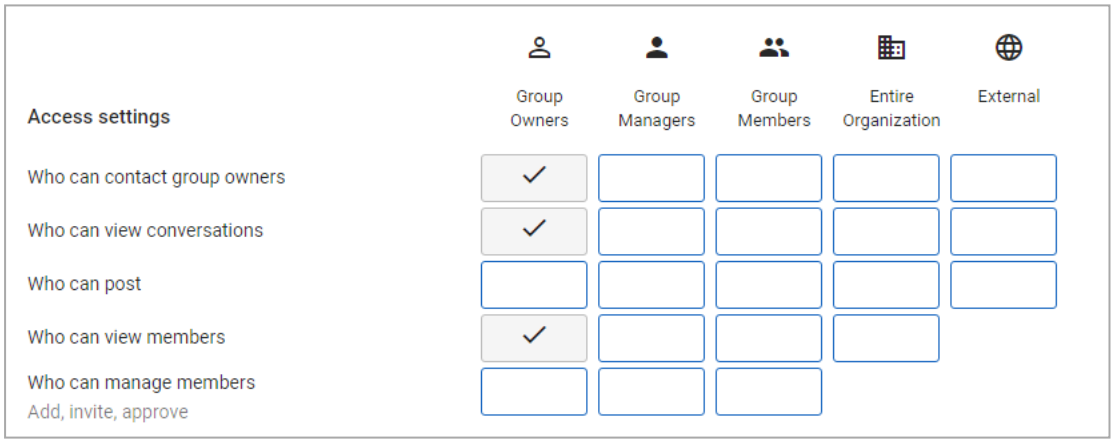
Note - If you use GCDS (Google Cloud Directory Sync) to synchronize your user groups on-premises and in the cloud, the synchronization triggers the deletion of these Avanan groups. Though this will not impact the email delivery, Avanan cannot scan the emails, and no security events get generated.

Before activating Google Workspace, you must create exclusion rules for these user groups. Select the exclusion type as **Group Email Address**, match type as **Exact Match**, and the group email address should be in the *groupname@[domain]* format.

For example, the group email addresses should be **avanan_inline_outgoing_policy@mycompany.com** and **avanan_monitor_outgoing_policy@mycompany.com**, where mycompany is the name of your company.

To create a group:

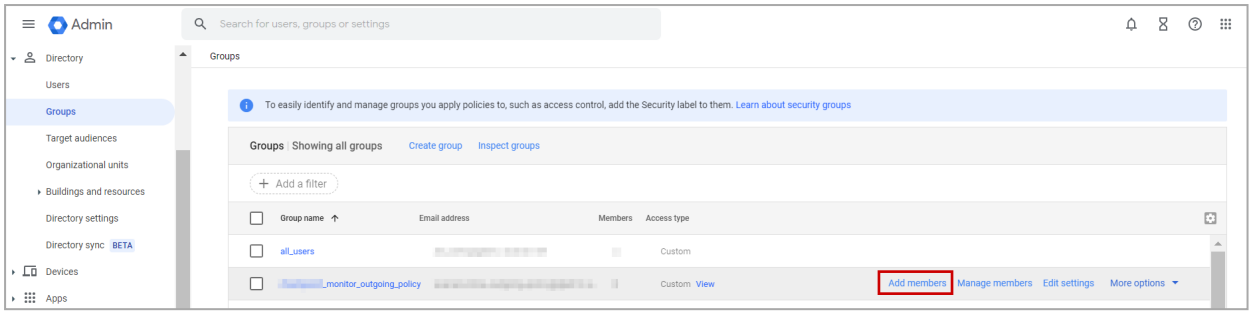
1. From the left navigation panel, click **Directory** > **Groups**.
2. Click **Create Group**.
3. In **Group name** field, enter the group name. For example, **avanan_inline_outgoing_policy**.
4. In **Group email** field, enter the group email. For example, **avanan_inline_outgoing_policy**.
5. Click **Next**.
6. In **Access Settings**, clear everything except the default settings.



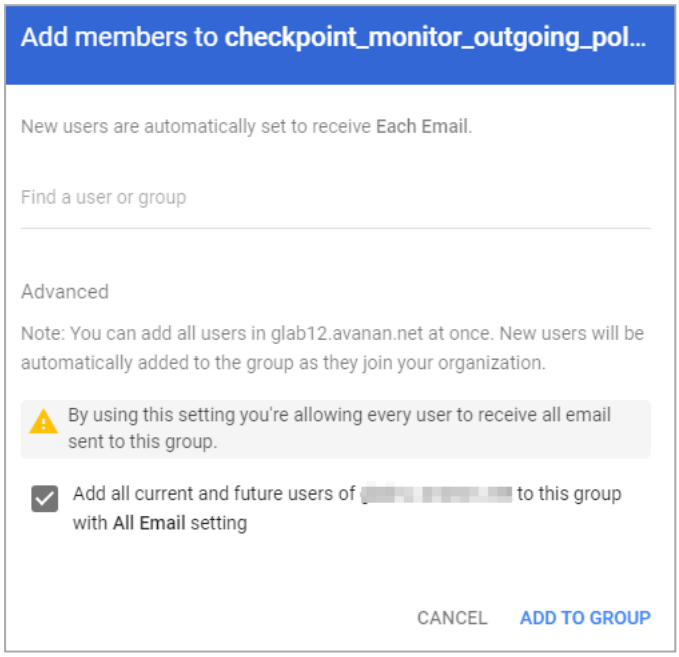
7. In **Who can join the group**, select **Anyone in the organization can join**.
8. Click **Create Group**.
9. Repeat the same procedure and create a group with **Group name** and **Group email** as **avanan_monitor_outgoing_policy**.

After creating the groups, you must do these to the **avanan_monitor_outgoing_policy** group.

1. From the left navigation panel, click **Directory** > **Groups**.
2. Hover over the **avanan_monitor_outgoing_policy** group you created and click **Add members**.



3. Click **Advanced** and select the **Add all current and future users of {domain} to this group with All Email setting** checkbox.



4. Click **Add to Group**.

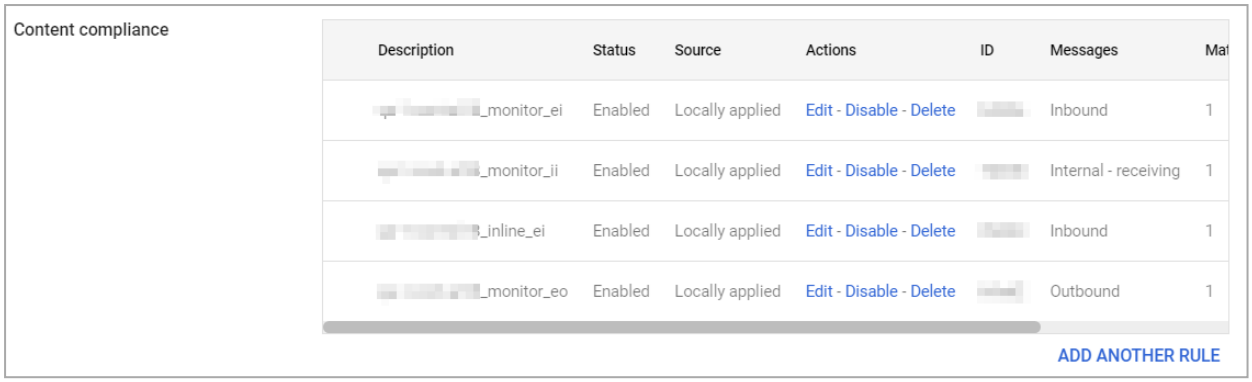
Step 5: Create a Compliance Rule

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll-down and click **Compliance**.

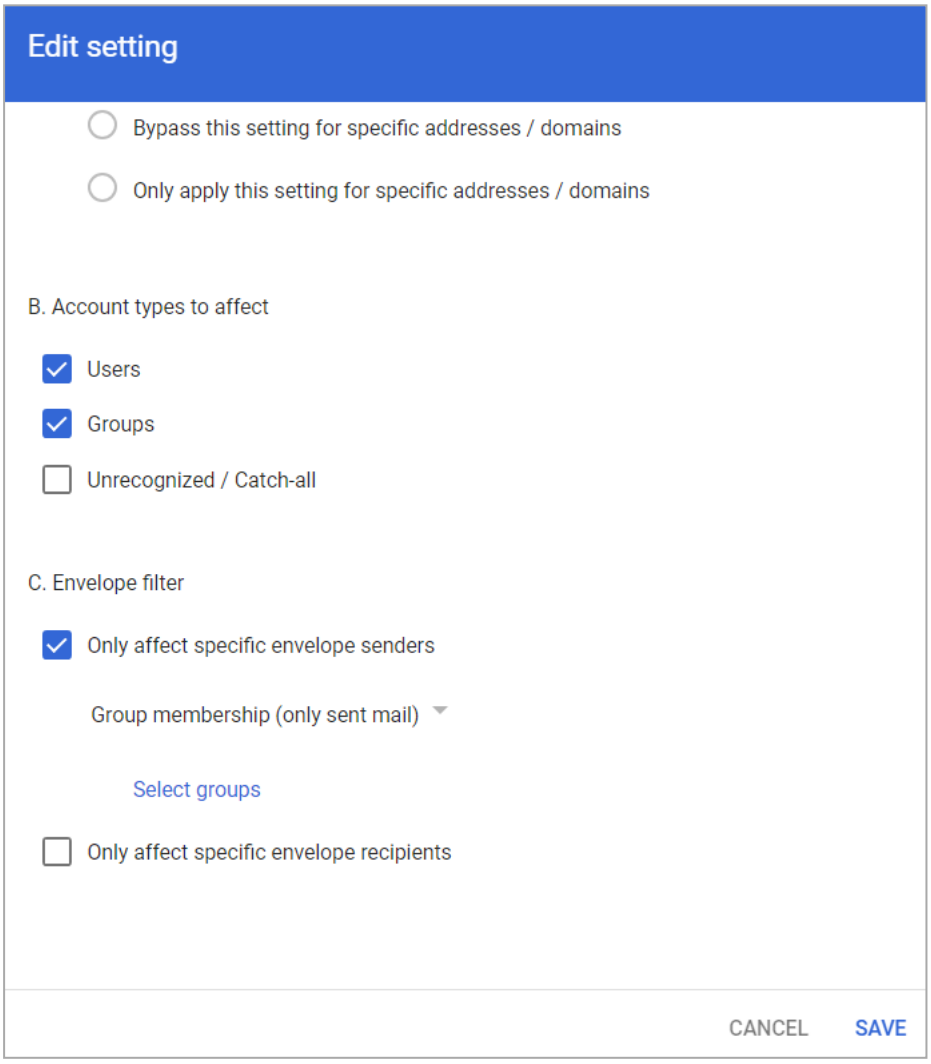
   By default, the system shows these rules in **Content compliance**:

   - [portal identifier]_monitor_ei
   - [portal identifier]_monitor_ii
   - [portal identifier]_monitor_eo
   - [portal identifier]_inline_ei

   To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.



3. Update the settings for **[portal identifier]_monitor_eo** rule.
    a. For **[portal identifier]_monitor_eo** rule, click **Edit**.
    b. Scroll-down to the end of the **Edit setting** pop-up and click **Show options**.
    c. Under **Envelope filter**, select the **Only affect specific envelope senders** checkbox.



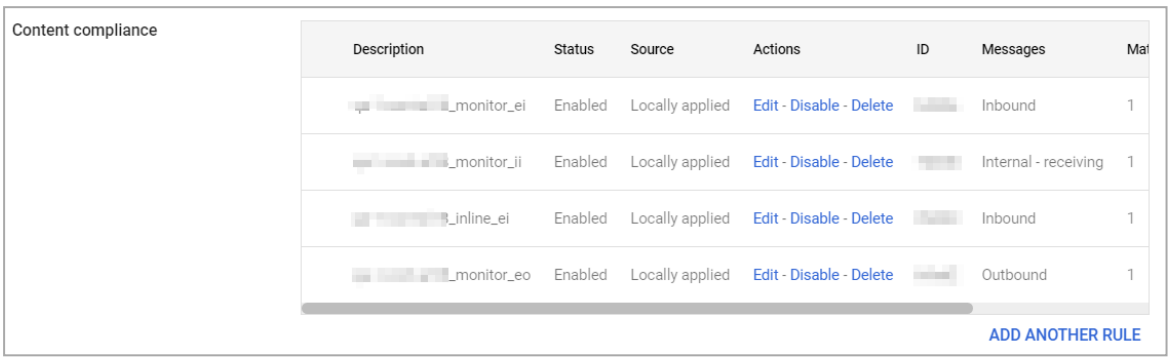
d. From the list, select **Group membership (only sent mail)**.

e. Click **Select groups** and select **avanan_monitor_outgoing_policy**.

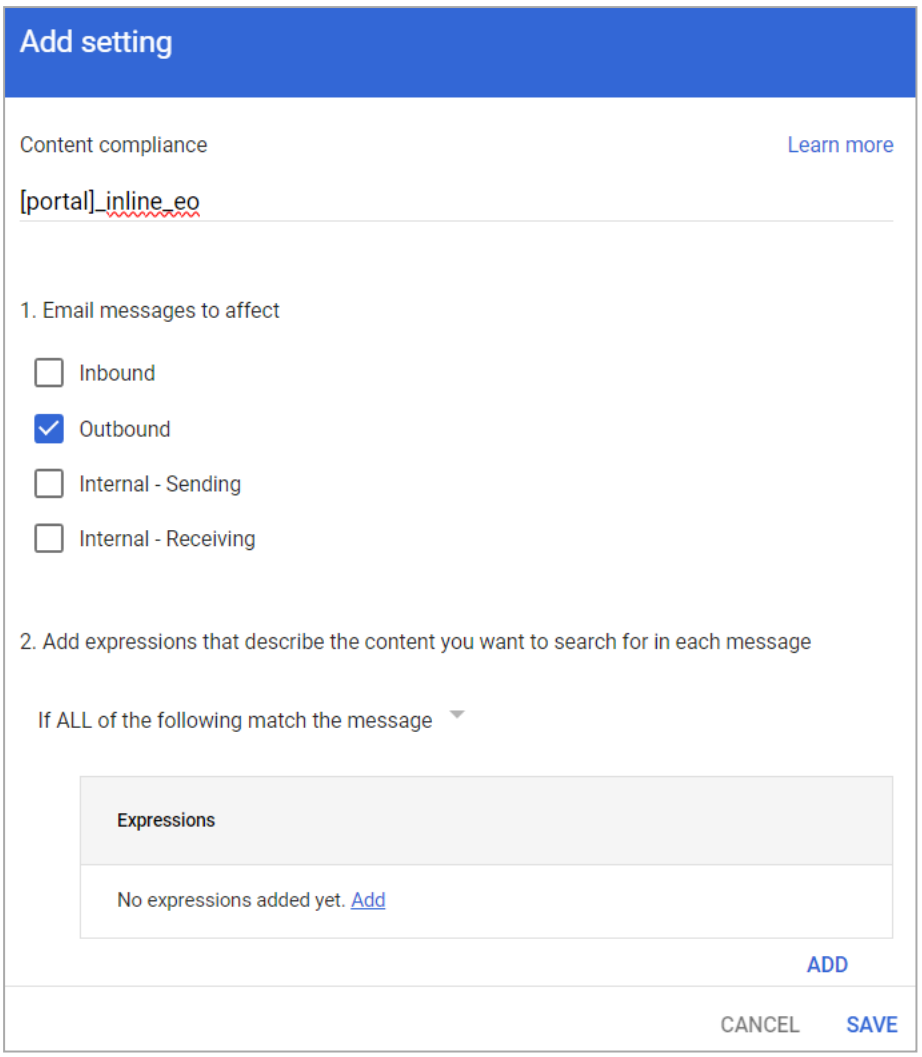
f. Click **Save**.

4. Create the **[portal identifier]_inline_eo** rule with these settings:

a. From the **Content compliance** rules, click **Add Another Rule**.



b. Enter the **Content compliance** rule name as **[portal identifier]_inline_eo**.



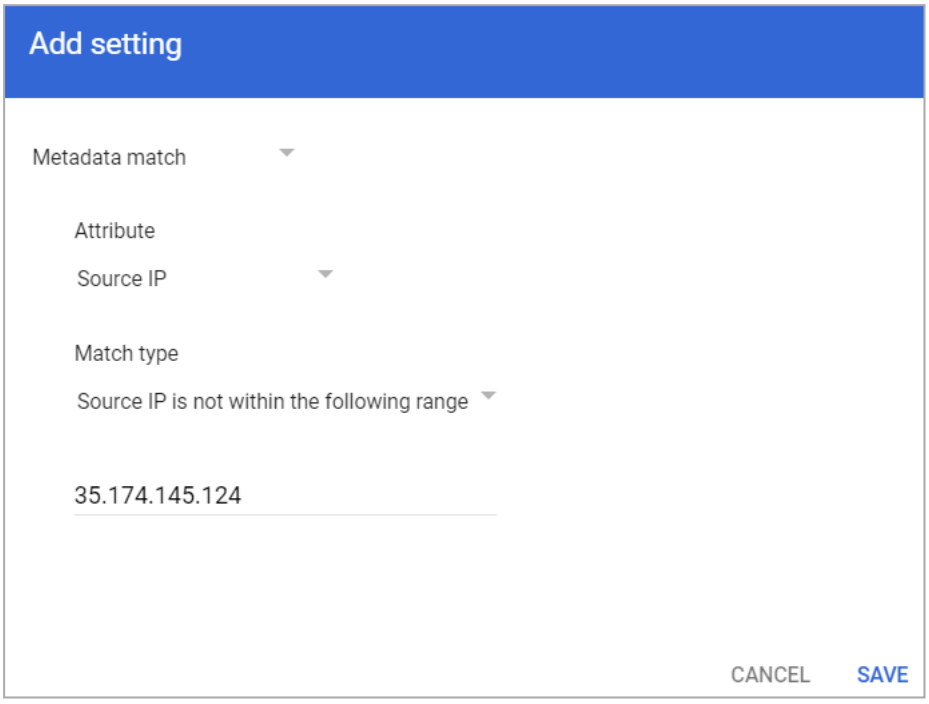
To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.

c. Under **Email messages to affect**, do these:

   i. Select **Outbound** checkbox.

   ii. In **Add expressions that describe the content you want to search for in each message**, select **If ALL of the following match the message**.

   iii. Click **Add**.



   iv. In the **Add setting** pop-up, select **Metadata match**.

   v. Under **Attribute**, select **Source IP**.

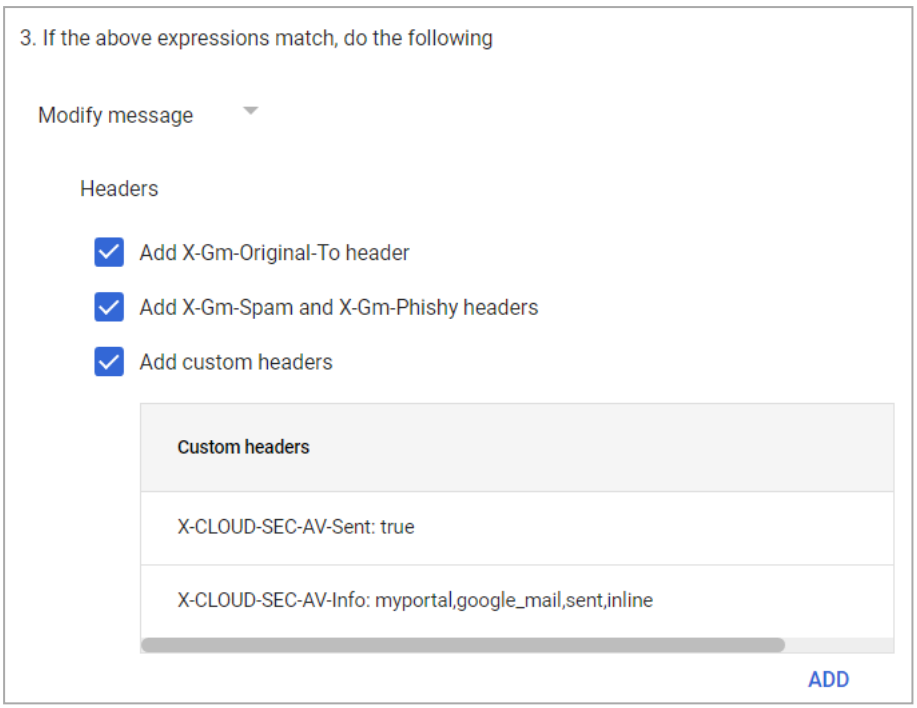
   vi. Under **Match type**, select **Source IP is not within the following range**.

   vii. Enter all the IP addresses relevant to your data region.

   For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 211*.

   viii. Click **Save**.

d. Under **If the above expressions match, do the following**, do these:



i. Select **Modify message**.

ii. Under **Headers**, do these:

i. Select **Add X-Gm-Original-To header** checkbox.

ii. Select **Add X-Gm-Spam and X-Gm-Phishy headers** checkbox.

iii. Select **Add custom headers** checkbox and add custom headers with these values.

Header Key	Header Value
CLOUD-SEC-AV-Sent	true
CLOUD-SEC-AV-Info	[portal],google_mail,sent,inline

To add a custom header:

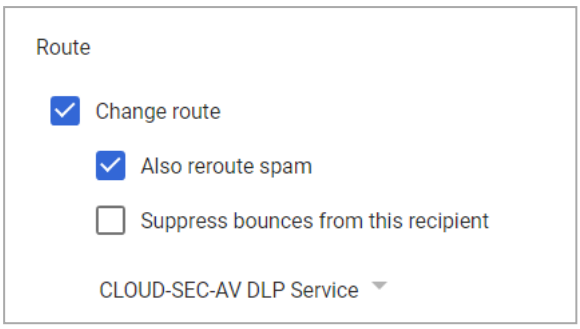
i. Click **Add**.

ii. In **Header key**, enter the header key.

iii. In **Header value**, enter the header value.

iv. Click **Save**.

iii. Under **Route**, do these:



i. Select the **Change route** checkbox.

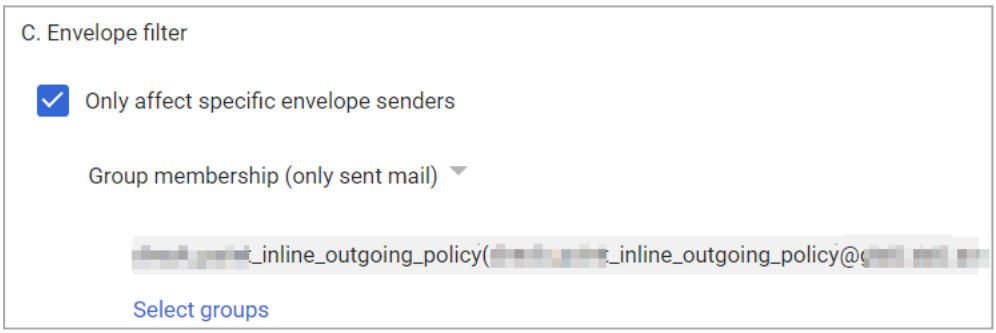
ii. Select the **Also reroute spam** checkbox.

iii. In the list, select **CLOUD-SEC-AV DLP Service**.

e. Scroll-down to the end of the page and click **Show options**.

f. Under **Account types to affect**, select **Users** and **Groups** checkbox.

g. Under **Envelope filter**, do these:



i. Select the **Only affect specific envelope senders** checkbox.

ii. From the list, select **Group membership (only sent mail)**.

iii. Click **Select groups** and select **avanan_inline_outgoing_policy**.

iv. Click **Save**.

IP Addresses Supported Per Region

- **United States**
  - 35.174.145.124
  - 3.214.204.181
  - 44.211.178.96/28
  - 44.211.178.112/28
  - 3.101.216.128/28

- 3.101.216.144/28

- **Australia**
  - 13.211.69.231
  - 3.105.224.60
  - 3.27.51.160/28
  - 3.27.51.176/28
  - 18.143.136.64/28
  - 18.143.136.80/28
- **Canada**
  - 15.222.110.90
  - 52.60.189.48
  - 3.99.253.64/28
  - 3.99.253.80/28
  - 3.101.216.128/28
  - 3.101.216.144/28
- **Europe**
  - 52.212.19.177
  - 52.17.62.50
  - 3.252.108.160/28
  - 3.252.108.176/28
  - 13.39.103.0/28
  - 13.39.103.23/28
- **India ***
  - 3.109.187.96
  - 43.204.62.184
  - 43.205.150.240/29
  - 43.205.150.248/29
  - 18.143.136.64/28

- 18.143.136.80/28

These regions are relevant only for tenants created using the Avanan MSP Portal.

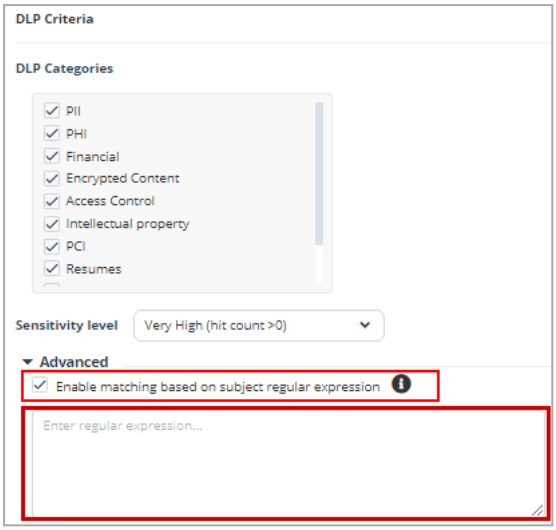
- **United Arab Emirates**
  - 3.29.194.128/28
  - 3.29.194.144/28
- **United Kingdom**
  - 13.42.61.32
  - 13.42.61.47
  - 13.42.61.32/28
  - 13.42.61.47/28
  - 13.39.103.0/28
  - 13.39.103.23/28

DLP Policy for Incoming Emails

To configure DLP policy for incoming emails:

1. Navigate to **Policy**.
2. Click **Add a New Policy Rule**.
3. Select the desired SaaS application under **Choose SaaS** drop-down.
4. Select **DLP** under **Choose Security** drop-down and click **Next**.
5. Select **Prevent (Inline)** mode.
6. Select the **Scope** of the policy:
   a. Select email direction as **Inbound**.
   b. Under **Senders**, select the **Specific Users and Groups** the policy applies to.
7. In the **DLP Criteria** section, do these:
   a. Select the required **DLP Categories**.
   b. Select the required **Sensitivity Level**. See *"DLP Policy Sensitivity Level" on page 198*.

c. If you need to add a subject regular expression as the matching criteria to the DLP policy, under **Advanced**, enable the **Enable matching based on subject regular expression** checkbox and enter the regular expression. See *"DLP Subject Regular Expression (Regex)" on page 191*.



8. In the **DLP Workflow** section, select the required workflow. See *"DLP Workflows for Incoming Emails" below*.
9. Select the required **Severity**.
10. Select the required **DLP Alerts**. See *"DLP Alerts for Incoming Emails" on the next page*.
11. Click **Save and Apply**.

Note - Applying a **Prevent (Inline)** rule could take up to an hour to take effect, depending on the number of protected users in the Avanan account.

For more details about configuring the DLP engine, see *"Data Loss Prevention (SmartDLP)" on page 110*.

DLP Workflows for Incoming Emails

Workflow	Description
Email is blocked. User is alerted and allowed to request a restore (admin must approve)	Detected email will not be delivered to the recipient and will be moved to quarantine mailbox. The user will receive an email with an alert of the quarantine action, and will be able to request to restore the original email (send the original email to the recipient).
Email is blocked. User is alerted and allowed to restore the email	Any detected email will not be delivered to the recipient and will be moved to quarantine mailbox; the user will receive an email with alert of the quarantine action, and will be able to restore the original email (send the original email to the recipient).

Workflow	Description
Do nothing	Any detected email will be delivered to the recipient without any changes.
User receives the email with a warning	The email is delivered to the user with a warning banner inserted in the body of the email. To customize the banner (text, background color etc.), click the gear icon next to the workflow.
Email is allowed. Header is added to the email	The detected email is delivered to the recipient with an additional header that can be configured in the policy.
Email is blocked. User is not alerted (admin can restore)	Detected email will not be delivered to the recipient and is automatically quarantined without any user notification. The administrator can restore the email.

To create Allow-List for DLP, see *"DLP Exceptions" on page 322*.

DLP Alerts for Incoming Emails

You can configure alerts for incoming emails detected to contain a DLP violation:

- Send alert on this violation to specific mailboxes.
- Send email alerts to admins.
- Alert the external sender about the violation when the email is quarantined.

Encrypting Outgoing Emails

Organizations often opt to encrypt outgoing emails to share sensitive information securely with the intended recipients while preventing access to others.

Avanan supports these two methods of secure email transmission:

- Microsoft 365 Email Encryption
- Avanan Email Encryption

Selecting between Avanan Email Encryption and Microsoft 365 Email Encryption

When deciding between Microsoft 365 Email Encryption and Avanan Email Encryption, consider these factors:

- **Maintaining user experience** - If you already use Microsoft 365 Email Encryption, triggering it through the Avanan DLP policy might be a good idea to have the same experience for your end users and external recipients.

- **Price and quality** - If you are unsatisfied with Microsoft 365 Email Encryption regarding price or quality, Avanan Email Encryption is highly recommended.

Microsoft Encryption for Outgoing Emails

Microsoft 365 provides the ability to encrypt the outgoing emails using Microsoft 365 Email Encryption. Encryption can be applied automatically for emails detected as sensitive by the DLP engine.

Note - The Microsoft 365 Email Encryption is available only for the outgoing emails.

For more information about the Microsoft 365 encryption mechanism, see the Microsoft Documentation.

Required License for Encrypting Outgoing Emails

In **Monitor only** mode, you can use the existing license of Office 365 as the minimum requirement. However if you want to use Microsoft Encryption as an action in policy, you must have license with Office 365 Message Encryption (OME) capabilities. For more details, see Microsoft plans with OME capabilities and Microsoft Documentation.

Encrypting Outgoing Emails

To encrypt emails using Microsoft, you must create a transport rule. To configure it, contact *Avanan Support*. Once the transport rule is configured, select the required DLP workflow that has encryption (**Email is allowed. Encrypted by Microsoft** or **Email is blocked and user can resend as encrypted**). Based on the workflow defined, the emails are encrypted automatically.

All outgoing emails that has data leak will be sent with a header:

- Microsoft Encryption: **X-CLOUD-SEC-AV-Encrypt-Microsoft**: True

Encrypting Outgoing Emails using Avanan Email Encryption

Avanan Email Encryption allows you to send emails containing sensitive information in a secured manner so that the external recipient can see the email in a secured portal, while the email and its content are stored only in the Avanan's tenant.

Activating Avanan Email Encryption

To activate Avanan Email Encryption:

1. Create or edit an existing Office 365 Mail DLP policy. For more information, see *"DLP Policy for Outgoing Emails" on page 190*.
2. Set the policy protection mode as **Prevent (Inline)**.
3. Under **Scope**, select **Direction** as **Outbound**.

4. Select a DLP workflow for Avanan Email Encryption as required. For the supported workflows, see *"Avanan Email Encryption Workflows" on page 194*.
5. Click **Save**.

Note - By default, the Avanan logo appears on the Avanan Email Encryption web pages and email notifications. To customize the logo, see *"Custom Logo" on page 450*.

Accessing Avanan Email Encryption Encrypted Emails

Validating the Identity of the External Recipient

When an external recipient receives a secured email notification from Avanan Email Encryption, the recipient must validate to view the email.

To validate the identity, the external recipient must do these:

1. Click the link in the email notification to access the secured portal.

   By default, the link is valid only for 10 hours.
2. Click **Authenticate** to receive the one-time authentication code.

   The recipient receives the authentication code through email. By default, the authentication code is valid only for 10 minutes.
3. Enter the code and click **Submit**.
4. After successful authentication, the recipient can view and respond to the email.

   Also, Avanan adds a cookie to the browser. By default, it remains valid for 30 days, and the recipient is not required to authenticate again from the same browser. After the cookie expires, the recipient must authenticate again.

   To configure the default time and validity of the cookie, see *"Configuring Avanan Email Encryption Parameters" on the next page*.

External Recipients Interacting with Emails Vaulted by Avanan Email Encryption

After successful authentication, the email opens in a secured portal and allows the recipient to:

- Read the email
- Download the attachments (if any)
- Reply to the sender.

Storage of Emails by Avanan Email Encryption

Avanan stores the secured emails by Avanan Email Encryption only in the Avanan servers associated with the data residency region of your Avanan tenant. The email and its attachments are stored encrypted by SSE-S3 encryption.

By default, these emails will be available only for 14 days, and you cannot access them later. To change the number of days they are available, see *"Configuring Avanan Email Encryption Parameters" below*.

Configuring Avanan Email Encryption Parameters

You can configure the security and retention parameters of the Avanan Email Encryption security engine. To do that:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for Avanan Email Encryption.
3. In the **Subject** field, enter the email's subject in the Avanan Email Encryption email notification.
4. In the **Body** field, enter the required information in the email notification.
5. In the **Email lifetime in days** field, enter the number of days before the emails expire. By default, Avanan Email Encryption emails expire after 14 days.
6. In the **Code expiration in minutes** field, enter the expiration time for the authentication code. By default, the code expires in 10 minutes.
7. In the **Cookie expiration in days** field, enter the expiration for the cookie. By default, the cookie expires after 30 days. After this period, the recipient must authenticate again.
8. In the **Link expiration in hours** field, enter when the secured link in the email notification expires.

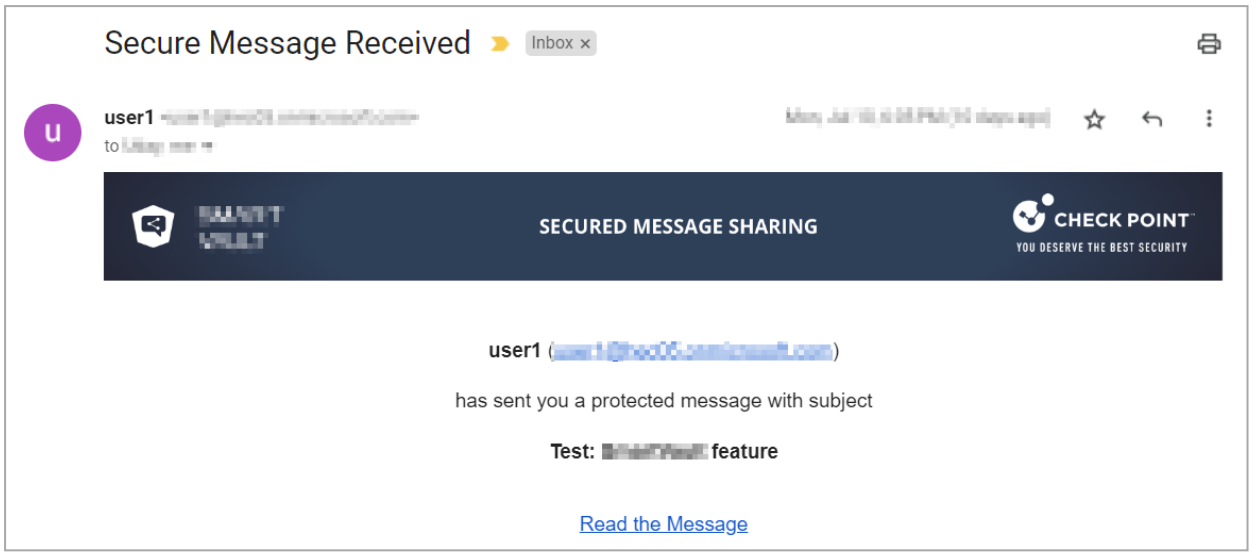
   By default, the link is valid only for 10 hours. After this period, the recipient cannot access the vaulted email using the encrypted link. However, the recipient can request a new link from the old encrypted link.
9. Click **Save**.

Emails Encrypted by Avanan Email Encryption - End User (External Recipient) Experience

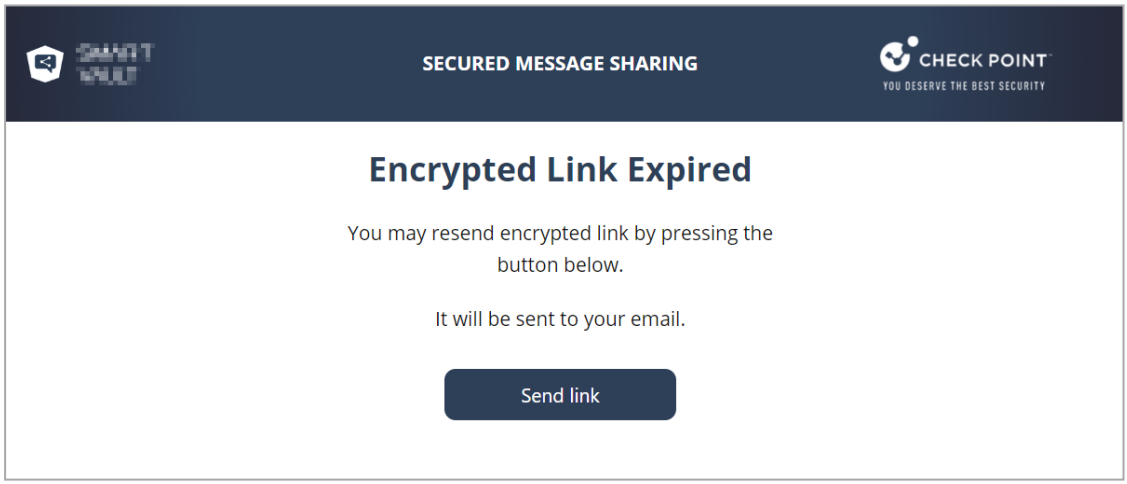
When Avanan detects sensitive information in an email, the email is vaulted, and the recipient receives an email notification from Avanan Email Encryption.

To view the secured email, the external recipient must do these:

1. Click the secured link in the email notification.



Note - By default, the secured link is valid only for 10 hours. After it expires, you must request a new link. To do that, click **Send link** from the **Encrypted Link Expired** page.



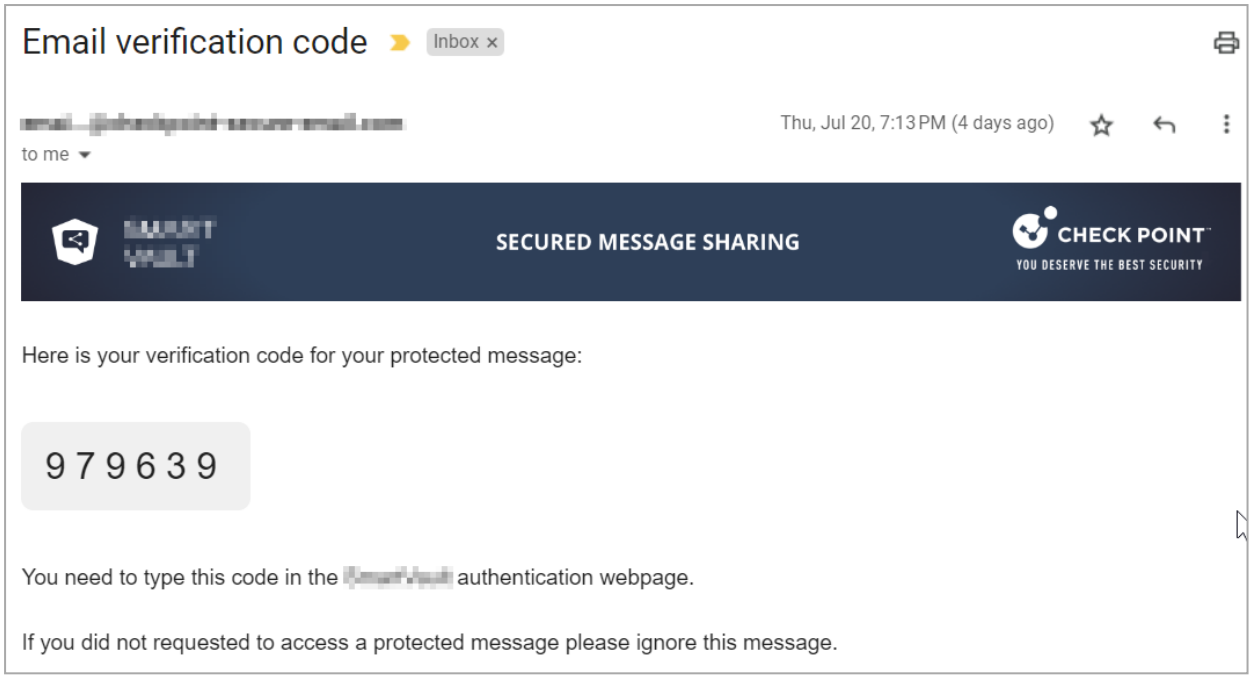
You will receive an email with the new secured link.

2. To read the email, click **Read the Message**.

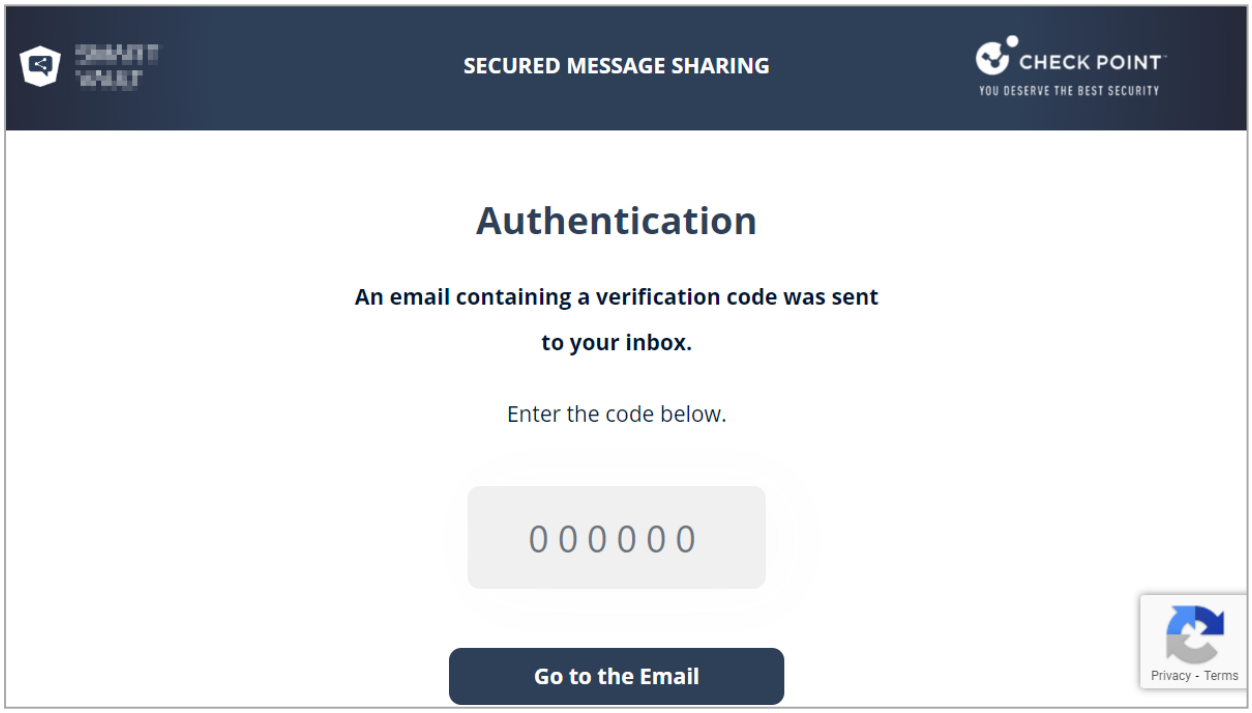
   The secured portal opens and requests for authentication.

3. Click **Get Authentication Code**.

   The recipient receives an authentication code through an email.

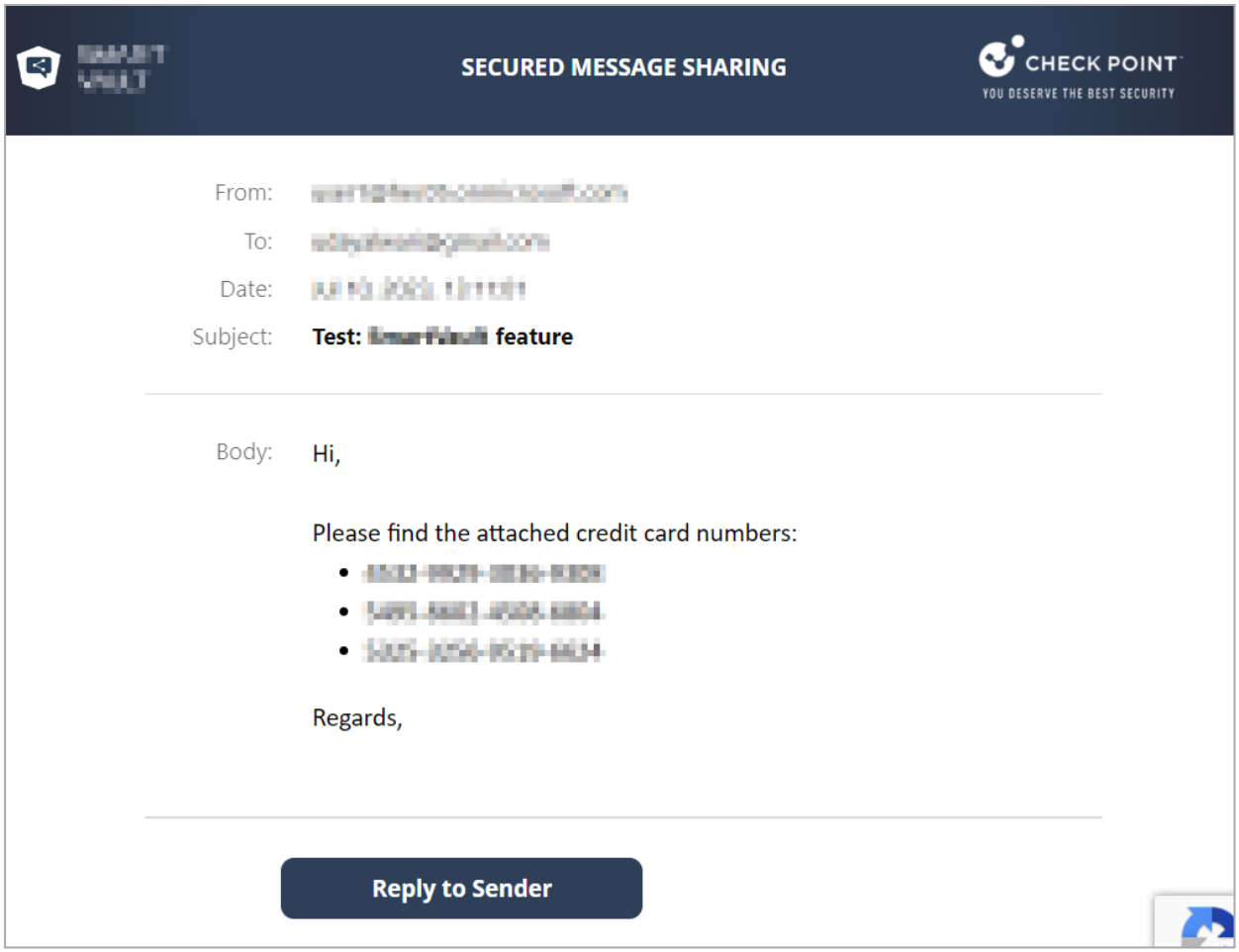


4. Enter the authentication code in the secured portal and click **Go to the Email**.

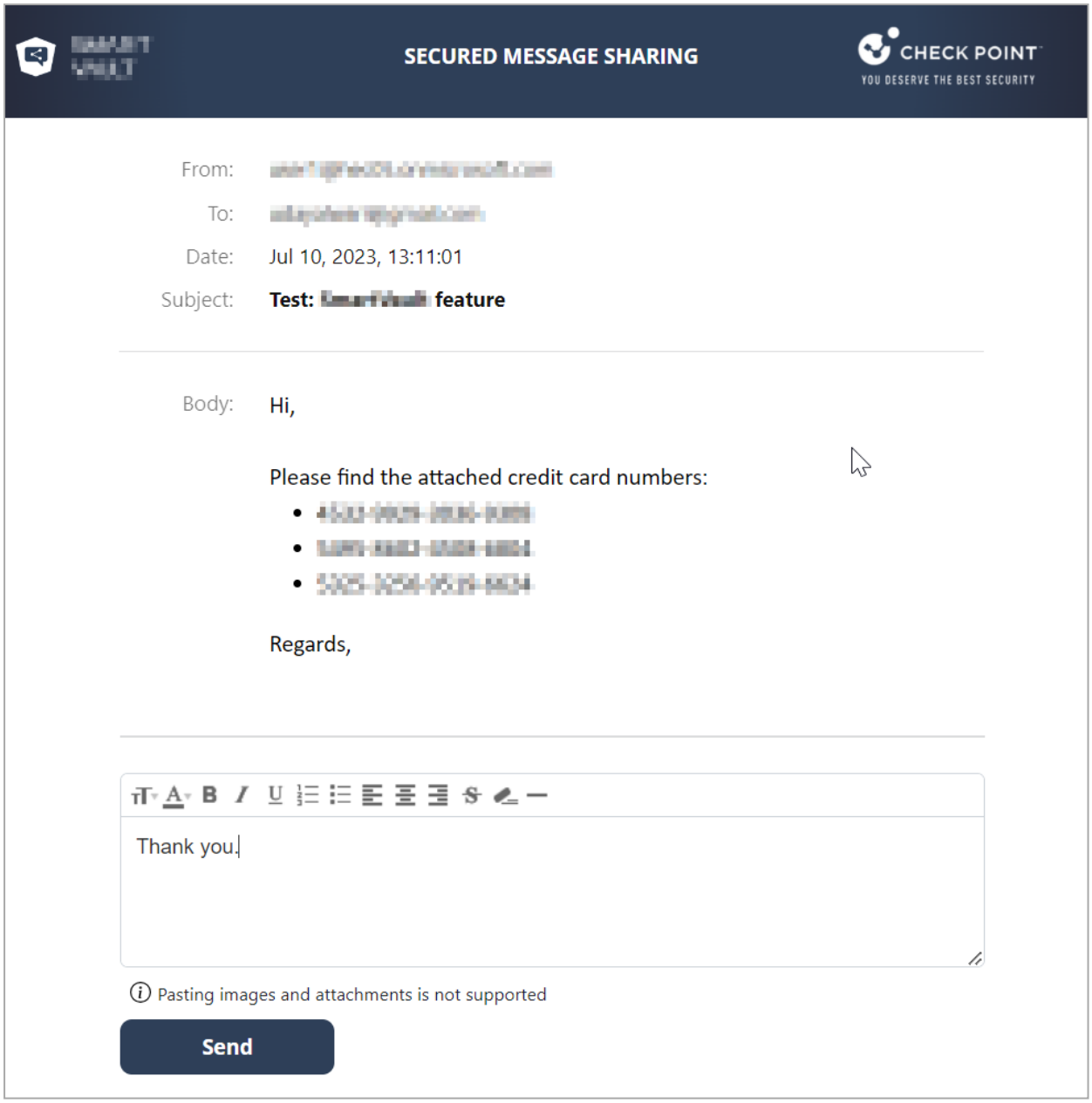


After successful authentication, the original email appears.

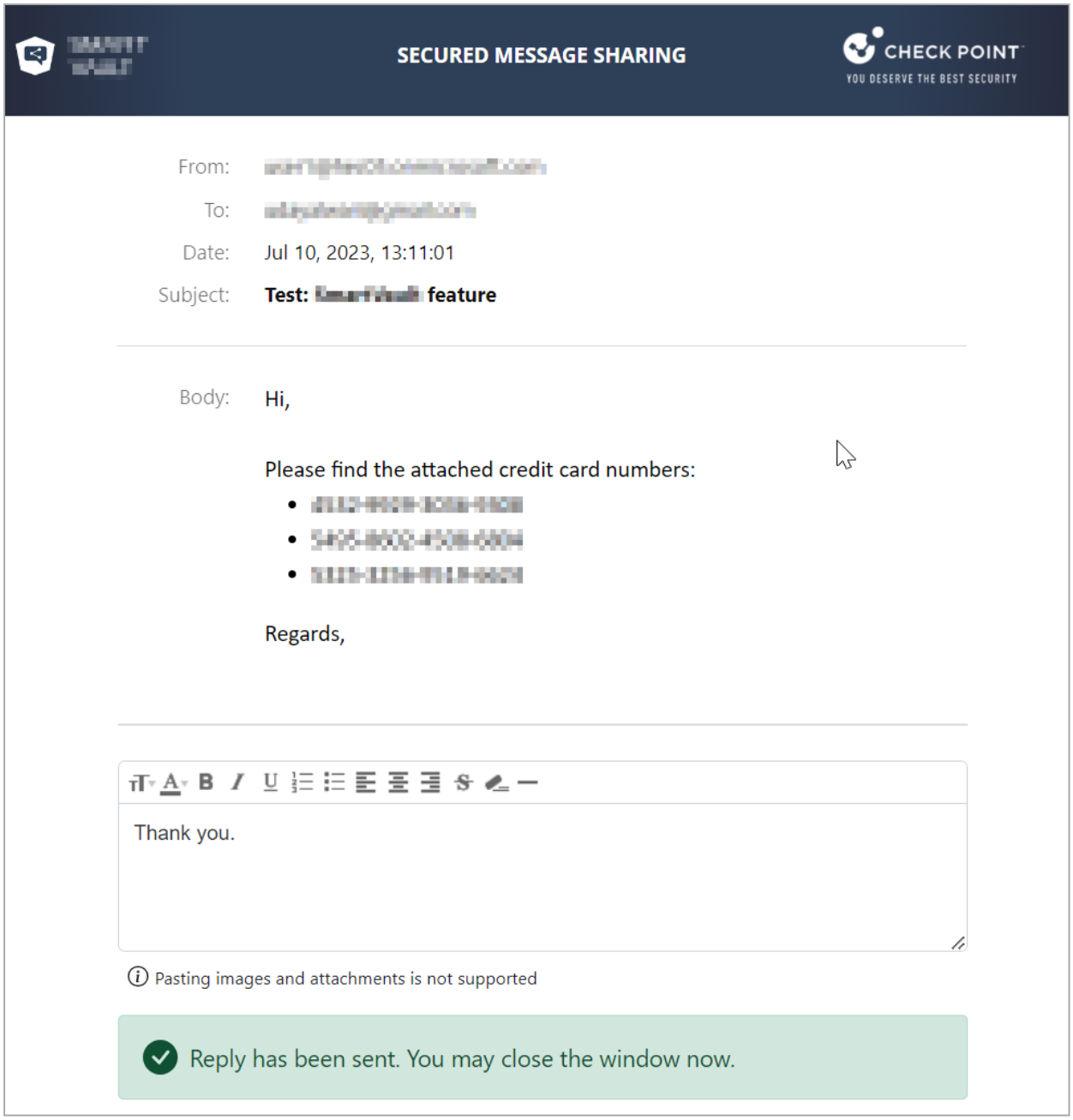
5. To reply to the email, click **Reply to Sender**.



6. Enter the required information and click **Send**.



The response is sent as an email to the original sender and the secured portal shows the email delivery status.



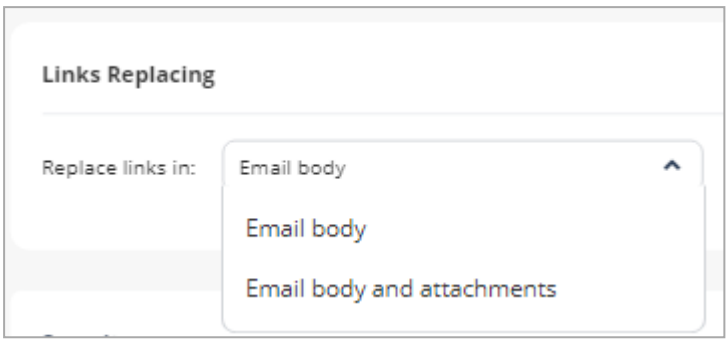
Click-Time Protection Policy

Configuring Click-Time Protection Policy

To configure Click-Time Protection policy:

1. Navigate to **Policy**.
2. Click **Add a New Policy Rule**.
3. Select the desired SaaS application under **Choose SaaS** drop-down.
4. Select **Click-Time Protection** under **Choose Security** drop-down and click **Next**.
5. Choose **Scope** for the policy.

6. Under **Links Replacing**, choose where to replace the links for the email.
   - **Email body**
   - **Email body and attachments**



7. Under **Severity**, select the severity of the events generated by Click-Time Protection security engine.
   - Auto
   - Critical
   - High
   - Medium
   - Low
   - Lowest
8. Click **Save and Apply**.

Note - For more details about workflow and additional settings, see *"Click-Time Protection" on page 120*.

Click-Time Protection Exceptions

See *"Click-Time Protection Exceptions" on page 324*.

Notifications and Banners

Configuring Email Notifications and Banners

Note - Avanan supports only PNG image links in email notification templates.

To configure email notifications:

1. Go to **Security Settings** > **SaaS Applications**.
2. Select the required email service (Office 365 Mail or Gmail).

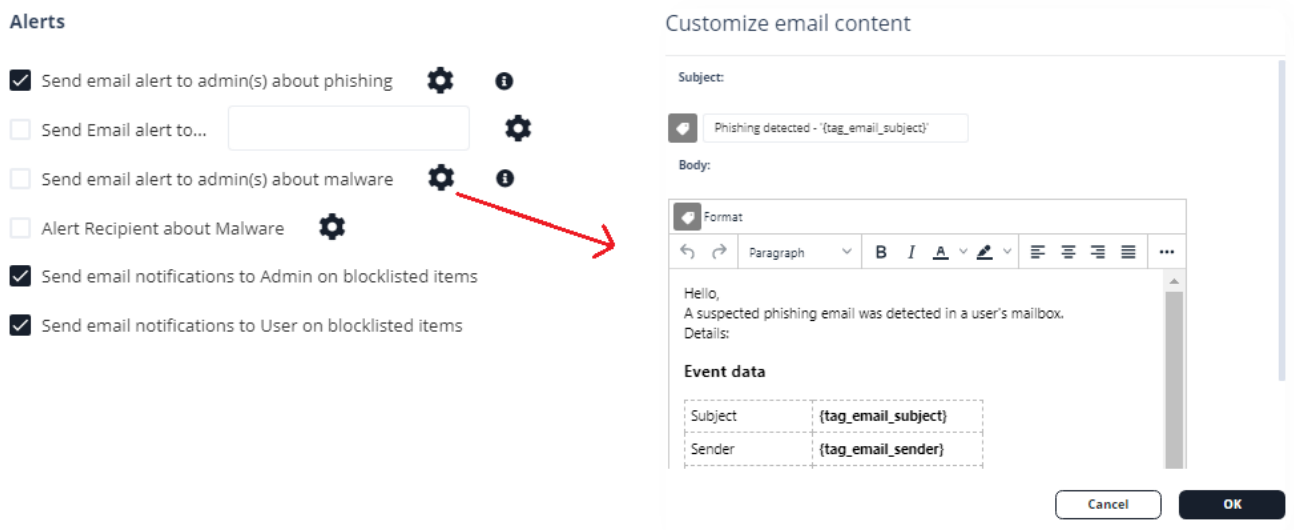
3. Click **Advanced** and select the template.
4. Configure the template as required.

Request / Report Type	Template Name
Rejected quarantine restore request	Decline message subject
	Decline message body
Declined Phishing report	Report Phishing decline subject
	Report Phishing decline body
Approved Phishing report	Report Phishing approve subject
	Report Phishing approve body

For more information about the supported placeholders, see *"Notification and Banner Templates - Placeholders" on page 238*.

5. Click **Save**.

Administrators can also configure the notifications and banners per policy. To configure them, click the cog icon next to the workflow and make the required changes.



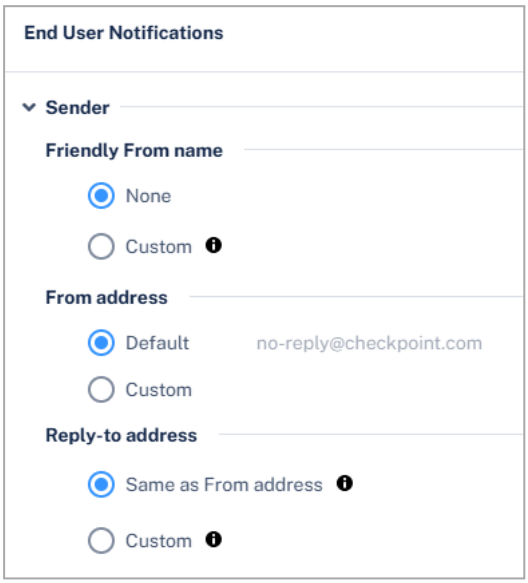
Sending Email Notifications to End Users

Avanan allows to send email notifications to end users for these actions:

- Rejected quarantine restore requests
- Approved phishing reports
- Rejected phishing reports

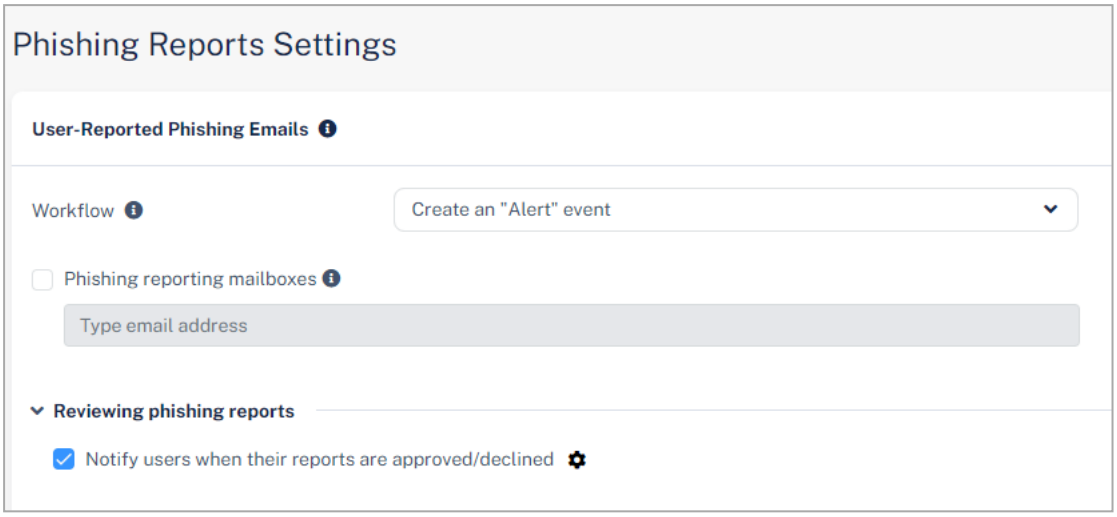
To enable Avanan to send email notifications to end users:

- To send email notifications for declined restore requests:
  1. Go to **Security Settings** > **User Interaction** > **Quarantine**.
  2. In the **End User Notifications** section, configure the required sender email address for notifications.



  3. To configure the sender email address for notifications, do these:
     - Friendly-From name
       - If no friendly-from name is required, select **None**.
       - To use a customized name, select **Custom** and enter the sender name.
     - From address
       - To use the default email address, select **Default**. The default email address is *no-reply@avanan-mail.net*.
       - To use a custom email address, see *"Customizing the From address for Email Notifications" on the next page*.
     - Reply-to address
       - To use **From address** as the Reply-to address, select **Same as From address**.
       - To use a custom email address, select **Custom** and enter the email address.
  4. Click **Save and Apply**.
- To send email notifications for approved and declined phishing reports:

1. Go to **Security Settings** > **User Interaction** > **Phishing Reports**.
2. In the **Reviewing phishing reports** section, select the **Notify users when their reports are approved/declined** checkbox.



3. To change the notification message, click the ⚙ icon next to the checkbox and make the required changes.
4. Click **Save And Apply**.

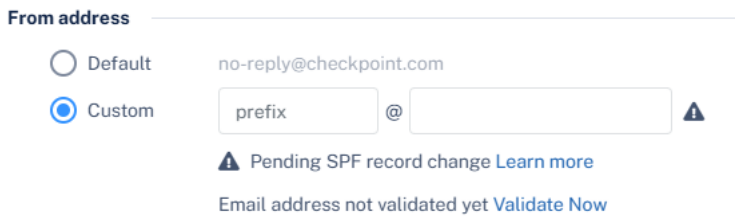
Customizing the From address for Email Notifications

To use a custom From address for email notifications sent to end users:

1. Go to **Security Settings** > **User Interaction** > **Quarantine** > **End User Notifications**.
2. To use a custom email address, select **Custom** in **From address**.
3. Add the Avanan include statement to the custom domain's DNS.

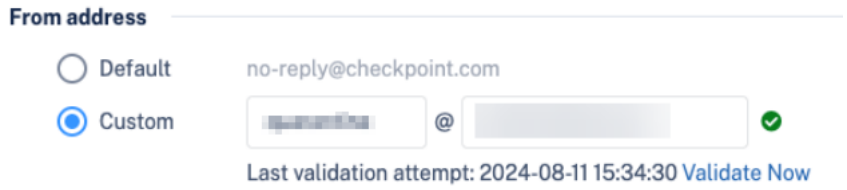
   ```
   include:spfa.cpmails.com
   ```

   Note - The custom domain must be one of the protected domains in your Infinity Portal tenant.
4. Click **Save and Apply**.



Note - Avanan continues to send email notifications from the default email address until the include statement is validated in the custom domain's DNS configuration.

Once the include statement is successfully validated, the system displays the validation status along with the date and time of the last validation check.



Warning Banners

For suspected (low confidence) email detections, the administrator can choose to allow the email to be delivered to the inbox. In such cases, Avanan allows to embed a warning banner in the email explaining the nature and potential risk to the end-users.

Note - Warning banners are available only in **Prevent (Inline)** and **Detect and Remediate** modes.

Warning banners are generated based on these detection attributes:

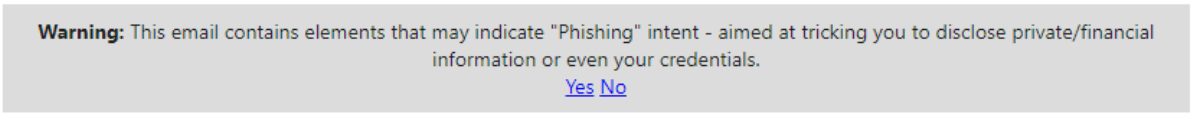
- **Suspected phishing**: This email contains elements that may indicate "Phishing" intent - aimed at tricking you to disclose private/financial information or even your credentials.
- **Encrypted Attachments**: Be careful when opening this email. It is carrying an encrypted attachment - often used for evading virus scans. Make sure you trust this email before opening the attachment.
- **Password Protected Attachments**: The email contains an attachment which is protected with a password. The user must provide password for the Anti-Malware engine to scan the attachment for malicious content.

To configure warning banners:

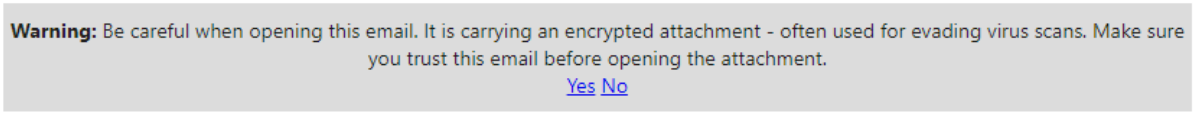
1. Navigate to **Policy**.
2. Open **Threat Detection** policy for the required SaaS.
3. Select the **workflow** for which the banner has to be configured.
4. To customize the banner (text, background color etc.), click the gear icon next to the workflow.
5. Click **Save and Apply**.

Warning banner samples

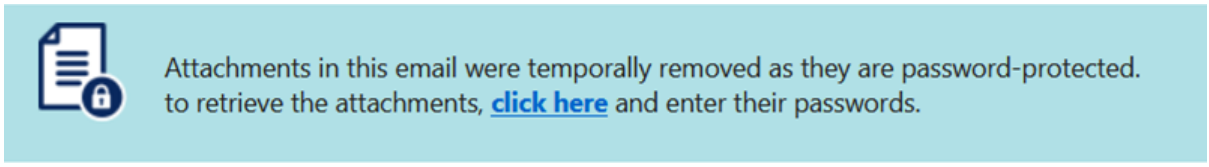
- Warning banner for **suspected phishing** emails.



- Warning banner for emails having **encrypted attachments**.



- Warning banner for emails having **password protected attachments**.



Smart Banners

Overview

Smart Banners are customizable banners added to incoming emails that Avanan found clean of threats.

These banners help distinguish external, unverified, or potentially fraudulent emails and so on that serve these main purposes:

- **Make users cyber-aware** - The banners draw user attention to suspicious elements in the email that - combined with the user insights - might lead to the understanding that the email is malicious.
- **Remind users to follow the company policy** - The banners alert the user to follow company policies for particular emails. For example, emails that contain invoices or requests to modify a partner's billing information.

Attaching Smart Banners to Emails

To attach Smart Banners to emails:

1. Create or edit an existing Threat Detection policy for Office 365 Mail or Gmail. See *"Threat Detection Policy for Incoming Emails" on page 150*.
2. Set the policy protection mode as **Prevent (Inline)**.

Note - Smart Banners are not supported for policies in **Detect** and **Detect and Remediate** protection mode.

3. Scroll down to **Clean Emails** section and for **Clean Workflow**, select **Deliver with Smart Banners**.
4. Click **Save**.

Notes:

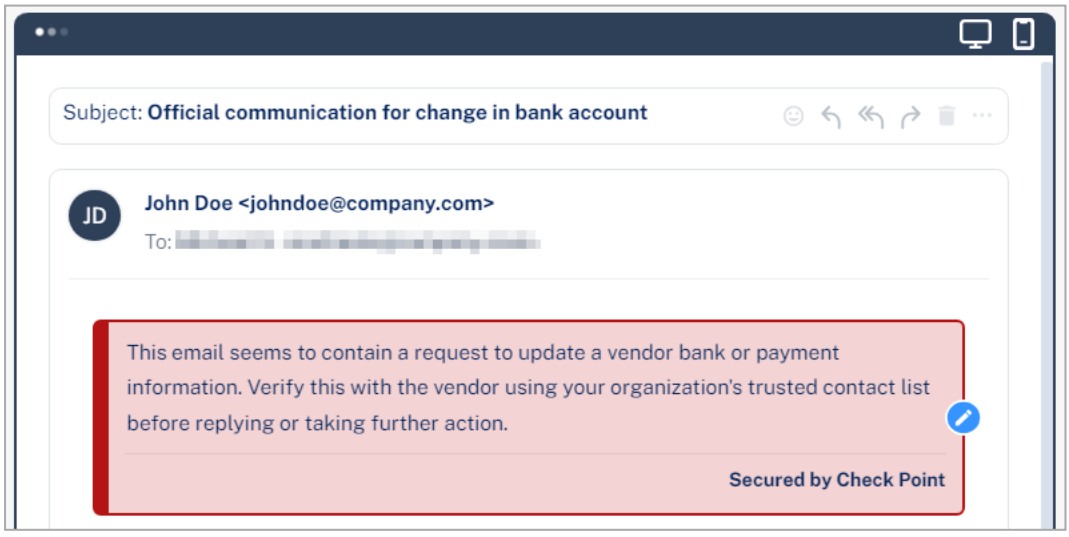
- For allow-listed emails, **Smart Banners** are not added.
- When more than one banner is applicable for an email, Avanan adds the banner with the highest severity. If there are multiple banners with the same severity, the one with the highest priority is added. For information about priority of the banners, see *"Supported Smart Banners" on page 233*.
- These banners apply only to emails written in English:
  - Request to update payment details
  - Invoice from a new vendor
  - Payroll information update request
  - Emails with Invoices / POs

Customizing Smart Banners

To customize a Smart Banner:

1. Click **User Interaction** > **Smart Banners**.
2. Click on the banner.

   The banner's preview appears.
3. Click the icon on the banner.



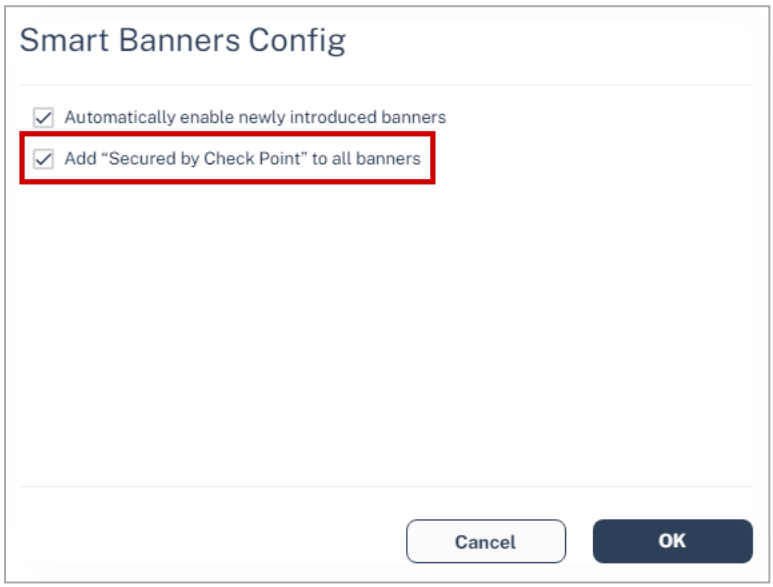
4. To change the banner's severity and color, select **Low**, **Medium**, or **High**.

5. Make the required changes to the text.
6. Click **Save and Apply**.

To remove the Secured by Avanan footer:

1. Click **User Interaction** > **Smart Banners**.
2. Click **Settings** next to **Smart Banners** from the top of the page.

   Smart Banners Config pop-up appears.



3. Clear the **Add "Secured by Check Point" to all banners** checkbox.
4. Click **OK**.

Enabling/Disabling Specific Smart Banners

Avanan delivers the emails with a specific **Smart Banner** if they match the use case the banner covers.

To enable or disable specific Smart Banners, do these:

1. Go to **User Interaction** > **Smart Banners**.
2. Toggle the button **On/Off** to the left of the required banner.

   Note - Smart Banners can only be turned on/off for all the protected users in the Avanan tenant (account) and does not apply per policy.

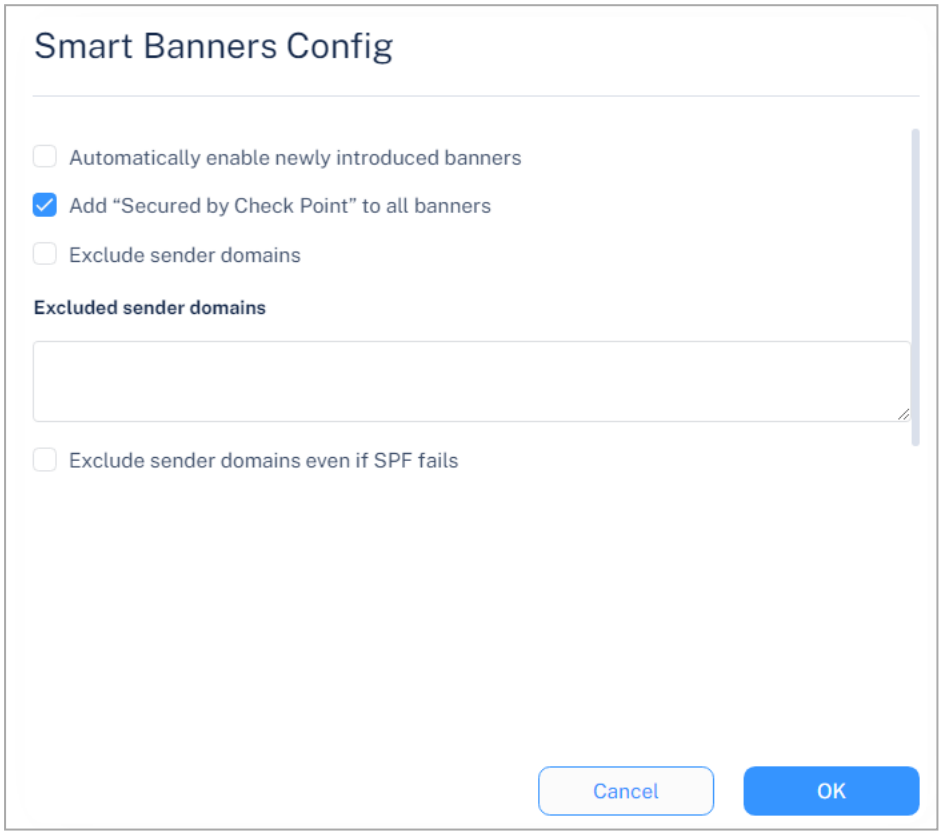
3. Click **Save and Apply**.

Automatically Enabling New Smart Banners

Avanan periodically introduces new banners for additional elements and characteristics. To enable these banners automatically:

1. Click **User Interaction** > **Smart Banners**.
2. Click **Settings** next to **Smart Banners** from the top of the page.

   The **Smart Banners Config** pop-up appears.



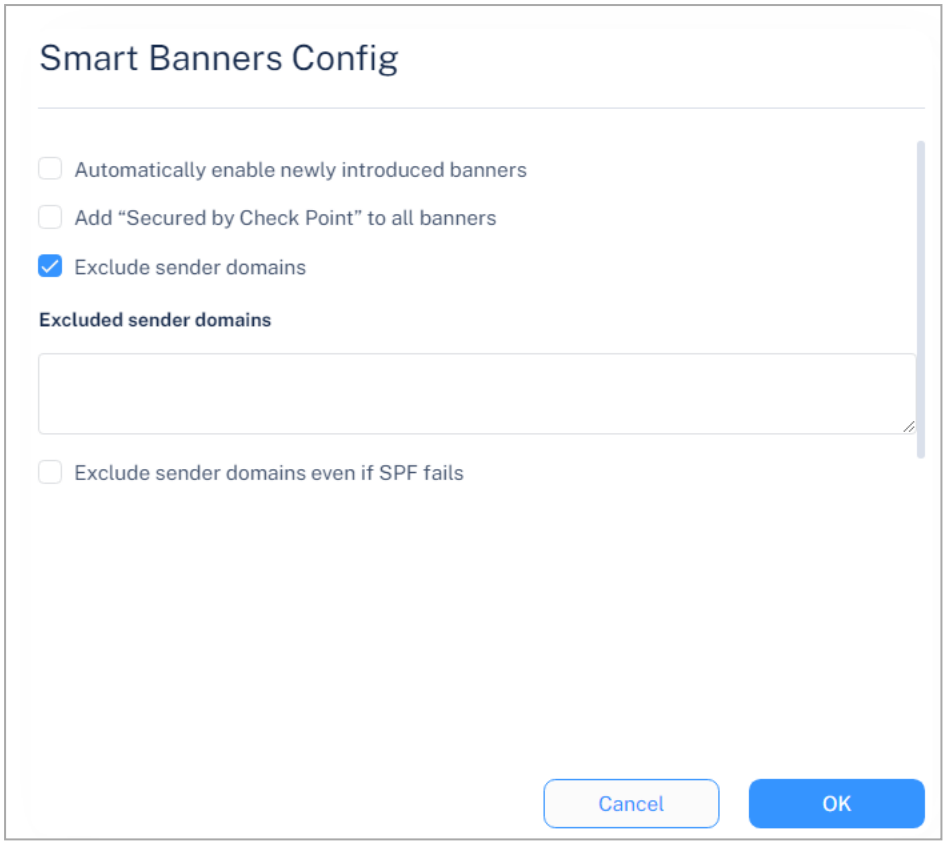
3. Enable the **Automatically enable newly introduced banners** checkbox.
4. Click **OK**.

Excluding Specific Sender Domains from Smart Banner

Avanan allows administrators to exclude Smart Banners from emails sent by specific domains. To do that:

1. Go to **User Interaction** > **Smart Banners** > **Settings**.

   The **Smart Banners Config** window appears.



2. Select the **Exclude sender domains** checkbox.
3. In the **Excluded sender domains** field, enter the selected domain(s) separated by commas.
4. Click **OK**.

Supported Smart Banners

Avanan supports these **Smart Banners**:

Category	Smart Banner Name	Description	Default Severity	Priority	Is enabled by default?
Business email compromise	Sender resembles a real contact	Email from a sender that resembles but is not identical to a contact the recipient is corresponding with.	High	1	Yes
	Request to update payment details [1]	Email that resembles a request from vendors to change their payment details.	High	2	Yes
	Invoice from a new vendor [1]	Email with an invoice from a vendor that never contacted before.	Medium	21	Yes
	Payroll information update request [1]	Emails from external senders requesting to update their payroll information.	Low	41	Yes

Category	Smart Banner Name	Description	Default Severity	Priority	Is enabled by default?
Financial transaction requests	Emails with Invoices / POs [1]	Email that contains a request for payment in the form of invoice or purchase order.	Low	42	Yes
	Payment request via payment service	Email that contains a payment request received via accounts in payment services.	Low	43	Yes
Avoiding inspection	Emails with links to restricted resources	Email with links to resources with restricted access, possibly in order to avoid inspection.	Low	44	Yes
	Emails that appear to be from an e-sign service [6]	Emails that contains a link to an e-sign document, possibly in order to avoid inspection.	Low	45	Yes

Category	Smart Banner Name	Description	Default Severity	Priority	Is enabled by default?
Fundamentals	Sender name different than address	Email from sender with a name that is significantly different from the email address which may indicate an impersonation attempt.	High	3	Yes
	Reply-to domain recently created and its address is different than the sender's	Email with reply-to address different from sender address and whose reply-to domain is created recently.	High	4	Yes
	Sender domain created recently [2]	Email whose sender domain was created recently.	Medium	23	Yes
	Sender SPF failed	Email that failed SPF checks.	Medium	24	Yes
	Incoming emails from external senders	Email from an external sender (outside the organization).	Informative (blue)	81	No

Category	Smart Banner Name	Description	Default Severity	Priority	Is enabled by default?
Impersonation	First-time sender to recipient [3,4,5]	Email from a sender that never sent an email to the recipient before.	Low	47	No
	First-time sender to recipient domain [4,5]	Email from a sender that never exchanged an email with the recipient domain before.	Low	46	No
	Sender resembles a person within the organization	Emails from a first-time sender whose display name is identical to a person within the organization.	Medium	22	Yes

[1] These banners apply only to emails written in English.

[2] This banner will be applied to emails only if the sender's domain was created in the last 100 days.

[3] The First-time sender banner will not be applied to the recipient's emails after 24 hours from the sender's first email.

[4] If an email is sent to multiple recipients, the banner will be added only if the condition applies to all recipients.

[5] The banner will not be added if the sender domain regularly interacts in high volumes with other recipients from your domain. This exception does not apply to public domains. For example, *gmail.com*.

[6] If an email appears to reference an electronic signature and may contain links that cannot be inspected for phishing or viruses, ensure its authenticity before clicking any links or taking further action.

Notification and Banner Templates - Placeholders

While configuring email notifications and banners, the administrator can use placeholders to replace content dynamically. For example, the placeholder *{subject}* gets replaced with the email subject that triggered the email notification.

- **Quarantine notifications**
  - **Quarantine notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

  - **Quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original subject	{subject}

- **Quarantined notification (admin restore request)**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original subject	{subject}

- **Outgoing quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original subject	{subject}

- **Outgoing quarantined notification (admin restore request)**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original subject	{subject}

■ **Restore request notifications**

- **Restore request subject**

Placeholder Name	Placeholder Value
Email of the requesting user	{requester}
Original subject	{subject}

- **Restore request body**

Placeholder Name	Placeholder Value
User request free text	{comment}
Original sender	{from_email}
Original sender's name	{from_name}
Restoration link	{link_to_restore}
Email of the requesting user	{requester}
Original subject	{subject}

- **Restore notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Decline message subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Decline message body**

Placeholder Name	Placeholder Value
Decline reason	{decline_reason}
Original sender	{from_email}
The original subject	{subject}

■ **Password-protected attachments notifications**

- **Password-protected quarantine notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Password-protected quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

Phishing quarantine notifications

- **Phishing quarantine notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Phishing quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **Phishing quarantine notification body (admin restore request)**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **Phishing decline message subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Phishing decline message body**

Placeholder Name	Placeholder Value
Decline reason	{decline_reason}
Original sender	{from_email}
The original subject	{subject}

- **Outgoing phishing quarantine notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Outgoing phishing quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **Outgoing phishing quarantine notification body (admin restore request)**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Detection reasons	{detection_reasons}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **Require password to release encrypted file notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
The original mail sender	{from_email}
Restoration link	{link_to_restore}

- **Threat extracted message notifications**

- **Threat extracted message format**

Placeholder Name	Placeholder Value
Action taken on malicious attachments	{actions_taken}
Original mail body	{body}
Original mail sender	{from_email}
Link to restoration link	{link_to_restore}
Original subject	{subject}

- **Threat extracted attachment name template**

Placeholder Name	Placeholder Value
Original attachment name	*_{original_name} For example, threat_ extraction_{original_ name}

■ **Spam quarantine notifications**

- **Spam quarantine notification subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Spam quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **Outgoing spam quarantine notification body**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **DLP notifications**

- **DLP quarantined notification body (admin restore request) - Outbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Data leak detection categories	{dlp_categories}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The sender name	{name}
Original email subject	{subject}

- **DLP quarantined notification body (user can restore) - Outbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Data leak detection categories	{dlp_categories}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The sender name	{name}
Original email subject	{subject}

- **DLP restoration notification body - Outbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **DLP quarantined notification body (admin restore request) - Inbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Data leak detection categories	{dlp_categories}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The sender name	{name}
Original email subject	{subject}

- **DLP quarantined notification body (user can restore) - Inbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Data leak detection categories	{dlp_categories}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The sender name	{name}
Original email subject	{subject}

- **DLP restoration notification body - Inbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The recipient name	{name}
Original email subject	{subject}

- **DLP alert subject to external sender - Inbound**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **DLP alert body to external sender - Inbound**

Placeholder Name	Placeholder Value
List of attachment names	{attachments_names}
Original mail body	{body}
Original mail sender	{from_email}
Original mail sender address	{from_email_address}
Restoration link	{link_to_restore}
The sender name	{name}
The email recipients	{recipients}
Original email subject	{subject}

■ **Report phishing notifications**

- **Report phishing approve subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Report phishing approve body**

Placeholder Name	Placeholder Value
Original mail sender	{from_email}
The recipient name	{name}
Original subject	{subject}

- **Report phishing simulation subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Report phishing simulation body**

Placeholder Name	Placeholder Value
Original mail sender	{from_email}
The recipient name	{name}
Original subject	{subject}

- **Report phishing decline subject**

Placeholder Name	Placeholder Value
Original email subject	{subject}

- **Report phishing decline body**

Placeholder Name	Placeholder Value
Decline reason	{decline_reaason}
Original mail sender	{from_email}
The recipient name	{name}
Original subject	{subject}

Email Alerts - Placeholders

- **Threat Detection Policy**

Placeholder Name	Placeholder Value
Email subject	{tag_email_subject}
Sender email address	{tag_email_sender}
Recipient email address	{tag_email_recipient}
Date when the email was received	{tag_email_received}
Detection reasons	{tag_detection_reasons}
Name of the detected attachment	{tag_affected_attachment_name}

- **DLP Policy**

Placeholder Name	Placeholder Value
Email subject	{tag_email_subject}
Sender email address	{tag_email_sender}
All recipient's email address	{tag_email_all_recipients}
Date when the email was received	{tag_email_received}
Name of the detected attachment	{tag_affected_attachment_name}
Email delivery status	{tag_delivery_status}
DLP categories	{tag_dlp_categories}

- **Click-Time Protection Policy**

Placeholder Name	Placeholder Value
Email subject	{tag_email_subject}
Sender email address	{tag_email_sender}
Recipient email address	{tag_email_recipient}
Date when the email was received	{tag_email_received}
Detection reasons	{tag_detection_reasons}
Name of the detected attachment	{tag_affected_attachment_name}

Smart Banners - Placeholders

Placeholder Name	Placeholder Value
The sender's display name resembles that of a known contact with whom the recipient is corresponding	<<sender nickname>>
Display name of the known contact with whom the recipient is corresponding	<<known contact>>
Sender's display name	<<sender>>
Sender domain	<<sender domain>>

Placeholder Name	Placeholder Value
Reply-to email address	<<reply-to>>
Reply-to domain	<<reply-to domain>>

Email Archiving

Overview

Avanan's **Archiving** is a cloud-based archiving solution for preserving email communications.

Archiving provides organizations with a variety of tools for one or more of these reasons:

- Business continuity and disaster recovery
- Email Backup and recovery of emails deleted by end-users or because of technical malfunction
- Regulatory compliance and records management
- Litigation and Legal Discovery
- Prove chain of custody and keep the authenticity of emails.

Activating Email Archiving

After your purchase request is processed, **Archiving** gets activated automatically.

After activation, **Archiving** starts archiving all the emails sent from and received by the protected user's mailboxes (users that are assigned Avanan license). For more information on assigning licenses, see *"Limiting license consumption and security inspection to a specific group" on page 40*.

Note - Though **Archiving** starts archiving the emails immediately, it might take up to 48 hours for these emails to be available in the **Archiving Search**.

If required, administrators can import the archived emails from an external source. See *"Importing Emails to Archive" on page 255*.

Deactivating Email Archiving

To deactivate **Archiving** or to delete the archive storage, contact *Avanan Support*.

Archived Emails

After activating **Archiving**, all the internal, outgoing and incoming emails (sent or received) from protected users will be archived.

For users not licensed for Avanan, the emails will not be archived.

Emails that were sent before activating **Archiving** are not archived. To import historical emails to the **Archiving**, see *"Importing Emails to Archive" on the next page*.

By default, the archived emails are stored for a period of 7 years and will be automatically deleted afterwards. To change the retention period, see *"Customizing the Retention Period of Archived Emails" below*.

Avanan encrypts and stores the archived emails in the same region as your Avanan tenant.

Customizing the Retention Period of Archived Emails

By default, the archived emails are stored for a period of 7 years and will be automatically deleted afterwards.

To customize the retention period of archived emails:

1. Go to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Avanan Email Archiving**.

   Configure Avanan Email Archiving pop-up appears.
3. In the **Archive emails for** dropdown, select the number of years to retain the emails.
   - 1 year
   - 2 years
   - 3 years
   - 5 years
   - 7 years (default)
   - 10 years
4. Click **Save**.

Notes:

- Change in the retention period applies retroactively to all the archived emails. For example, if you change the retention period to 1 year, Avanan deletes the emails older than one year from the archive.
- To retain emails for more than 10 years, contact *Avanan Support*.

Viewing Archived Emails

From the **Archiving Search** screen, administrators can use filters, and search for the required emails. The **Archiving Search** screen gives a detailed view of all the archived emails (whether they have been archived or imported from an external source).

Note - After the emails are archived, it takes up to 48 hours for the archived emails to appear in the **Archiving Search**.

Importing Emails to Archive

Administrators can import emails from the email archiving solutions they used in the past or from other sources.

Supported Archiving import file format and size

Before importing the existing email archive to the Avanan **Archiving**, do these:

1. Export the existing emails as EML files with a maximum size of 150 MB per file.
2. Group your EML files and compress them into ZIP files with a maximum size of 25 GB per ZIP file.
3. Follow the procedure below to import emails to **Archiving**.

   Notes:
   - To import the emails to **Archiving**, the combined size of all uploaded ZIP files must be less than 6 TB.
     For example, you can upload up to 100 ZIP files, each with a maximum size of 25 GB, or alternatively, upload 250 ZIP files, each with a maximum size of 10 GB.
   - The ZIP files should contain only EML files, without any subfolders.
   - You can follow the same procedure multiple times to upload ZIP files totaling up to 12 TB, 18 TB, and so on. If you need to upload an archive significantly larger than that, contact *Avanan Support*.

To import emails to Archiving:

1. Go to **Archiving**.
2. From the top, select the **Archiving Search** tab.
3. Click **Import Archive**.

   Note - If **Import Archive** is not available in your Avanan tenant, contact *Avanan Support*.
4. In the **Import Emails to Archive** window that appears, click **Get credentials** to receive credentials to a temporary upload path.

   Note - This upload path and credentials are valid only for 30 days.
5. Use the path and credentials (Host name, user name and password) to log in to SFTP.
6. Upload the ZIP file(s) to the **uploads** folder.

7. After uploading all the files, click **Done uploading**.
8. Click **Confirm** to initiate the import.

   Note - After importing the emails, it takes up to 48 hours for the archived emails to appear in the **Archive Search**.

Exporting Emails from Archive

If required, administrators can export the archived emails from **Archive**. Each archive export creates encrypted ZIP file(s), which includes EML files. If the export file size exceeds 10 GB, then the export is divided into multiple ZIP files with each file size not exceeding 10 GB.

To export archived emails:

1. Go to **Archiving**.
2. From the top, select the **Archiving Search** tab.
3. Using filters, refine the search criteria for the required emails.
4. Select the emails to export, and click **Export**.
5. In the **Export Archive Emails** window that appears, enter the required **Export Name** and **Passphrase** for the archive export.
6. Click **OK**.

   Note - The export process could take several hours. After it is complete, the administrator who initiated the export process receives an email notification.

   The export process could take several hours. After it is complete, the administrator who initiated the export process receives an email notification
7. To download the archive export file(s), go to **Archiving Export** tab.
8. Click **Download** for the required export file(s).

   Note - The link to download the exported file(s) will only be available for 7 days after the export is completed.

Auditing

Avanan audits all the archive search, archive import, archive export, and archive download actions and adds them to the **System Logs** (**Security Settings > System Logs**).

Messaging Apps Protection

Microsoft Teams

Overview

Microsoft Teams is a communication platform developed by Microsoft as part of the Microsoft 365 family of products. It offers employees and external collaborators to chat, meet online, and share files. Avanan adds security, privacy, and compliance to Microsoft Teams by scanning messages and files shared on a chat or a team for malicious content and data loss prevention (DLP) and generates actionable events on malicious content.

Avanan scans the messages and files shared through direct messaging or a team.

How it works

Avanan adds a layer of security that provides these security features for Microsoft Teams:

- Data Leak Prevention (DLP): Protecting sensitive text messages and files
- Anti-Malware: Scanning of files for malicious content
- URL Reputation: Blocking malicious links within files and messages
- User Behavior Anomaly: Identifying suspicious login and compromised accounts
- Remediation: Tombstoning malicious files or sensitive files and messages

Required Permissions

Avanan requires these permissions to protect Microsoft Teams.

Note - All these permissions are required to access your data in the Avanan Administrator Portal.

Permissions required from Microsoft	Functions performed by Avanan
Send channel messages	Allows an app to send channel messages in Microsoft Teams on behalf of the signed-in user.
Sign in and read user profile	Allows users to sign in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Read domains	Allows the app to read all domain properties without a signed-in user.

Permissions required from Microsoft	Functions performed by Avanan
Read and write tabs in Microsoft Teams	Read and write tabs in any team in Microsoft Teams without a signed-in user. This does not give access to the content inside the tabs.
Read tabs in Microsoft Teams	Read the names and settings of tabs inside any team in Microsoft Teams without a signed-in user. This does not give access to the content inside the tabs.
Read and write all group memberships	Allows the app to list groups, read basic properties, read and update the membership of the groups this app has access to without a signed-in user. Group properties and owners cannot be updated, and groups cannot be deleted.
Read all group messages	Allows the app to read memberships and basic group properties for all groups without a signed-in user.
Manage all users' Teams apps	Allows the app to read, install, upgrade, and uninstall Teams apps for any user without a signed-in user. It does not give the ability to read or write application-specific settings.
Read all users' installed Teams app	Allows the app to read the Teams apps that are installed for any user without a signed-in user. It does not give the ability to read application-specific settings.
Read all users' teamwork activity feed	Allows the app to read all users' teamwork activity feed without a signed-in user.
Read directory data	Allows the app to read data in your organization's directory, such as users, groups, and apps, without a signed-in user.
Read and write all groups	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.
Read all groups	Allows the app to read group properties and memberships, and read the calendar and conversations for all groups, without a signed-in user.
Flag channel messages for violating policy	Allows the app to update Microsoft Teams channel messages by patching a set of Data Loss Prevention (DLP) policy violation properties to handle the output of DLP processing.

Permissions required from Microsoft	Functions performed by Avanan
Read all channel messages	Allows the app to read all channel messages in Microsoft Teams.
Read all chat messages	Allows the app to read all 1-to-1 or group chat messages in Microsoft Teams.
Flag chat messages for violating policy	Allows the app to update Microsoft Teams 1-to-1 or group chat messages by patching a set of Data Loss Prevention (DLP) policy violation properties to handle the output of DLP processing.
Read all users' full profiles	Allows the app to read user profiles without a signed-in user.
Read files in all site collections	Allows the app to read all files in all site collections without a signed-in user.
Read and write all chat messages	Allows an app to read and write all chat messages in Microsoft Teams without a signed-in user.
Read items in all site collections	Allows the app to read documents and list items in all site collections without a signed-in user.
Read all hidden memberships	Allows the app to read the memberships of hidden groups and administrative units without a signed-in user.

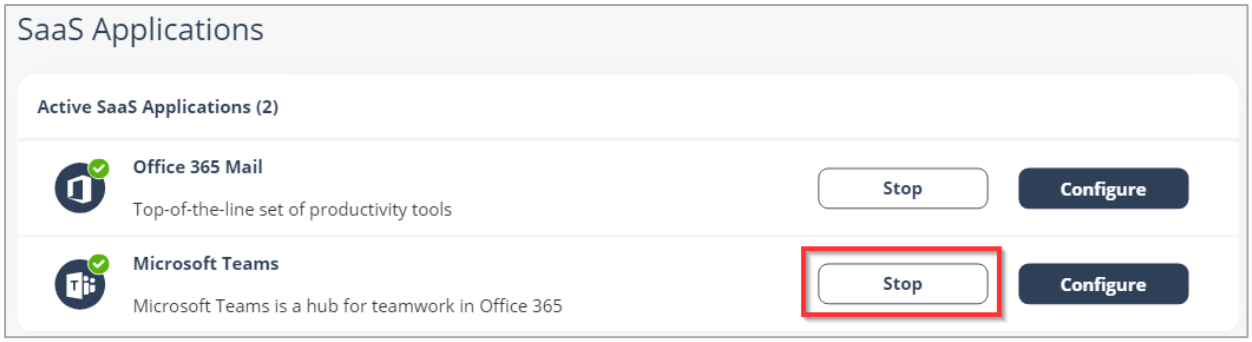
Activating Microsoft Teams

For details about the procedure to activate Microsoft Teams, see *"Activating Microsoft Teams" on page 82*.

Deactivating Microsoft Teams

To deactivate Microsoft Teams:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Microsoft Teams.



Microsoft Teams Security Settings

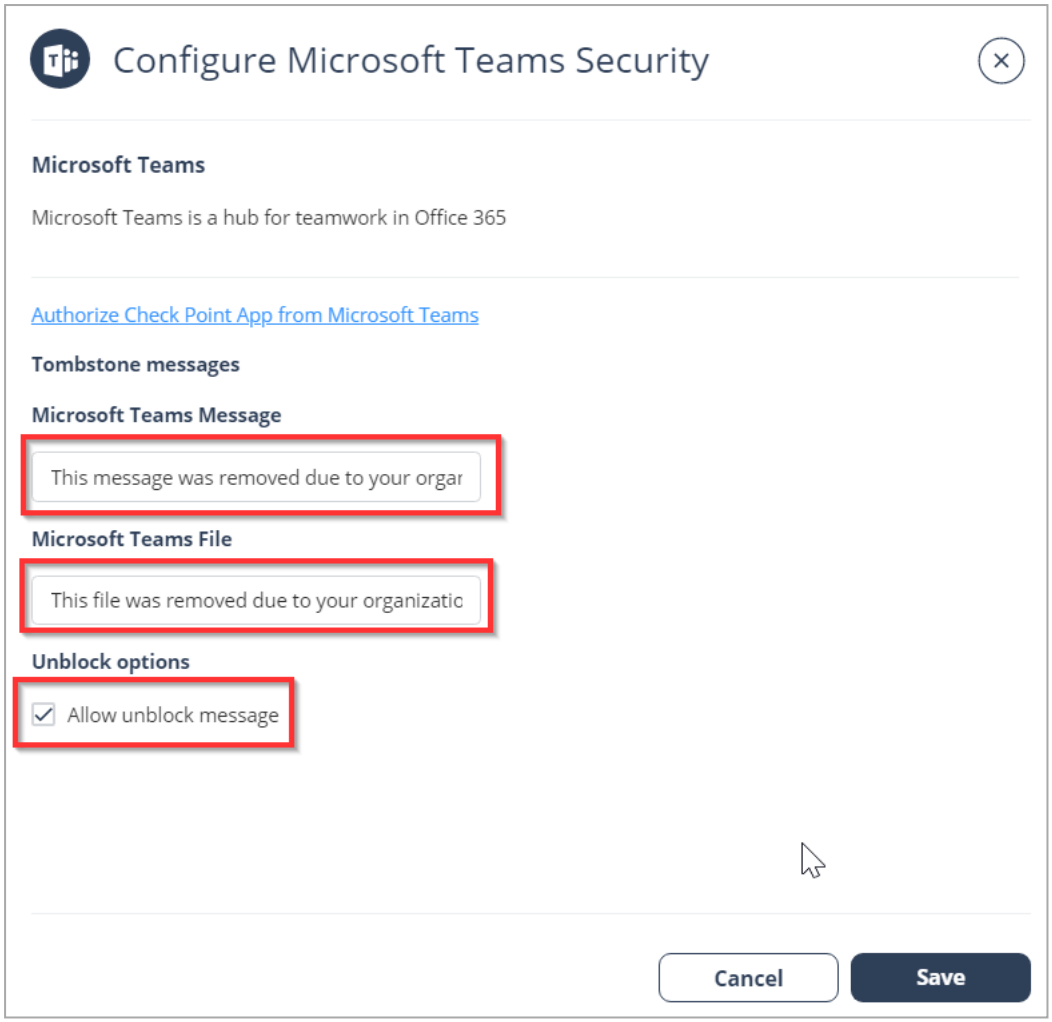
Customizing Tombstone Messages

If a message/file is tombstoned, a tombstone message will appear instead of the tombstoned message/file. The original message/file becomes inaccessible to the sender and the recipients in the chat/channel.

Administrators can customize the tombstone message for both messages and files.

To customize the tombstone messages:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Microsoft Teams.
3. To customize the tombstone message for messages, update the **Microsoft Teams Message** field.
4. To customize the tombstone message for files, update the **Microsoft Teams Files** field.
5. To allow users to unblock tombstoned messages, enable the **Allow unblock message** checkbox.



6. Click **Save**.

Configuring Microsoft Teams Policy

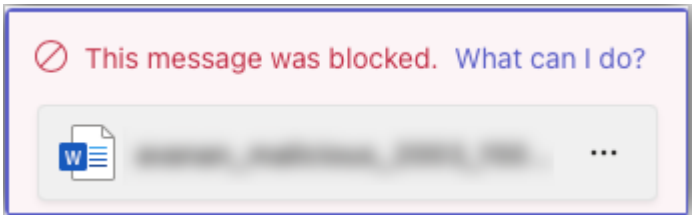
Malware Policy

By default, the Microsoft Teams malware policy scans for malicious content in the files sent using Microsoft Teams.

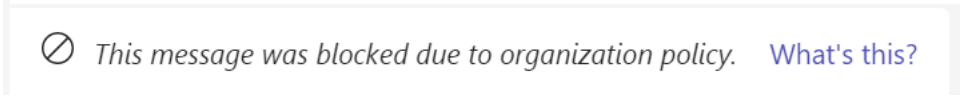
Supported Actions

Microsoft Teams malware policy supports these actions:

- Tombstone of files and text messages that contain malicious content.
  - If malicious content is found, the sender will get the tombstoned message.

    For information about unblocking the tombstoned message, see *"Unblocking Messages" on page 267*.
  - If malicious content is found, the recipient(s) will get the tombstoned message.

- Alert sender: Sends an email notification to the sender of a file or message that contains malicious content.
- Alert admin(s): Sends an email notification to the admin(s) about the malicious files or messages.

Configuring Malware Policy

To configure Malware policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Microsoft Teams.
4. From the **Choose Security** drop-down list, select **Malware** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Under **Blades**, select the threat detection blades required for the policy.

   Note - To select all the blades available for malware detection, enable **All running threat detection blades** checkbox.
7. Configure **Actions** required from the policy.

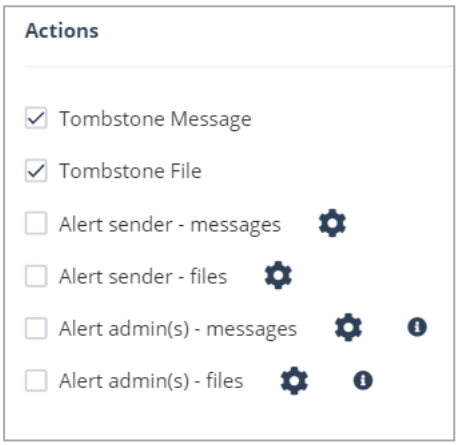
- To tombstone messages, enable the **Tombstone Message** checkbox.

  Note - This option will be available only in **Detect and Remediate** protection mode and when **URL Reputation** threat detection blade is enabled.

- To tombstone files, enable the **Tombstone File** checkbox.

  Note - This option will be available only in **Detect and Remediate** protection mode and when the **Anti-Malware** threat detection blade is enabled.

- To send email alerts to the sender about malware in messages and files, enable the **Alert sender - messages** and **Alert sender - files** checkbox.
- To send email alerts to admins about malware in messages and files, enable the **Alert admin(s) - messages** and **Alert admin(s) - files** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

8. Click **Save and Apply**.

DLP Policy

By default, the DLP policy scans the messages and files for potentially leaked information, such as credit card number and Social Security Number (SSN).

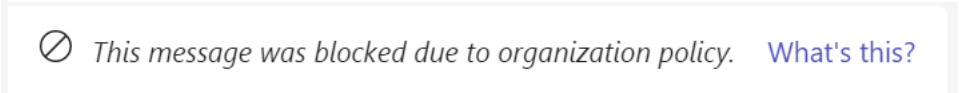
Supported Actions

Microsoft Teams DLP policy supports these actions:

- Tombstone of files and text messages that contain sensitive information.
  - If sensitive information is found, the sender will get the tombstoned message.

    For information about unblocking the tombstoned message, see *"Unblocking Messages" on page 267*.

  - If sensitive information is found, the recipient(s) will get the tombstoned message.



- Alert sender: Sends an email notification to the sender of a file or message that contains sensitive information.
- Alert admin(s): Sends an email notification to the admin(s) about the files or messages that contain sensitive information.

Configuring DLP Policy for Microsoft Teams

To configure DLP policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Microsoft Teams.
4. From the **Choose Security** drop-down list, select **DLP** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Under **DLP Criteria**, select the DLP categories required for the policy.

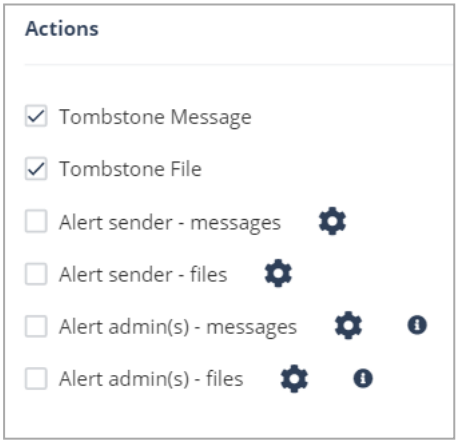
   For more details about the DLP Data Types and categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.
7. Select the sensitivity level required for the policy.

- Very high (hit count > 0)
- High (hit count > 2)
- Medium (hit count > 5)
- Low (hit count > 10)
- Very Low (hit count > 20)

8. To exclude DLP policy for the messages and files shared only with the internal users, enable the **Skip Internal items** checkbox.
9. Configure **Actions** required from the policy.
   - To tombstone messages, enable the **Tombstone Message** checkbox.

     Note - This option will be available only when **Detect and Remediate** protection mode is enabled.
   - To tombstone files, enable the **Tombstone File** checkbox.

     Note - This option will be available only when **Detect and Remediate** protection mode is enabled.
   - To send email alerts to the sender about DLP in messages and files, enable the **Alert sender - messages** and **Alert sender - files** checkbox.
   - To send email alerts to admins about DLP in messages and files, enable the **Alert admin(s) - messages** and **Alert admin(s) - files** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

10. Click **Save and Apply**.

Secured Microsoft Teams Messages

Avanan connects with Microsoft Teams using Microsoft APIs.

As Microsoft APIs are primarily designed to tackle DLP challenges and not malware/phishing messages, they allow different security levels based on whether the sender is within the organization and whether it is a direct message or part of a team channel conversation. These limitations affect both DLP and malicious message scenarios.

Message direction		Message visible in the portal	Generate events and alerts	Block malicious messages and files
Direct Messages				
Messages within the organization (Internal > Internal)		Yes	Yes	Yes
Messages sent from the organization to outside the organization (Internal > External)		Yes	Yes	Yes
Messages sent from outside the organization to the organization (External > Internal)		Yes	Yes	No
Messages sent in Microsoft Teams channels				
Channels created by internal (protected) users	Messages sent by internal users	Yes	Yes	Yes
	Messages sent by external users	Yes	Yes	Yes
Channel created by external users	Messages sent by internal users	No	No	No
	Messages sent by external users	No	No	No

Handling Partially Secured Messages

To protect the Microsoft Teams messages that cannot be inspected or tombstoned, administrators can do these:

- Configure the *"Malware Policy" on page 261* and *"DLP Policy" on page 263* to receive alerts and respond quickly to the detected malicious messages from external parties.
- Enhance the security settings for external meetings and chat with people outside the organization. See Microsoft documentation.

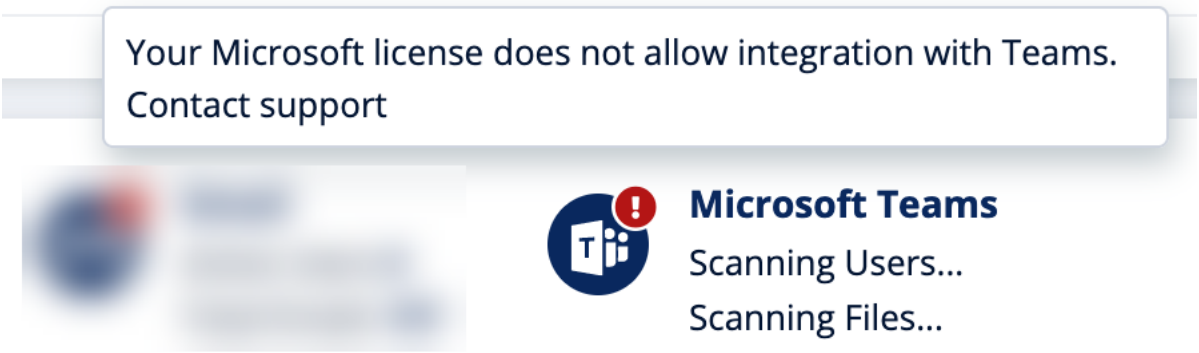
Secured Users

Like in any application, to protect a user's Microsoft Teams messages, the user must have one of the supported licenses. For more information, see *"Minimum License Requirements to Activate SaaS Applications" on page 43*.

Avanan does not protect messages sent by users and sent from external parties to users without a supported license. Also, these messages do not appear in the Avanan Administrator Portal.

If Avanan detects users with unsupported Microsoft Teams licenses, it shows the status on the **Overview** page.

- If there are no users with a supported license, Avanan shows an error indicator that Microsoft Teams is not secured.



- If there are some users with unsupported licenses, Avanan shows a warning indicator that some of the users are not protected.

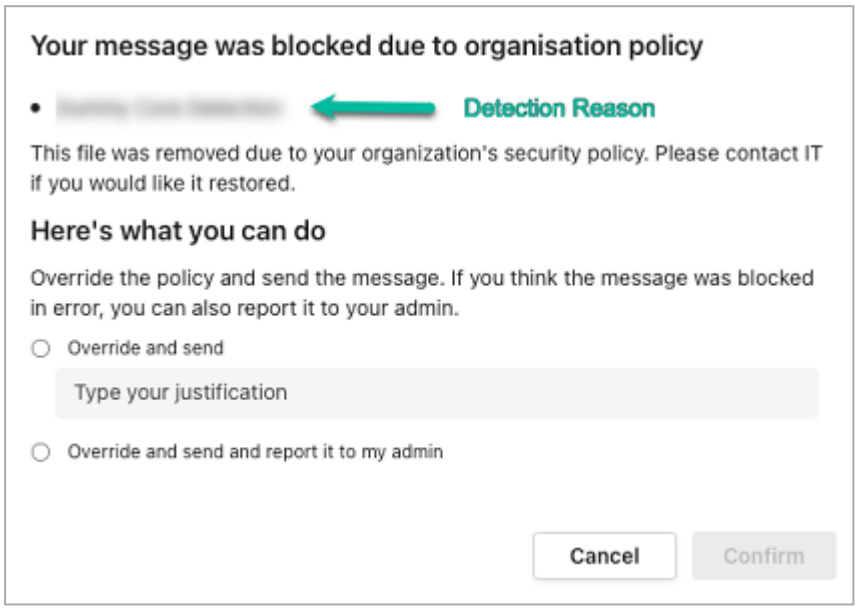
Unblocking Messages

When malicious or sensitive information is detected, Avanan tombstones the messages.

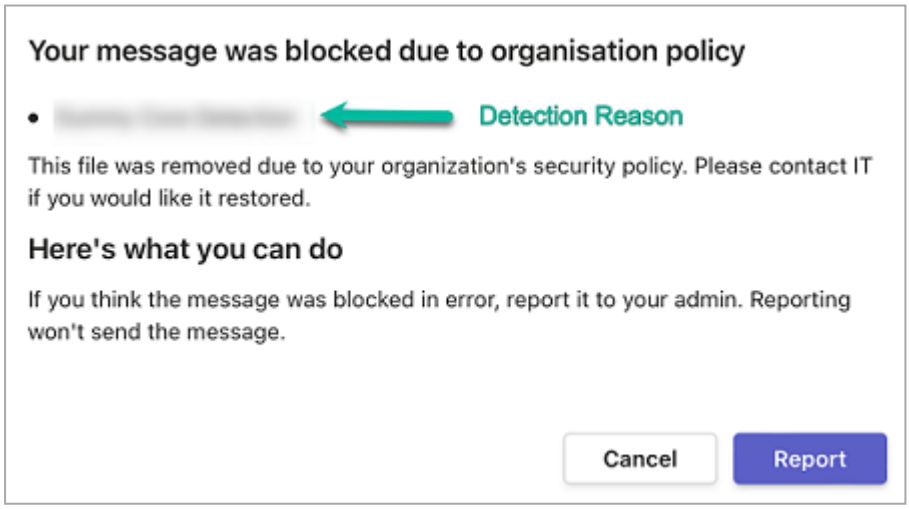
To unblock the message, the user should click **What can I do?**.

- If it is configured to allow unblocking the messages in *"Customizing Tombstone Messages" on page 260*, the sender can select one of these.

- To unblock the message:
  1. Select **Override and send**.
  2. Enter the justification for sending the message.
  3. Click **Confirm**.
- To unblock the message and also report it to the administrator, the sender can select **Override and send and report it to my admin** and click **Confirm**.



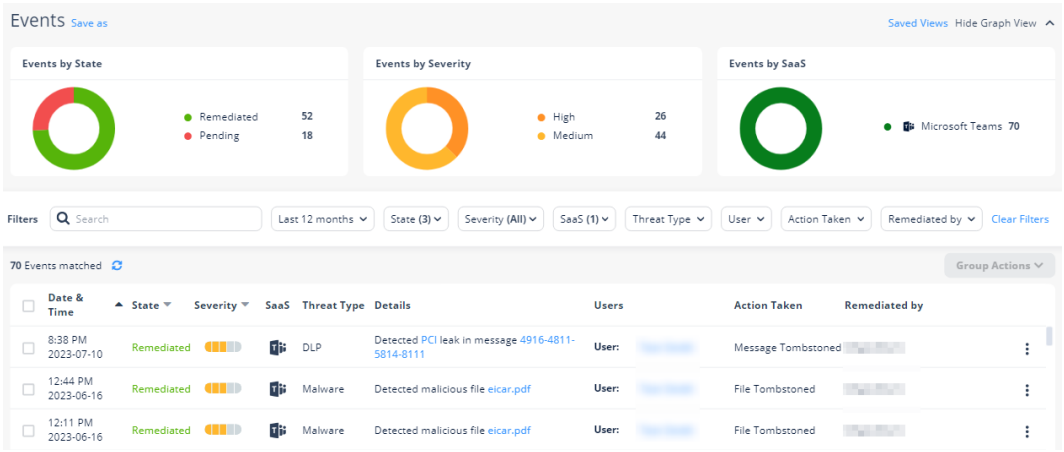
- If it is not configured to allow unblocking the messages, the sender will see the following message:



Viewing Microsoft Teams Security Events

Avanan records the Microsoft Teams detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.



Slack

Overview

Slack is a messaging platform designed for the workplace. It offers employees and external collaborators to chat, meet online, and share files. Avanan adds security, privacy, and compliance to Slack by scanning messages and files for malicious content and data leakage (DLP) and generates actionable events on malicious content.

Avanan scans the messages and files shared through direct messaging or channels (private (internal users) and private-to-public channels).

How it works

Avanan adds a layer of security that provides these security features for Slack:

- Data Leak Prevention (DLP): Protecting sensitive text messages and files
- Anti-Malware: Scanning of files for malicious content
- URL Reputation: Blocking malicious links within files and messages
- Remediation: Tombstoning malicious files or sensitive files and messages

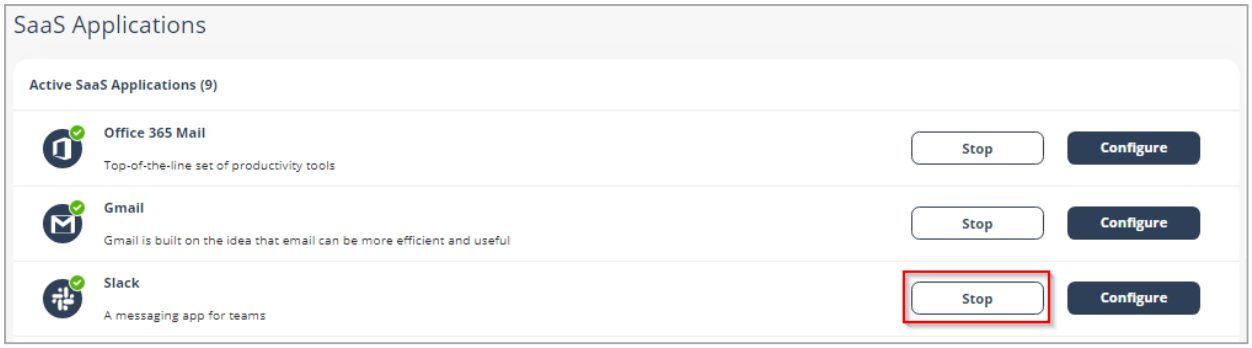
Activating Slack

For details about the procedure to activate Slack, see *"Activating Slack" on page 93*.

Deactivating Slack

To deactivate Slack:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Slack.



Slack Security Settings

Customizing Tombstone Messages

If a message/file is tombstoned, a tombstone message will appear instead of the tombstoned message/file. The original message/file becomes inaccessible to the sender and the recipients in the chat/channel.

Administrators can customize the tombstone message for both messages and files.

To customize the tombstone messages:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Slack.
3. To customize the tombstone message for messages, update the **Slack Message** field.
4. To customize the tombstone message for files, update the **Slack Files** field.
5. To allow users to unblock messages, clear the **Allow unblock message** checkbox.
6. Click **Save**.

Configuring Slack Policy

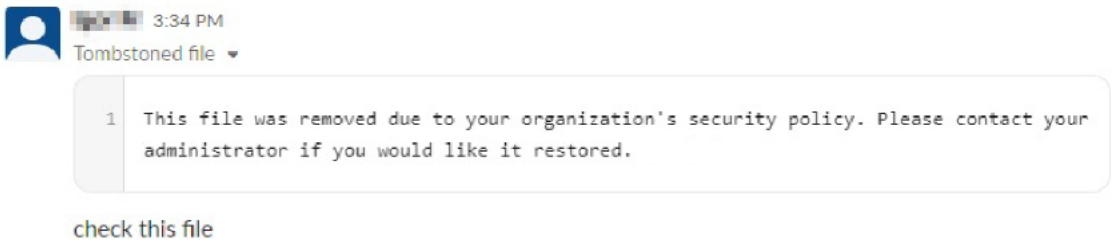
Malware Policy

By default, the Slack malware policy scans for malicious content in the files sent using Slack.

Supported Actions

Slack malware policy supports these actions:

- Tombstone of files and text messages that contain malicious content.
  - If malicious content is found, the sender will get the tombstoned message.
  - If malicious content is found, the recipient(s) will get the tombstoned message.



- Alert sender: Sends an email notification to the sender of a file or message that contains malicious content.
- Alert admin(s): Sends an email notification to the admin(s) about the malicious files and messages.

Configuring Malware Policy

To configure Malware policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Slack.
4. From the **Choose Security** drop-down list, select **Malware** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Under **Blades**, select the threat detection blades required for the policy.

   Note - To select all the blades available for malware detection, enable the **All running threat detection blades** checkbox.
7. Configure **Actions** required from the policy.
   a. To tombstone messages, enable the **Tombstone Message** checkbox.

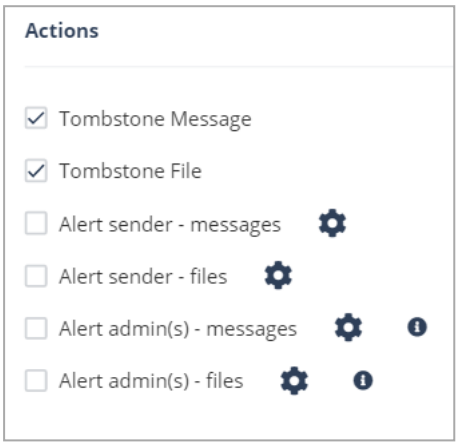
      Note - This option will be available only in **Detect and Remediate** protection mode and when **URL Reputation** threat detection blade is enabled.

b. To tombstone files, enable the **Tombstone File** checkbox.

Note - This option will be available only in **Detect and Remediate** protection mode and when **Anti-Malware** threat detection blade is enabled.

c. To send email alerts to the sender about malware in messages and files, enable the **Alert sender - messages** and **Alert sender - files** checkbox.

d. To send email alerts to admins about malware in messages and files, enable the **Alert admin(s) - messages** and **Alert admin(s) - files** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

8. Click **Save and Apply**.

DLP Policy

By default, the DLP policy scans the messages and files for potentially leaked information, such as credit card number and Social Security Number (SSN).

Supported Actions

Slack DLP policy supports these actions:

- Tombstone of files and text messages that contain sensitive information.
  - If sensitive information is found, the sender will get the tombstoned message.
  - If sensitive information is found, the recipients(s) will get the tombstoned message.
- Alert sender: Sends an email notification to the sender of a file or message that contains sensitive information.
- Alert admin(s): Sends an email notification to the admin(s) about the files or messages that contain sensitive information.

Configuring DLP Policy for Slack

To configure DLP policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Slack.
4. From the **Choose Security** drop-down list, select **DLP** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

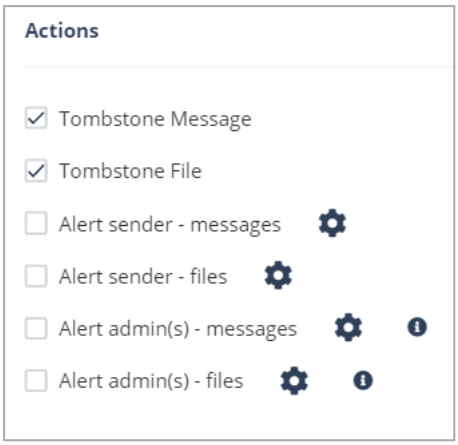
   If required, you can change the **Rule Name**.
6. Under **DLP Criteria**, select the DLP categories required for the policy.

   For more information about the DLP Data Types and categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.
7. Select the sensitivity level required for the policy.
   a. Very high (hit count > 0)
   b. High (hit count > 2)
   c. Medium (hit count > 5)
   d. Low (hit count > 10)
   e. Very Low (hit count > 20)
8. To exclude DLP policy for the messages and files shared only with the internal users, enable the **Skip Internal items** checkbox.
9. Configure **Actions** required from the policy.
   a. To tombstone messages, enable the **Tombstone Message** checkbox.

      Note - This option will be available only when **Detect and Remediate** protection mode is enabled.
   b. To tombstone files, enable the **Tombstone File** checkbox.

      Note - This option will be available only when **Detect and Remediate** protection mode is enabled.
   c. To send email alerts to the sender about DLP in messages and files, enable the **Alert sender - messages** and **Alert sender - files** checkbox.

d. To send email alerts to admins about DLP in messages and files, enable the **Alert admin(s) - messages** and **Alert admin(s) - files** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

10. Click **Save and Apply**.

Viewing Slack Security Events

Avanan records the Slack detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.

For information about how collects and handles your information, see privacy policy.

File Storage Protection

Office 365 OneDrive

Overview

Office 365 OneDrive is a cloud storage system that allows sharing files and collaboration. Avanan adds security, privacy, and compliance to Office 365 OneDrive by scanning files shared in OneDrive for malicious content and data loss prevention (DLP) and generates actionable events on malicious content.

Note - Avanan scans only the organization's Office 365 OneDrive and does not scan files and folders outside the organization, even if the user has access to them.

How it works

Avanan adds a layer of security that provides these security features for Office 365 OneDrive:

- Data Leak Prevention (DLP): Protecting sensitive text messages and files
- Anti-Malware: Scanning of files for malicious content
- Remediation: Quarantine malicious files and send files containing sensitive data to the vault

Required Permissions

Avanan requires these permissions to protect Office 365 OneDrive.

Note - All these permissions are required to access your data in the Avanan Administrator Portal.

Permissions required from Microsoft	Functions performed by Avanan
Manage all access reviews	Allows the app to read, update, delete and perform actions on access reviews, reviewers, decisions, and settings in the organization without a signed-in user.
Read and write all applications	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.

Permissions required from Microsoft	Functions performed by Avanan
Read and write contacts in all mail boxes	Allows the app to create, read, update, and delete all contacts in all mailboxes without a signed-in user.
Read and write directory data	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.
Read and write domains	Allows the app to read and write all domain properties without a signed-in user. Also allows the app to add, verify and remove domains.
Read and write files in all site connections	Allows the app to read, create, update and delete all files in all site collections without a signed-in user.
Read and write all groups	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.
Read and write all user mailbox settings	Allows the app to create, read, update, and delete user's mailbox settings without a signed-in user. Does not include permission to send mail.
Read and write mail in all mailboxes	Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user. Does not include permission to send mail.
Send mail as any user	Allows the app to send mail as any user without a signed-in user.
Read all usage reports	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Microsoft 365 and Microsoft Entra ID (formerly Azure AD).
Read and update your organization’s security events	Allows the app to read your organization’s security events without a signed-in user. Also allows the app to update editable properties in security events.
Read and write items in all site collections	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed-in user.

Permissions required from Microsoft	Functions performed by Avanan
Read and write all users' full profiles	Allows the app to read and update user profiles without a signed-in user.
Sign in and read user profile	Allows users to sign in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

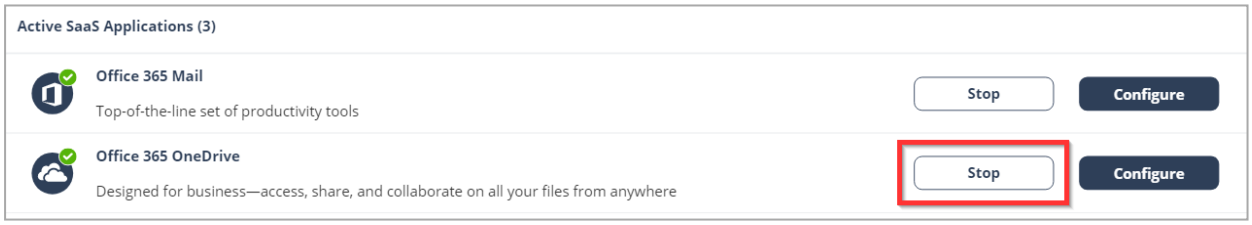
Activating Office 365 OneDrive

For details about the procedure to activate Office 365 OneDrive, see *"Activating Office 365 OneDrive" on page 83*.

Deactivating Office 365 OneDrive

To deactivate Office 365 OneDrive:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Office 365 OneDrive.



Office 365 OneDrive Security Settings

Customizing Quarantine and Vault

Administrators can customize the Quarantine and Vault folders (folder names, quarantine/vault messages, etc.)

Quarantine Folder

The Quarantine folder is used to quarantine malware-infected or sensitive files related to OneDrive. Infected or sensitive files of all the users gets quarantined and is placed in a single predefined **Quarantine** folder for your complete organization.

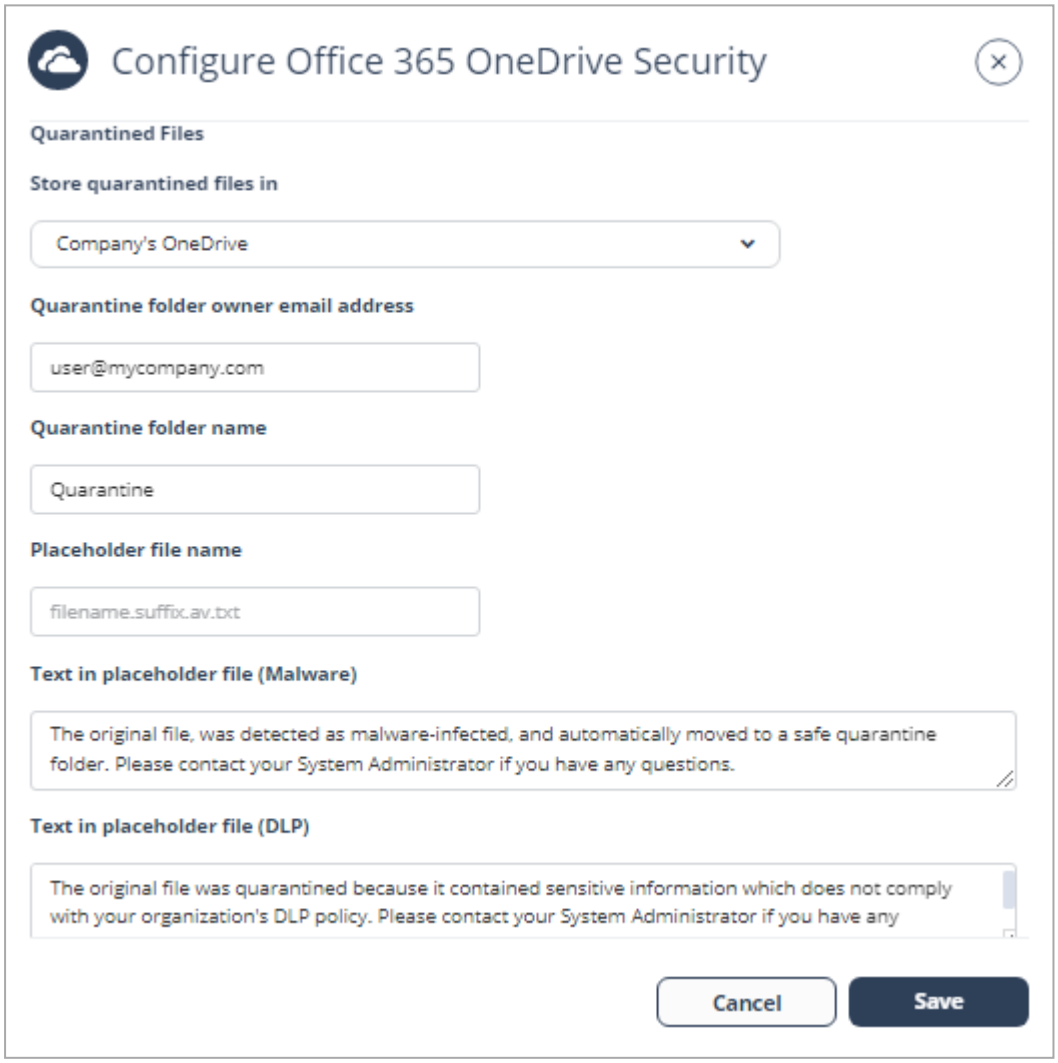
You can configure the Threat Detection policy and DLP policy to quarantine only malware and not sensitive files (which can be placed in end-user's Vault).

Notes:

- The Quarantine folder can be stored in your organization's OneDrive or in the Avanan cloud in the region associated with your organization's Avanan account.
- End users do not have access to this folder.

To customize the Quarantine folder:

1. Navigate to **Security Settings** > **SaaS Applications**.
2. Click **Configure** for Office 365 OneDrive.
3. Go to **Quarantined Files** section.
4. Under **Store quarantined files in**, select where you want to store the quarantined files:
   - **Check Point** - Stores the quarantined files in the Avanan cloud in the region associated with your organization's Avanan account.
   - **Company's OneDrive** - Stores the quarantined files in a Quarantine folder located in your organization's OneDrive account.



5. If you selected **Company's OneDrive** in the previous step, enter these details for the quarantine folder:
   - Under **Quarantine folder owner email address**, enter the required email address.

     Note - OneDrive must exist for the email address you enter here.

   - Under **Quarantine folder name**, enter the required folder name.

     Note - A **Quarantine folder** gets created with the entered name in the root directory of the given email address.
6. (Optional) If you need to configure the content of the file that replaces the quarantined malicious file in its original folder, enter the text under **Text in placeholder file (Malware)**.
7. (Optional) If you need to configure the content of the file that replaces the quarantined sensitive file in its original folder, enter the text under **Text in placeholder file (DLP)**.
8. Click **Save**.

Vault Folder

A Vault folder is used to remediate DLP detections related to OneDrive files. It is a non-shared folder that is created for every OneDrive user.

If a file contains sensitive information that does not comply with your organization's data-sharing policies, it is removed and placed in the Vault folder.

Notes:

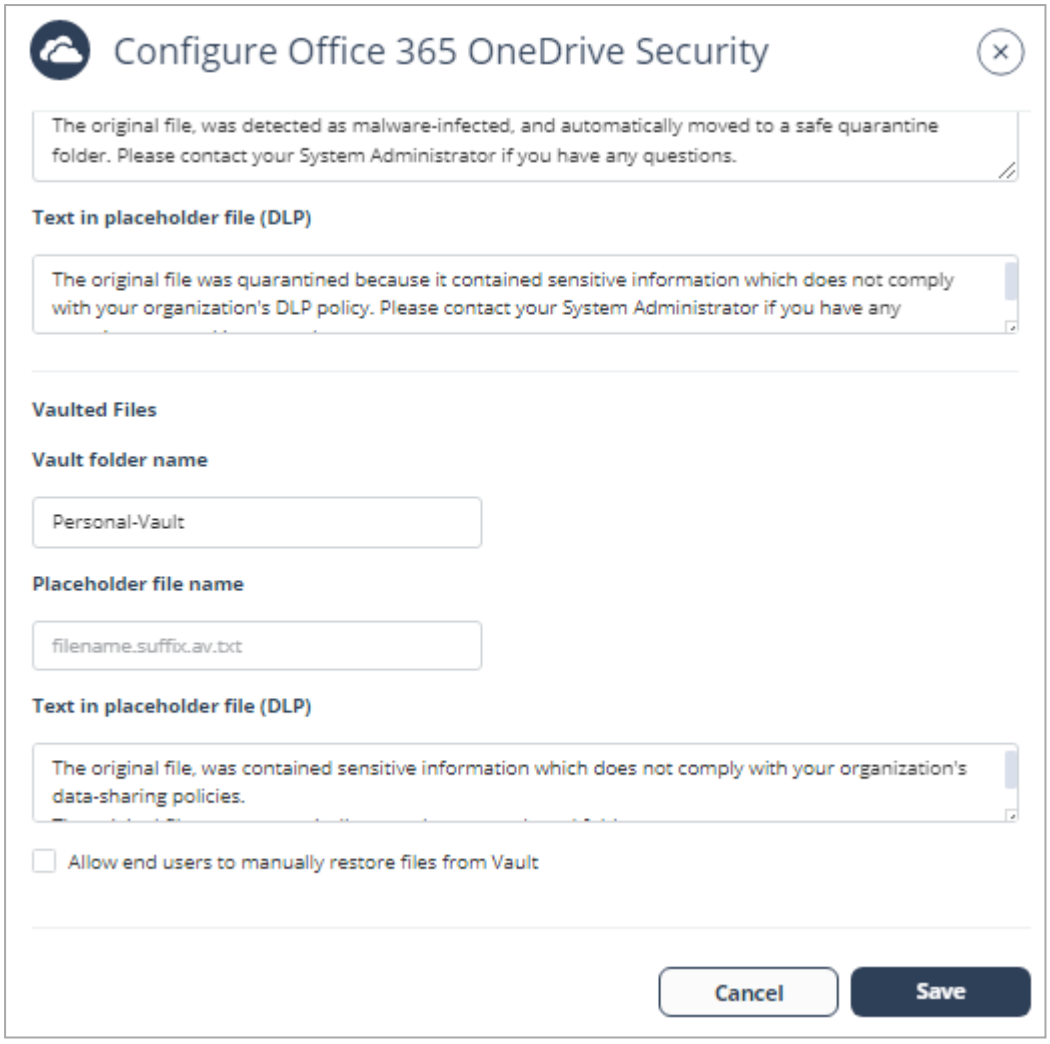
- The Vault folder gets created with the specified name in the root directory of each user.
- The user can access the file from the Vault but cannot share it with others.

To customize the Vault folder:

1. Click **Security Settings > SaaS Applications**.
2. Click **Configure** for Office 365 OneDrive.
3. Go to **Vaulted Files** section.
4. Under **Vault folder name**, enter the required vault folder name.

   Note - The Vault folder gets created with the specified name in the root directory of each user.

5. If you want to allow end users to manually restore files from the Vault, enable the **Allow end users to manually restore files from Vault** checkbox.



6. (Optional) If you need to configure the content of the file that replaces the vaulted sensitive file in its original folder, enter the text under **Text in placeholder file (DLP)**.
7. Click **Save**.

Configuring Office 365 OneDrive Policy

Malware Policy

By default, the Office 365 OneDrive malware policy scans the uploaded files for malicious content.

Supported Actions

Office 365 OneDrive malware policy supports these actions:

- Quarantine/removal of malware-infected files.
- Alert owner: Sends an email notification to the user who uploaded a file that contains malicious content.
- Alert admin(s): Sends an email notification to the admin(s) about the malicious files.

Configuring Malware Policy

To configure Malware policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Office 365 OneDrive.
4. From the **Choose Security** drop-down list, select **Malware** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Choose **Scope** for the policy.
   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.
7. Under **Blades**, select the threat detection blades required for the policy.

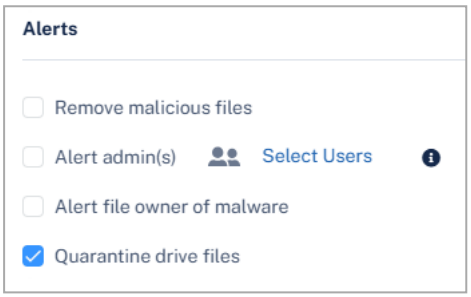
   Note - To select all the blades available for malware detection, enable **All running threat detection blades** checkbox.
8. Under **Suspected malware attachments workflow**, select the workflow required for the policy.
   - Quarantine. User is not alerted (admin can restore)
   - Do nothing

   Note - The **Workflows** are available only when **Detect and Remediate** protection mode is enabled.
9. To quarantine malware-infected files, enable the **Quarantine drive files** checkbox under **Alerts**.

   Note - This option is available only in **Detect and Remediate** protection mode.
10. To remove malware-infected files, enable the **Remove malicious files** checkbox under **Alerts**.

Notes:
- If you enable this option, malicious files will be removed permanently, and you cannot restore them.
- For a policy, you can only enable **Quarantine drive files** or **Remove malicious files**.

11. Configure **Alerts** for the policy.
    a. To send email alerts to the file owner of malware, enable the **Alert file owner of malware** checkbox.
    b. To send email alerts to admins about malware, enable the **Alert admin(s)** checkbox.



Notes:
- To customize the email alert templates, click on the gear icon to the right of the alert.

12. Click **Save and Apply**.

DLP Policy

By default, the DLP policy scans the uploaded files to OneDrive for potentially leaked information, such as credit card number and Social Security Number (SSN).

Supported Actions

Office 365 OneDrive DLP policy supports these actions:

- Send files with sensitive data to the vault.
- Alert owner: Sends an email notification to the user who uploaded a file that contains sensitive information.
- Alert admin(s): Sends an email notification to the admin(s) about the files that contain sensitive information.

Configuring DLP Policy for OneDrive

To configure DLP policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Office 365 OneDrive.
4. From the **Choose Security** drop-down list, select **DLP** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Choose **Scope** for the policy.
   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.
7. Under **DLP Criteria**, select the DLP categories required for the policy.

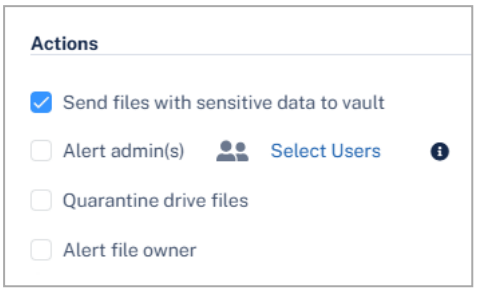
   For more information about the DLP Data Types and categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.
8. Select the sensitivity level required for the policy.
   a. Very high (hit count > 0)
   b. High (hit count > 2)
   c. Medium (hit count > 5)
   d. Low (hit count > 10)
   e. Very Low (hit count > 20)
9. To exclude DLP policy for the files shared only with the internal users, enable the **Skip Internal items** checkbox.
10. Configure **Actions** for the policy.
    a. To send a detected file with sensitive data to its owner's vault, enable the **Send files with sensitive data to vault** checkbox.

       Note - This option will be available only in **Detect and Remediate** protection mode.

b. To send email alerts to admins about DLP, enable the **Alert admin(s)** checkbox.

c. To send email alerts to the file owner about DLP, enable the **Alert file owner(s)** checkbox.

d. To quarantine drive files, enable the **Quarantine drive files** checkbox.



Notes:

- For a policy, you can only enable **Send file with sensitive data to vault** or **Quarantine drive files**.
- To customize the email alert templates, click on the gear icon to the right of the alert.

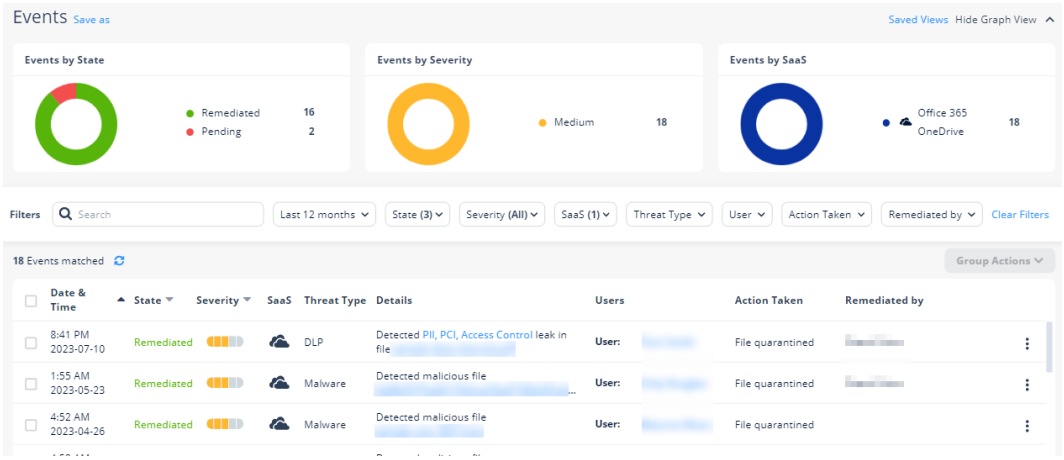
11. Click **Save and Apply**.

Viewing Office 365 OneDrive Security Events

Avanan records the OneDrive detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.

Note - For files marked as malware by Microsoft, scan results are unavailable and access to these files is prevented by Microsoft.



Office 365 SharePoint

Overview

Office 365 SharePoint empowers teamwork with dynamic and productive team sites for every project team, department, and division. Avanan adds security, privacy, and compliance to Office 365 SharePoint by scanning files shared in SharePoint for malicious content and data loss prevention (DLP) and generates actionable events on malicious content.

Note - Avanan scans only the organization's Office 365 SharePoint and does not scan files and folders outside the organization, even if the user has access to them.

How it works

Avanan adds a layer of security that provides these security features for Office 365 SharePoint:

- Data Leak Prevention (DLP): Protecting uploaded files containing sensitive data
- Anti-Malware: Scanning of files for malicious content
- Remediation: Quarantine malicious files and send files containing sensitive data to the vault

Required Permissions

Avanan requires these permissions to protect Office 365 SharePoint.

Note- All these permissions are required to access your data in the Avanan portal.

Permissions required from Microsoft	Functions performed by Avanan
Manage all access reviews	Allows the app to read, update, delete and perform actions on access reviews, reviewers, decisions, and settings in the organization without a signed-in user.
Read and write all applications	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.
Read and write contacts in all mail boxes	Allows the app to create, read, update, and delete all contacts in all mailboxes without a signed-in user.
Read and write directory data	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.

Permissions required from Microsoft	Functions performed by Avanan
Read and write domains	Allows the app to read and write all domain properties without a signed-in user. Also allows the app to add, verify and remove domains.
Read and write files in all site connections	Allows the app to read, create, update and delete all files in all site collections without a signed-in user.
Read and write all groups	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.
Read and write all user mailbox settings	Allows the app to create, read, update, and delete user's mailbox settings without a signed-in user. Does not include permission to send mail.
Read and write mail in all mailboxes	Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user. Does not include permission to send mail.
Send mail as any user	Allows the app to send mail as any user without a signed-in user.
Read all usage reports	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Microsoft 365 and Microsoft Entra ID (formerly Azure AD).
Read and update your organization’s security events	Allows the app to read your organization’s security events without a signed-in user. Also allows the app to update editable properties in security events.
Read and write items in all site collections	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed-in user.
Read and write all users' full profiles	Allows the app to read and update user profiles without a signed-in user.
Sign in and read user profile	Allows users to sign in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

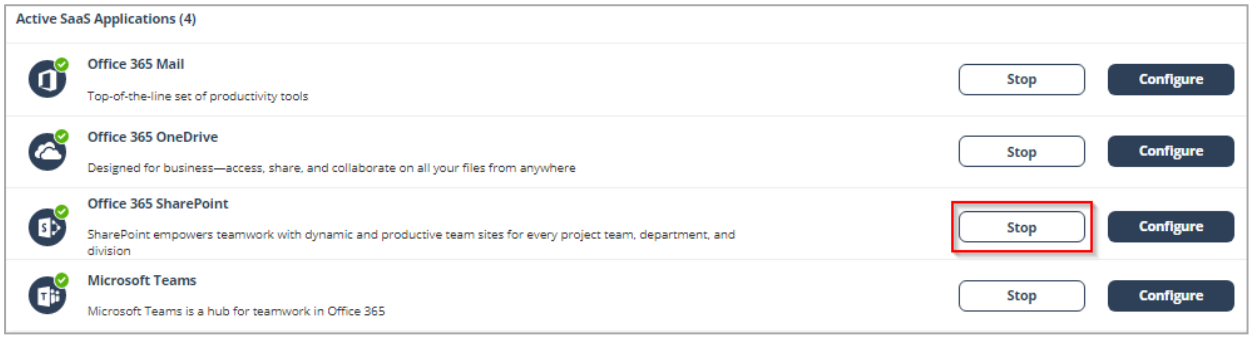
Activating Office 365 SharePoint

For details about the procedure to activate Office 365 SharePoint, see *"Activating Office 365 SharePoint" on page 84*.

Deactivating Office 365 SharePoint

To deactivate Office 365 SharePoint:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for Office 365 SharePoint.



Office 365 SharePoint Security Settings

Customizing Quarantine and Vault

Administrators can customize the quarantine and vault folders (folder names, quarantine/vault messages, etc.)

Quarantine folder

The quarantine folder is used to quarantine malware-infected files from SharePoint. The infected files of all the users will be quarantined to a single predefined quarantine folder.

Notes:

- The quarantine folder gets created with the configured name on the root directory of the root site of the organization. End users will not have access to this folder.
- Only Microsoft stores these quarantined files.

Vault folder

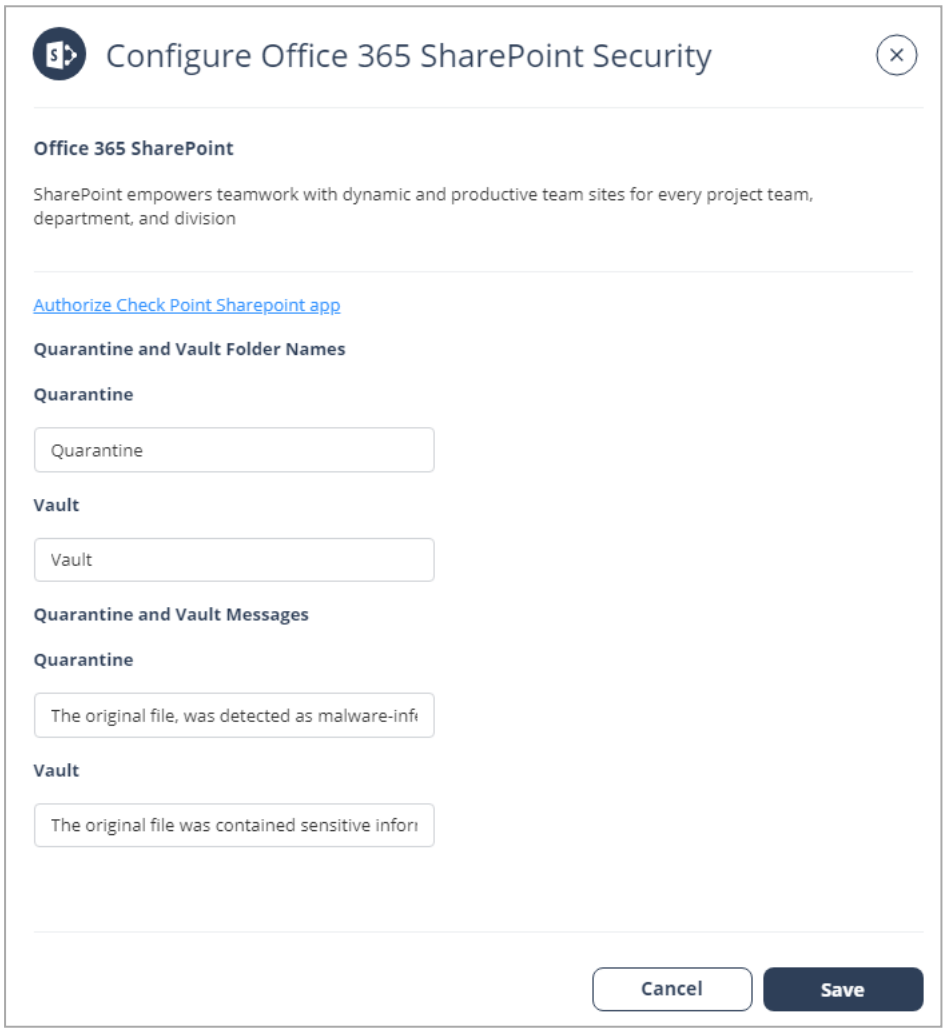
A vault folder is used to remediate DLP detections related to SharePoint files. It is a non-shared folder that is created for every SharePoint user.

If a file contains sensitive information that does not comply with your organization's data-sharing policies, it is removed and placed in the vault folder.

Note - Vault folder is created with the configured folder name in the root directory of each user's drive. The user can access the file from the vault but cannot share it with others.

To customize the quarantine and vault folders:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Configure** for Office 365 SharePoint.
3. Under **Quarantine**, enter the required quarantine folder name.
4. Under **Vault**, enter the required vault name.
5. Click **Save**.



Configuring Office 365 SharePoint Policy

Malware Policy

By default, the Office 365 SharePoint malware policy scans the uploaded files for malicious content.

Supported Actions

Office 365 SharePoint malware policy supports these actions:

- Quarantine of malware-infected files.
- Alert owner: Sends an email notification to the user who uploaded a file that contains malicious content.
- Alert admin(s): Sends an email notification to the admin(s) about the malicious files.

Configuring Malware Policy

To configure Malware policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Office 365 SharePoint.
4. From the **Choose Security** drop-down list, select **Malware** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

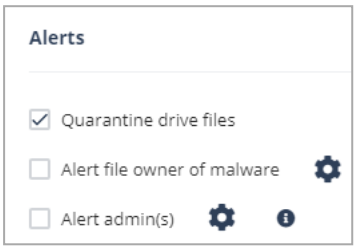
   If required, you can change the **Rule Name**.
6. Choose **Scope** for the policy.
   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.
7. Under **Blades**, select the threat detection blades required for the policy.

   Note - To select all the blades available for malware detection, enable **All running threat detection blades** checkbox.
8. Under **Suspected malware workflow (Attachment)** in **Workflows**, select the workflow required for the policy.
   - Quarantine. User is not alerted (admin can restore)
   - Do nothing

   Note - The **Workflows** are available only when **Detect and Remediate** protection mode is enabled.
9. To quarantine malware-infected files, enable the **Quarantine drive files** checkbox.

Note - This option will be available only in **Detect and Remediate** protection mode.

10. Configure **Alerts** for the policy.
    a. To send email alerts to the file owner of malware, enable the **Alert file owner of malware** checkbox.
    b. To send email alerts to admins, enable the **Alert admin(s)** checkbox.



Notes:
- To customize the email alert templates, click on the gear icon to the right of the alert.

11. Click **Save and Apply**.

DLP Policy

By default, the DLP policy scans the uploaded files to SharePoint for potentially leaked information, such as credit card number and Social Security Number (SSN).

Supported Actions

Office 365 SharePoint DLP policy supports these actions:

- Send files with sensitive data to the vault.
- Alert owner: Sends an email notification to the user who uploaded a file that contains sensitive information.
- Alert admin(s): Sends an email notification to the admin(s) about the files that contain sensitive information.

Configuring DLP Policy for SharePoint

To configure DLP policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Office 365 SharePoint.
4. From the **Choose Security** drop-down list, select **DLP** and click **Next**.

5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.

6. Choose **Scope** for the policy.

   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.

7. Under **DLP Criteria**, select the DLP categories required for the policy.

   For more information about the DLP Data Types and categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.

8. Select the sensitivity level required for the policy.

   a. Very high (hit count > 0)

   b. High (hit count > 2)

   c. Medium (hit count > 5)

   d. Low (hit count > 10)

   e. Very Low (hit count > 20)

9. To exclude DLP policy for the messages and files shared only with the internal users, enable the **Skip Internal items** checkbox.

10. Configure **Actions** for the policy.

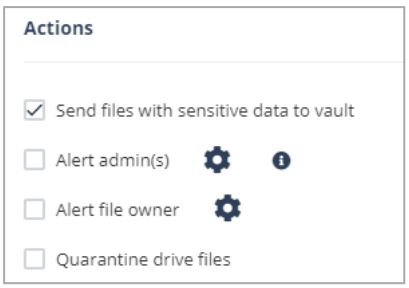
    a. To send a detected file with sensitive data to its owner's vault, enable the **Send files with sensitive data to vault** checkbox.

       Note - This option will be available only in **Detect and Remediate** protection mode.

    b. To send email alerts to admins about DLP, enable the **Alert admin(s)** checkbox.

    c. To send email alerts to the file owner about DLP, enable the **Alert file owner(s)** checkbox.

d. To quarantine drive files, enable the **Quarantine drive files** checkbox.



Notes:

- For a policy, you can only enable **Send file with sensitive data to vault** or **Quarantine drive files**.
- To customize the email alert templates, click on the gear icon to the right of the alert.

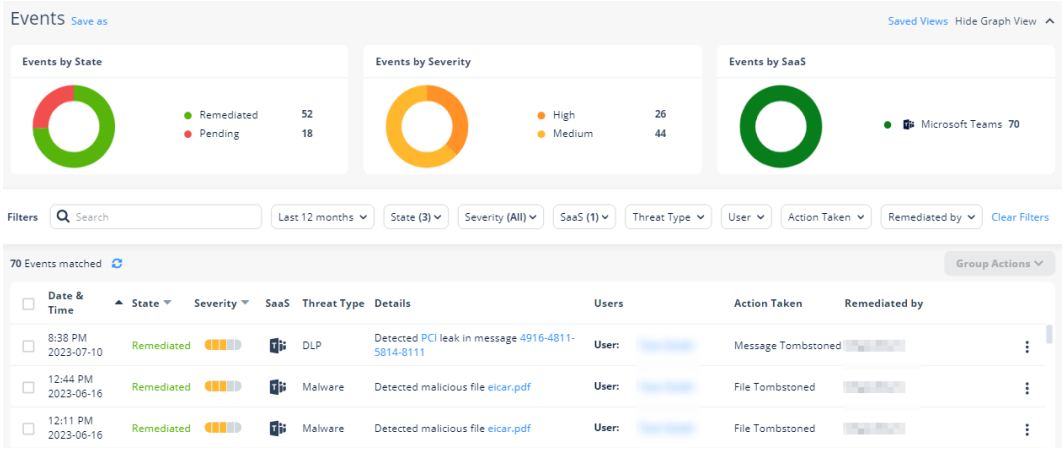
11. Click **Save and Apply**.

Viewing Office 365 SharePoint Security Events

Avanan records the SharePoint detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.

Note - For files marked as malware by Microsoft, scan results are unavailable and access to these files is prevented by Microsoft.



Google Drive

Overview

Google Drive is a cloud storage system that allows file sharing and collaboration. Avanan adds security, privacy, and compliance to Google Drive by scanning files shared in Google Drive for malicious content and data loss prevention (DLP) and generates actionable events on malicious content.

How it works

Avanan adds a layer of security that provides these security features for Google Drive:

- Data Leak Prevention (DLP): Protecting uploaded files containing sensitive data
- Anti-Malware: Scanning of files for malicious content
- Remediation: Quarantine malicious files and files containing sensitive data.

Required Permissions

The cloud state for Google Drive used by Avanan is composed of the following entities:

- Users
- Groups and Memberships
- Tokens
- Apps
- Files and Folders
- Permissions

Once the cloud state is saved, Avanan starts monitoring the changes for each user. To track changes for each user in the cloud, Avanan uses the following channels:

- Subscribe each user to Google Push Notifications for changes (https://developers.google.com/drive/v3/web/push).
- Fallback to polling each user every minute if push notifications fails (https://developers.google.com/drive/v3/web/manage-changes)
- Subscribe each user to Google Reports API to get its activities related to permissions, authorization to external apps, and tokens. (https://developers.google.com/admin-sdk/reports/v1/get-start/getting-started)

Avanan uses the following resources for Google Drive from the APIs:

- Files and Folders metadata (not include file contents)
- Users and Groups metadata

- Permissions
- Changes (not including the content of files changed)
- Channels
- Tokens
- Applications

Activating Google Drive

For details about the procedure to activate Google Drive, see *"Activating Google Drive" on page 89*.

Deactivating Google Drive

To deactivate Google Drive:

1. Click **Security Settings > SaaS Applications**.
2. Click **Stop** for Google Drive.

Google Drive Security Settings

Customizing Quarantine

Administrators can customize the quarantine folder and location (email address).

Quarantine folder

The quarantine folder is used to quarantine malware-infected files and files containing sensitive information that does not comply with the organization's data-sharing policies. All these files will be quarantined to a single predefined quarantine folder.

Notes:

- The quarantine folder gets created in the root directory of the given email address. End users will not have access to this folder.
- Only Google stores these quarantined files.

Configuring Google Drive Policy

Malware Policy

By default, the Google Drive malware policy scans the uploaded files for malicious content.

Supported Actions

Google Drive malware policy supports these actions:

- Quarantine malware-infected files.
- Alert owner: Sends an email notification to the user who uploaded a file that contains malicious content.
- Alert admin(s): Sends an email notification to the admin(s) about the malicious files.

Configuring Malware Policy

To configure Malware policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Google Drive.
4. From the **Choose Security** drop-down list, select **Malware** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Choose **Scope** for the policy.
   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.
7. Under **Blades**, select the threat detection blades required for the policy.

   Note - To select all the blades available for malware detection, enable **All running threat detection blades** checkbox.
8. Under **Suspected malware workflow (Attachment)** in **Workflows**, select the workflow required for the policy.

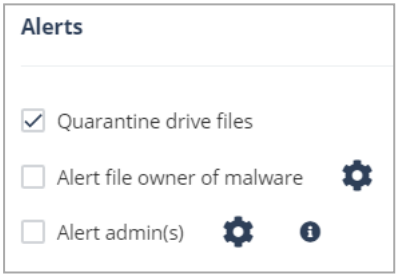
- Quarantine. User is alerted and allowed to restore
- Quarantine. User is alerted, allowed to request a restore (admin must approve)
- Quarantine. User is not alerted (admin can restore)
- Do nothing

Note - The **Workflows** are available only when **Detect and Remediate** protection mode is enabled.

9. To quarantine malware-infected files, enable the **Quarantine drive files** checkbox.

   Note - This option will be available only in **Detect and Remediate** protection mode.

10. Configure **Alerts** for the policy.
    a. To send email alerts to the file owner of malware, enable the **Alert file owner of malware** checkbox.
    b. To send email alerts to admin(s) about malware, enable the **Alert admin(s)** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

11. Click **Save and Apply**.

DLP Policy

By default, the DLP policy scans the uploaded files to Google Drive for potentially leaked information, such as credit card number and Social Security Number (SSN).

Supported Actions

Google Drive DLP policy supports these actions:

- Quarantine potentially leaked information files.
- Alert owner: Sends an email notification to the user who uploaded a file that contains sensitive information.

- Alert admin(s): Sends an email notification to the admin(s) about the files that contain sensitive information.

Configuring DLP Policy for Google Drive

To configure DLP policy:

1. Click **Policy** on the left panel of the Avanan Administrator Portal.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** drop-down list, select Google Drive.
4. From the **Choose Security** drop-down list, select **DLP** and click **Next**.
5. Select the desired protection mode (**Detect and Remediate** or **Detect**).

   If required, you can change the **Rule Name**.
6. Choose **Scope** for the policy.
   - To apply the policy to specific users or groups, select the users and groups and click **Add to Selected**.
   - To apply the policy to all users and groups in your organization, enable **All Users and Groups** checkbox.
   - To exclude specific users or groups from the policy, select the users/groups and click **Add to Excluded**.
7. Under **DLP Criteria**, select the DLP categories required for the policy.

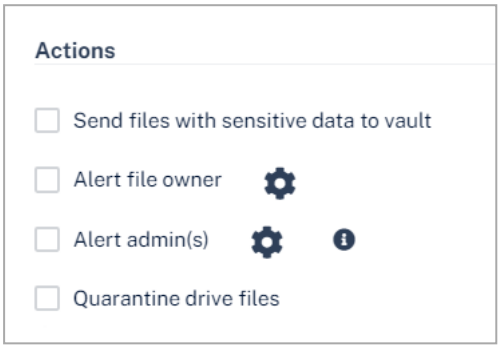
   For more information about the DLP Data Types and categories, see *"Appendix C: DLP Built-in Data Types and Categories" on page 594*.
8. Select the sensitivity level required for the policy.
   a. Very high (hit count > 0)
   b. High (hit count > 2)
   c. Medium (hit count > 5)
   d. Low (hit count > 10)
   e. Very Low (hit count > 20)
9. To exclude DLP policy for the messages and files shared only with the internal users, enable the **Skip Internal items** checkbox.
10. Configure the **Actions** required for the policy.

a. To send files with sensitive data to vault, select the **Send files with sensitive data to vault** checkbox.

b. To send email alerts to admins about DLP, select the **Alert admin(s)** checkbox.

c. To send email alerts to the file owner about DLP, select the **Alert file owner(s)** checkbox.

d. To send a detected file with sensitive data to quarantine (no access for the file owner), select the **Quarantine drive files** checkbox.



Notes:

- To customize the email alert templates, click on the gear icon to the right of the alert.

11. Click **Save and Apply**.

Viewing Google Drive Security Events

Avanan records the Google Drive detections as security events. The event type depends on the type of policy that created the event. You can handle the security events in different ways, whether they are detected/prevented automatically or discovered by the administrators after not being prevented.

The **Events** screen shows a detailed view of all the security events.

Action on Files Placed in Vault

When a data leak is detected in a file, Avanan takes these steps:

- Revokes the file permissions.
- Moves the file to a secure Vault folder.

Avanan stores this vault folder on the user's local drive and cannot be shared with others.

Vault Action in Externally Shared Drives

For files stored in **My Drive**, access is managed by the file owner unless the file or folder is specifically shared with others.

For shared drives, when the drive is shared externally, the permissions set on the drive apply to all files within it.

Note - If a drive is shared externally, the standard Vault process may not function as expected. It is not possible to revoke access from individual files as they inherit permissions from the shared drive.

To restrict external access, the permissions of the entire drive must be modified. However, customers often prefer to limit access to a specific files flagged by a Data Loss Prevention (DLP) policy without impacting the entire drive.

Handling DLP Detections on Externally Shared Drives

To manage DLP detections on externally shared drives, these configuration options are available to control the Vault:

- Use Vault Folder (Default): Removes direct permissions (not inherited from the shared drive) from the file and moves it to a Vault folder at the root of the drive. This ensures the file remains accessible internally while preventing external access.
- Use Quarantine as Vault: Transfers the file to a quarantine location within Check Point's infrastructure.
- Fail Vault Action: If a DLP detection occurs on an externally shared drive, selecting this option causes the Vault action to fail, returning an error and ensuring no changes are made if that is the preferred behavior.

Compromised Account (Anomaly) Detection

The **Anomaly Detection** engine detects behaviors and actions that seems abnormal when observed in the context of an organization and a user's historical activity. It analyzes the behavior using machine-learning algorithm that builds a profile based upon historical events including login locations and times, data-transfer behavior, and email message patterns. Anomalies are often a sign that an account is compromised.

When an anomaly is detected, a security event is generated providing the context and other information necessary for investigation. Depending on the **Severity Level**, the anomaly is categorized as **Critical** or **Suspected**.

- Critical anomalies are events indicating a high probability for compromised accounts. These anomalies require investigation and validation from administrators and should be handled immediately.

  Note - You can configure the **Anomaly Detection** engine to automatically block the detected compromised accounts. For more information, see *"Configuring Anomaly Detection Workflows" on page 304*.

- Suspected anomalies are events that might indicate a compromised account and can be reviewed with a lesser sense of urgency.

Note - Compromised accounts refer to anomalies (events) with a Critical severity level, while Suspected compromised accounts refer to anomalies with lower severity levels - High, Medium, and Low.

By default, for critical anomalies, the **Anomaly Detection** engine only sends email alerts to administrators. To configure the **Anomaly Detection** engine to not only send email alerts but also automatically block the detected compromised accounts, see *"Configuring Anomaly Detection Workflows" on page 304*.

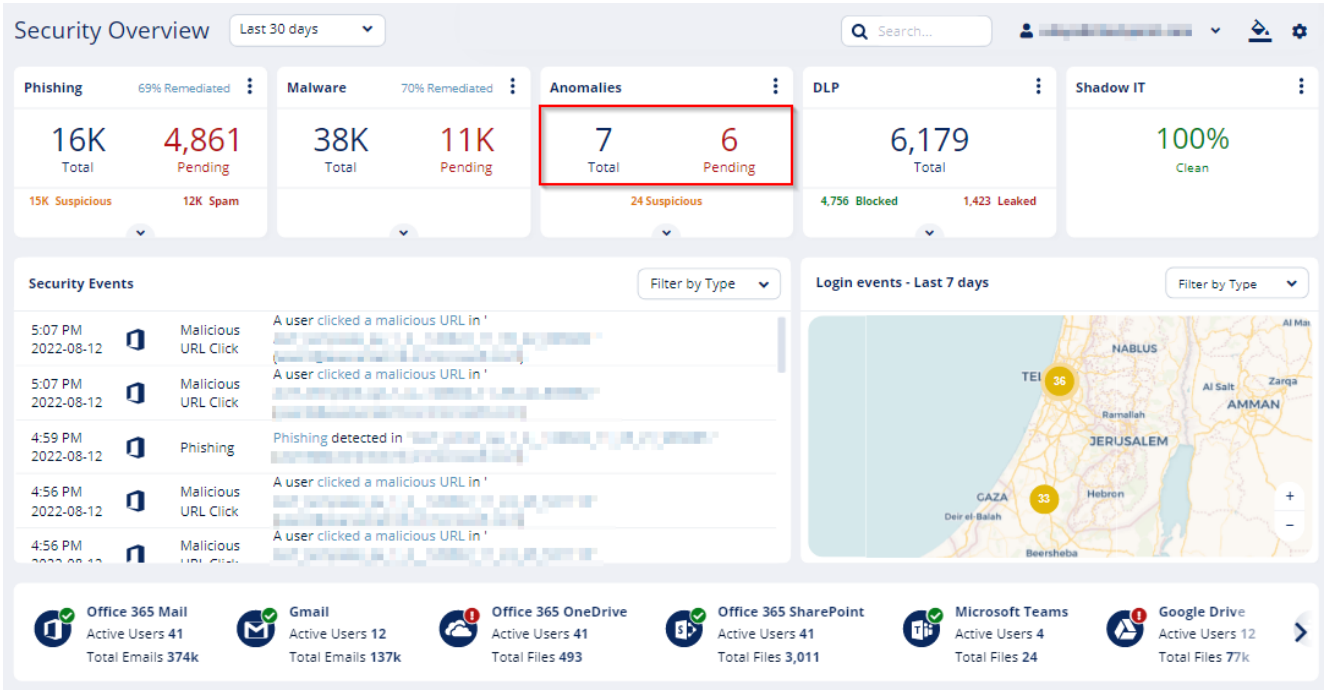
Some organizations manage security alerts through dedicated mailboxes shared between different security team members or use them for integration with 3rd party solutions.

With Avanan, you can configure a dedicated mailbox for alerts on detected compromised accounts. To configure the mailbox, see *"Configuring Anomaly Detection Workflows" on page 304*.

To focus on high probability account takeover, do one of these:

- On the **Events** page, filter the events by **Type (Anomaly)** and **Severity Level (Critical)**.
- On the **Overview** page, click on the **Anomalies** card main indicators.

- On the **Overview** page, under **Security Events**, click on **Filter by Type** and select **Critical Anomalies**.



Compromised Accounts (Anomaly) Workflows

When Avanan detects a high-confidence compromised account, it automatically re-inspects the user's emails for the last three hours.

As these emails are more suspicious of being malicious, the Anti-Phishing security engine performs this inspection with increased sensitivity.

If it detects phishing emails sent from this user, it takes remediation action based on the policy applied to the user.

- If the policy is in **Detect** mode, it takes no action.
- If the policy is in **Prevent (Inline)** or **Detect & Remediate** mode, it quarantines the email.

Supported Anomalies

Critical Anomalies

New delete-all-emails rule

This anomaly inspects new rules configured to delete all the incoming emails. It detects potential malicious configuration to delete all the incoming emails. This behavior may indicate an account takeover.

This anomaly has the highest impact.

Users Sending Malicious Emails

This anomaly is triggered when an internal user sends a phishing or spam email to internal and/or external recipients.

Note - Using exceptions, administrators can disable this anomaly for a specific user or for all users.

Move all emails to a subfolder

This anomaly inspects new rules configured to move all the incoming emails to a subfolder. It detects possible malicious configurations to move all the incoming emails to a specific subfolder. This behavior could indicate an account takeover.

AI-Based Detection of Anomalous Logins

This anomaly uses an AI engine designed to inspect all the parameters of login events to pinpoint those that malicious actors do.

The AI engine inspects a variety of parameters, including IP address, browser type, browser version, device, VPN brand, etc.

Login events detected by this AI engine flag the corresponding users as compromised.

Login from Malicious IP Address

This anomaly detects the compromised accounts based on the IP address from which attackers logged into Microsoft 365.

Users logging into Microsoft 365 from IP addresses detected as sources of phishing emails or from the IP address known to Check Point as malicious will be flagged as compromised.

Suspected Anomalies

First Time in New Country

This anomaly is triggered when a user log in from a country they have never logged in from.

Note - If the user's title includes the name of a country, logging in from that country will not be flagged.

Auto-forwarding to External Email Address

This anomaly is based on reading the Office 365 management events. It processes specific events triggered when a mailbox auto-forwarding rule is created.

The anomaly does these tasks:

- Inspects new auto-forwarding rules created in Office 365.
- Checks if the target email is 'external' to the organization. If the email is external, then an anomaly is triggered.

Note - The anomaly's severity is decided based on the forwarding condition. If there is no condition, the severity is set to high. By default, the severity is set to medium.

Unusual Country Anomaly

This anomaly detects incoming email from countries associated with phishing attempts and various types of cyber attacks.

By default, these countries are Nigeria and China. The Allow-List allows you to ignore events from either of these two countries.

Suspicious Geo Anomaly (Impossible Travel)

This anomaly detects possible credential theft and use from another location. It detects the frequent login and email events from different locations, and alerts the administrator about what is likely to be another person operating from an account of a company employee.

It is possible to create Allow-List rule of accounts (for example, employees that use VPN or similar tools on a frequent basis).

Suspicious MFA Login Failure

This anomaly detects login operations that failed during Multi Factor Authentication (MFA)/Second Factor Authentication (2FA). To reduce the rate of false detection, it correlates the failed MFA with additional events or follow-up successful login.

Event text - A suspicious login failure for <email>, attempting to login from <geo location>, failing at the MFA stage.

Note - The detection is not generated in real time as it correlates and analyzes the past events and successful logins. Alert may be generated a few hours after the failed login.

Client is a vulnerable browser

This anomaly checks the client browser's vulnerability. It checks the browser version used by the end user performing the event (when reported by the SaaS), and compares it to the list of old versions (with known vulnerabilities).

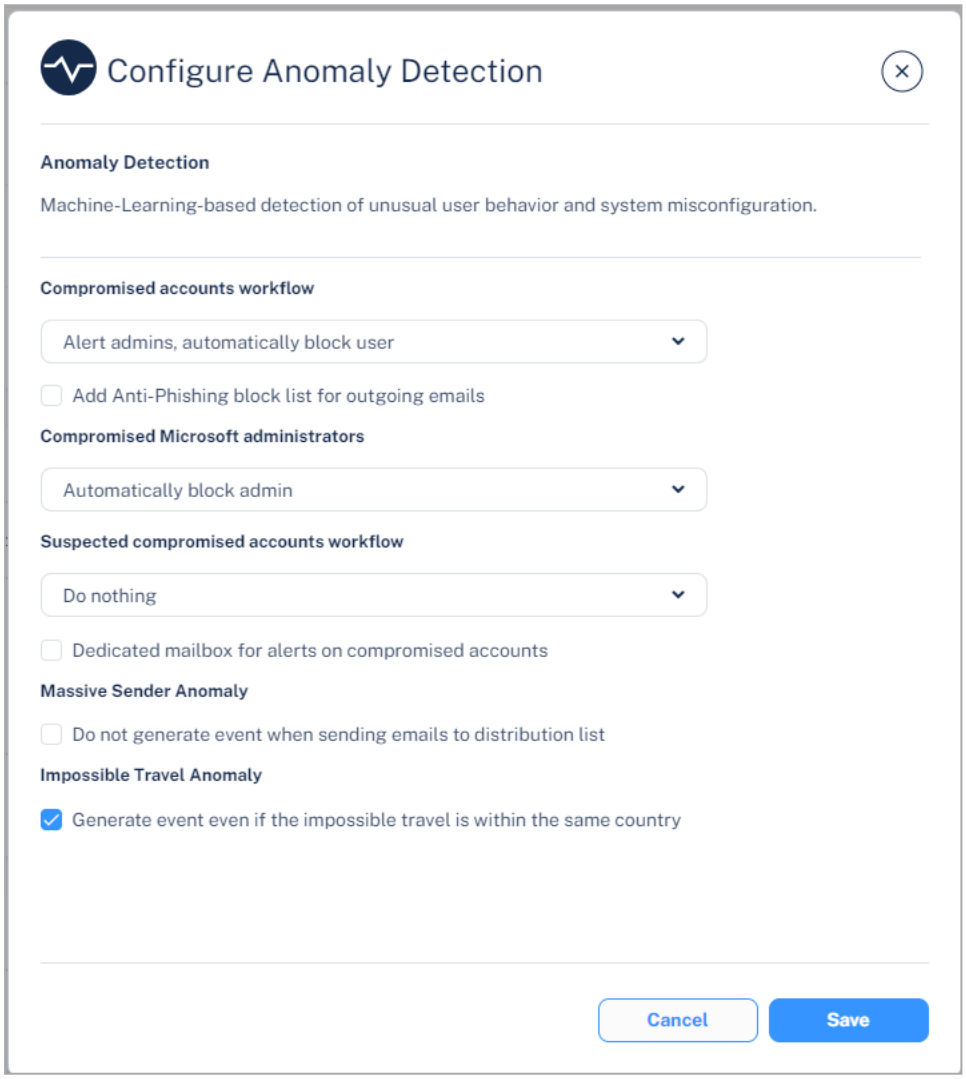
Note - Compromised accounts refer to anomalies (events) with a Critical severity level, while Suspected compromised accounts refer to anomalies with lower severity levels - High, Medium, and Low.

Configuring Anomaly Detection Workflows

When Avanan detects a compromised or suspected compromised account, the administrator can configure the **Anomaly Detection** security engine to take automatic actions. To do that, the administrator must select the required workflow for different scenarios.

To configure Anomaly Detection workflows:

1. Navigate to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Anomaly Detection**.



3. Under **Compromised accounts workflow**, select the required workflow when critical anomalies (which indicates that an account is compromised) are detected.
   - To send email alerts to the administrator and automatically block the compromised account, select **Alert admins, automatically block user**.
   - To send only email alerts to the administrator, select **Alert admins**.

- To automatically block outgoing emails for compromised accounts, in the **Compromised accounts workflow** section, select the **Add Anti-Phishing block list for outgoing emails** checkbox. For more information, see *"Automatically Blocking All Outgoing Emails" below*.

4. Under **Compromised Microsoft administrators**, select the required workflow when compromised global admin accounts are detected.
   a. To block compromised global admin accounts, select **Automatically block admin**.
   b. To avoid blocking compromised global admin accounts, select **Do nothing**.
5. To send email alerts when suspected anomalies (which indicates that an account may be compromised) are detected, under **Suspected compromised accounts workflow**, select **Alert Admins**.
6. To configure a dedicated mailbox for alerts on compromised accounts:
   a. Select the **Dedicated mailbox for alerts on compromised accounts** checkbox.
   b. Under **Dedicated Alert Mailbox**, enter the email address.
7. Click **Save**.

Notes:

- To enable login events for **Office 365 GCC** environment, contact *Avanan Support*.
- To create exceptions for anomalies, see *"Anomaly Exceptions" on page 307*.
- Compromised accounts refer to anomalies (events) with a Critical severity level, while Suspected compromised accounts refer to anomalies with lower severity levels - High, Medium, and Low.
- If you are using Microsoft Entra ID (formerly Azure AD) as the SAML/SSOIdentity Provider for your corporate assets, the users gets blocked from accessing all the assets including Microsoft 365.
- Blocking a user account terminates all the active sessions associated with the account.
- Blocking a Microsoft user account resets the account password and requires the user to set a new password when unblocking their account.

Automatically Blocking All Outgoing Emails

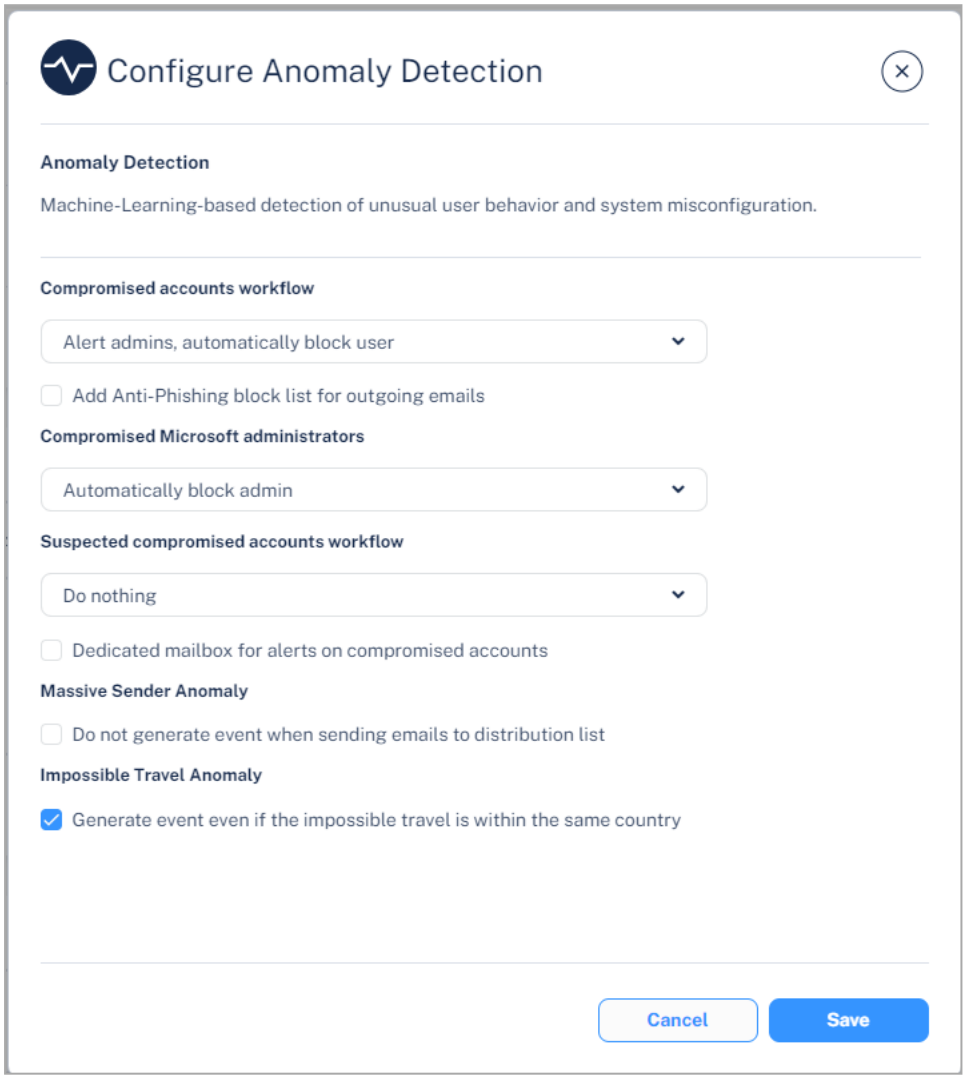
Even after a compromised account is detected and blocked, administrators may choose to add another layer of security by blocking all outgoing emails from the compromised account for these reasons:

- Scheduled Malicious Messages: Attackers might schedule emails to be sent later, anticipating that the compromised account could be blocked at any time.

- Hybrid Environments: In environments where the on-premises Active Directory overrides the Azure Active Directory, blocked users may get unblocked. Blocking all outgoing emails ensures that even if the user is unblocked, no emails can be sent from the compromised account.

To automatically block all outgoing emails:

1. Navigate to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Anomaly Detection**.



3. To automatically block outgoing emails for compromised accounts, in the **Compromised accounts workflow** section, select the **Add Anti-Phishing block list for outgoing emails** checkbox.
4. To automatically block outgoing emails for suspected compromised accounts, in the **Suspected compromised accounts workflow** section, select the **Add Anti-Phishing block list for outgoing emails** checkbox.
5. Click **Save**.

Notes:

- Once this option is selected, when the system detects a compromised user account, it automatically creates a Anti-Phishing block-list. It flags all the emails from this user as phishing and enforces the configured phishing workflow.
- After unblocking a blocked compromised account, you must manually remove the block-list for the account. See *"Deleting Anti-Phishing Exceptions" on page 317*.

Configuring Settings for Specific Anomalies

Impossible Travel Anomaly

To generate **Impossible Travel Anomaly** event even when the user logs in from multiple locations inside the same country:

1. Go to **Security Settings** > **Security Engines**.
2. Click **Configure** for **Anomaly Detection**.
3. Under **Impossible Travel Anomaly**, select the **Generate event even if the impossible travel is within the same country** checkbox.

   For more information, see *"Suspicious Geo Anomaly (Impossible Travel)" on page 303*.
4. Click **Save**.

Anomaly Exceptions

At times, to handle falsely flagged events, administrators may need to create exceptions for anomaly detections.

To create Anomaly exceptions:

1. Go to **Events** screen.
2. Select the anomaly event for which you want to create an exception.
3. Click on the vertical ellipses icon (in the right side of the selected anomaly event), and then select **Add Exception**.

   Create allow-list for anomaly pop-up screen appears.
4. Under **Allow-List type**, select the required exception from the drop-down.

   Note - The drop-down shows different options applicable for the anomaly event you selected.
5. Under **Apply for all past events**, select **Yes** or **No**.

- **Yes** - The exception gets applied to all the events in the past and to the future events.
- **No** - The exception gets applied only to the event you selected and to all the future events.

6. If required, enter a **Comment** for the anomaly exception.
7. Click **OK**.

To see all the anomaly exceptions, go to **Security Settings** > **Exceptions** > **Anomaly**.

Partner Risk Assessment (Compromised Partners)

Organizations take measures to secure their users, collaboration applications, and emails. However, partners are one of the greatest threats to an organization. These are other companies that the organization maintains a business relationship with.

If one of the partners gets compromised, it is difficult for the email security solutions and the end users to detect these malicious and impersonated emails.

With **Partner Risk Assessment** in Avanan, you can proactively detect compromised partners.

Using the **Partner Risk Assessment** dashboard, you can view these:

- All your organization's business partners
- Risk indicators of partners that are possibly compromised.

To view the **Partner Risk Assessment**, click **Analytics** > **Partner Risk**.

Identifying a Partner

Avanan automatically identifies partners while inspecting the incoming and outgoing emails for threats and DLP.

To identify an organization as a partner, Avanan uses multiple methods like these:

- External domain sending invoices to your organization's domain.
- External domain with a significant volume of emails exchanged with your organization's domain.

Reviewing the Partners

Avanan shows the identified partners (compromised and uncompromised) in a table under the **Partner Risk Assessment** dashboard.

The Partners table has these columns:

Column Name	Description
Risk Score	The severity of the detected *"Risk Indicators" below*. ■ Critical ■ High ■ Medium ■ Low ■ Lowest ■ None
Partner Domain	The partner's domain and its name. **Note** - Avanan sometimes does not show the partner name.
Communication Volume	An indicator of how many emails were exchanged with the partner in the last two weeks. ■ High ■ Medium ■ Low
Internal Contacts	The internal contacts that corresponded with the partner domain. **Note** - If there are many contacts, it shows five contacts with the highest communication volume with the partner domain.
Partner Contacts	The contacts from the partner domain that corresponded with your domain. **Note** - If there are many contacts, it shows five contacts with the highest communication volume with your domain.
Risk Indicators	A list of reasons a partner is considered potentially compromised. If Avanan detects a partner as uncompromised, it shows no indicators. For more information, see *"Risk Indicators" below*.
Last Risk Date	Last time when a risk indicator was detected.

Risk Indicators

Avanan detects different risk indicators and assigns them to partners. Each risk indicator has a risk score attached to it.

The risk indicators have these values:

Severity	Risk Indicator	Description
Highest	Phishing emails sent to your organization	Avanan detected high-confidence phishing emails sent to your organization from this domain, and the sender was authenticated (SPF pass).
High	Phishing emails sent to other organizations	Avanan detected high-confidence phishing emails sent to other Avanan customers from this domain, and the sender was authenticated (SPF pass).
High	Partner impersonation emails sent to your organization	Avanan detected high-confidence phishing emails sent to your organization from this domain, but the sender was not authenticated (SPF fail).
High	Service being used to send phishing emails to your organization	Avanan detected high-confidence phishing emails sent to your organization from this domain. This domain is a publicly available service that allows sending emails from it.
Medium	Partner impersonation emails sent to other organizations	Avanan detected high-confidence phishing emails sent to other Avanan customers from this domain, but the sender was not authenticated (SPF fail).
Medium	Service being used to send phishing emails to other organizations	Avanan detected high-confidence phishing emails sent to other Avanan customers from this domain, and this domain is a publicly available service that allows sending emails from it.

Stop Considering a Partner as Compromised

When Avanan detects a partner as compromised, it adds the relevant risk indicator to the partner. This risk indicator remains valid only for the next 72 hours.

For example, Avanan detected a partner as compromised and added **Phishing emails sent to your organization** risk indicator. If no phishing emails from its domain are detected in the next 72 hours, Avanan removes the risk indicator.

When no risk indicators are available, the partner is considered uncompromised.

Removing a Partner from the List

Administrators can override the automatic identification of a partner and remove a partner from the list.

To do that, click the ⋮ icon for the partner from the last column of the table and select **Not a partner**.

Note - If you remove a partner, you cannot add again. To add a removed partner, contact *Avanan Support*.

Acting on Compromised Partners

Anti-Phishing Higher Sensitivity

By default, when Avanan detects a partner as suspicious, it inspects the emails from their domain with high sensitivity. This way, they are more likely to be found as phishing.

Investigating Emails from Compromised Partners

To view and investigate the emails from the partner domain, click the ⋮ icon for the partner from the last column of the table and select **Emails from partner**.

Mail Explorer opens and, by default, shows the emails from the partner domain in the last seven days.

Impersonation of Partners

By default, the Anti-Phishing security engine treats emails from domains that resemble one of your partner's domains with more suspicion.

Administrators can select to trigger a specific workflow in these cases. For more information, see *"Impersonation of your Partners" on page 104*.

Managing Security Exceptions

Avanan supports these exceptions:

- **Security Engine Exceptions** - These exceptions are specific to individual security engines within the system. For example, an Anti-Phishing exception will not affect the Anti-Malware inspection of an email.
  - *"Anti-Phishing Exceptions" below*
  - *"Anti-Malware Exceptions" on page 317*
  - *"DLP Exceptions" on page 322*
  - *"Click-Time Protection Exceptions" on page 324*
  - *"URL Reputation Exceptions" on page 325*
  - *"Trusted Senders - End-User Allow-List" on page 327*

Security Engine Exceptions

Anti-Phishing Exceptions

The Anti-Phishing engine supports defining Allow-Lists and Block-Lists.

The Anti-Phishing engine stops scanning emails that match an Allow-List or Block-List rule. The Anti-Phishing verdict will automatically be clean (for Allow-List) or Phishing / Suspected Phishing / Spam (for Block-List).

Notes:

- Emails in the Anti-Phishing Allow-List and Block-List are evaluated by other security engines, such as Anti-Malware and DLP.
- If an email matches both the Allow-List and Block-List rules, the Allow-List takes precedence, and the email will be delivered.

Viewing Anti-Phishing Exceptions

To view the configured Allow-List or Block-List rules:

1. Go to **Security Settings** > **Exceptions** > **Anti-Phishing**.
2. In the drop-down from the top of the page, select the require exception type (**Allow-List** or **Block-List**).

   The page shows a table with all the exceptions and the defined criteria.

In the **Anti-Phishing Allow-List** table, the **Affected emails** column shows the number of emails flagged as phishing or spam by the Anti-Phishing engine but marked as clean because of the allow-list rule.

Note - The numbers for each allow-list rule in the **Affected emails** column do not update in real time. It might take up to an hour for them to update.

Adding Anti-Phishing Exceptions (Allow-List or Block-List Rule)

You can add Allow-List or Block-List rule from any of these:

- **From the Anti-Phishing Exceptions**

  1. Go to **Security Settings** > **Exceptions** > **Anti-Phishing**.
  2. In the drop-down from the top of the page, select the require exception type (**Allow-List** or **Block-List**).
  3. Under **Filters**, define the criteria for filtering the emails, and click **Search**.
  4. After refining the email criteria, click **Create Allow-List Rule** to create a allow-list rule or **Create Block-List Rule** to create a block-list rule.
  5. If required, enter a description for the rule in the **Comment** field and click **OK**.

- From the **Mail Explorer** (see *"Creating Allow-List and Block-List Rule" on page 377*)

- **From the email profile page**

  1. Open the required email profile.
  2. Under **Security Stack**, select **Similar Emails / Create Rules**.
  3. Under **Filters**, define the criteria for filtering the emails, and click **Search**.
  4. After refining the email criteria, click **Create Allow-List Rule** to create a allow-list rule or **Create Block-List Rule** to create a block-list rule.
  5. If required, enter a description for the rule in the **Comment** field and click **OK**.

Note - If a phishing email is sent to multiple recipients, the system allow-lists it only if a rule applies to all recipients. If even one recipient does not have an allow-list rule, the system applies the phishing workflow to everyone.

Filters to refine the email criteria for Allow-List or Block-List

While refining the criteria for creating Allow-List or Block-List, you can use these filters.

Filter Name	Description
Date Received	Events in the last year, month, week, day, or hour. Also, using Range, you can choose to select the emails on a specific date and time.
Quarantine State	Select the events based on these quarantine states. ■ Quarantined ■ Non Quarantined ■ Display All
Recipients	Emails that contain a specific recipient or a recipient that match a specific term.
Subject	Emails that match a specific subject.
Sender Name	Emails from a specific sender.
Sender Domain	Emails from a specific domain.
Sender Email	Emails from a specific email address.
Client Sender IP	Emails from a specific client and IP address.
Server IP	Emails from a specific server IP address. Supports the CIDR notation for IP ranges. Examples: ■ Exact IP - 192.0.2.1 ■ Subnet Mask - 192.0.2.0/24 or 10.0.0.0/8
Links in body	Emails that has links to external resources in the body of the email.
Attachments MD5	Emails that has attachments with specific MD5.
Headers	Emails that contain specified headers. **Note** - You can use the **Headers** field to create an Allow-List or Block-List, but you can not filter the emails based on headers.

Interaction between Avanan Allow-List and Microsoft 365 Allow-List

Administrators can configure whether allow-lists defined in Avanan will affect email enforcement by Microsoft, and vice versa.

To customize this interaction:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for Anti-Phishing.
3. Scroll-down to **Allow-List Settings** and select the required settings.

   For more information, see *"Overriding Microsoft / Google sending emails to Junk folder" below* and *"Applying Microsoft Allow-List also to Avanan" below*.
4. Click **Save**.

Overriding Microsoft / Google sending emails to Junk folder

When an email is allow-listed by Check Point, administrators can ensure that it is not delivered to the Junk folder by Microsoft / Google. To do that:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for Anti-Phishing.
3. Scroll-down to **Allow-List Settings** and select the **Allow-List emails that are allow-listed by Check Point also in Microsoft/Google** checkbox.
4. Click **Save**.

Note - This setting applies only when the email is processed by a Threat Detection policy in **Prevent (Inline)** protection mode.

Applying Microsoft Allow-List also to Avanan

Administrators can choose to treat every email that is allow-listed by Microsoft (SCL=-1) as allow-listed by Avanan as well. To do that:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for Anti-Phishing.
3. Scroll-down to **Allow-List Settings** and select the **Allow-List emails that are allow-listed in Microsoft (SCL = -1) also in Avanan** checkbox.
4. Click **Save**.

Importing Allow-List or Block-List from External Sources

For various use-cases, predominantly migrating from a legacy solution to Avanan, you might need to import a large number of items to the Allow-List or Block-List.

To import Allow-List or Block-List, contact *Avanan Support*.

Deleting Anti-Phishing Exceptions

To delete the Anti-Phishing Allow-List or Block-List:

1. Go to **Security Settings** > **Exceptions** > **Anti-Phishing**.
2. In the drop-down from the top of the page, select the require exception type (**Allow-List** or **Block-List**).
3. Select the exception(s) you want to delete.
4. Click **Actions** from the top-right corner of the page and select **Delete**.
5. In the confirmation pop-up that appears, click **OK**.

Anti-Malware Exceptions

Anti-Malware Allow-List

Administrators can exclude files from malware inspection so that the Anti-Malware engine always returns a clean verdict for them. You can use the following criteria to create an Anti-Malware Allow-List rule:

- Sender Email
- Sender Domain
- File MD5/Macro MD5
- File type

You can add Anti-Malware Allow-List rule from any of these:

- **From the Anti-Malware Allow-List**

    1. Click **Security Settings** > **Exceptions** > **Anti-Malware**.
    2. In the drop-down from the top of the page, select the exception type as **Allow-List**.
    3. Click **Create Allow-List**.

        The **Create Anti-Malware Allow-List** pop-up appears.

4. To create an allow-list for the sender's email address or domain:
    a. In the **Allow-List Type** list, select **Sender**.
    b. In the **Sender Email Address / Domain** field, enter the email address or domain.

    Note - If you add multiple email addresses or domains, the system creates an allow list separately.

5. To create an allow-list for file MD5 hash:
    a. In the **Allow-List Type** list, select **File MD5**.
    b. In the **File MD5** field, enter the File MD5.
6. To create an allow-list for the file type:
    a. In the **Allow-List Type** list, select **File Type**.
    b. In the **File Type** field, enter the file extension.

    Note - If you add multiple file types, the system creates an allow list separately.

    For certain file types such as PDF, you can choose to allow files only when they contain links. To do that, in the **Links** list, select the required option.

    - **Allow always (with or without links)**
    - **Allow only if contains links**
    - **Allow only if does not contain links**
7. (Optional) In the **Comment** field, enter a comment for the Allow-List rule.

    Notes:
    - Administrators can view this comment on the Email page to understand the reason for allowing the email.
    - Administrators can also use the comment text to filter specific Allow-Lists.
8. Click **OK**.

- **From the Entity Profile page**

1. Open the required attachment profile from the **Security Events**.
2. Under **Security Stack**, select **Create Allow-List** for Anti-Malware.

    The **Create Anti-Malware Allow-List** pop-up appears.

3. To create an allow-list for the sender's email address or domain:
   a. In the **Allow-List Type** list, select **Sender**.
   b. In the **Sender Email Address / Domain** field, enter the email address or domain.

   Note - If you add multiple email addresses or domains, the system creates an allow list separately.

4. To create an allow-list for file MD5 hash or Macro MD5:
   - In the **Allow-List Type** list, select **File MD5**.

   The File MD5 or the file's detected Macro MD5 will be displayed automatically.

   Notes:
   - Administrators can see the code of each Macro MD5 by selecting a specific Macro MD5.
   - You can add only one Macro in an Allow-List rule and the files containing the allow-listed macro will not be flagged as malicious.

5. To create an allow-list for the file type:
   a. In the **Allow-List Type** list, select **File Type**.
   b. In the **File Type** field, enter the file extension.

   Note - If you add multiple file types, the system creates an allow list separately.

   For certain file types such as PDF, you can choose to allow files only when they contain links. To do that, in the **Links** list, select the required option.
   - **Allow always (with or without links)**
   - **Allow only if contains links**
   - **Allow only if does not contain links**

6. (Optional) In the **Comment** field, enter a comment for the Allow-List rule.

   Notes:
   - Administrators can view this comment on the Email page to understand the reason for allowing the email.
   - Administrators can also use the comment text to filter specific Allow-Lists.

7. Click **OK**.

Note - Macro MD5 Allow-List supports these file formats: DOC, DOCM, DOCX, DOTM, DOTX, POT, POTM, POTX, PPA, PPAM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, XLAM, XLS, XLSB, XLSM, XLSX, XLTM, and XLTX.

Anti-Malware Block-List

Administrators can create Anti-Malware Block-List to mark any file type as malware. By adding a Block-List rule for a file type, the Anti-Malware engine automatically marks all matching file types as containing malware.

Note - For file types (PDF, EML, HTML) that support link identification, you can choose to block these files based on whether they contain links or not.

You can add Anti-Malware Block-List rule from any of these:

- **From the Anti-Malware Block-List**

  1. Click **Security Settings** > **Exceptions** > **Anti-Malware**.
  2. In the drop-down from the top of the page, select the exception type as **Block-List**.
  3. Click **Create Block-List**.
  4. Enter the required **File Type**.

     Note - When you add multiple file types, each file type will be added as a separate exception.

  5. For the file types that support link identification (PDF, EML, and HTML), select one of these.

     - **Block always (with or without links)**
     - **Block only if contains links**
     - **Block only if does not contain links**

     Note - This option is available only for PDF, EML, and HTML file types.

  6. If required, enter a comment for the Block-List rule.

     Administrators can use the commented text to filter and find the Block-Lists with a specific text from their comments.

  7. Click **OK**.

- **From the Entity Profile page**

  1. Open the required attachment profile from the **Security Events**.
  2. Under **Security Stack**, click **Create Block-List** for Anti-Malware.

     The detected file type displays automatically.

3. If required, add the required file types.

   Note - When you add multiple file types, each file type will be added as a separate exception.

4. For the file types that support link identification (PDF, EML, and HTML), select one of these.

   - **Block always (with or without links)**
   - **Block only if contains links**
   - **Block only if does not contain links**

   Note - This option is available only for PDF, EML, and HTML file types.

5. If required, enter a comment for the Block-List rule.

   Administrators can use the commented text to filter and find the Block-Lists with a specific text from their comments.

6. Click **OK**.

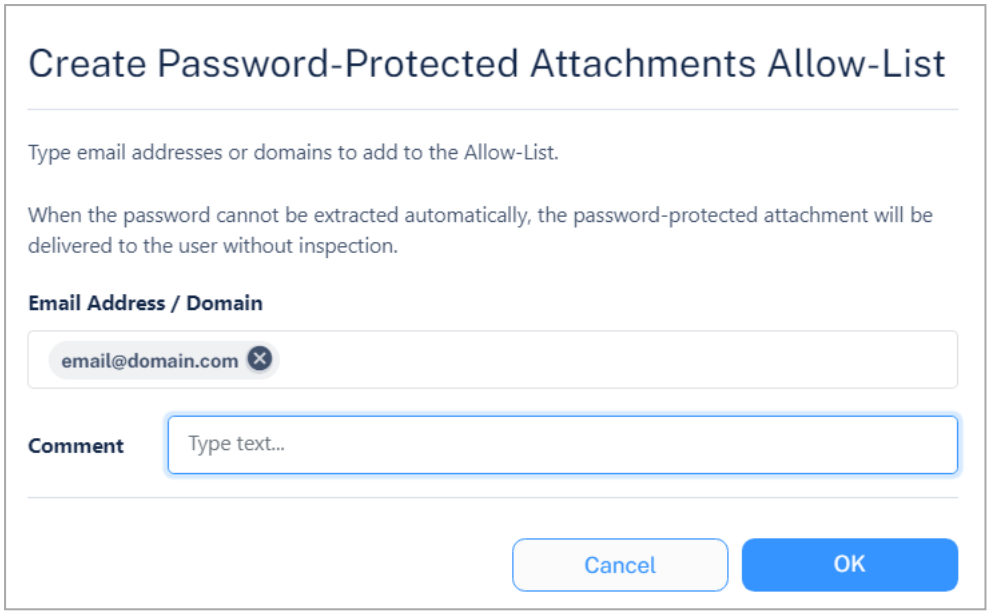
Password-Protected Attachments Allow-List

When a Password-Protected Attachment allow-list is detected for an email address or domain, the system ignores the Password-Protected Attachments workflow configured in the policy and delivers the attachment to the end-user.

- Password detected: The system scans the attachments for malware and gives the verdict.
- Password not detected: The system gives the verdict as allow-listed (clean) and delivers the attachment to the user.

To create a Password-Protected Attachments Allow-List:

1. Click **Security Settings** > **Exceptions** > **Anti-Malware**.
2. In the drop-down from the top of the page, select the exception type as **Password-Protected Attachments**.
3. Click **Create Allow-List**.



4. In the **Email Address / Domain** field, enter the email addresses or domains.

   If you enter multiple email addresses or domains, the system creates separate allow-list for each email address / domain.

5. If required, enter a comment for the Allow-List rule.
6. Click **OK**.

DLP Exceptions

The DLP engine supports defining Allow-Lists by Sender, Recipient, File MD5, and Strings.

The DLP engine stops scanning emails, messages, and files that match an Allow-List rule. The DLP verdict will automatically be clean for the Allow-List.

Notes:

- DLP Allow-List applies to both the incoming and outgoing DLP policy rules. For information about DLP policies, see *"Data Loss Prevention (DLP) Policy" on page 188*.
- Emails, messages, and files in the DLP Allow-List are evaluated by other security engines, such as Anti-Malware and Anti-Phishing.
- When you add multiple strings, each string will be added as a separate exception. Allow-listed strings will not be flagged as a DLP violation.

Adding DLP Allow-List

You can add DLP Allow-List rule from any of these:

- **From the DLP Allow-List**

  1. Click **Security Settings** > **Exceptions** > **DLP**.
  2. In the drop-down from the top of the page, select **Allow-List**.
  3. Click **Create Allow-List**.
  4. Select the required **Allow-List Type**.
     - Sender
     - Recipient
     - File MD5
     - String
  5. Enter the required sender/recipient's email address or domain, File MD5 or strings.
  6. If required, enter a comment for the Allow-List rule and click **OK**.

     You can use the commented text to filter and find the Allow-Lists with a specific text from their comments.
  7. Click **OK**.

- **From the Entity Profile page**

  1. Open the required email profile, message, or file from the **Security Events**.
  2. Under **Security Stack**, select **Create Allow-List**.
  3. Select the required **Allow-List Type**.
     - Sender
     - Recipient
     - File MD5
     - String

     The File MD5 or file's detected strings will be displayed automatically.
  4. Enter the required sender/recipient's email address or domain, or strings.
  5. If required, enter a comment for the Allow-List rule and click **OK**.

     You can use the commented text to filter and find the Allow-Lists with a specific text from their comments.
  6. Click **OK**.

Click-Time Protection Exceptions

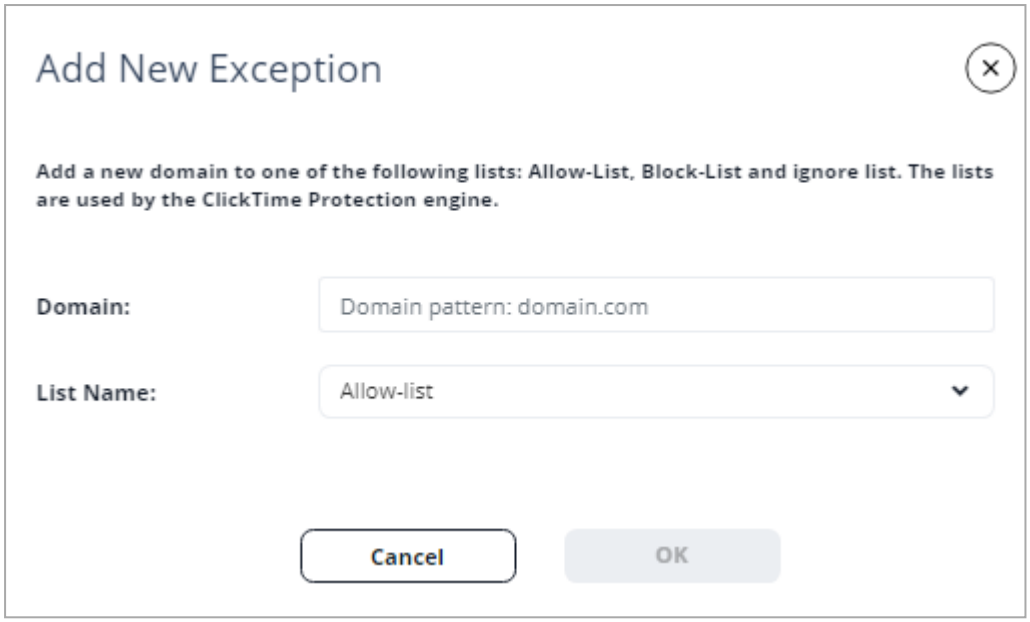
Avanan allows administrators to override Avanan detections or prevent link rewriting by defining exceptions to the inspection on replaced links.

Administrators can add URLs and domains to these exceptions list:

- **Allow-list** - Even if Avanan finds the website malicious, Avanan allows the user to access the website. However, Avanan replaces the link, and clicking on it is logged into the system.
- **Block-list** - Even if Avanan finds the website benign, Avanan blocks the user from accessing it and shows it is blocked.
- **Ignore-list** - Avanan does not replace the links to these URLs/domains. Therefore, Avanan does not monitor clicks on these links or track them.

To configure Click-Time Protection exceptions:

1. Navigate to **Security Settings** > **Exceptions** > **Click-Time**.
2. From the drop-down in the top, select the exception type.
   - Allow-List
   - Block-List
3. To create an allow-list, click **Create Allow-List**.
4. To create a block-list, click **Create Block-List**
5. Under **Domain**, enter the required domain in the *Domain pattern: domain.com* format.
6. In the **List Name** drop-down, select the required exception type (**Block-list**, **Allow-list**, **Ignore-list**).



7. Click **OK**.

Link Shorteners and Re-Directions

Click-Time Protection exceptions apply only to the URLs written in the email and its attachments.

If an email contains a shortened link or a link that automatically redirects to one of the URLs/domains in the exception lists, the link in the email will not be excluded.However, these links will be re-written and inspected, and access to them will be enforced based on the inspection result and policy, as if they were not part of any exception list.

For example, if a domain *domain.com* is in the block list and the email contains the shortened link *bit.ly/12345* that redirects to *domain.com*, the link will be re-written and inspected like any other link and users clicking on the link will not be automatically blocked from accessing the website.

URL Reputation Exceptions

You can add **URL Reputation** exceptions (Allow-List or Block-List) from any of these:

- **From the URL Reputation Exceptions page**

    1. Click **Security Settings** > **Exceptions** > **URL Reputation**.
    2. In the drop-down from the top of the page, select the required exception type.
        - Allow-List
        - Block-List

3. To add exception for a domain:
    a. In the exception **List Type** drop-down, select **Domain**.
    b. In the **Domain** field, enter the required domain name in the *domain.com* format.

    Note - You must enter each subdomain you want to allow-list or block-list separately.
    For example, to add an allow-list or block-list, you must add a separate entry for both domain.com and subdomain.domain.com.

4. To add exception for an exact URL:
    a. In the exception **List Type** drop-down, select **Exact URL**.
    b. In the **Exact URL** field, enter the required URL.

    Note - Only URLs identical to the typed exact URL will be allow-listed / block-listed.

5. If required, enter a description for the exception under **Comment**, and click **OK**.

Notes:
- Allow-listed URLs will not be flagged as malicious.
- Block-listed URLs will not be flagged as clean.

- **From the Microsoft Teams / Slack message profile page**

1. Open the required message profile from the **Security Events**.
2. To create an allow-list, under **Security Stack**, click **Create Allow-List** next to the malicious URL / Domain.

    or

    Click **More Info** and then click **Create Allow-List** next to the malicious URL / Domain.

3. To create a block-list, under **Security Stack**, click **Create Block-List** next to the URL / Domain.

    or

    Click **More Info** and then click **Create Block-List** next to the URL / Domain.

4. Select the exception type (**Exact URL** or **Domain**).

    Avanan automatically detects and shows the URL or Domain.

    Note - Only URLs identical to the typed exact URL will be allow-listed / block-listed.

5. If required edit the URL / Domain.
6. If required, enter a description for the exception under **Comment**, and click **OK**.

Notes:

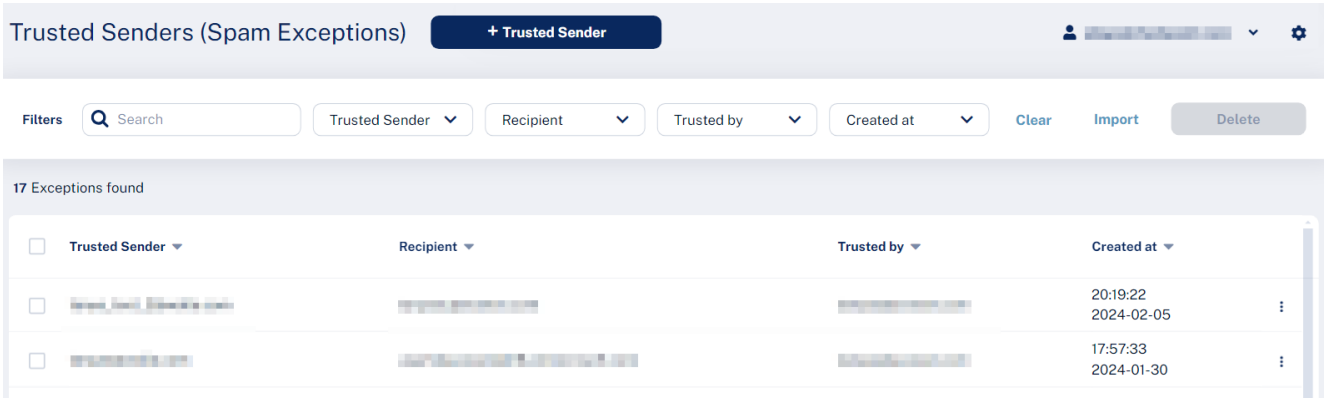
- Allow-listed URLs will not be flagged as malicious.
- Block-listed URLs will not be flagged as clean.

Trusted Senders - End-User Allow-List

When an end user adds a sender / domain to trusted senders for spam emails from the *"End-User Daily Quarantine Report (Digest)" on page 423*, Avanan shows the details in the **Trusted Senders (Spam Exceptions)** page.

To manage the list of senders trusted by end users, click **Security Settings** > **Exceptions** > **Anti-Spam**.

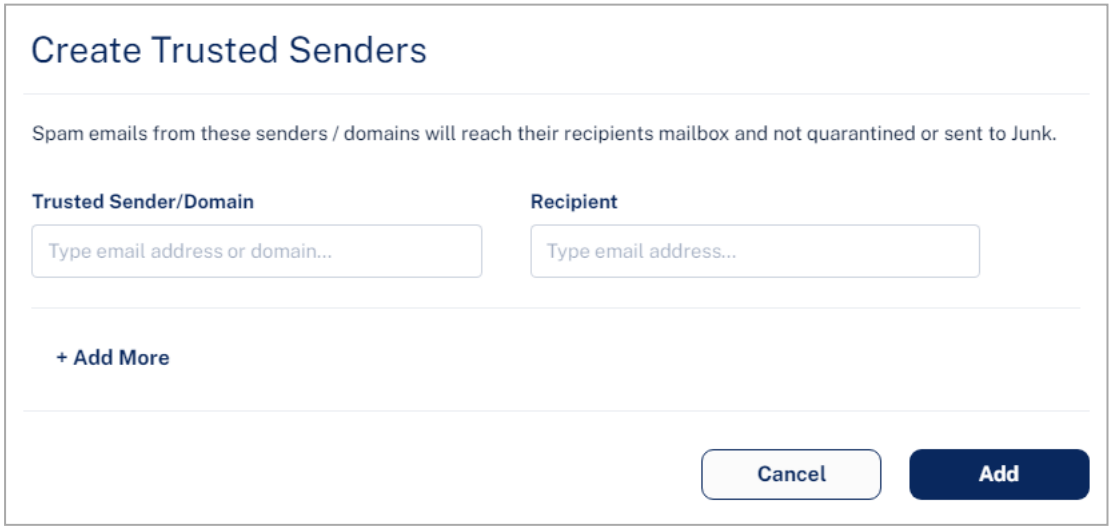
For the procedure to allow end users to trust senders, see *"Trusted Senders" on page 181*.



Adding Trusted Senders

To add trusted senders manually:

1. Click **Trusted Sender**.

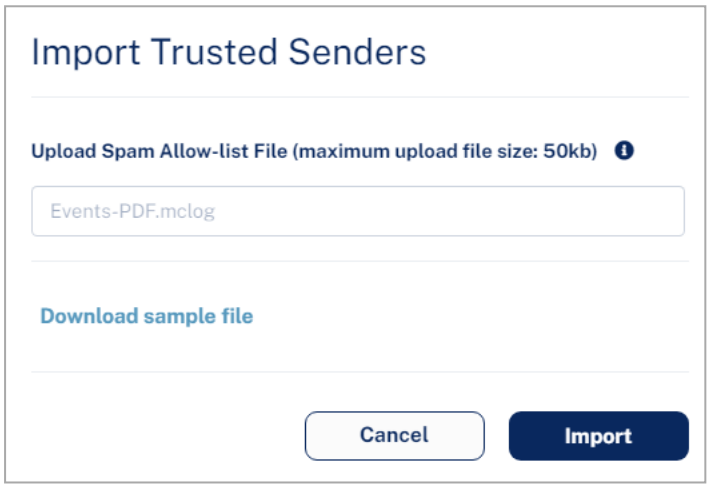


2. In the **Trusted Sender/Domain** field, enter the sender email address or domain.
3. In the **Recipient** field, enter the recipient email address.
4. To add more senders or domains, click **+Add More** and repeat steps 2 to 3.
5. Click **Add**.

To upload a CSV file with trusted senders:

Note - You can upload CSV file only upto 50 kb.

1. Click **Import**.



2. In the **Upload Spam Allow-list File** field, click **Choose a file** and select the CSV file.
3. Click **Import**.

To edit the trusted senders:

1. Click the ⋮ icon from the last column of the trusted sender.
2. To edit a trusted sender:
   a. Click **Edit** and make the necessary changes.
   b. Click **Edit**.
3. To delete a trusted sender, click **Delete**.
4. To delete multiple trusted senders at a time, select the trusted senders and click **Delete** from the top right corner of the page.

Managing Security Events

This chapter explains about the ways to handle security events, whether they are detected/prevented automatically or found by the administrators/end users after not being prevented.

Note - To search through events, manage and act on the detected security events via API, refer to *Avanan API Reference Guide*

Dashboards, Reports and Charts

Overview Dashboard

The **Overview Dashboard** page is the landing page of the Avanan Administrator Portal. It lets you quickly understand your organization's threats and the pending tasks for review and action.

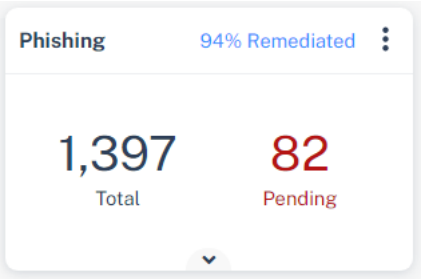
The **Overview Dashboard** has these:

- Security widgets
  - *"Phishing" on the next page*
  - *"Business Email Compromise (BEC)" on the next page*
  - *"Malware" on page 331*
  - *"DLP" on page 332*
  - *"User Interaction" on page 333*
- *"Security Events" on page 334*
- *"Application Protection Health" on page 334*
- *"Login Events Map" on page 335*

Note - By default, the **Overview Dashboard** page does not show security events and analytics for Microsoft quarantined emails. To view the security events and analytics for Microsoft quarantined emails, toggle the **Include Microsoft Quarantine** button to **On** from the top-right corner of the page.

Security Widgets

Phishing

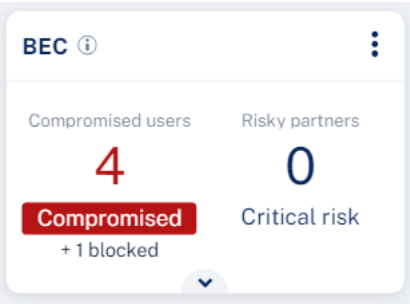


The **Phishing** widget shows the total number of phishing events detected in the selected time frame, including pending events.

To view the number of suspected phishing events, spam events, and events specific to a SaaS application, click the icon.

To view specific events, click the indicators within the widget, and the system shows the filtered events on the **Events** page.

Business Email Compromise (BEC)



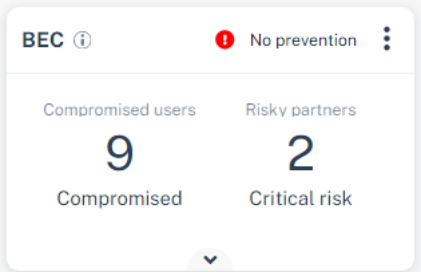
The **Business Email Compromise (BEC)** widget shows the number of compromised users and risky partners detected in the selected time frame.

To view the number of suspected anomaly events and lower risk partners, click the icon.

To view specific events, click the indicators within the widget, and the system shows the filtered events on the **Events** page.

Compromised Users

The **Compromised Users** are the users detected as compromised with high probability. It shows the number of **Anomaly** events with **Critical** severity.



For Microsoft SaaS applications, these tags appear at the top of the widget based on the configured anomaly detection workflow:

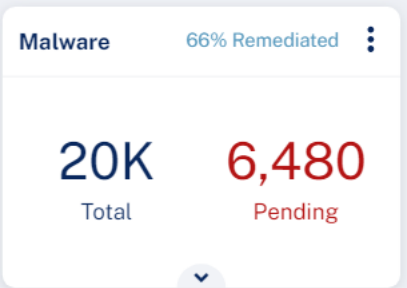
- **No prevention** - Appears if the anomaly detection workflow is configured not to block the user automatically when an account is detected as compromised.
- **Full prevention** - Appears if the anomaly detection workflow is configured to block the user automatically when an account is detected as compromised.

For more information, see *"Configuring Anomaly Detection Workflows" on page 304*.

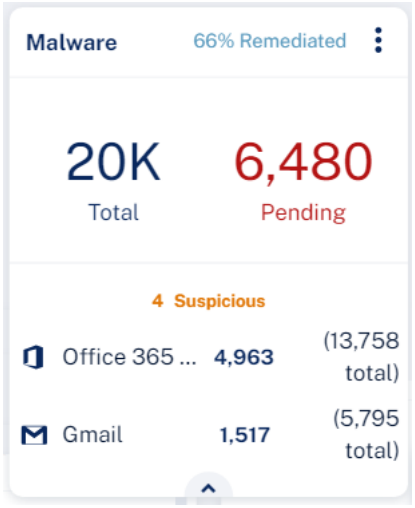
Note - In rare cases, this widget might be replaced with the **Anomalies** widget that shows information about the compromised users.

Malware

The **Malware** widget shows the total number of malware events detected in the selected time frame, including pending events.



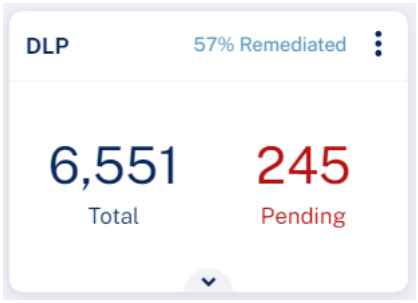
To view the number of suspected malware events, and events specific to a SaaS application, click the ⌄ icon.



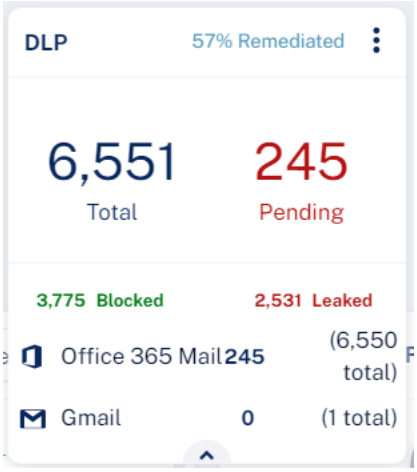
To view specific events, click the indicators within the widget, and the system shows the filtered events on the **Events** page.

DLP

The **DLP** widget shows the total number of DLP events detected in the selected time frame, including pending events.

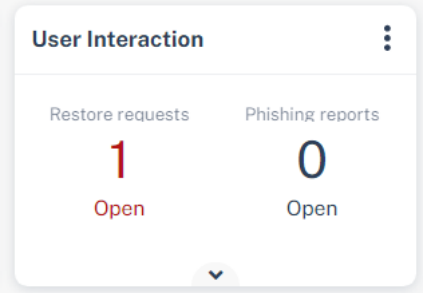


To view the number of blocked DLP events, leaked DLP events, and events specific to a SaaS application, click the icon.



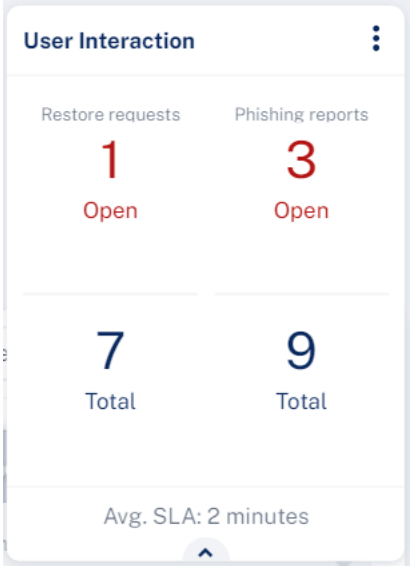
To view specific events, click the indicators within the widget, and the system shows the filtered events on the **Events** page.

User Interaction



The **User Interaction** widget shows the number of pending restore requests and phishing reports in the selected time frame.

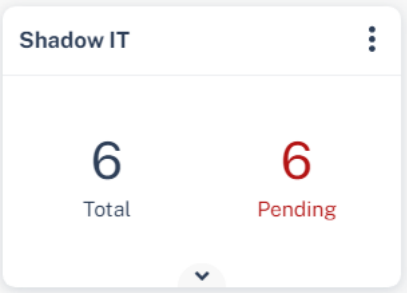
To view the total number of restore requests, phishing reports and their average SLA in the selected time frame, click the icon.



To view specific requests, click the indicators within the widget, and the system shows the filtered events on the **Restore Requests** / **Phishing Reports** page.

Note - In rare cases, this widget might be replaced with the **Shadow IT** widget.

Shadow IT

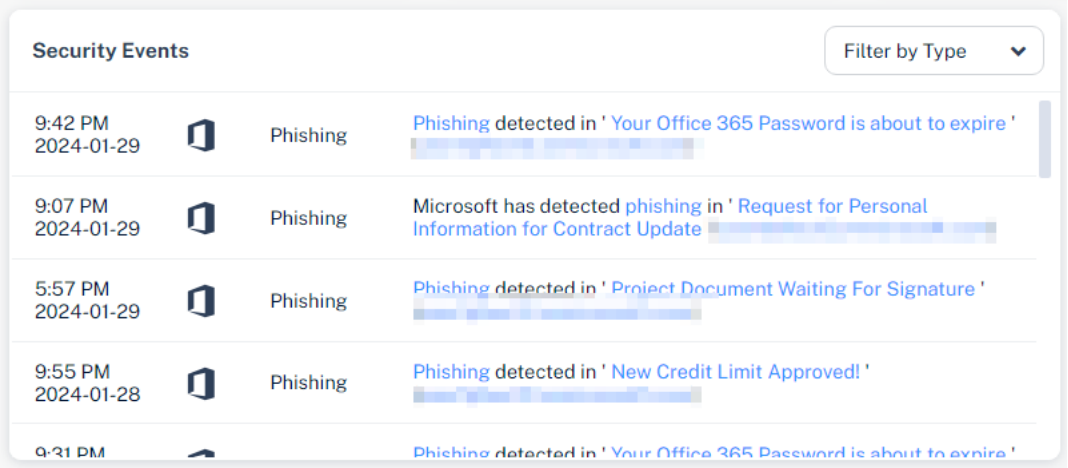


The **Shadow IT** widget shows the total number of Shadow IT events detected in the selected time frame, including pending events.

To view the Shadow IT events, click the icon.

To view specific events, click the indicators within the widget, and the system shows the filtered events on the **Events** page.

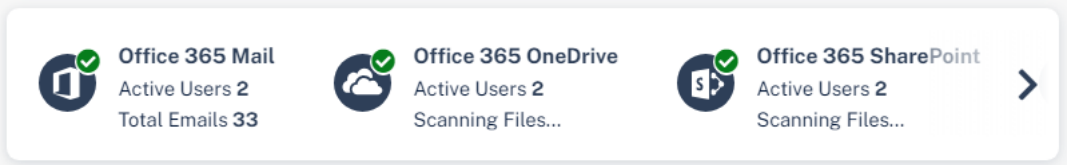
Security Events



The **Security Events** widget shows the most recent security events on the Avanan Administrator Portal.

To filter events for a specific event type, click the **Filter by Type** drop-down and select the event type.

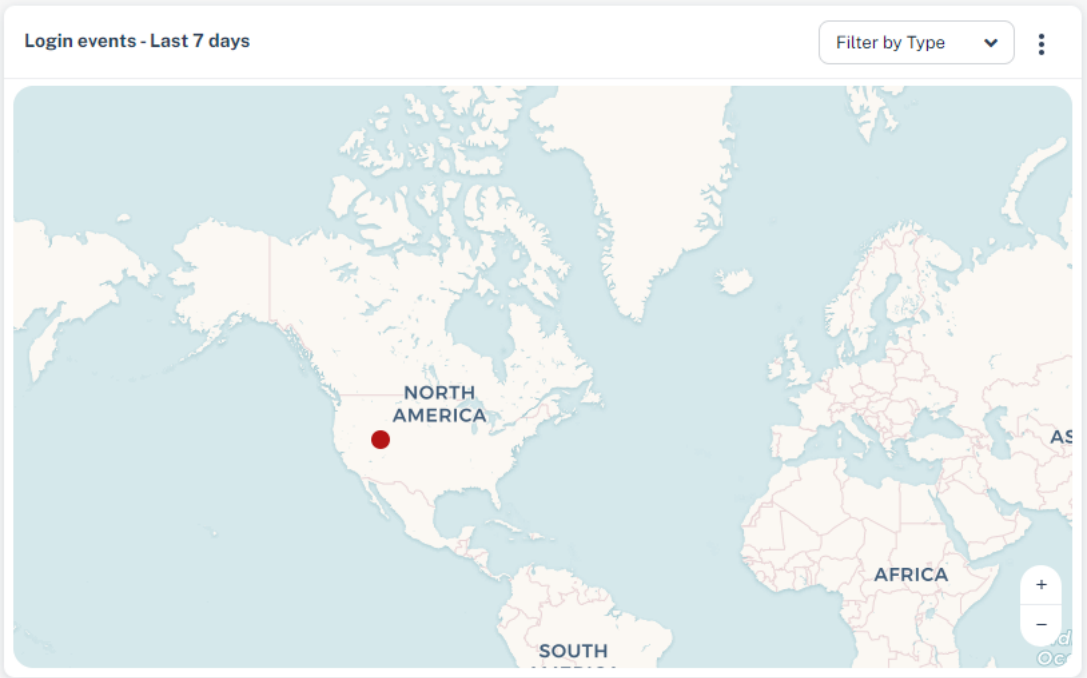
Application Protection Health



The **Application Protection Health** widget shows all the SaaS applications onboarded with Avanan. To view the list of users protected with the SaaS application, click **Active Users**.

The indicator at the top of the application's icon shows the health of the application. Hover over the icon to view the issues if any with the application.

Login Events Map



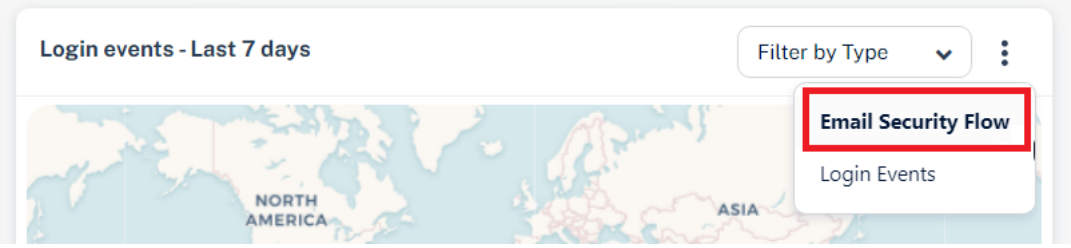
The **Login Events** map shows all the successful and failed login events over the last seven days.

To filter events for a specific type, click the **Filter by Type** drop-down and select the event type.

Note - After activating the SaaS application, Avanan takes up to 36 hours to start showing the login events.

Email Security Flow Charts

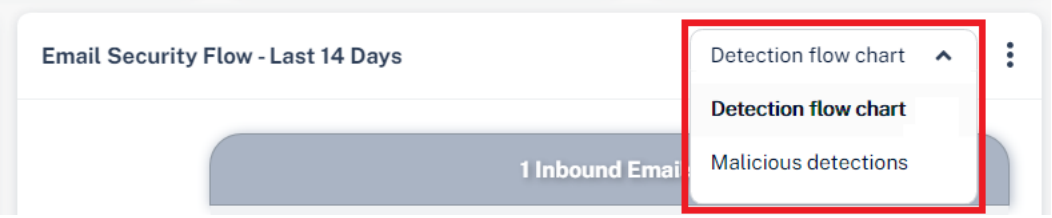
By default, the **Overview** page shows the **Login Events** map. To view **Email Security Flow Charts**, click the ⋮ icon for **Login Events** widget and select **Email Security Flow**.



Detection Flow Chart

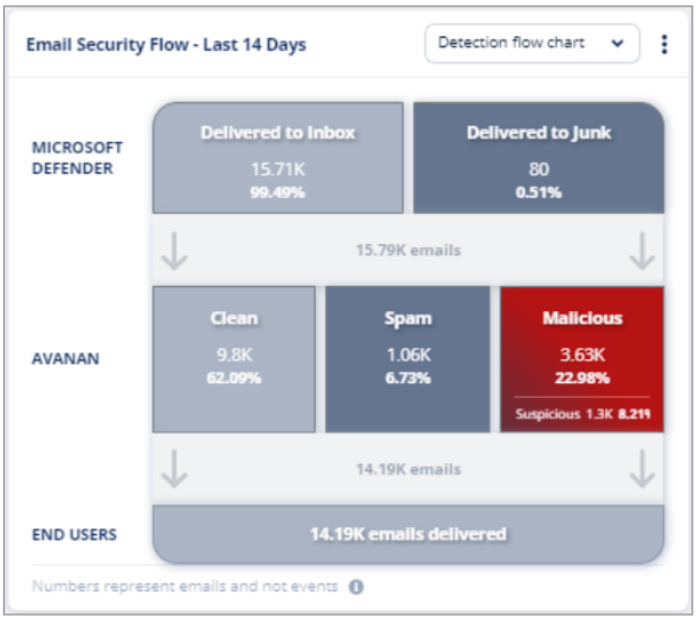
The **Detection flow chart** shows an overview of how many emails Microsoft decided to let through to the end users (delivered to Inbox/Junk folder) and how Avanan classified these emails.

To view the chart, go to **Overview** page and in the **Email Security Flow** widget, select **Detection flow chart** from the drop-down in the top-right corner.



Notes:

- The numbers in the chart may seem inconsistent with the numbers you see in other parts of the dashboard as the chart represents emails and not security events.
- To view the emails filtered per selection, click on the relevant section. You will be redirected to the **Mail Explorer** page and it shows the relevant emails.



Row name	Email classification	Description
Microsoft Defender	Delivered to Inbox	Emails Microsoft intended to deliver to the inbox.
	Delivered to Junk	Emails Microsoft intended to deliver to the Junk folder.
Avanan	Clean	Emails detected as **Clean** by Avanan.
	Spam	Emails detected as **Spam** by Avanan.
	Malicious	Emails detected as **Phishing** and/or **Malware** by Avanan.
	Suspicious	Emails detected as **Suspected Phishing** and/or **Suspected Malware** by Avanan.

Row name	Email classification	Description
End Users	-	Number of emails delivered to the end users.

Malicious Detections Chart

The **Malicious detections** chart provides a deeper analysis of the distribution of the malicious detection by threat type.

To view the chart, go to **Overview** page and in the **Email Security Flow** widget, select **Malicious detections** from the drop-down in the top-right corner.

To view the emails filtered per selection, click on the relevant section. You will be redirected to the **Mail Explorer** page and shows the relevant emails.

Analytics Dashboard

Avanan's Analytics examines the scanned data and presents it in the form of useful information for your analysis and necessary remedial actions.

Avanan supports Analytics for these SaaS applications:

- *"Office 365 Email and Gmail" on page 340*
- *"Office 365 OneDrive" on page 342*

- Office 365 SharePoint
- Citrix ShareFile
- Microsoft Teams
- *"Google Drive" on page 343*
- Slack
- Box

To view analytics for a SaaS application:

1. Access the Avanan Administrator Portal.
2. From the left navigation panel, click **Analytics** > **Dashboard**.
3. Select the required SaaS application.
4. Select the period to view the analytics (Last 24 hours, 7 days, 30 days, 60 days, and 90 days).

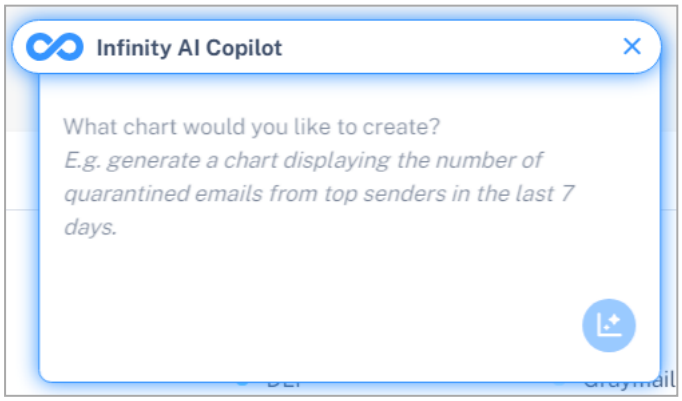
Customizing the Analytics Dashboard using Infinity AI Copilot

In the **Analytics** page, the **Infinity AI Copilot** feature allows you to generate customized reports, charts, and dashboards using GenAI prompts.

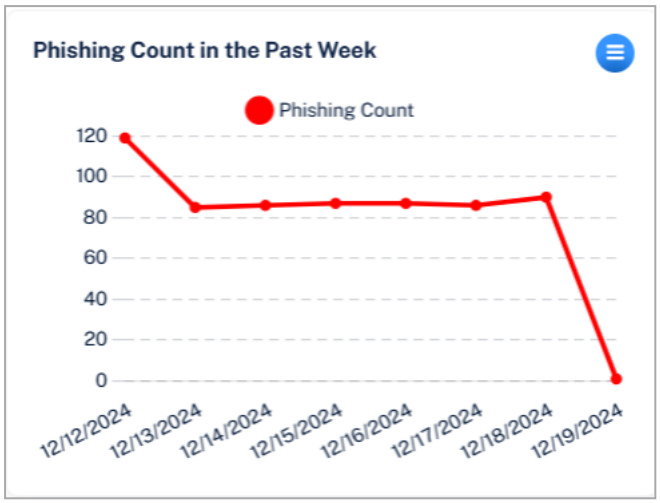
If **Infinity AI Copilot** is unavailable in the Analytics dashboard, contact *Avanan Support*.

To customize the Analytics dashboard using Infinity AI Copilot:

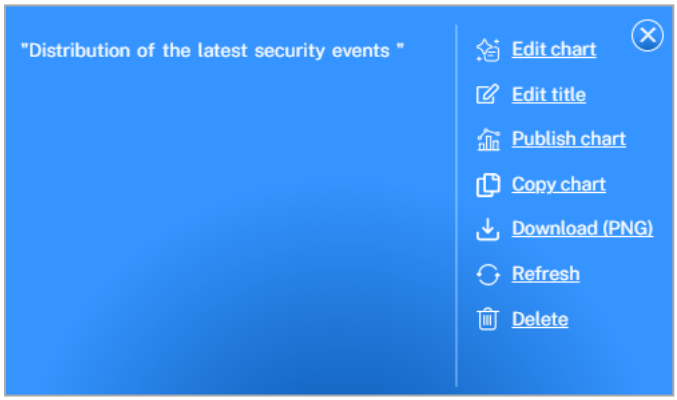
1. Access the Avanan Administrator Portal.
2. From the left navigation panel, click **Analytics** > **Dashboard**.
3. Click **Infinity AI Copilot** next to the time frame from the top of the page.
4. Enter your prompt and click .



The system generates actionable data insights and analytics such as charts, tables, and other visualizations, in response to the provided GenAI prompt.



5. To make changes to the analytics generated using GenAI prompts, click the icon from the top left corner of the chart.



- To change the title of the chart, click **Edit title**, make the necessary changes, and click **Save**.
- To modify the prompt for the chart, click **Edit chart**, make the necessary changes, and then click at the bottom of the chart.

  Note - Until the chart is published, it remains visible only to you. To make the chart visible for all users, click **Publish chart**.
  After publishing the chart, all users of the Avanan Administrator Portal in your organization can see them.

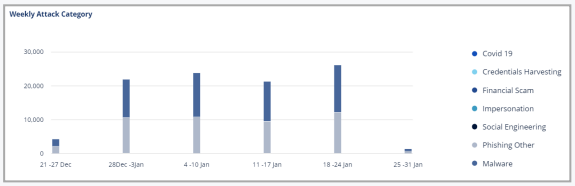
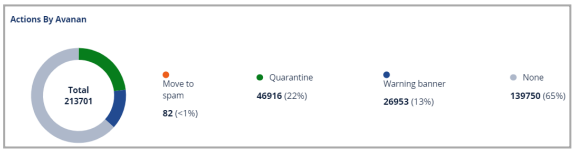
- To move the chart to the desired location in the dashboard:
  a. Click **Drag chart**.
  b. Move the chart to the desired location.
  c. Click **Stop Drag Mode** from the top left corner of the chart.

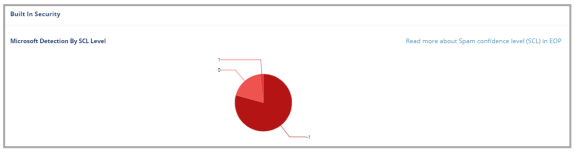
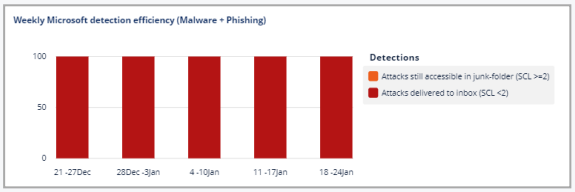
  Notes:
  - This option is available only when there are multiple analytics created using **Infinity AI Copilot**.
  - You cannot change the position of the default analytics widgets.
- To copy the chart, click **Copy chart**.
- To download the chart as a PNG file, click **Download (PNG)**.
- To reload the chart, click **Refresh**.
- To delete the chart, click **Delete**.
- To return to the options and generated chart, click  .

Office 365 Email and Gmail

Note - For Office 365 Mail, to include/exclude the analytics for Microsoft quarantined emails, toggle **Include Microsoft Quarantine** to **On**/**Off** from the top-right corner of the page.

Overview of the activities in Office 365 Email and Gmail:

Analytics	Sub-category	Actions
Attack Detections	**Detections by Type** The number of attacks detected per type. 	1. Click on an attack type or action. The Analytics Events page shows the list of security events. 2. To export the list in a CSV file format, click **Export to CSV**. 3. Click on a security event to view its Email Entity page.
	Weekly Attack Category Weekly data of the number of attacks per type. 	
	Action by Avanan 	
My User	**Top Attacked Users** List of top attacked users. 	None
	Top Attacked Departments List of top attacked departments. 	

Analytics	Sub-category	Actions
Built In Security (Does not apply to Gmail)	**Microsoft Detection By SCL** The number of detections by Microsoft with Spam Confidence Level (SCL).  **Weekly Microsoft detection efficiency (Malware +Phishing)** Weekly data of the number of detections by Microsoft with SCL. 	None

Office 365 OneDrive

The analytics for Office 365 OneDrive shows an overview of the activity in Office 365 OneDrive.

Widget	Description
All Files	The total number of files in your Office 365 OneDrive.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with people outside the company
System Users	The number of users that can access your cloud application (not suspended or deleted).
All Folders	The number of directories in your Office 365 OneDrive.
Incoming Folders	The number of folders created by an external user and shared with an internal user.
Outgoing Folders	The number of folders created internally and shared with external users.
Applications	Number of application detected that have access to the service.
Security Scan Panel	The number of files flagged as malicious.

Widget	Description
Users with full access to files	All users who have view access to files.
Users with view access to files	All users who have view access only.

Google Drive

The analytics for Google Drive shows an overview of the activity in Google Drive.

Widget	Description
All Files	The total number of files in your Google Drive.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with external users or publicly.
System Users	The number of users that can access your cloud application (not suspended or deleted).
All Folders	The number of directories in your Google Drive.
Incoming Folders	The number of external directories received.
Outgoing Folders	The number of internal directories sent.
Recent Files	The number of incoming and outgoing files within the past 24 hours.
Security Scan Panel	The number of files found to be malicious.
Live event log	Detailed list of events in real time.

Shadow IT

Shadow IT is hardware or software within an enterprise that is not supported by the organization's central IT department.

This implies that the organization has not explicitly approved the technology, or it does not know that employees are using it.

Avanan's Approach to Shadow IT in Avanan

Based on email analysis (Office 365 and/or Gmail), Avanan gives you a direct line of sight into cloud applications in use at your company.

Avanan identifies emails from cloud applications to users that suggest they have been using a cloud application. For example, emails containing messages such as "Thank you for registering" or "You have a notification" suggest that a user has been using a cloud application. When such an email is detected in a user's mailbox, a security event is created with the type of Shadow IT.

Avanan inspects all licensed users' emails for Shadow IT.

Shadow IT Dashboard and Events

Shadow IT events are listed under **Events**. SaaS usage can then be visualized in the Shadow IT dashboard visible under **Analytics** > **Shadow IT**.

Shadow IT panel and description:

Panel	Description
Most Popular Services	Most popular SaaS applications discovered.
Accounts created over time	SaaS applications usage pattern over time.
Applications by Risk	A breakdown of apps per risk-score. The application risk is given by the Check Point app wiki:
Applications by Category	The categories of apps that are used.
Latest SaaS Usage	The most recent discovered events of app usage.

Shadow IT classifies the severity of events using these terms:

Panel	Description
Low	Events found during historical scan.
Medium	First event for a user.
High	Second or more event for the same user.

These actions can be performed on Shadow IT events:

Panel	Description
Dismiss	Changes the event state to DISMISSED. The event will be removed from the Shadow IT dashboard.
Approve this app	This will add the cloud application to Allow-List. Future occurrences of emails from this specific application to any user will not trigger an event. However, this will not update past events. Consequently, this will not impact the Shadow IT dashboard that will show past usage of the application. To view and manage the approved applications. contact *Avanan Support*.

User Interaction Dashboard

The **User Interaction Dashboard** provides an overview of the most common day-to-day tasks performed in Avanan:

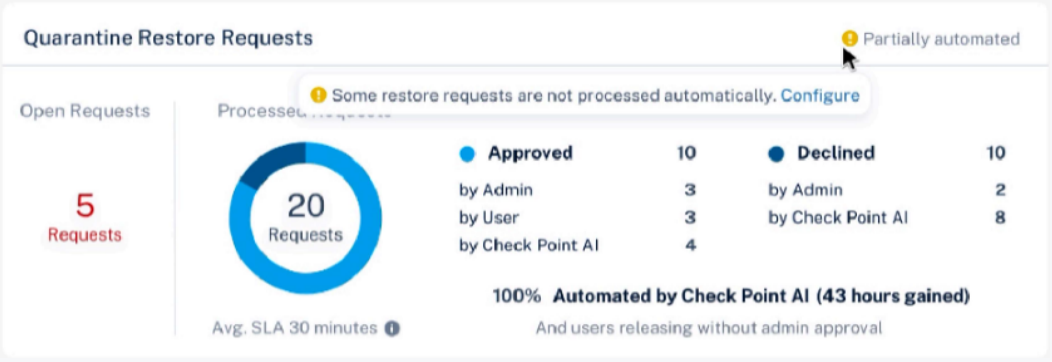
- Handling Quarantine Restore Requests
- Handling Phishing emails reported by end users

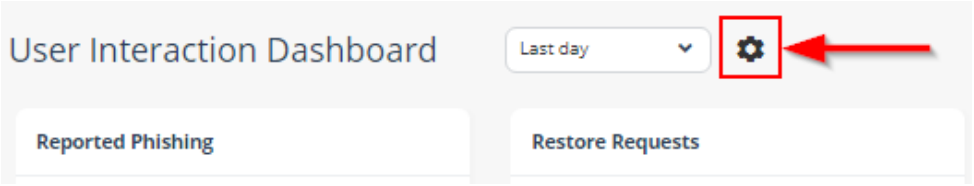
For more information on how to handle these tasks, see *"Phishing Reports Dashboard" on page 362* and *"Managing Restore Requests" on page 433*.

To access the **User Interaction Dashboard**, go to **User Interaction** > **Dashboard**.

The **User Interaction Dashboard** has these widgets:

Widget Name	Description
Phishing Reports	Shows the number of phishing emails reported by end users and the automation level indicator. ■ **Open Reports** - Shows the number of open reports that are not yet handled by help desk. ■ **Processed Reports** - Shows the number of reports that are handled by help desk. • **Approved** - Shows the number of emails approved by help desk from the user reported phishing emails. • **Declined** - Shows the number of emails declined by help desk from the user reported phishing emails. ■ Automation level Indicator - Shows the level of automation in phishing reports. • Automated - All selected phishing report workflows are configured to **Send for admin review**. • Partially automated - At least one selected phishing report workflow is configured to **Send for admin review**. • Manual - All selected phishing report workflows are configured for automated processing, and no workflows are configured to **Send for admin review**. For more information, see *"Automatic Handling of User Reported Phishing Emails" on page 368*. 

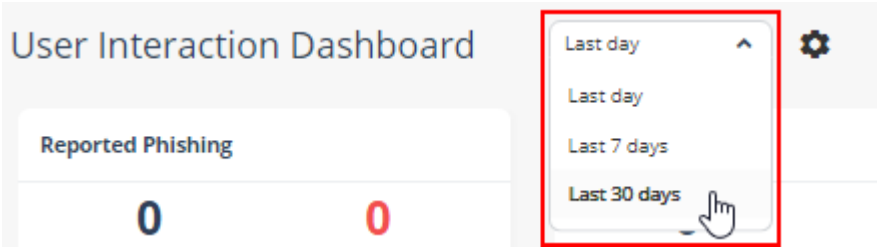
Widget Name	Description
Quarantine Restore Requests	Shows the number of quarantined restore requests received from the end users and the automation level indicator. ■ **Open Requests** - Shows the number of open requests that are not yet handled by help desk. ■ **Processed Requests** - Shows the number of restore requests that are handled by help desk. • **Approved** - Shows the number of requested emails that are released from quarantine, either by help desk or by an end user. • **Declined** - Shows the number of requests that are rejected by help desk. ■ Automation level Indicator - Shows the level of automation in quarantined restore requests. • Automated - All selected quarantined restore requests workflows are configured to **Send for admin review**. • Partially automated - At least one selected quarantined restore requests workflow is configured to **Send for admin review**. • Manual - All selected quarantined restore requests workflows are configured for automated processing, and no workflows are configured to **Send for admin review**. For more information, see *"Automatic Handling of Quarantined Restore Requests" on page 434*. 

Widget Name	Description
SLA Trend	Shows the SLA trend line for the amount of time it took for the help desk to handle requests/reports on a daily basis. ■ The chart includes a SLA line, meant to mark the required SLA in your organization, so that you can easily see if you meet your SLA or not. ■ The default value for the SLA is 30 minutes. To configure it, click the settings icon at the top of the dashboard window. 
User Trend	Shows the trend line of different requests/reports and how they are handled.
User Events	Shows the list of recent requests reported by the end users.
Top Users	Shows the list of top requesting/reporting users in your organization.

Extending the Time Frame of the Analytics

By default, the **User Interaction Dashboard** shows analytics for the last day.

To view analytics for extended time periods, select a time frame from the top of the dashboard.



Security Checkup Report

The **Security Checkup** report gives a periodic overview of all the threats detected in the SaaS applications protected by Avanan.

It gives insights into the threats detected and how Avanan handled these threats based on the configured policies.

Security Checkup Report Recipients

By default, all the Avanan users receive Security Checkup report.

To exclude users from receiving the Security Checkup report:

1. Click **System Settings** > **User Management**.
2. Search for the user and click the ⋮ icon on the last column of the user.
3. Click **Edit**.
4. Scroll down to the **Alerts and Reports** section and clear the **Receive Weekly Reports** checkbox.

5. Click **Update**.

Generating a Security Checkup Report

When required, administrators can generate the **Security Checkup** report from the Avanan portal.

To generate Security Checkup report:

1. Go to **Analytics** > **Security Checkup**.
2. Click **Generate now**.
3. Enter the required report name.
4. Select the required **Time Frame**.
   - **Last 7 days**
   - **Last 14 days**
   - **Last 30 days**
   - **Previous month**
   - **Previous quarter**
   - **Date range**, and select the dates
5. Select the scope of the report:

- **All users**
- **Company** and then enter the company name as specified in the **Company** field in **Azure AD**.
- **Department** and then enter the department name.

6. Click **Generate**.

   The system starts generating the **Security Checkup** report.

7. Click **OK**.

   You can track the report generation status from the **System Settings > System Tasks** page.

   After the report gets generated, you can view the report from the **Security Checkup** page.

Last 30 Days Security Checkup Report

The **Security Checkup** report for the last 30 days has fewer sections than the 14-day and 7-day reports. The report does not show these:

- Number of incoming emails
- Number of scanned elements (files, messages, attachments, emails, and so on)
- Malicious file types and
- Detection samples

In addition, specific pages in the report include a note stating that the data on these pages is based only on the last 14 days.

Scheduling the Security Checkup Report

Avanan allows you to schedule the **Security Checkup** reports and send them to specific internal and external recipients.

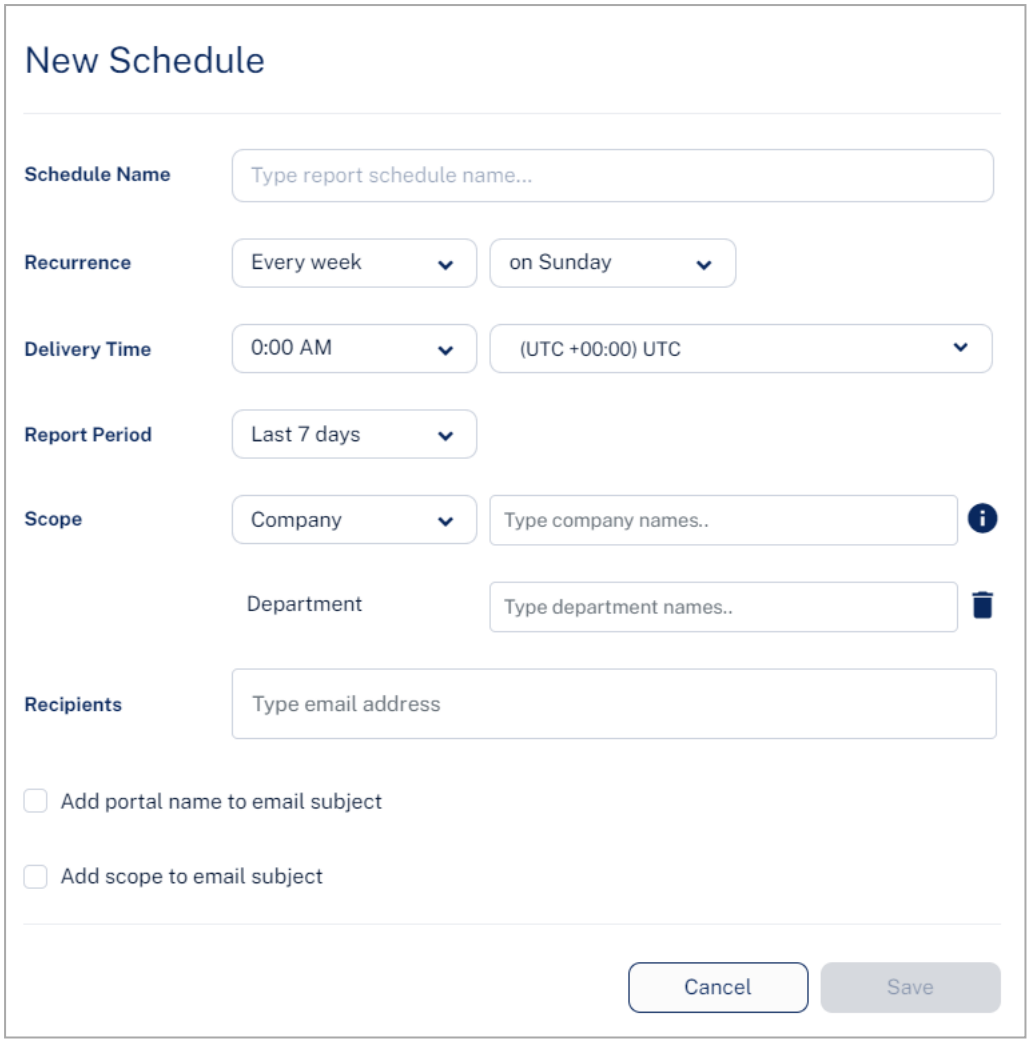
To view the **Report Scheduler** page, go to **Analytics** > **Reports Scheduler**.

By default, the **Security Checkup** report is sent on every Sunday to all the administrators configured to receive it.

Configuring a Report Schedule

To configure a report schedule:

1. Go to **Analytics** > **Report Scheduler**.
2. Click **Create Schedule**.



3. Enter the required **Schedule Name**.
4. For **Recurrence**, select when you need to schedule the report.
    - **Every week**
        - Select the week day.

- **Every month**
  - To schedule the report for specific week of every month:
    a. Select the week of the month (**on first**, **on second**, **on third**, **on fourth**, **on last**).
    b. Select the week day.
  - To schedule the report for specific day of every month:
    a. Select **on specific day**.
    b. Enter the specific date (1st to 28th) of the month.
  - To schedule the report for last day of every month, select **last day**.

5. For **Delivery Time**, select the required time and time zone.
6. For **Report Period**, select the period over which the report has to be generated:
   - **Last 7 days**
   - **Last 14 days**
   - **Last 30 days**
   - **Previous month**
   - **Previous quarter**
7. Select the scope of the report:
   - **All users**
   - **Company** and then enter the company name as specified in the **Company** field in **Azure AD**.
   - **Department** and then enter the department name.
8. For **Recipients**, enter the email addresses of users for whom the report has to be sent.
9. To add the portal tenant name to the email subject of the report, select the **Add portal name to email subject** checkbox.
10. Click **Save**.

Default Weekly Report

By default, the **Default weekly report** is configured to send the **Security Checkup** report to all the administrators in your organization.

By default, the report has these values.

- **Schedule Name** - Default weekly report
- **Report Period** - Last week
- **Recipients** - All administrators

  Note - The **Security Checkup** report is sent to all the administrators with **Receive weekly reports** checkbox selected in **System Settings** > **User Management**.

The **Default weekly report** schedule appears as the first row of the **Report Scheduler** table.

To edit the report schedule, click on the vertical ellipses icon (in the right side of the scheduled report row) and select **Edit**. For more information on how to schedule a report, see *"Configuring a Report Schedule" on page 350*.

Sending a Scheduled Report Immediately

After you schedule a report, if needed, you can send the scheduled report immediately.

To send a scheduled report immediately:

1. Go to **Analytics** > **Report Scheduler**.
2. Click on the vertical ellipses icon (in the right side of the scheduled report row) and select **Run now**.

   Avanan generates the report immediately and sends it to the configured recipients.
3. In the confirmation pop-up that appears, click **Yes**.

Editing a Report Schedule

To edit a report schedule:

1. Go to **Analytics** > **Report Scheduler**.
2. Click on the vertical ellipses icon (in the right side of the scheduled report row) and select **Edit**.
3. Make the required changes and click **Save**.

Deleting a Report Schedule

To delete a report schedule:

1. Go to **Analytics** > **Report Scheduler**.
2. Click on the vertical ellipses icon (in the right side of the scheduled report row) and select **Delete**.
3. In the confirmation pop-up that appears, click **Yes**.

Reviewing Security Events

Events

On the **Events** page, you can search for specific events, filter events that represent the most critical tasks, manual actions, and more.

You can see security events for these SaaS applications:

- Office 365 Mail
- Office 365 OneDrive
- Office 365 SharePoint
- Microsoft Teams
- Gmail
- Google Drive
- Slack
- Citrix ShareFile
- Box

Events Table Columns

The **Events** table has these columns:

Events Table Column Name	Description
Date & Time	The time at which the event was generated.

Events Table Column Name	Description
State	■ **Pending** - The administrator is requested to perform an action to remediate the event. For example, the policy is in **Monitor** mode, and a detected phishing email is in a user's mailbox. ■ **Remediated** - The event has been remediated, manually or automatically based on the policy. Event may be remediated in many ways, such as quarantining the email, removing attachments, or delivering it to the Junk/Spam folder. ■ **Detected** - Security event took place, but the administrator cannot manually remediate it. For example, a malicious email was sent by an internal user to an external recipient. ■ **Dismissed** - The event was manually dismissed by an administrator.
Action Taken	The action that was taken to remediate the event.
Remediated By	The system or administrator that remediated the event. ■ **Avanan** - Avanan took the remediation action automatically based on the policy. ■ **Microsoft** - Microsoft took the remediation action automatically. ■ Admin - Administrator performed manual remediation on the event. For example, the administrator quarantined the email post-delivery. ■ **Avanan analyst** - An Avanan analyst checked the end-user requests and reports. This is relevant only for customers that purchased the Incident Response as a service add-on.
Severity	Severity of the security event. ■ **Critical** ■ **High** ■ **Medium** ■ **Low** ■ **Very Low**
SaaS	The SaaS application the event was triggered in.

Events Table Column Name	Description
Threat Type	■ DLP ■ Malware ■ Phishing • Under Phishing, in many cases, the exact phishing category will be available. ■ Anomaly ■ Suspected Phishing ■ Suspected Malware ■ Shadow IT ■ Spam ■ Alert - Based on the policy and configurations, event generated alerts sent to all users. ■ Malicious URL Click ■ Proceed to Malicious URL
Details	Information about the event.
User	The users involved in the event. Examples: ■ For a phishing event, the column shows the sender and the recipients. ■ For a compromised account (anomaly) event, the column shows the compromised user.

Filtering the Events

To filter the list of events, do one of these:

- Click on the relevant sections in the charts above the table.
- Use the built-in filters for the different fields, including the free text search for strings across all fields.

To clear the filters, click **Clear Filters**.

Taking Actions on Events

Administrators can take actions on different event types. For example, if the event is about a phishing email that made it through to the user's mailbox, the administrator can quarantine the email.

To take action on a single event, click the ⋮ icon for the event from the last column of the table and select the required action.

To take action on multiple events, select the relevant events, click **Groups Actions** and select the required action.

Dismissing Events

Sometimes, the administrators need to remove an event from the open events list.

To do that, do one of these:

- To dismiss a single event, click the icon for the event from the last column of the table and select **Dismiss**.
- To dismiss multiple events, select the relevant events, click **Groups Actions** and select **Dismiss**.

A dismissed event will not be counted in the charts or in any other statistics.

To view the dismissed events, under filters, select **Dismissed** from the **State** field.

Managing Views

Departments with responsibilities related to email security are comprised of different teams and different roles, each often interested in a different set of security events.

Administrators can create multiple views which are a combination of filters in the **Events** screen for filtering the relevant events. Each administrator can set a different view to be presented by default.

To add a new View:

1. Go to **Events**.
2. Using filters, set the criteria for filtering the relevant events.
3. Click **Save as** from the top left side of the **Events** screen.
4. In the **Save View** window that appears, enter the required **View Name**.
5. Click **Save**.

Note - If an administrator adds (or deletes) a View, it gets added (or deleted) for all the administrators.

To select a saved View:

1. Go to **Events**.
2. Click **Saved views** from the top right side of the **Events** screen.
3. In the **Saved Views** window that appears, select the required view.
4. Click **Close**.

Notes:

- To edit a View, select the View, change the required filters, and click **Save** from the top left side of the **Events** screen.
- After saving, the View gets updated for all the administrators.

To set a default View:

1. Click **Saved views** from the top right side of the **Events** screen.
2. In the **Saved Views** window that appears, click the Star icon next to the relevant view.
3. Click **Close**.

Note - The default view selected is relevant only to the administrator that set it. Each administrator can select different default View.

Reviewing Phishing Events

Phishing events are triggered by the Anti-Phishing and Click-Time Protection security engines.

The Anti-Phishing security engine prevents the most sophisticated phishing and spam emails from being delivered to the end users' mailboxes.

The Click-Time Protection security engine re-writes the links in emails, emulates and checks the reputation of websites behind the links every time an end user clicks on them.

Acting on Phishing Events

To review and investigate the phishing event:

- To see reasons for the detection of an event as phishing, under **Security Stack**, click **More Info** for Anti-Phishing.
- To investigate the header of the raw email, under **Email Profile**, click **Show** for **Header from raw email**.
- To investigate the body of the raw email, under **Email Profile**, click **Show** for **Show body from raw email**.
- To download the raw email, under **Email Profile**, click **Download** for **Download this email**.
- To send the original email to the end-user, under **Email Profile**, click **Send** for **Send Original Email**.

  Note - This option appears only when there are links that were re-written by the Click-Time Protection security engine.
- To recheck the email for phishing, under **Email Profile**, click **Recheck** for **Recheck email**.

To filter emails similar to the event generated:

1. Under **Security Stack**, select **Similar Emails / Create Rules**.
2. Under **Filters**, define the criteria for filtering the emails.
3. Click **Search**.

Note - After filtering the emails, you can create Anti-Phishing Allow-List and Block-List. See *"Anti-Phishing Exceptions" on page 313*.

To report mis-classification of an event:

1. Under **Security Stack** in the event profile, click **Report mis-classification** for Anti-Phishing.
2. Under **Report this email as**, select how you want to classify the event:
   - Legit Marketing Email
   - Clean Email
   - Spam
   - Phishing
3. Under **How confident are you**, select how confident you are about the classification you selected:
   - Not so sure
   - Medium confidence
   - High confidence
4. Click **OK**.

Post-delivery Email Recheck

Sometimes emails are rechecked after delivering to the end user mailbox, which may result in emails being removed from the user mailbox.

Post-delivery email recheck can be initiated in these cases:

1. Recheck initiated by the inputs from the end users (reported phishing, malicious url clicks) and other sources.
2. Emails are processed by the Anti-Phishing security engine and when needed by the Avanan security analysts.
3. When a global block action is issued. The block action includes all emails that match the relevant match criteria, across all protected mailboxes.

4. Emails processed by the relevant policy workflows.

   When a policy is configured to block emails, the emails are removed from the mailbox and placed in quarantine. Avanan generates the relevant security events and sends the email notifications.

Reviewing Malicious Links

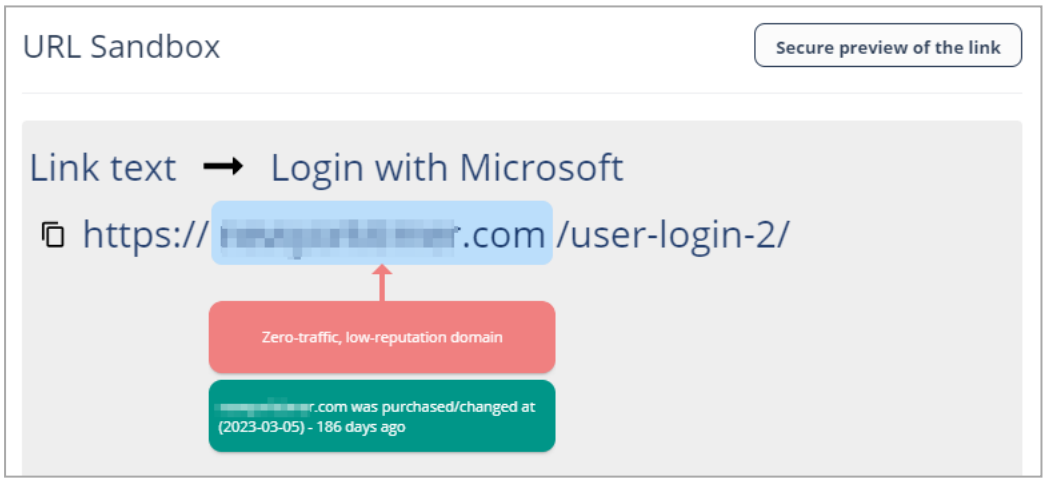
Link Analysis card on the **Email Profile** page shows the reasons why Avanan flagged links and QR codes as malicious or not. It also shows a secure preview (image) of the link.

For information about the malicious QR codes, see *"Detecting Malicious QR Codes" on page 107*.

To review and investigate the malicious links:

1. Open the malicious event.
2. Scroll-down to **Link analysis**.
3. Hover over the link and click **Analyze link**.

   The **URL Sandbox** pop-up appears.



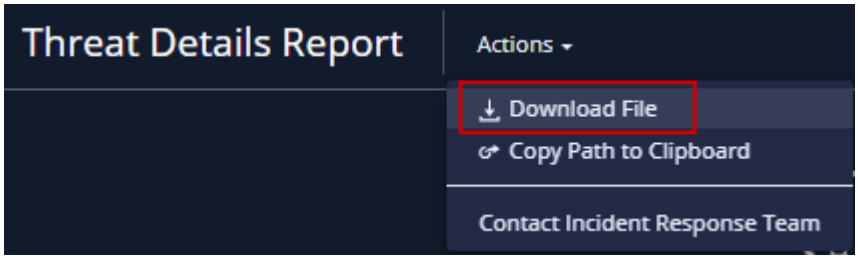
4. To view the image of the link, click **Secure preview of the link**.

Reviewing Malware Events

Malware events are triggered by the Anti-Malware engine. It comprises of matching the file against a data base of known malicious files (Anti-Virus) and running it through an advanced sandbox (Threat Emulation).

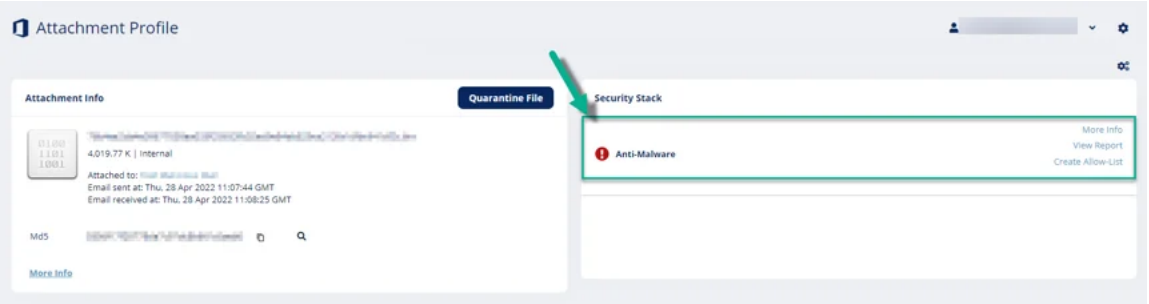
To review the event details, open the attachment profile page for the malicious event. In the Anti-Malware section under **Security Stack**, you can do these.

- To view the sandbox report with detailed explanation about why the file was deemed malicious, click **View Report**.
  - To download the malicious file from the report to your local computer, click **Actions** > **Download File**.



Warning - You should use the downloaded file with care as the malware can cause significant damage to computers, networks and corporate data.
  - To help you not run the malicious file accidentally on your local computer, the malicious file gets downloaded in the compressed tar.gz format as a password protected file.
  - Use *infected_te_report* as the password to extract the malicious file.

- To view the confidence level of the detection by the sandbox or the signature used by the static engines used to detect the malware, click **More Info**.



Note - Avanan Administrator Portal does not currently support Attachment preview.

Acting on Malware Events

- To quarantine an email, click **Quarantine Email** from the email profile.
- To release an email from quarantine, click **Restore Email** if the email is already in quarantine.
- To exclude a file that you believe was falsely detected as containing malware, add the file to Allow-List. See *"Anti-Malware Exceptions" on page 317*.
- To mark any file type as malware, add the file to Block-List. See *"Anti-Malware Block-List" on page 320*.

Automatic Ingestion of End User Reports

Avanan automatically ingests end user phishing reports without requiring organizations to change existing phishing reporting methods.

- If your organization uses Microsoft's Report Message Add-In, Avanan ingests all phishing reports automatically without any additional configuration. See *"Microsoft Report Message Add-in" on page 366*.
- If your organization uses a dedicated mailbox where end users forward phishing emails to it, configure Avanan to scan such mailboxes. See *"Dedicated Phishing Reporting Mailboxes" on page 365*.
- If your organization uses a third party solution with a phishing report button to report phishing emails, configure the solution to send reported emails to a dedicated folder and follow the steps in the *"Dedicated Phishing Reporting Mailboxes" on page 365*.

Note - If you have any queries about these configurations, contact *Avanan Support*.

Reviewing User Reported Phishing Emails

Email users are key in fighting against phishing. Users can help detect missed attacks, let the security administrators remediate the detected attacks, and adjust the policies to prevent similar attacks in the future.

Avanan automatically ingests these reports, alerts administrators about them, and presents them in a dedicated dashboard. This allows administrators to investigate and take necessary actions.

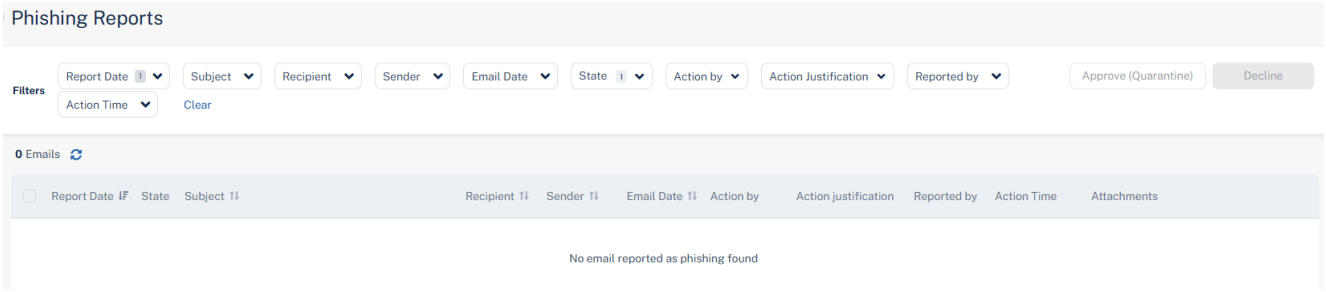
Benefits

- Present potentially missed attacks in the Avanan Administrator Portal.
- Integrated solution for the security admins to investigate and take actions.
- Simple, powerful way to increase end-users involvement and interact with them.

Phishing Reports Dashboard

The **Phishing Reports** dashboard shows the suspected phishing emails from the end users. Whenever a user marks an email as suspected phishing, a new entry is created in the dashboard. This allows the administrator to review and take the relevant actions.

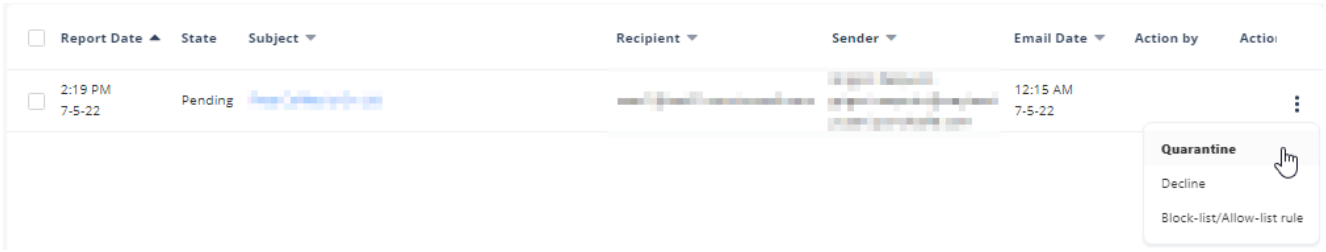
To see the user reported phishing emails, navigate to **User Interaction** > **Phishing Reports**.



Acting on Phishing Reports

Administrators can perform one of these actions on phishing reports:

- Decline - The report will be declined as the reported email does not seem to be malicious. The email remains in the user's mailbox.
- Quarantine - The report will be approved and the email will be sent to quarantine.
- Block-list/Allow-list rule - The administrator will choose to create an exception. See *"Anti-Phishing Exceptions" on page 313*.



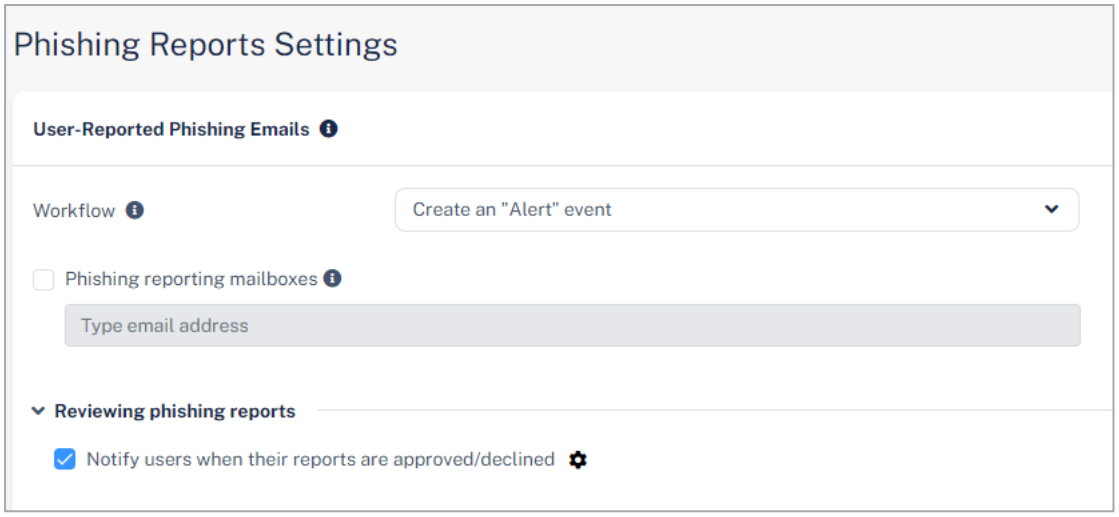
Notes:

- If the user action occurs beyond the data retention period, the system will exclude the emails and will not trigger any workflows.
  For example, if a user reports an email as phishing after the data retention period, Avanan will not process the email or trigger the workflow.
- If a user reports an email sent to multiple recipients as phishing, the **Email Profile** section will show the reported phishing status only for the specific copy of the email reported by the user.

Notifying End Users about Approving/Declining their Reports

Administrators can choose to notify end users whenever their phishing reports are approved or declined. To enable these notifications:

1. Go to **Security Settings** > **User Interaction** > **Phishing Reports**.
2. In the **Reviewing phishing reports** section, select the **Notify users when their reports are approved/declined** checkbox.



3. To change the notification message, click the ⚙ icon next to the checkbox and make the required changes.
4. Click **Save And Apply**.

Note - This will also enable end user notifications for rejected quarantine restore requests. See *"Managing Restore Requests" on page 433*.

To configure the notification subject and body:

1. Go to **Security Settings** > **SaaS Applications**.
2. To configure the templates for Office 365 Mail, click **Configure** for Office 365 Mail.
3. To configure the templates for Gmail, click **Configure** for Gmail.
4. Scroll-down to **Advanced** and edit these templates:
    - Phishing report decline:
        - Report Phishing decline subject
        - Report Phishing decline body
    - Phishing report approve:
        - Report Phishing approve subject
        - Report Phishing approve body

Events for User Reported Phishing

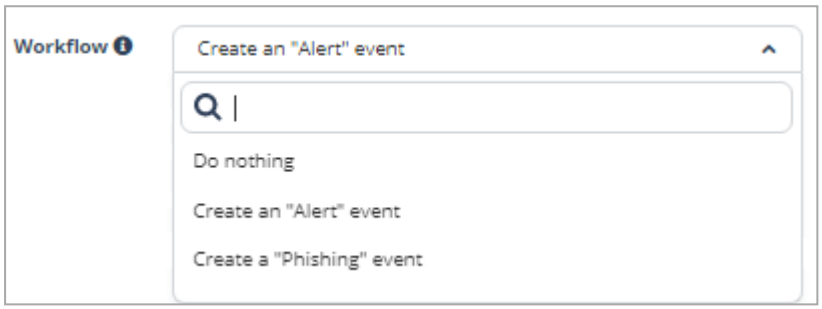
When a user reports a phishing email, the administrators can determine the event type to be generated by the Avanan.

The available options are:

- Create an "Alert" event
- Create a "Phishing" event
- Do nothing

To configure event type for the Phishing Reports emails:

1. Go to **Security Settings** > **User Interaction** > **Phishing Reports**.
2. In the **User-Reported Phishing Emails** section, in **Workflow**, select the event type to be generated.



3. Click **Save and Apply**.

Automatic Ingestion of End User Reports

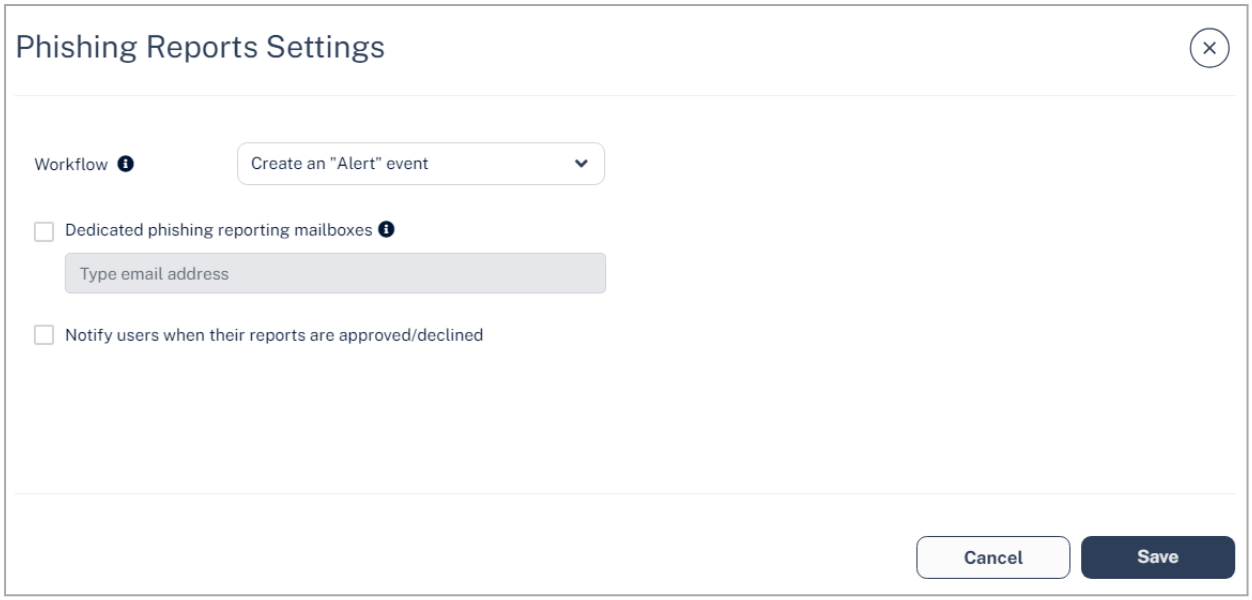
Dedicated Phishing Reporting Mailboxes

Some organizations provide one or more dedicated mailboxes to end-users to forward phishing emails to (for example, *phishing_reports@mycompany.com*). You can configure Avanan to scan such mailboxes, add every email forwarded to them to the **Phishing Reports** dashboard and create a user-reported phishing event.

To add dedicated mailboxes to the Phishing Reports dashboard:

1. Go to **Security Settings** > **User Interaction** > **Phishing Reports**.
2. Select the **Dedicated phishing reporting mailboxes** checkbox.
3. Enter the required mailbox email address.

   Note - To add multiple mailboxes, enter the mailbox addresses separated by a comma.



4. Click **Save and Apply**.

Note - All emails sent by protected users to these mailboxes generate events for administrators to review in the **Phishing Reports** dashboard. Make sure these are dedicated mailboxes to report phishing.

Microsoft Report Message Add-in

Microsoft offers a built-in **Mark as Phishing** option in Outlook. When a user clicks this option, Microsoft gets notified of the missed suspected phishing email and sends a reports to *phish@office365.microsoft.com*.

Avanan integrates with the native **Report Message** add-in for Microsoft 365. When a user reports an email as phishing, Avanan immediately shows the email in the **Phishing Reports** dashboard and creates a user-reported phishing event.

Enabling Report Message Add-in in Outlook

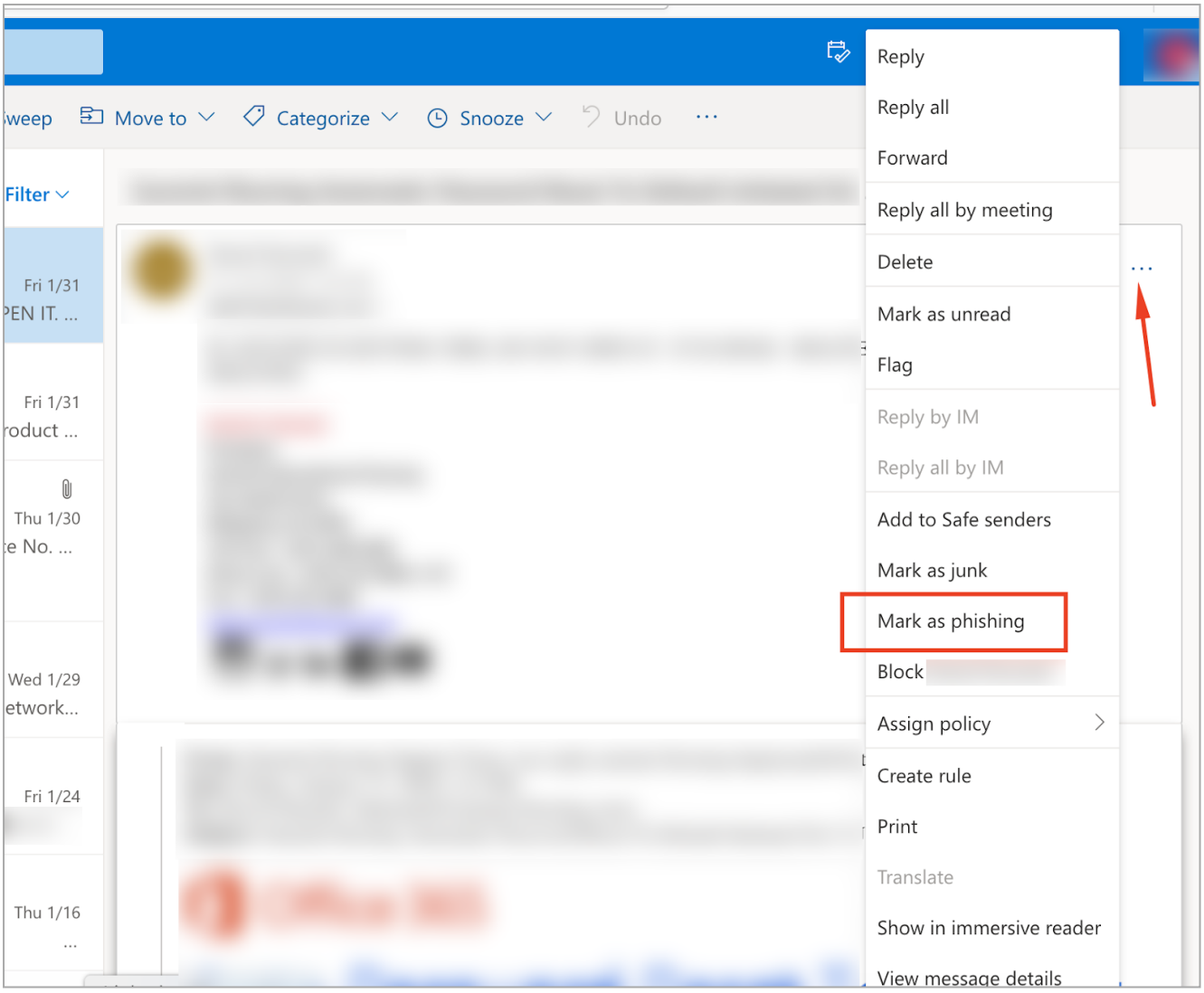
By default, in Outlook, the ability to report an email as phishing is enabled.

Office 365 administrators can add the *Report Message* add-in to their users' desktop clients if it is not already enabled. To enable the *Report Message* add-in, refer to Microsoft documentation.

Reporting Phishing Email from Outlook - End-User Experience

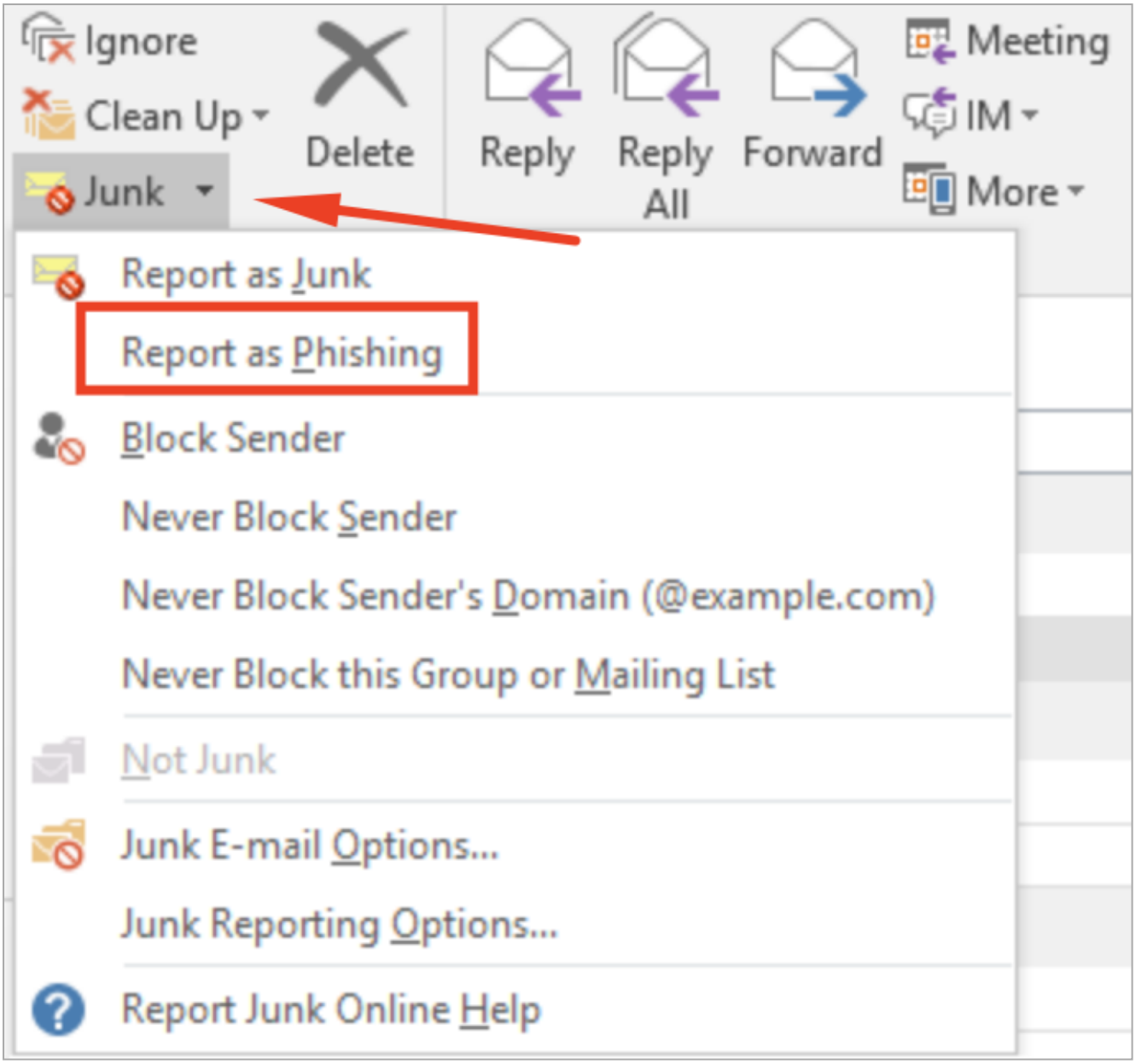
Web Client

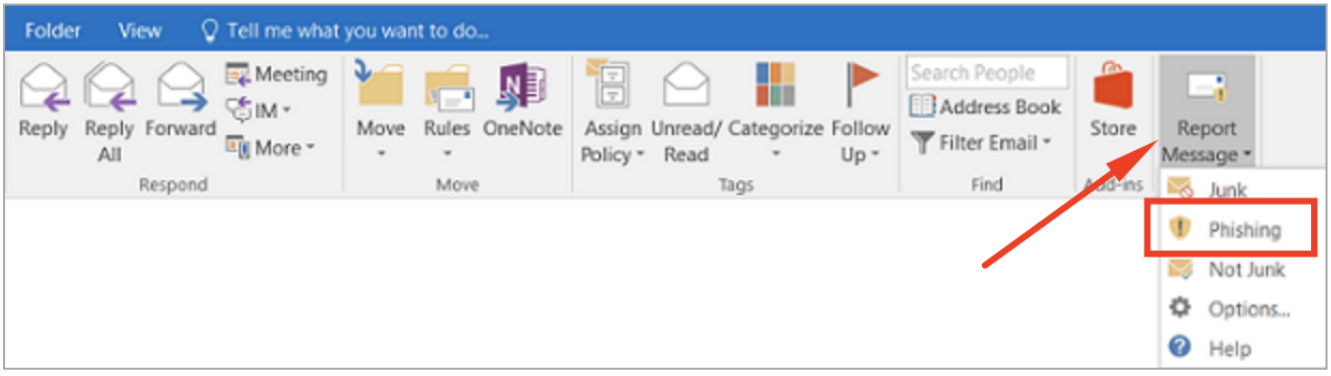
In the web client, open the email and select **Mark as phishing**.



Desktop Client

In the desktop client, go to **Home** tab, click **Junk** and select **Report as Phishing**.





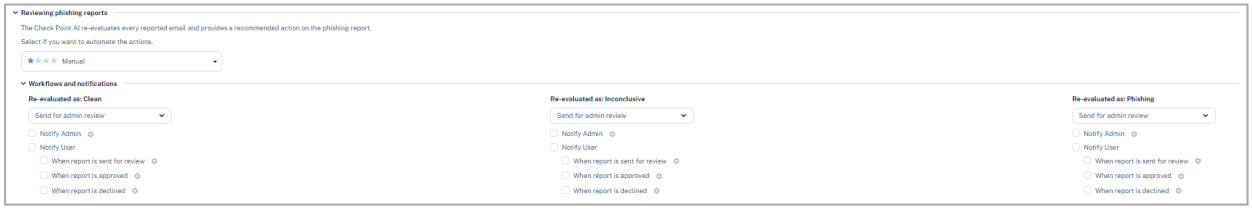
Automatic Handling of User Reported Phishing Emails

With Avanan, you can automate the handling of user reported phishing email reports, significantly reducing administrator's workload.

Every time a user submits a phishing report, Avanan re-evaluates the email and gives a re-evaluated verdict (clean, phishing, or inconclusive).

For each re-evaluated verdict, administrators can configure a workflow. To do that:

1. Go to **Security Settings** > **User Interaction** > **Phishing Reports**.
2. Expand **Reviewing phishing reports** and from the list, select one of these:
   a. **Manual** - Every report is manually reviewed by Administrator.
      - Clean: Send for admin review
      - Inconclusive: Send for admin review
      - Phishing: Send for admin review
   b. **Semi-automatic** - Automated actions for some updated verdicts and manual review for others.
      - Clean: Decline report. Email remains in mailbox
      - Inconclusive: Send for admin review
      - Phishing: Approve report. Quarantine the email
   c. **Automatic** - Automatic recommendation is performed.
      - Clean: Decline report. Email remains in mailbox
      - Inconclusive: Approve report. Quarantine the email
      - Phishing: Approve report. Quarantine the email



3. Expand **Workflows and notifications**.
4. Select one of these from the list:

Re-evaluated Verdict	Available Workflows
Re-evaluated as: Clean	■ **Send for admin review** ■ **Decline report. Email remains in mailbox**

Re-evaluated Verdict	Available Workflows
Re-evaluated as: Inconclusive	■ **Send for admin review** ■ **Decline report. Email remains in mailbox** ■ **Approve report. Quarantine the email**
Re-evaluated as: Phishing	■ **Send for admin review** ■ **Approve report. Quarantine the email**

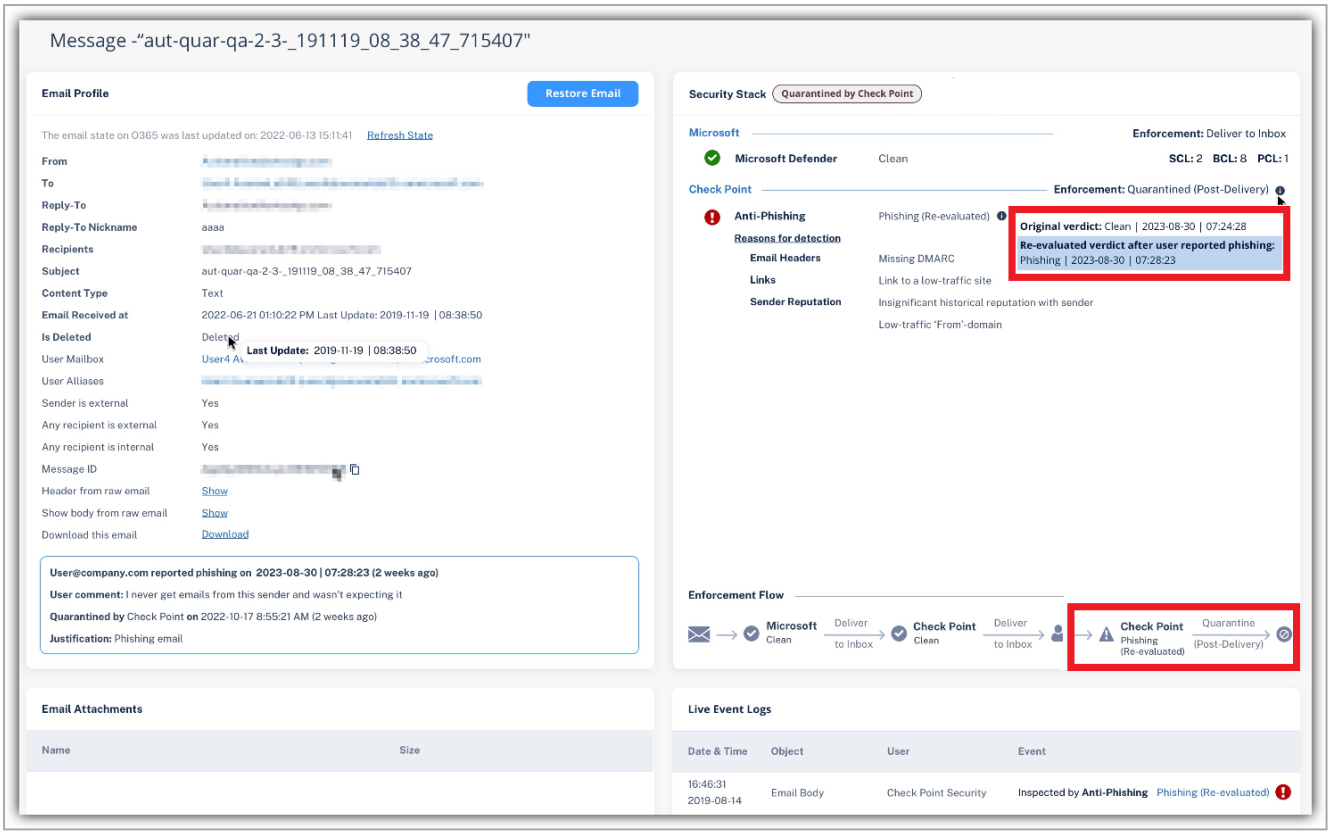
5. Select whom to notify:
   - **Notify Admin** - The administrator gets a notification when a report is sent for their review.
   - **Notify User**
     - **When report is sent for review** - The end user gets a notification when the report is sent for review.
     - **When report is approved** - The end user gets a notification when the report Is approved.
     - **When report is declined** - The end user gets a notification when the report is declined.

   Note - The availability of these options depends on the workflow selected.

6. To customize an email notification (subject and body), click next to the specific notification, make the necessary changes, and then click **Save**.
7. Click **Save and Apply**.

Re-evaluated Verdict of User Reported Phishing Emails- Administrator Experience

Once the Avanan re-evaluates the user reported phishing email, you can find the re-evaluated verdict under **Security Stack**.



Retention of Security Events

Avanan retains security events and shows them in the **Events** dashboard for 12 months.

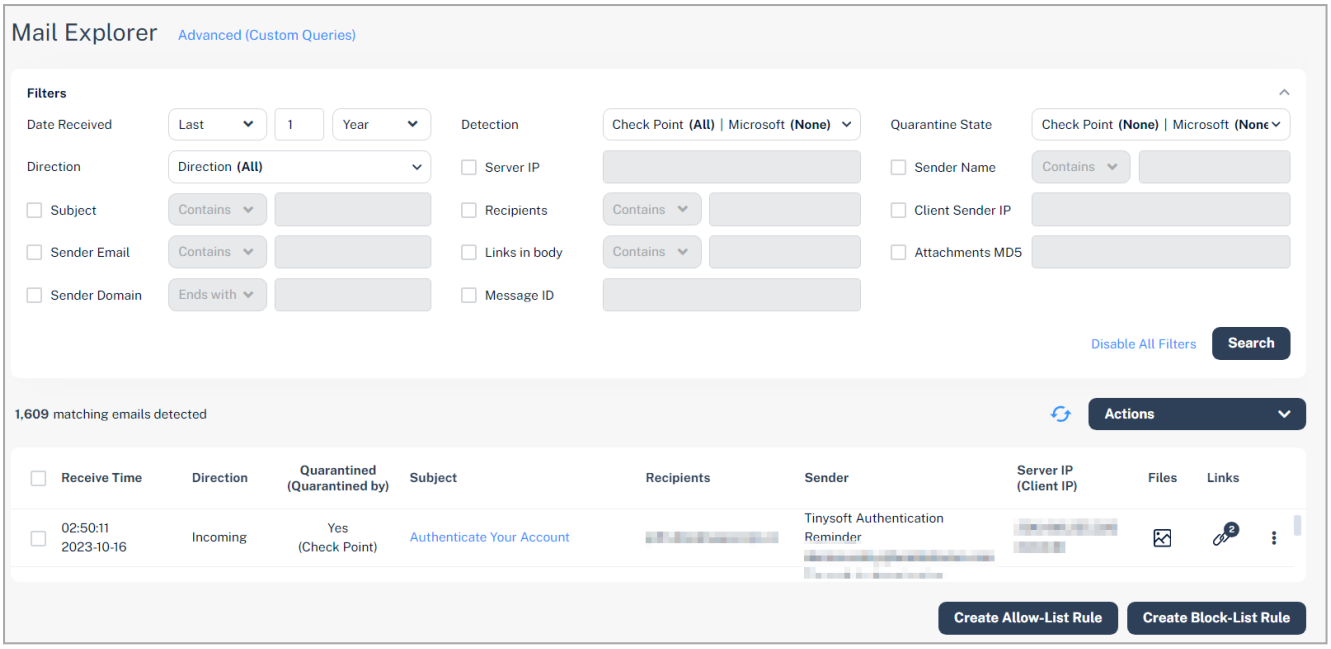
To export events to external sources and retain them, see:

- *"Forwarding Logs in Syslog Format" on page 395*
- Exporting security events via APIs

Searching for Emails

Mail Explorer

Mail Explorer allows you to view and search for emails Avanan viewed and processed on the protected email platforms.



It allows administrators to search for emails without using complex queries. To search for specific emails using advanced fields and operators, click **Advanced (Custom Queries)**. The system redirects to the *"Custom Queries" on page 379* page.

Searching for Emails in Mail Explorer

From the **Mail Explorer**, you can filter and view emails based on a specific search criteria.

To filter emails:

1. Under the **Date Received** field, select **Last** or **Range** and choose the relevant period.
2. Enable the relevant checkboxes and enter the search criteria for the query.
3. Click **Search**.

Available Search Fields

- Date received
- Detection (Microsoft or Avanan)
- Quarantine State (Microsoft, Google, Avanan or administrators)
- Direction (incoming, outgoing or internal)
- Subject
- Sender Email
- Sender Domain
- Sender Name
- Recipients

- Server IP address
- Client sender IP address
- Attachments MD5
- Links in email body
- Message ID

Contains vs Match

For search fields that need a string as input, administrators can select **Match** or **Contains** conditions.

- **Match** condition - Shows only the emails that exactly match the string.
- **Contains** condition - Shows the emails that contains the string.

For example, if an email has *Check out the invoice for this month* as subject and you searched for *Check out this* with **Match** condition, the system does not show the email.

Searching for Emails with Email Subject

When filtering the emails with the subject field, the system shows the search results with this logic:

- If you use the **Match** condition, the system shows the emails with subject that exactly match the search input string.
- If you use the **Contains** condition, the system shows all the emails whose subject contains the words (full words, not parts of them) in the search input string, regardless of their order.

  This is how the system performs the search operation:

  1. Splits the search string in to words, where the delimiter is every character that is not a letter or a number (a-z, A-Z, 0-9)

     For example, the search string *Check:this out now!* is split into the words *Check*, *this*, *out*, *now*

  2. The subject itself is also split into words like the search string.

     For example, for the search subject *Check:this out now!*, the system also returns *Now! Check this: out* as a result.

3. To search for words in specific order in an email subject, use quotation marks ("").
    - Special characters will be presented in the results if they are used in the input search string.
    - If you enter special characters in the search, the system returns the email subjects with those special characters.

      For example, if the search string is *"Check this out now!"*, the system will not return *Check:this out now!* and *Now check this out* subjects.
4. Returns all the emails whose subject contains all of the search string input words, regardless of their order.

   For example, the system returns *Now check this out* subject also .

Detailed example:

Subject	Search that will return the email	Search that will NOT return the email
Lorem: ipsum's dolor sit amet, consectetur adipiscing elit	■ Lorem: ipsum's ■ Lorem ■ Lorem: ipsum's dolor sit amet, consectetur adipiscing elit ■ Lorem ipsum's ■ Ipsum ■ Lorem-ipsum ■ Lorem------ipsum ■ S ■ Ipsum lorem ■ "lorem: ipsum" ■ "lorem:ipsum" ■ "ipsum's"	■ Lor ■ Lorem: ipsu ■ "lorem" ■ "lorem-ipsum"

Searching for Emails with Sender Email

While filtering for emails from a specific sender using the **Contains** condition, Avanan considers the sender email address as a single string.

Example:

Email Sender	Search that will return the email	Search that will NOT return the email
john@company.com	■ oh ■ john ■ hn@comp	■ joh pany ■ john company.com

Searching for Emails with Recipient Address

Recipient address contains a list of all email addresses the email was sent to.

Similar to searching on the subject field, the system splits the input string and the list of email recipients into words, where all non-alphabetical characters are delimiters.

Then, the system searches for emails with the string containing those words (not part of them) in the same order as they appear in the input string.

For example, the recipient *john@mycompany.com* is split in to three consecutive words: john company com

Email Sender	Search that will return the email	Search that will NOT return the email
john@gmail.com jeremy@company.com (the email was sent to both the addresses)	■ john ■ jeremy ■ Jeremy company ■ john gmail com	■ john company ■ joh

Searching for Emails with Links in the Email Body

When searching for links in the email body, the system supports searching for three letters and above.

The system returns an email in the search results if it contains a link in its body where the search string is either:

- A sub string or a full copy of the link domain without protocol. For example, domain.com
- An exact copy of the entire link, including the full path (not only the domain) and the protocol. For example, *https://domain.com/path.html*

Example:

Link in email body	Search that will return the email	Search that will NOT return the email
https://Link_ domain.com/path- additionalwords?highlig ht:yes	■ Link ■ Link_dom ■ ain.com ■ Link_domain.com ■ https://Link_ domain.com/path- additionalwords?highli ght:yes	■ Li ■ Path ■ path- additionalwords?highli ght:yes ■ Link_ domain.com/path- ■ https://Link- Domain.com

Searching for Emails Based on Detection

Administrators can search for emails based on the Microsoft and Avanan detections.

In addition, administrators can control the search condition between the Avanan and Microsoft detections.

Examples:

Search for	Mail Explorer Query
All detected phishing emails	Avanan detection = Phishing OR Microsoft detection = High-Confidence Phishing
Microsoft misdetections	Avanan detection = all but clean AND Microsoft detection = clean
Microsoft phishing misdetections	Avanan detection = Phishing, Malware AND Microsoft detection = all but high-confidence phishing

Searching for Emails Based on Quarantine State

Administrators can search for emails based on the enforcement decision of Microsoft / Google, Avanan, administrators or Avanan analysts (see *"Incident Response as a Service (IRaaS)" on page 454*).

In addition, the administrators can control the search condition between Avanan and Microsoft / Google enforcement decisions.

Examples:

Search for	Mail Explorer Query
All quarantined emails	Avanan detection = Quarantined OR Microsoft / Google = Quarantined
Google / Microsoft misses	Avanan = Quarantined AND Microsoft / Google = Not quarantined

Search for	Mail Explorer Query
Emails quarantined by administrators	Avanan = Quarantined by admin AND Microsoft / Google = select all
Malicious emails that would have been delivered to Junk by Microsoft / Google	Avanan = Quarantined AND Microsoft / Google = Delivered to Junk

Acting on Filtered Results

Restore quarantined emails

To restore the quarantined emails:

1. Open **Mail Explorer** from the left navigation panel.
2. Under **Filters**, define the criteria for filtering the emails, and click **Search**.
3. To restore emails from the search criteria, select the emails and click **Restore selected emails** under **Actions**.

Quarantine delivered emails

To quarantine the delivered emails:

1. Open **Mail Explorer** from the left navigation panel.
2. Under **Filters**, define the criteria for filtering the emails, and click **Search**.
3. To quarantine emails from the search criteria, select the emails and click **Quarantine selected emails** under **Actions**.

Creating Allow-List and Block-List Rule

Administrators can use the filters in **Mail Explorer** to create an Anti-Phishing Allow-List or Block-List.

The Anti-Phishing engine automatically marks all the emails matching these filters as clean for Allow-List or as Phishing for Block-List.

Notes:

- The search criteria defined under the **Date Received** and **Quarantine State** fields do not apply to any rule.
- Emails are scanned for malware and DLP even if they are in Anti-Phishing Allow-List.

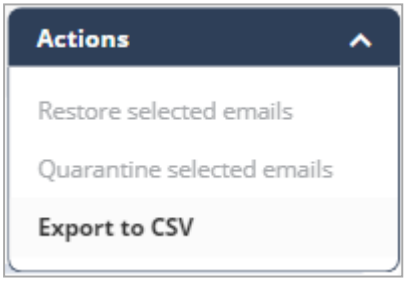
To create an Allow-list rule that marks emails as clean that match the defined criteria, select the filters and click **Create Allow-List Rule**.

To create a Block-List rule that blocks emails that match the defined criteria, select the filters and click **Create Block-List Rule**.

Export Results to CSV

To export the search results to CSV:

1. Open **Mail Explorer** from the left navigation panel.
2. Under **Filters**, define the criteria for filtering the emails, and click **Search**.
3. Select the emails to export.
   - To export all the emails from the search results, under **Actions**, click **Export to CSV**.



   - To export specific emails from the search results, select the emails and under **Actions**, click **Export to CSV**.

     Note - Only the selected emails will be exported.

Note - You can export only up to 20000 emails at a time.

Getting the Exported CSV File

- If the export contains less than 500 emails, the CSV file gets downloaded immediately.
- If the export contains more than 500 emails, the CSV file gets generated in the background. After the export is complete, the administrator that requested the export receives the CSV file through an email.

Notes:

- You can see the export status under **System Settings > System Tasks**.
- The export action gets logged under **System Settings > System Logs**.

Custom Queries

Avanan stores the metadata of all items (emails, files, user logins, etc.) obtained through the public APIs of the cloud applications you are protecting and inspected by the system.

For items found to be harmless, metadata is retained for two weeks.

For malicious items, the data is stored indefinitely.

Custom Queries give you direct access to this database of metadata.

Use Custom Queries to:

- Troubleshoot
- Build custom reports
- Perform bulk action such as quarantining phishing emails

Creating and Saving a New Query

You can create and save custom queries to analyze a specific SaaS for immediate and future use.

To create and save a new query

Step	Description
1	From the left panel, click **Analytics** > **Custom Queries**.
2	Click **Create New Query**. A list of available templates for each protected cloud app is displayed.
3	Select a template. A **Filter by** box allows you to search through the templates.
4	After you select a template, then a query with predefined conditions and columns is displayed. You can edit the **Conditions** and **Columns** to fit your needs. See the section below.

Step	Description
5	To save the query for future use: 1. Click **Query**. 2. Click **Save As**. 3. Enter the query details and click **OK**.

Editing the Query Columns and Conditions

After you have selected a template, use the options in **Custom Queries** to edit the template for your specific needs.

You can edit the template's predefined columns by choosing to add, remove or rename columns.

In addition, you can set conditions on columns.

To add a column

Step	Description
1	In **Custom Queries**, click **Columns**. A drop-down list opens.
2	Click on a column to select it, and then click **Apply**. **Note** - Certain columns are marked with an arrow. Click on the arrow to see more options.

To remove a column

Step	Description
1	Click the column's name. A condition box opens.
2	Select **Remove column**. The column is removed.

To edit a column's name

Step	Description
1	Click on the column's name. A condition box opens.
2	Select **Rename column**. The **Rename column** box opens.
3	In the **Column name**, delete the column's current name, and then enter a new name.
4	Click **OK**.

To sort a column

Step	Description
1	Click the columns name. A condition box opens.
2	In the **Sort** field, choose either **Sort ascending** or **Sort descending**. **Note** - If the query returns more than 1,000 results, then sorting is not available.

To add a condition to a column

Step	Description
1	Click the column's name. An editing box opens.
2	In the condition box, set the condition's parameters. **Note** - You can add more than one condition to a column. To add another condition to the same column, click **Add condition**.
3	Click **OK**. After adding a condition, it appears next to **Add condition**.

You can also add conditions without the need to display the corresponding column. In the section above the query's result table, click **Add condition**, and then select from the list of available fields.

Note - By default, all conditions are evaluated with an AND relationship when returning the query's results. For more advanced conditions, click on the gear icon (in the top right corner), and then select **Edit conditions**.

Bulk Actions on Query Results

Click on **Manual Actions** to see options for bulk remediation: quarantine, move to junk or add phishing alert.

If no items in the query's results are selected, the action will be taken on all items. You can select only some items before choosing a manual action to apply that action on those items only.

Additionally, the **Send email report** option sends an email alert to your email for each item selected in the query's result. A pop-up enables you to configure the template before sending alerts.

Exporting a Query Results

In **Custom Queries**, you have an option to export the query's results to your email.

This sends an email to your email address with the query's results in any of these file formats.

- CSV
- JSON
- XLSX

To export a query's results to your email:

Step	Description
1	Go to **Analytics** > **Custom Queries**.
2	Run and save the query. For more information, see *"Creating and Saving a New Query" on page 379*.
3	Click **Query Actions**, and then select **Export Results**.
4	In the **Email report to** field, enter the email address.
5	In the **Format** field, select the required file format. ■ CSV ■ JSON ■ XLSX
6	Click **Export**.

Scheduled reports based on Custom Query results

To schedule a query's result export

Step	Description
1	Run the query.
2	Ensure that the query is saved.
3	Click **Query**, and then choose **Scheduled Report**. **Note** - Choose the email address to have the query sent to, the frequency (daily/weekly/monthly) and the exact day and time. Double-click the report to open it.

Using a Query as a Detect and Remediate Policy Rule

Sometimes you may want to create an action (such as quarantine) that will apply to future events matching the query's conditions. In such a case, you can use your query as a policy rule in the **Detect and Remediate** mode.

Note - No action will be taken on the current results of the query, only future results will be impacted.

To use the query as a Detect and Remediate rule:

1. In **Custom Queries**, open a saved query.
2. Click **Query Actions**.
3. Choose an action, such as quarantine, from the list of available actions.
4. In the pop-up window that opens, you can choose to edit the name of the action, and then click **OK**.

   Afterward, the action should appear in the menu under **Query Actions**.

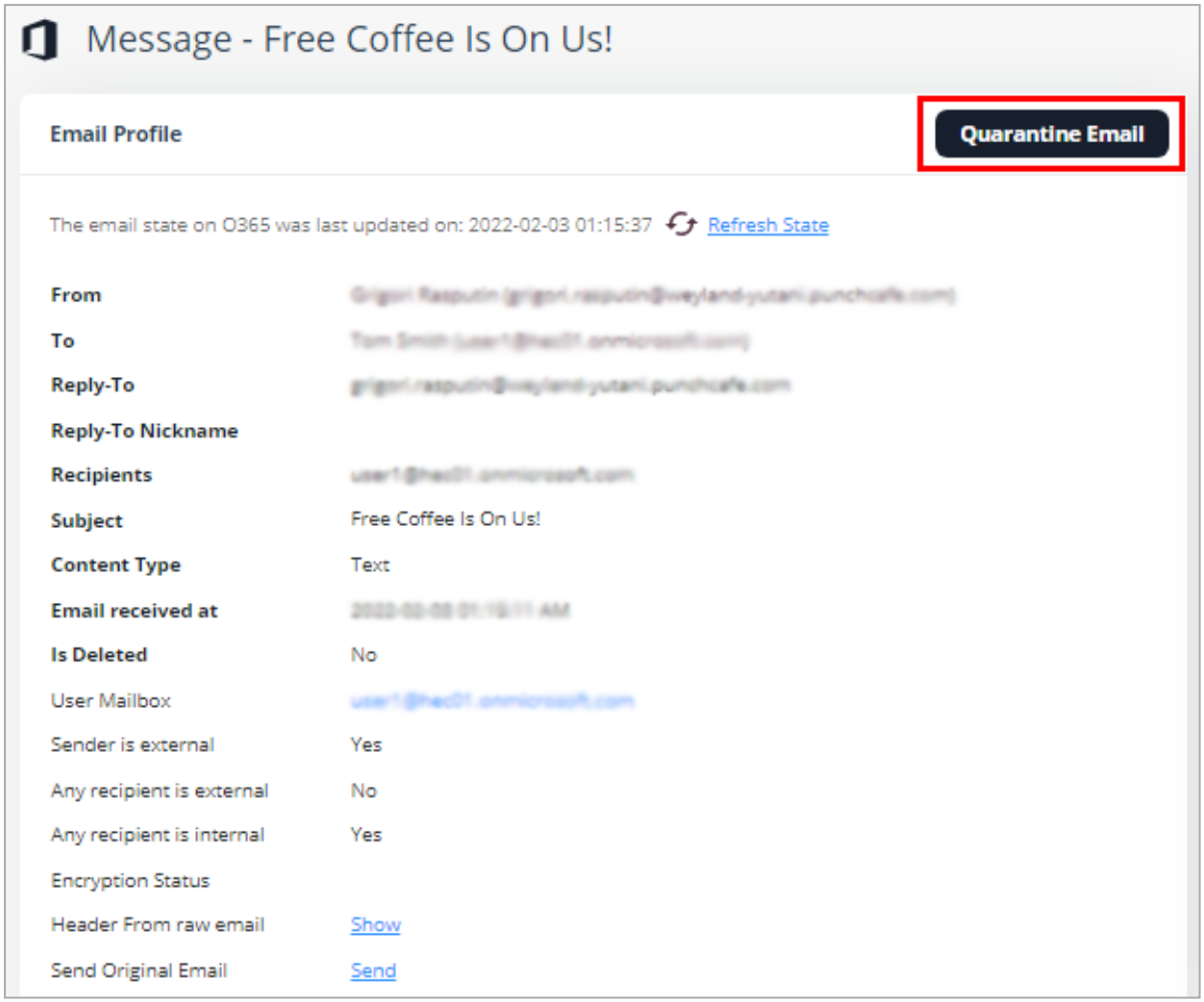
   Note - Actions linked to queries are automatically taken from that point forward in the **Detect and Remediate** mode. However, policy rules keep priority over custom queries.

Manually Sending Items to Quarantine

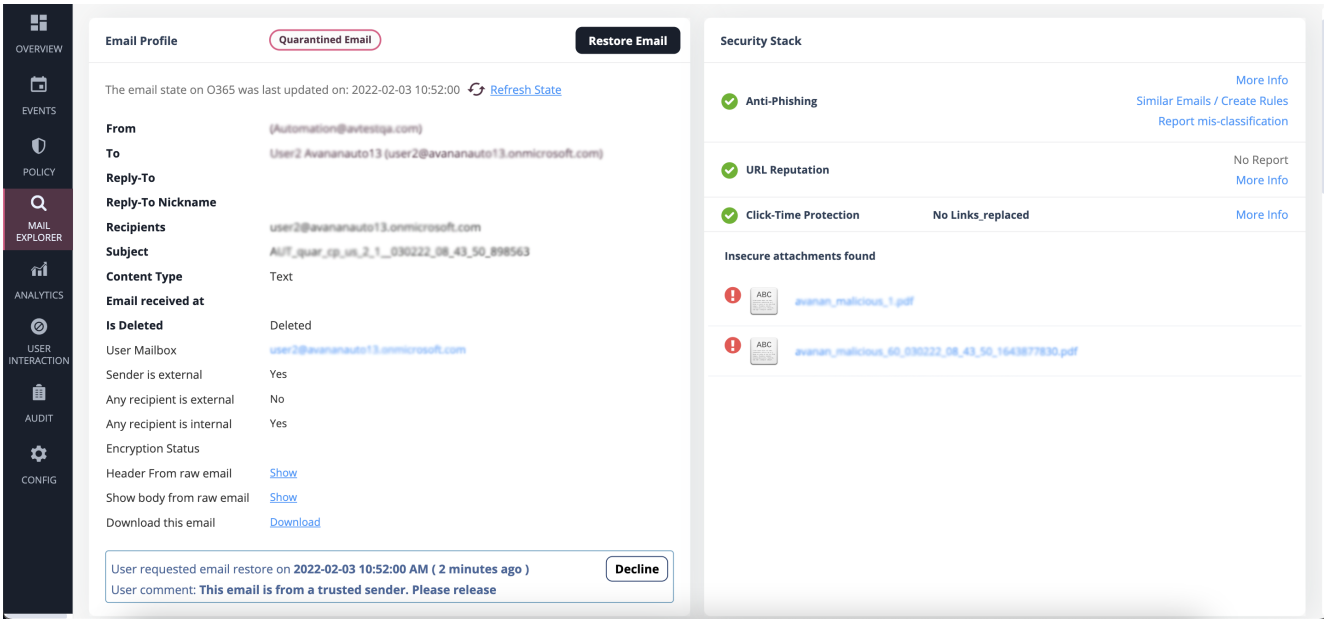
Single Item Quarantine

You can quarantine emails via two workflows from the Avanan Administrator Portal.

1. Using the event workflow
2. From the email profile



When an email is quarantined, it is removed from the user mailbox and moved to the designated quarantine mailbox. This effectively removes access to the email by the user. Once an email is quarantined, it can be managed using the Quarantine workflow or from the Avanan Administrator Portal for investigations and if needed the email can be released back to the user.



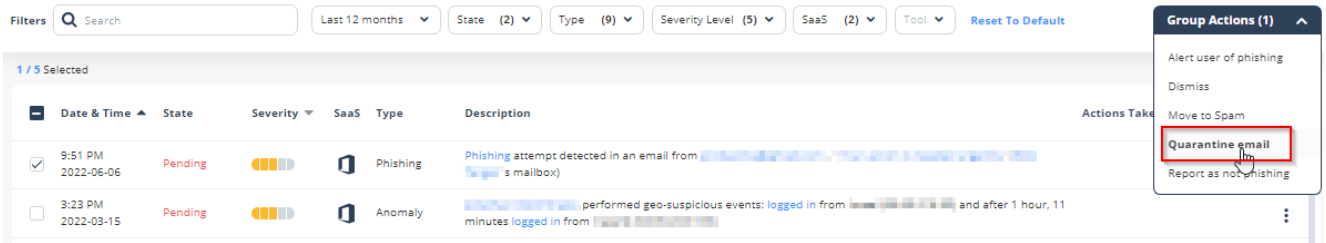
Notes:

- By default, the notifications for manual action is set as no notification to the user. For more information, see *"Notifications and Banners" on page 224*.
- If an administrator quarantines a user-reported phishing email with multiple recipients, Avanan removes the email from all recipient's mailboxes and quarantines it.

When implementing notifications to end-users an optional admin approval release workflow can be delivered to the user. In this configuration admins will be notified of pending requests in the quarantine work flow.

Bulk Manual Quarantine Process

The manual quarantine process can also be initiated in bulk via multi-select in the event workflow.



Note - If an administrator quarantines a user-reported phishing email with multiple recipients, Avanan removes the email from all recipient's mailboxes and quarantines it.

Query based Quarantine Process

For performing quarantine in bulk, the custom query engine gives you a robust search capability. Once your search criteria are established, manual actions can be executed on the search results. For more details about how to build custom queries, refer to *"Custom Queries" on page 379*.

Remediating Compromised Accounts

When Avanan detects compromised user accounts (BEC), it allows you to perform actions (**Block User**, **Reset Password**, **Unblock User**, and **Reset Password & Unblock**) on these accounts from the Avanan Administrator Portal itself.

Blocking a User Account

To block a user account from the Avanan Administrator Portal:

1. Open the **User** page of the user you need to block.
2. From the **User Meta Data** section, click **Block User**.

   or

   From the **Events** page, click on the vertical ellipses icon (in the right side of the selected compromised account), and then select **Block User**.
3. In the **Block User Account** pop-up that appears, click **OK**.

Notes:

- If you are using Microsoft Entra ID (formerly Azure AD) as the SAML/SSO Identity Provider for your corporate assets, the users gets blocked from accessing all the assets including Microsoft 365.
- Blocking a user account terminates all the active sessions associated with the account.
- Blocking a Microsoft user account resets the account password and requires the user to set a new password when unblocking their account.
- Blocking a Google user account will suspend the account. When a user account is suspended:
  - Email, documents, calendars, and other data are not deleted.
  - Shared documents are still accessible to collaborators.
  - New email and calendar invitations are blocked.

Resetting a User Account Password

To reset a user account password from the Avanan Administrator Portal:

1. Open the **User** page of the user you need to reset the password.
2. From the **User Meta Data** section, click **Reset Password**.

   or

   From the **Events** page, click on the vertical ellipses icon (in the right side of the selected compromised account), and then select **Reset Password**.
3. In the **Reset User Account Password** pop-up that appears, click **OK**.

   One time password gets generated automatically and the **User Account One-Time Password** pop-up shows the password for the user account.
4. Share the one time password with the user.

   Notes:
   - Resetting a user account password terminates all the active sessions associated with the account.
   - After logging in with the one time password, the user is prompted to set a new valid password.

Unblocking a Blocked User Account

To unblock a blocked user account from the Avanan Administrator Portal:

1. Open the **User** page of the user you need to unblock.
2. From the **User Meta Data** section, click **Unblock User**.

   or

   From the **Events** page, click on the vertical ellipses icon (in the right side of the selected compromised account), and then select **Unblock User**.
3. In the **Unblock User Account** pop-up that appears, click **OK**.

Note - The **Unblock User Account** option appears only for the blocked Google user accounts. For Microsoft user accounts, you can unblock the user account by using the **Reset Password & Unblock User Account** option.

Resetting Password and Unblocking a Blocked User Account

To reset the password and unblock a blocked user account from the Avanan Administrator Portal:

1. Open the **User** page of the user you need to unblock.
2. From the **User Meta Data** section, click **Reset Password & Unblock**.

   or

   From the **Events** page, click on the vertical ellipses icon (in the right side of the selected compromised account), and then select **Reset Password & Unblock**.
3. In the **Reset Password & Unblock User Account** pop-up that appears, click **OK**.

   One time password gets generated automatically and the **User Account One-Time Password** pop-up shows the password for the user account.
4. Share the one time password with the user.

   After logging in with the one time password, the user is prompted to set a new valid password.

Note - The **Reset Password & Unblock** option appears only for the blocked user accounts.

Monitoring and Auditing Actions on Users

Avanan audits all the user actions and adds them to the **System Logs** (**System Settings** > **System Logs**).

To monitor the action status of Microsoft user accounts, go to **System Tasks** (**System Settings** > **System Tasks**).

System Settings

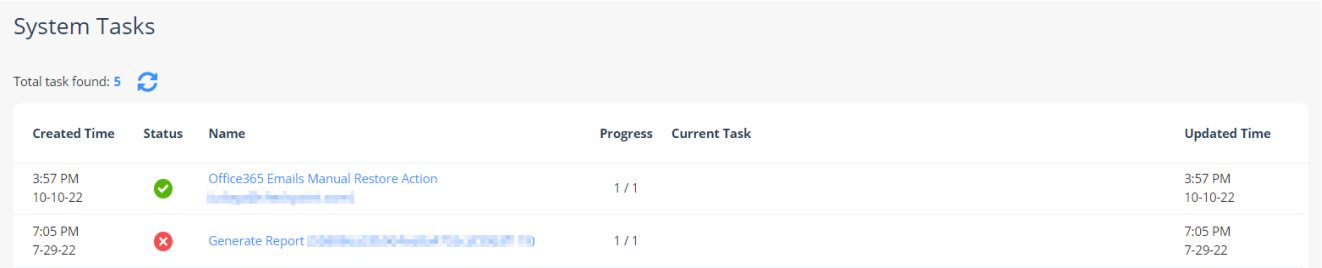
You can view **System Tasks** and **System Logs** from the **System Settings** menu. It allows you to track the actions performed in Avanan and helps in auditing purposes.

It also provides a **Service Status** page that shows the system's health, reported issues related to your tenant in the Avanan Administrator Portal, and their status.

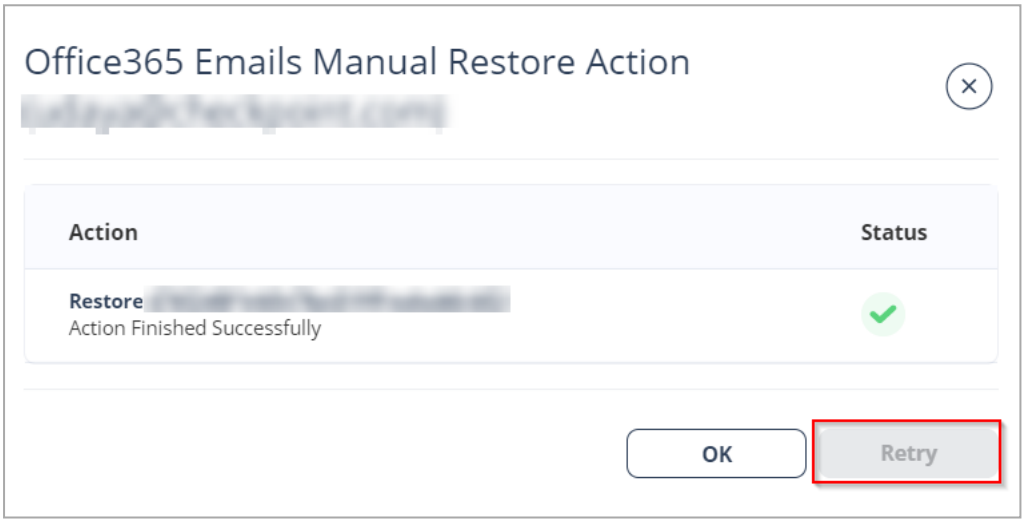
System Tasks

Avanan performs operations that can take a few minutes or even longer. To prevent users from waiting until the operation is complete, Avanan includes a **System Tasks** screen that shows these long tasks' status.

System Tasks are located under the **System Settings** menu. You can see all the tasks that were executed with their status.



To see the task status, click on the task **Name**. It opens a status screen that shows all the steps executed. If the task has failed, it shows the error reason. To retry a failed task, click **Retry**.



System Logs

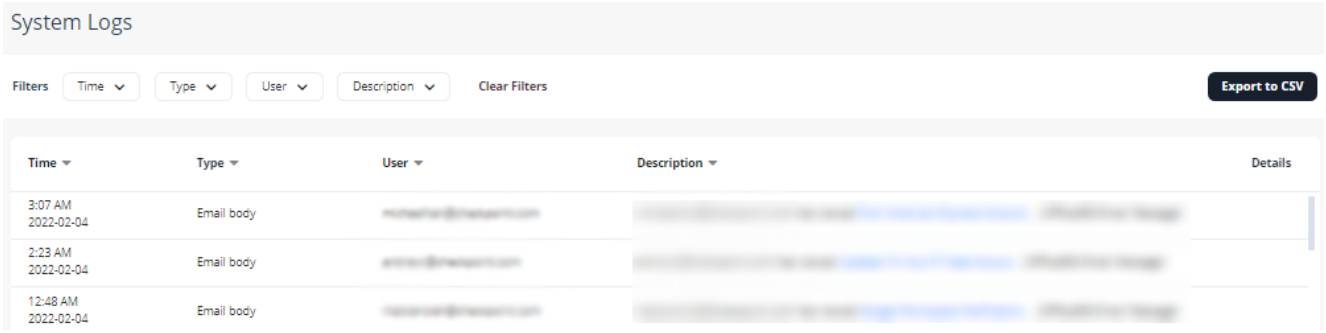
All actions are reported to the **System Logs**. To see the logs, go to **System Settings > System Logs**.

You can use **Filters** to search for the required logs.

To export logs to an excel file, click **Export to CSV**.

Notes:

- The **System Logs** are retained only for 12 months.
- The time displayed under the **Time** column reflects your browser's time zone.



Service Status

Avanan notifies the administrators on system health status and maintenance activities relevant only to your tenant.

The **Service Status** page allows you to:

- View the current health of the system and see if there are any ongoing issues.
- Browse through the history of the issues relevant to your tenant.
- Subscribe to email and/or SMS updates on any issue related to your tenant.

You will see a warning icon in the **Service Status** menu (Service Status) when there is any ongoing issue. The icon disappears after the issue is resolved.

To view the **Service Status** page, go to **System Settings** > **Service Status**.

Under **Service Status**, you can view the current health of the system.

- If there are no issues, it shows **Operational**.
- If there are any ongoing issues, you can view the status, and the configured administrators receive the status updates.

  After the issue is resolved, you can click on the **Root Cause Analysis** link to view the RCA document.

Under **Issues history**, using the drop-down, you can choose to view the issues reported in the **Past week** or **All issues**.

To select the users to receive notifications on service status updates:

1. Go to **System Settings** > **Service Status**.
2. Click **Subscribers**.

   The **Subscribers** page opens and shows a list of users.

3. In the **Notify Via** column, select **Email** and/or **SMS** for the user you want to send alerts.

   Notes:
   - Administrators with the **Receive Alerts** role enabled in the **Specific Service Roles** are automatically subscribed for email and SMS notifications.
   - To select SMS, the user should have a phone number. For the procedure to update the user information, see *"User Management" on page 508*.

4. Click **Save**.

You can add group mailboxes or users that are not Avanan Portal users to receive notifications on service status updates.

To add group mailboxes or users outside Avanan Portal:

1. Go to **System Settings** > **Service Status**.
2. Click **Subscribers**.
3. Click **+ Add Subscriber**.
4. In the **Add Subscriber** page, add the relevant details.
   a. Enter **First name** and **Last name**.
   b. Enter **Email address**.
   c. In the **Phone number** column, select the country code and enter the phone number.
5. In the **Notify Via** column, select **Email** and/or **SMS** for the user you want to send alerts.
6. Click **Add Subscriber**.

To edit or remove group mailboxes or users outside Avanan Portal:

Note - You cannot edit or remove Avanan Portal users.

1. Go to **System Settings** > **Service Status**.
2. Click **Subscribers**.

   The **Subscribers** page opens and shows a list of users.

3. To edit the details:
   a. Click the ⋮ icon (in the right corner of the row) and select **Edit Subscriber**.
   b. Update the relevant details and click **Save**.
4. To remove a user:

a. Click the ⋮ icon (in the right corner of the row) and select **Remove Subscriber**.

b. In the confirmation pop-up, click **Yes**.

SIEM / SOAR Integration

Avanan allows to integrate with multiple Security Information and Event Management (SIEM) platforms and Cortex XSOAR by Palo Alto Networks.

Encryption - For SIEM, unless configured otherwise, all events are forwarded over HTTPS.

Source IP Address

Avanan can be deployed in one of several geographic regions. The security events get forwarded from a unique static IP for each region.

The static IP address for different regions:

- United States - `34.192.247.192`
- Europe - `54.247.106.52`
- Australia - `52.63.125.59`
- Canada - `35.182.23.24`
- India * - `13.126.227.64`
- United Arab Emirates * - `3.29.198.97`
- United Kingdom * - `13.42.125.75`

* These regions are relevant only for tenants created using the Avanan MSP portal.

Configuring SIEM Integration

To configure SIEM integration from the Infinity Portal:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for **SIEM Integration**.
3. Select the required **Transport** method and enter the relevant details.

Supported Transport methods

Transport Method	Required Fields
Splunk HTTP Event Collector (HEC)	HTTP Event Collector Host / URI
	HTTP Event Collector Token
	(Optional) To use Indexer acknowledgment, select the checkbox and enter the Channel ID.
	(Optional) To use Splunk Index, select the checkbox and enter the Splunk index name.
HTTP Collector	HTTP Collector URL (HTTP/HTTPS) For example, *https://myconnector.mycompany.com*
AWS S3	AWS IAM Role ARN
	AWS S3 Bucket Name
	AWS S3 Bucket Region
	AWS S3 Bucket Directory Path
	(Optional) To use External ID, select the checkbox and enter the External ID.
AWS SQS	AWS SQS Queue URL
Azure Log Workspace	Azure Log Workspace ID
	Azure Log Workspace Shared Key
TCP	TCP Host
	TCP Port

Transport Method	Required Fields
Google Chronicle	Customer ID - Unique identifier (UUID) corresponding to your Chronicle instance. Account Region - Region where your Chronicle instance is created. Credentials JSON - Google Service Account credentials. **Note** - If the Credentials JSON is not available, contact Google support. Ingestion API - Google Chronicle Ingestion API type ■ Unified Data Model (UDM) event ■ Unstructured log

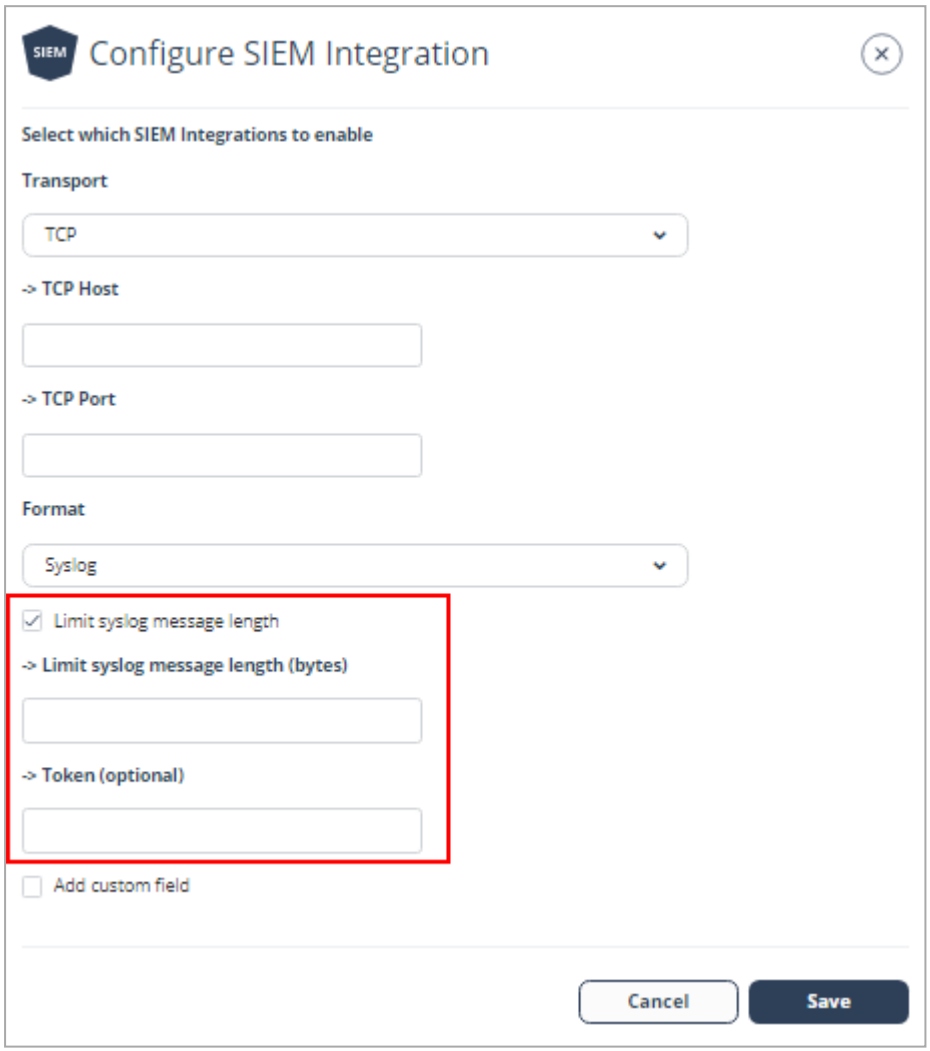
4. Select the required log **Format**.
   - JSON (Splunk HEC/CIM compatible)
   - JSON (CIM compatible)
   - JSON
   - JSON Flat (dot notation)
   - JSON (Rapid7, <8k characters)
   - JSON (Google UDM Compatible)
   - Syslog (See *"Forwarding Logs in Syslog Format" on the next page*)
   - Google Chronicle Unstructured logs
5. (Optional) If you need to add custom fields to every event forwarded from Avanan to your SIEM platform:
   a. Select the **Add custom field** checkbox.
   b. Enter the required **Custom field name**.
   c. Enter the required **Custom field value**.

   Note - You can add only up to five custom fields.
6. Click **Save**.

Note - After you configured the SIEM integration, Avanan starts sending logs. You have to configure your SIEM platform to receive Avanan logs.

Forwarding Logs in Syslog Format

- Syslog messages are RFC 5424 compliant.
- If you need to limit the syslog message size, select the **Limit syslog message format** checkbox, and under **Limit syslog message length (bytes)**, enter the message limit in bytes.



- If you need to add authentication token to all the syslog messages, enter the token under **Token (optional)**.
- You can configure TLS when using TCP transport. To define the certificate, contact *Avanan Support*.

- Supported certificate types:
  - CA certificate:
    - Use the CA certificate for our servers to validate the remote server that forwards events.
    - Ensure the certificate includes all necessary components: Root CA, Intermediate Certificates, and Server Certificate, all in .pem format.
    - List the certificates in the following order: Server Certificate, Intermediate Certificates, Root CA.
    - The Common Name (CN) of the server certificate must match the domain or IP address specified in the SIEM configuration.
  - Client certificate:
    - Use the Client certificate when the remote server needs to validate the client (our SIEM server) for TLS.
    - The certificate must be in .pem format and include two parts: the client certificate and the unencrypted private key.

Supported Security Events for SIEM

Avanan supports to send these security events to the integrated SIEM platforms.

- Phishing
- Suspected Phishing
- User Reported Phishing
- Malware
- Suspected Malware
- Malicious URL
- Malicious URL Click
- DLP
- Anomaly
- Shadow IT
- Spam

Notes:

- Avanan generates logs for each one of these security events.
- Avanan does not add sensitive data to the DLP SIEM logs.

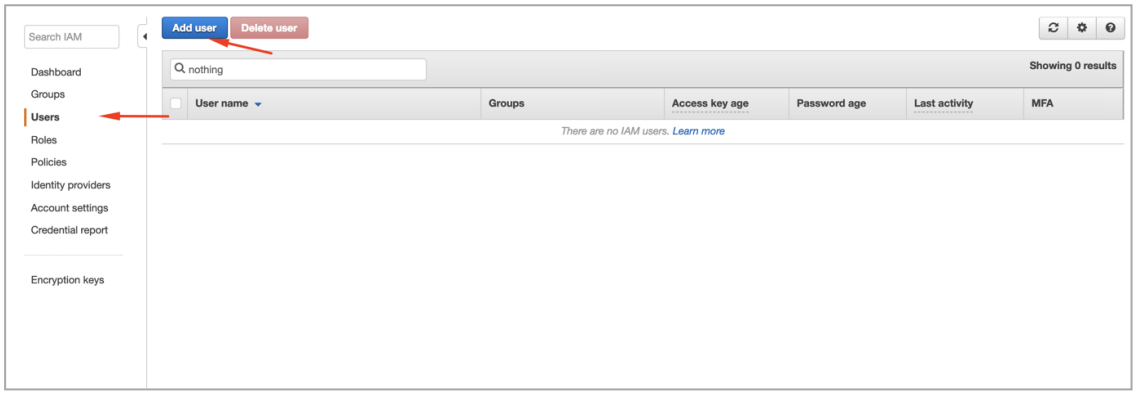
Forwarding Events to AWS S3

Configuring AWS S3 to Receive Avanan Logs

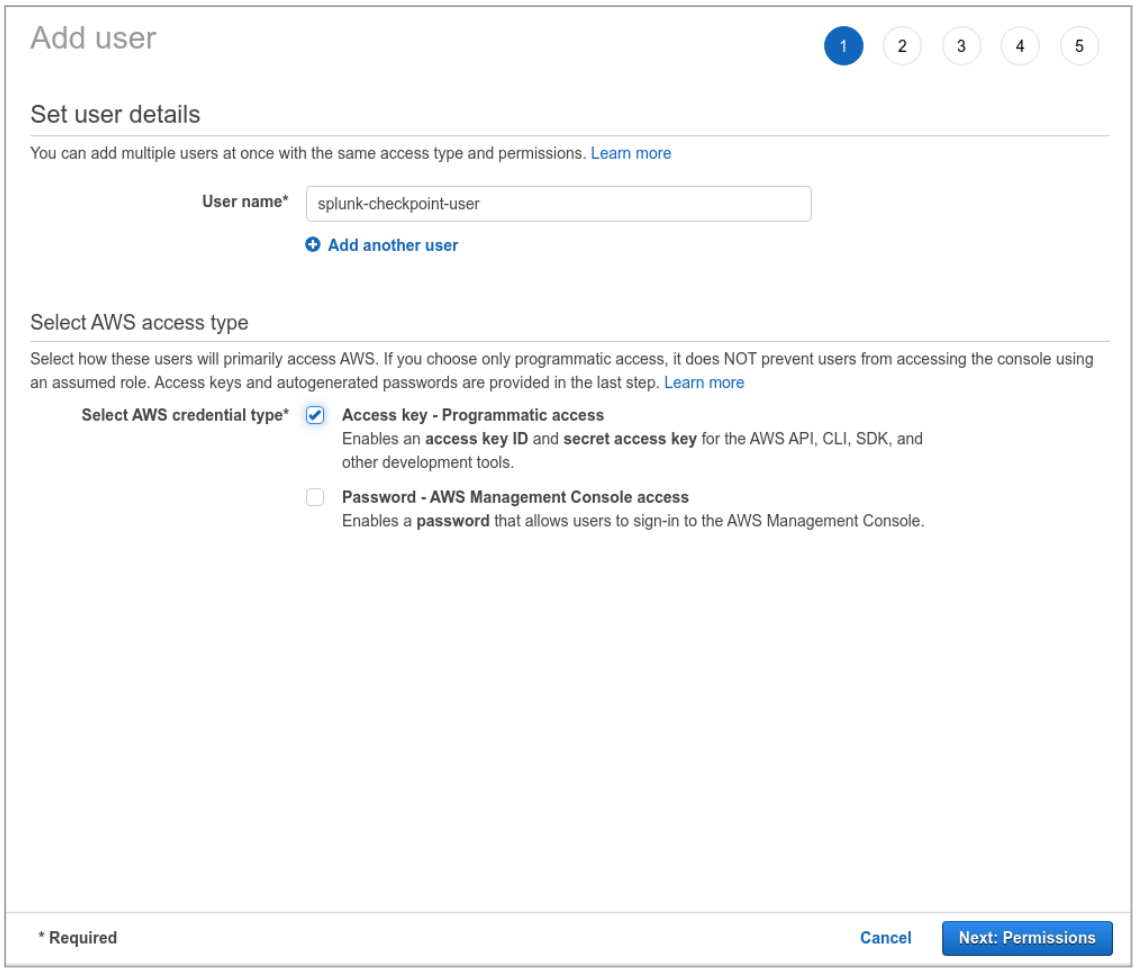
1. Go to AWS IAM: https://console.aws.amazon.com/iam/home#/home.
2. **Create a new user.**

   To create a new user:

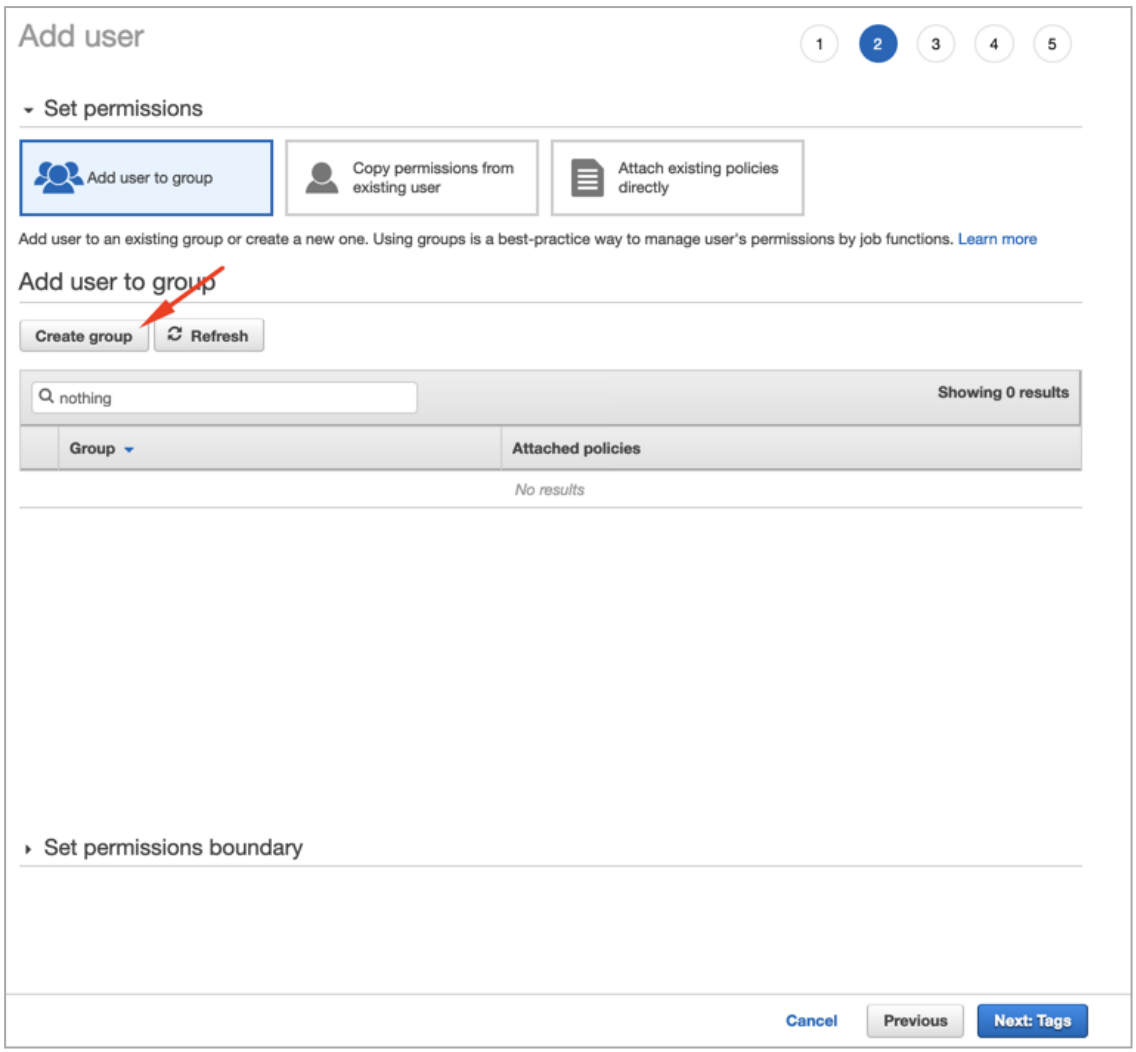
   a. Click on **Users > Add user**.



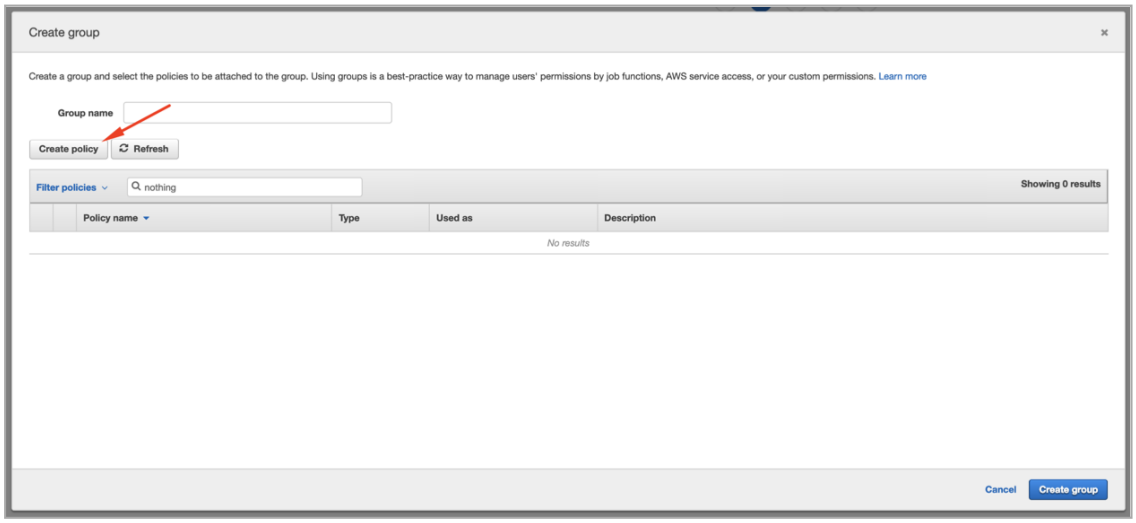
b. Select a user name, enable **Access Type** as **Programmatic access** and click **Next: Permissions**.



c. Click **Create Group** or select the group if already created.



d. Click **Create policy** or select the policy if already created.

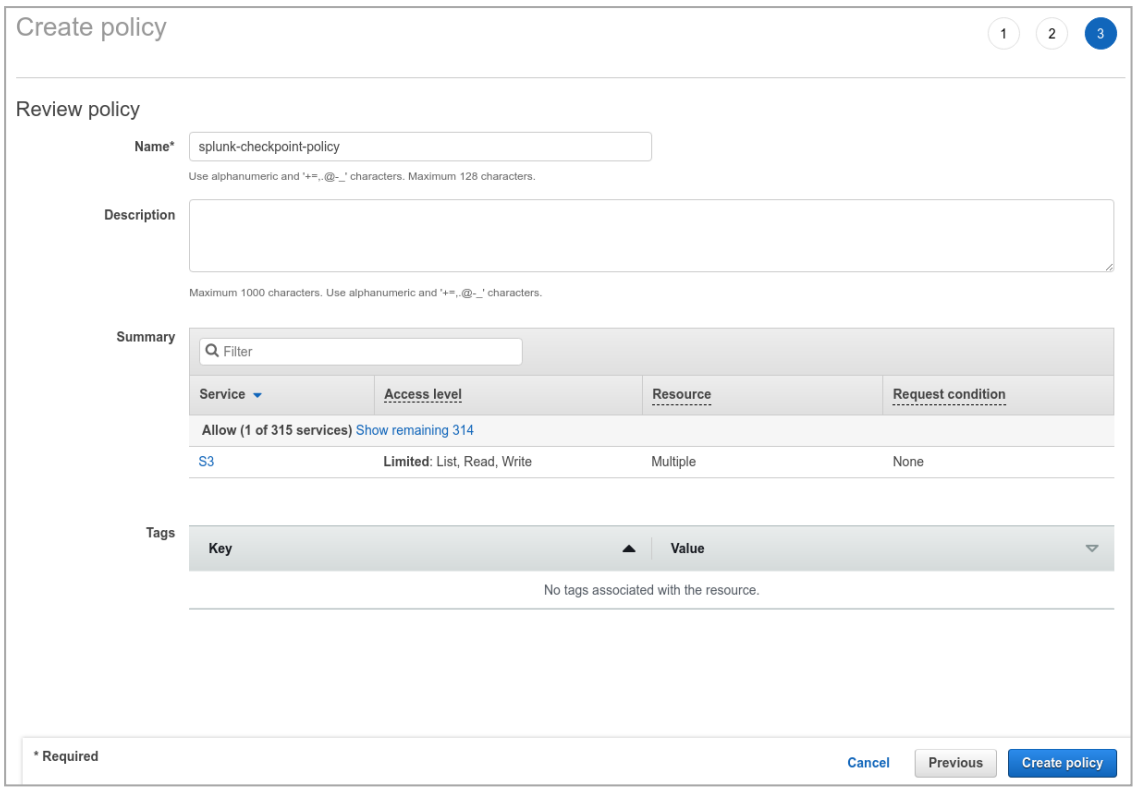


e. On the new tab, click **JSON** and copy this over.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR_S3_BUCKET"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR_S3_BUCKET/THE_LOG_FOLDER_IF_
ANY/*"
      ]
    }
  ]
}
```

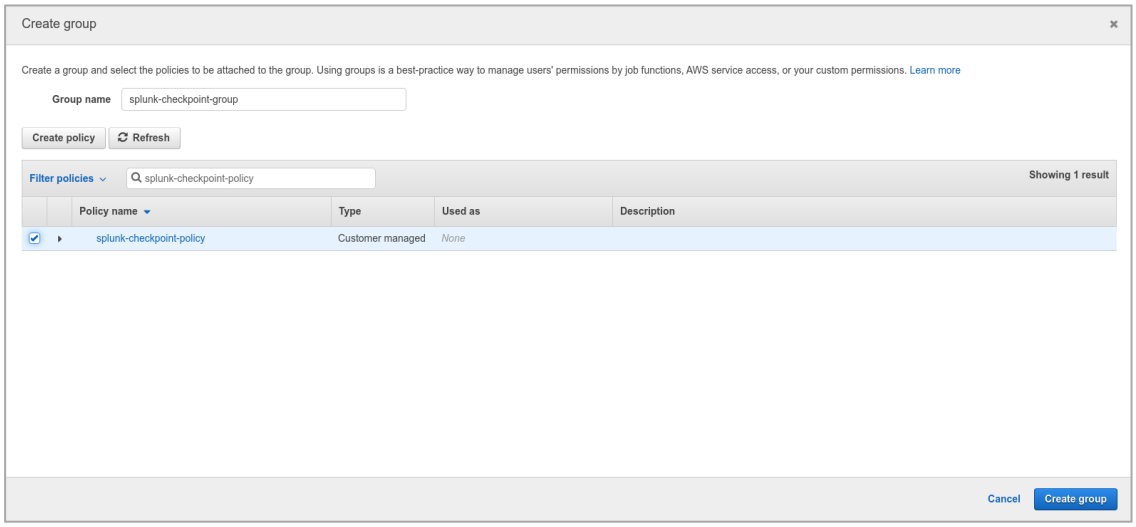
f. Click on **Review Policy** and select the policy you just created.

g. Enter the required name to the policy and click **Create policy**.

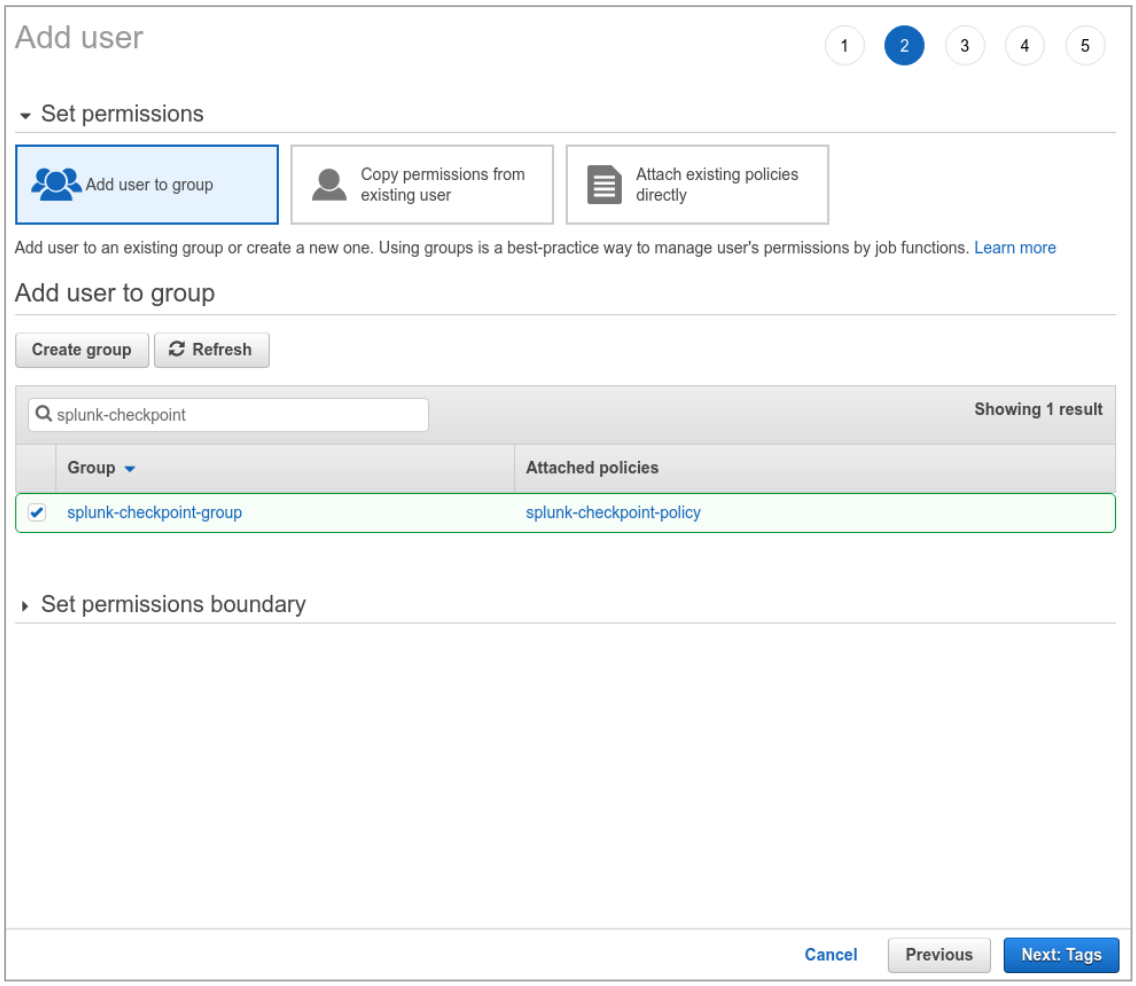


h. After the policy is created, go back to the previous tab and click **Refresh**.

i. On the next screen, select the policy name you created and click **Create Policy**.

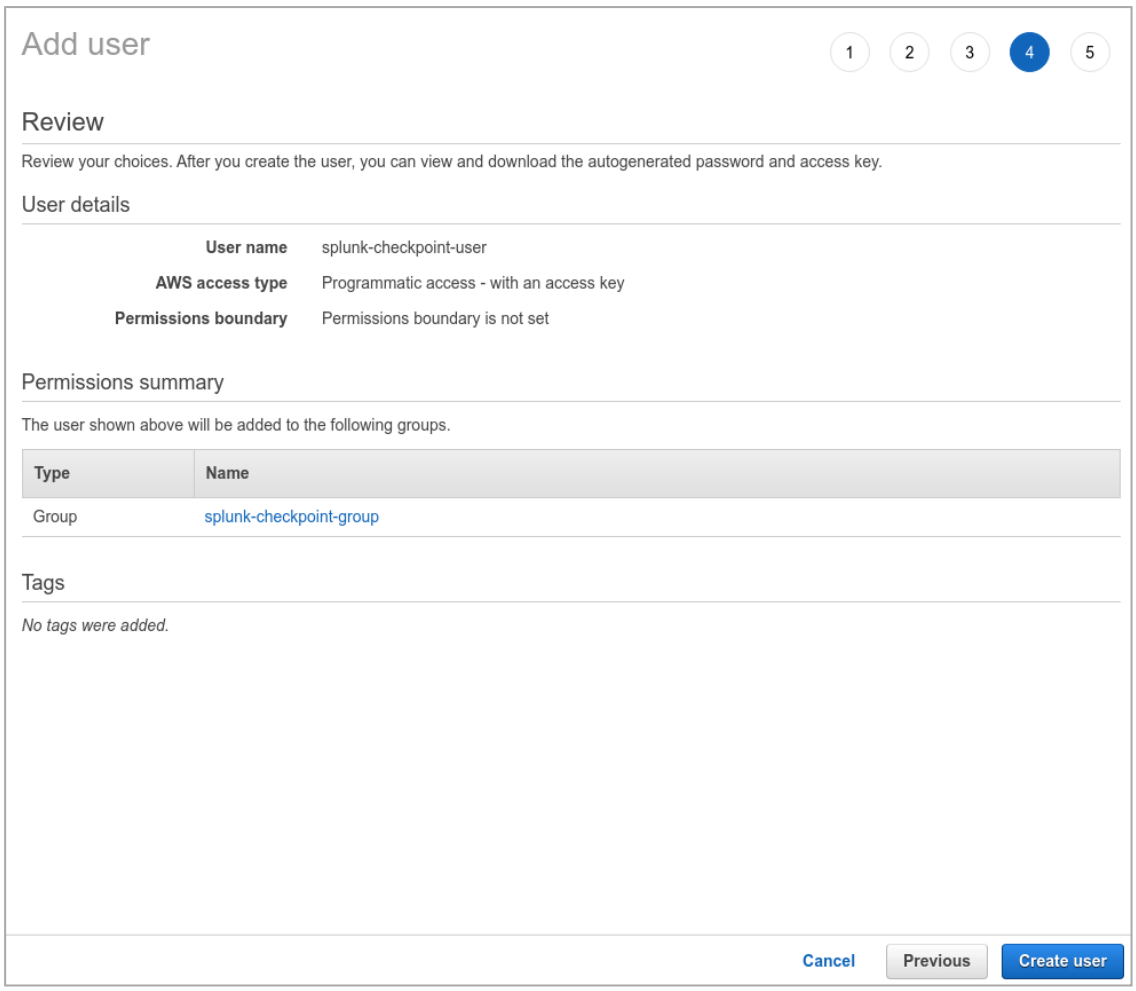


j. Go back to the **Add user** screen and confirm that the group you created is selected and then click **Next: Tags**.



k. Add the necessary Tags (in accordance with your environment directives) and click **Next: Review**.

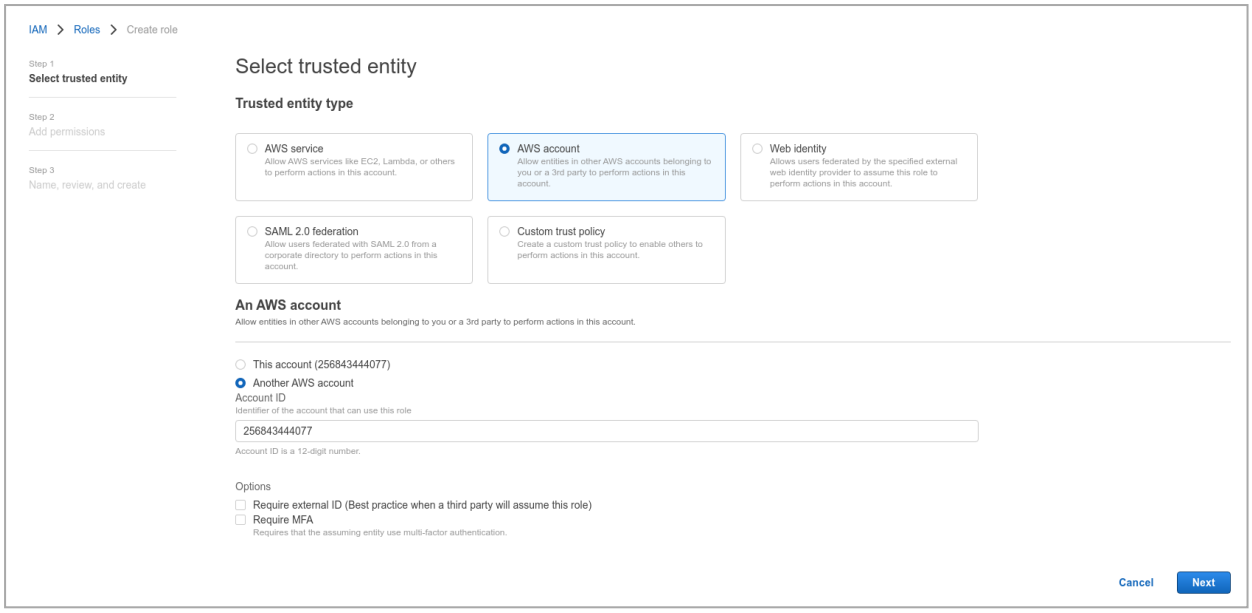
l. Confirm all the configurations and click **Create user**.



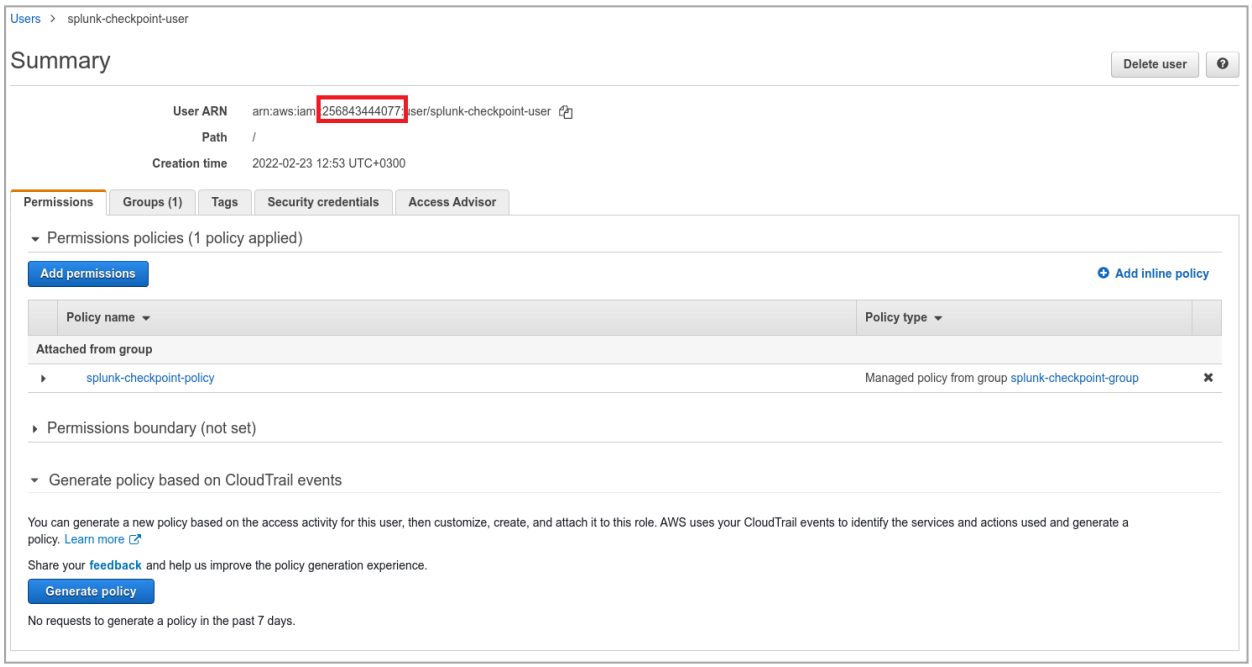
Note - Download the CSV file or copy the Access Key and Secret access key to a safe location. This information won't be available again.

m. Click **Close**.

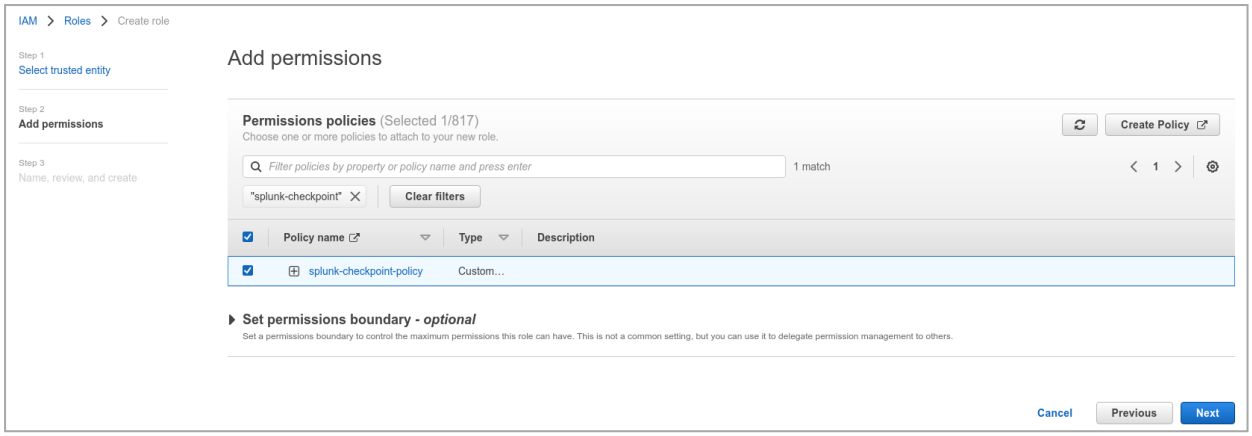
3. Click **Roles > Create role**.
4. Select **Another AWS Account**.
5. Insert the 12 digit number of the user created in step 2 and click **Next: Permissions**.



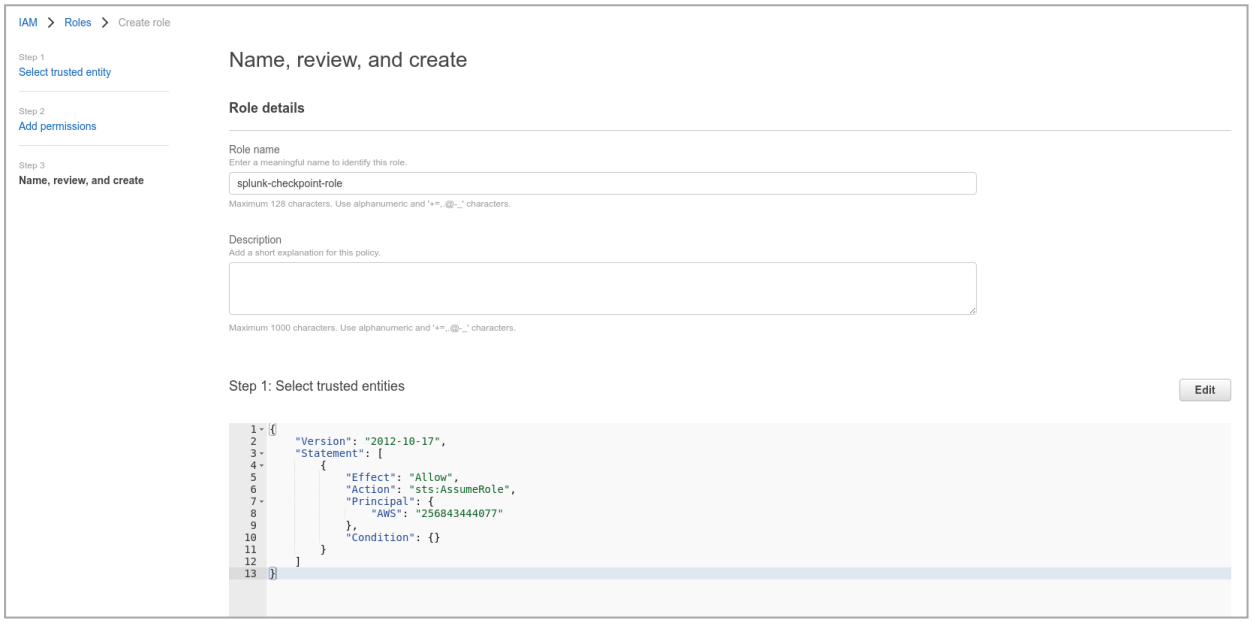
Note - To find the 12 digit number, open the user on another screen.



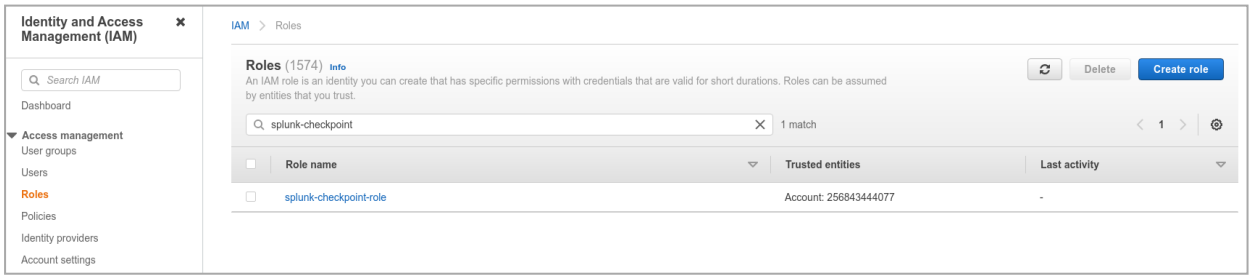
6. Select the policy created and click **Next: Tags**.



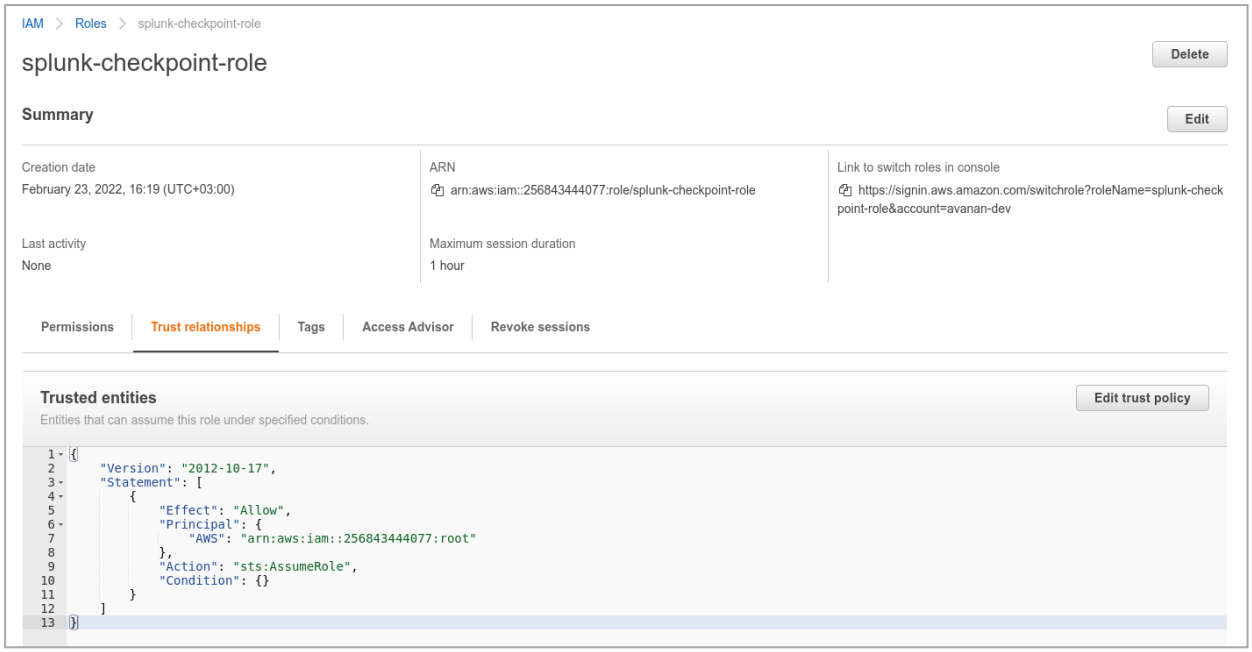
7. Add the necessary Tags (in accordance with your environment directives), select a role name and click **Create Role**.



8. Search for the role you created and click on its name.



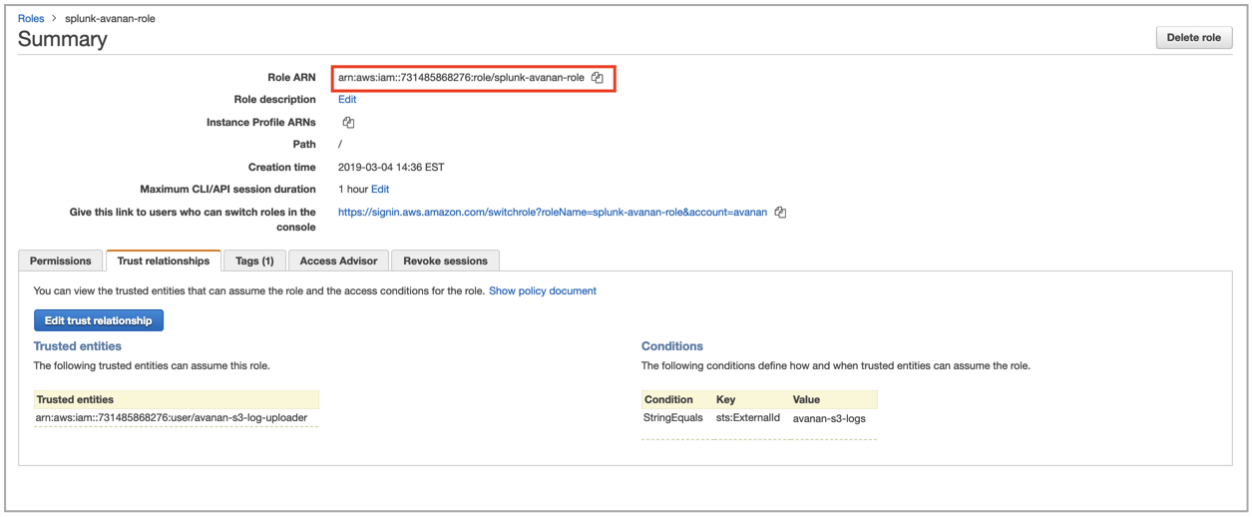
9. Select **Trust relationships** and click **Edit trust relationship**.



10. Copy the following JSON code and click **Update Trust Policy**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::731485868276:user/checkpoint-s3-log-
uploader"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "checkpoint-s3-logs"
        }
      }
    }
  ]
}
```

11. Copy the **Role ARN**.



Note - This **Role ARN** is used while configuring SIEM Integration in the Avanan.

12. Log in to Avanan and complete SIEM integration. For more details, see *"Configuring SIEM Integration" on page 392*.

    Note - After this integration, Avanan starts sending the logs to the AWS S3 bucket. You have to configure your SIEM platform to receive logs from the AWS S3 bucket.

Configuring AWS S3 to Send Avanan Logs to Splunk

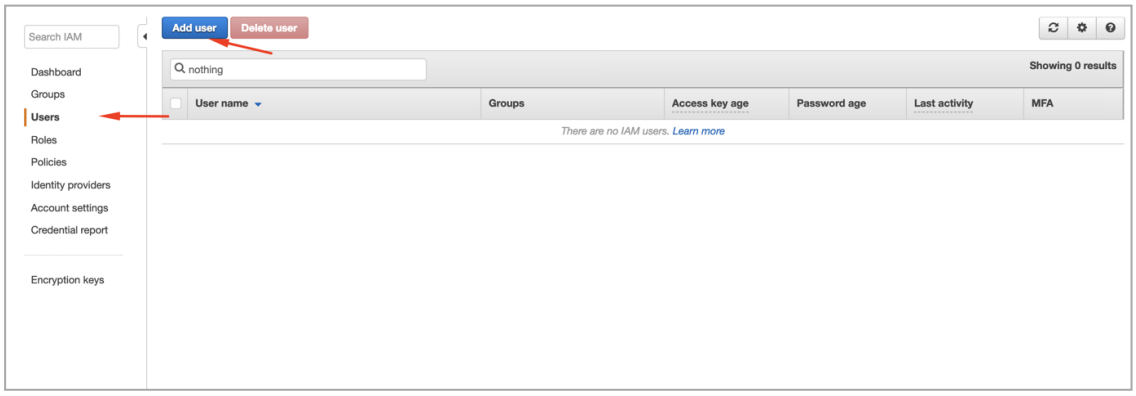
1. Go to AWS IAM: https://console.aws.amazon.com/iam/home#/home.

   Note - To limit Avanan's access to your AWS S3 bucket, you have to create a new user, group, policy, and role to use.

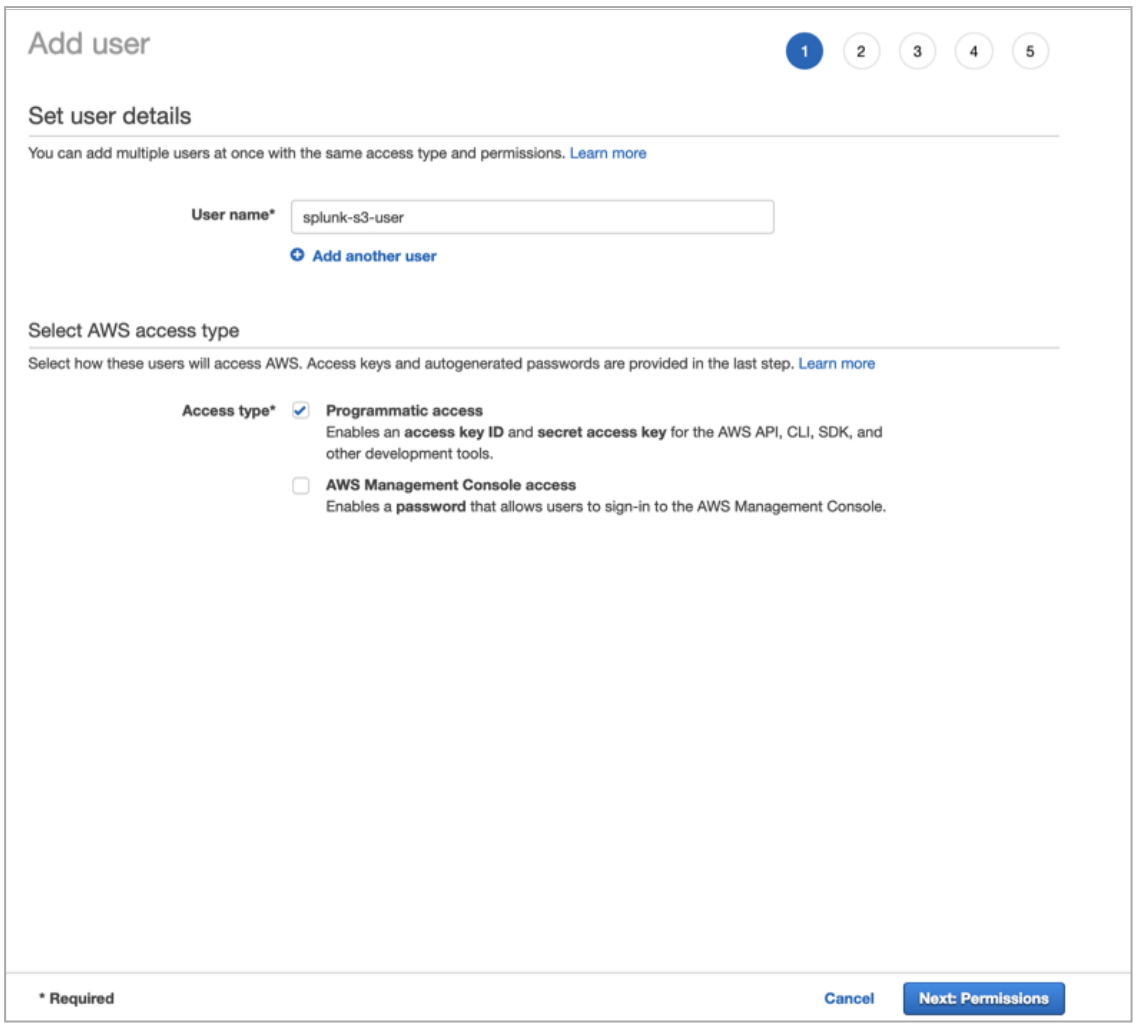
2. **Create a new user.**

   To create a new user:

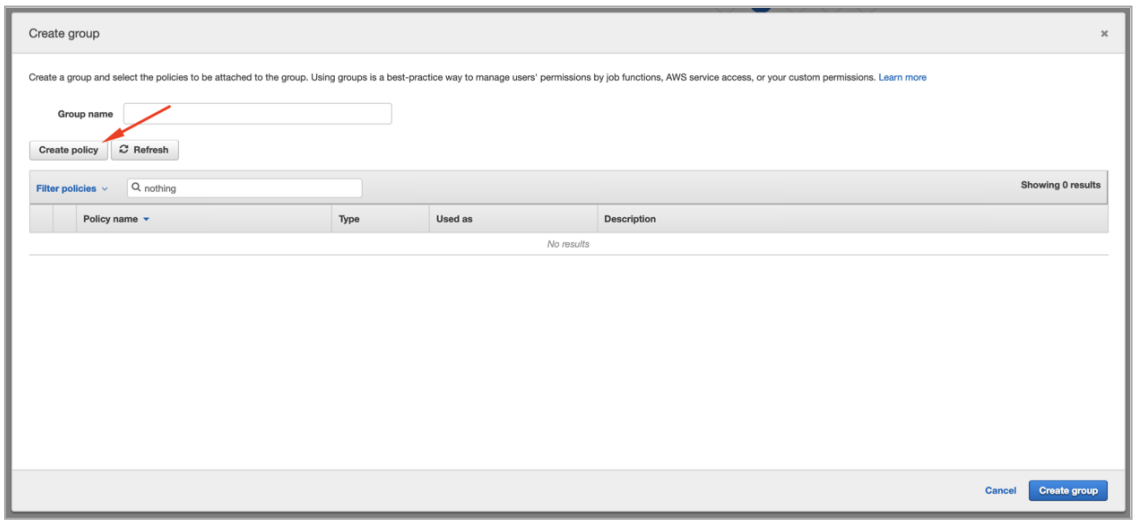
   a. Click **Users > Add User**.



b. Select a name, enable **Programmatic access**, and click **Next: Permissions**.



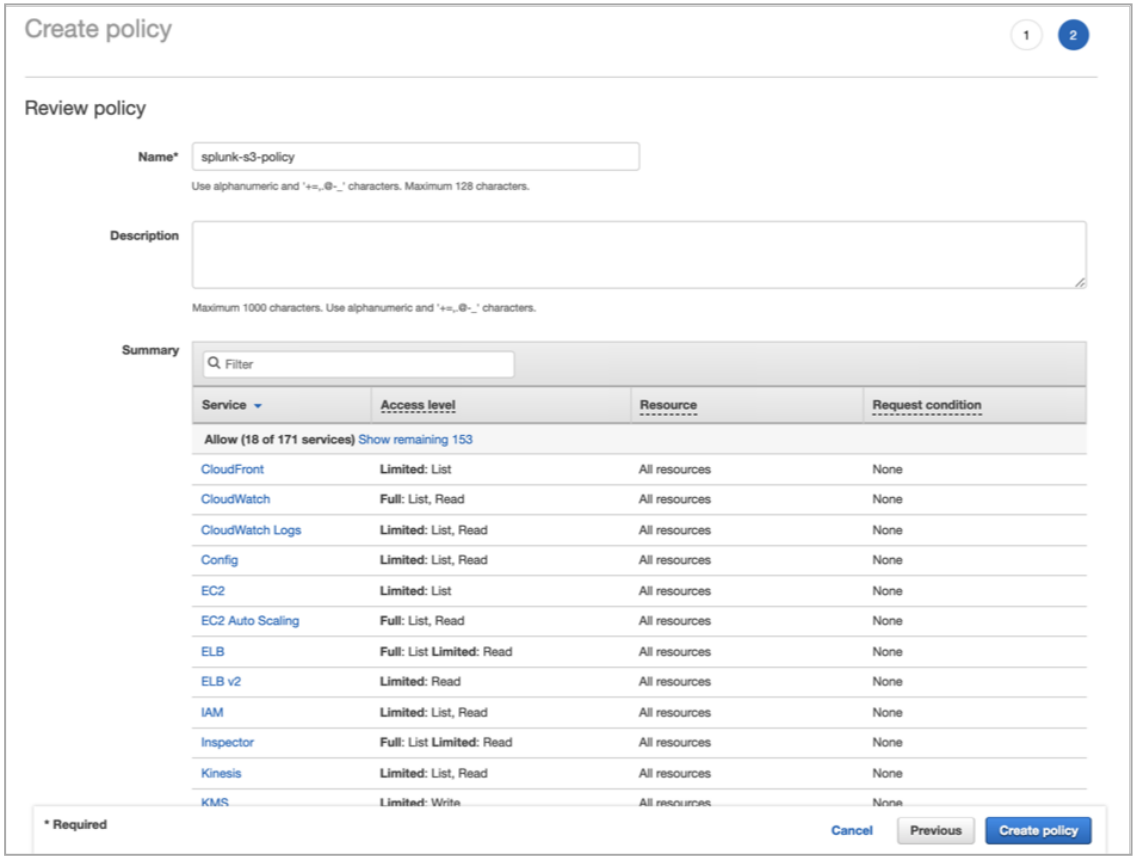
c. Click **Create group** or select the group if already created.



d. On the new tab, click **JSON** and copy this over.

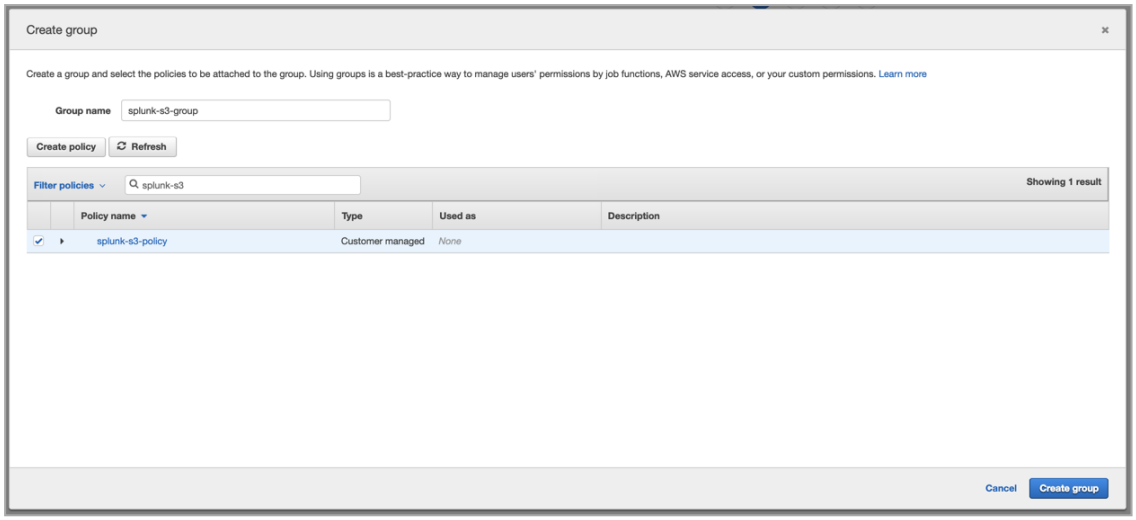
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

e. Click **Review Policy**, select the policy name and click **Create Policy**.

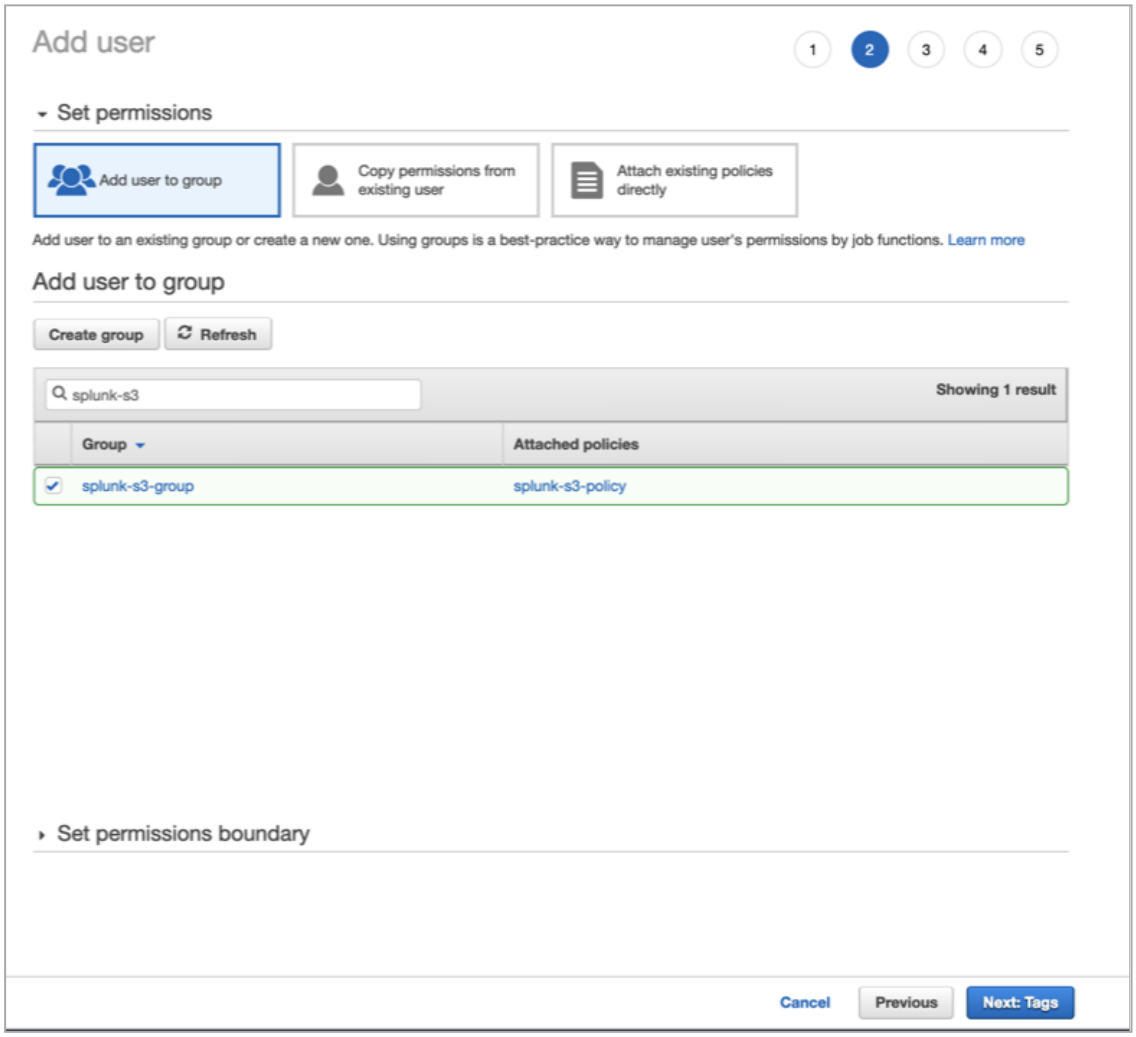


f. Go back to the previous tab and click **Refresh**.

g. Select the policy created, give a group name and click **Create group**.

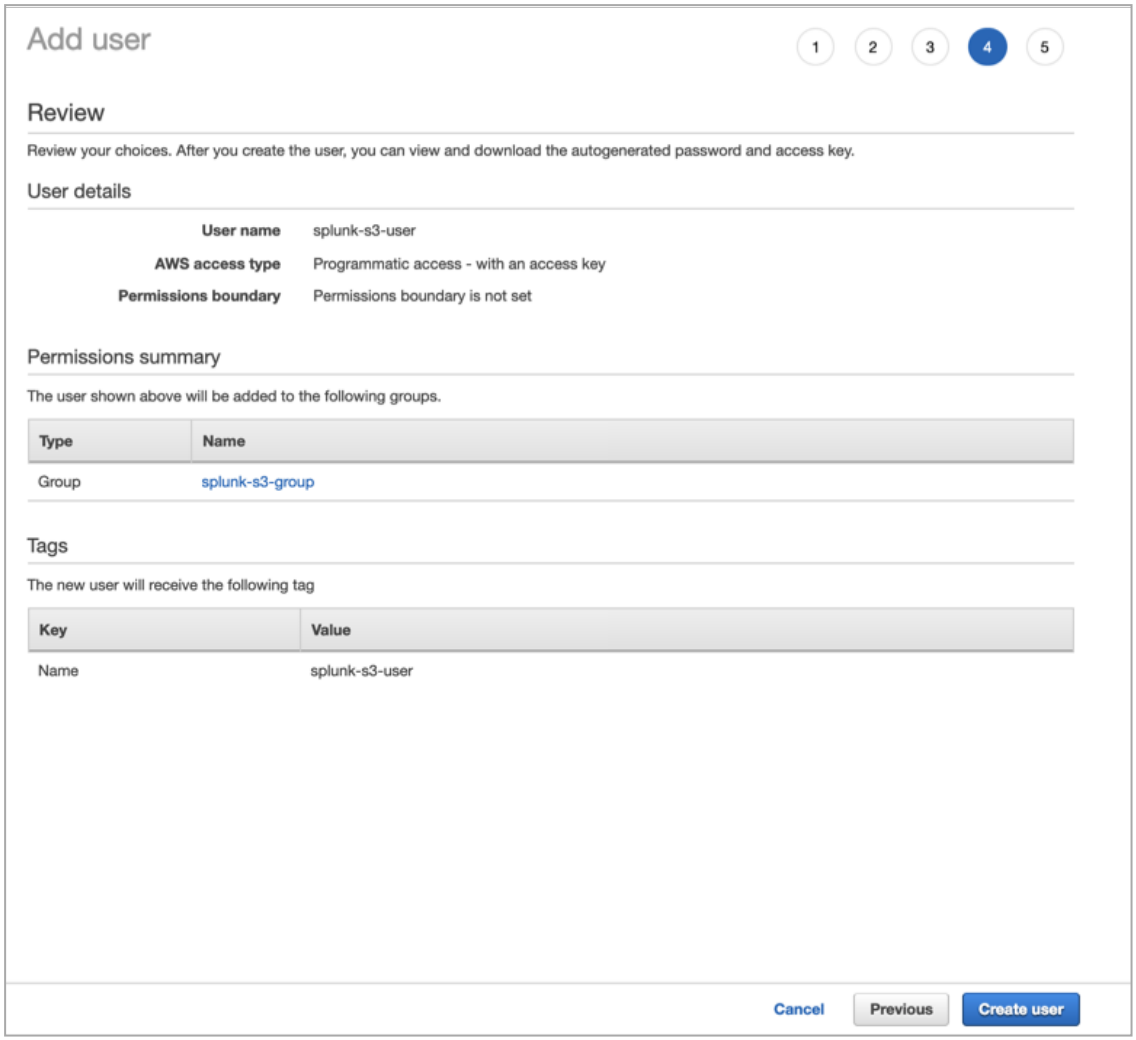


h. Go back to the **Add user** screen, confirm that the group you just created is selected and click **Next: Tags**.



i. Add the necessary Tags (in accordance with your environment directives) and click **Next: Review**.

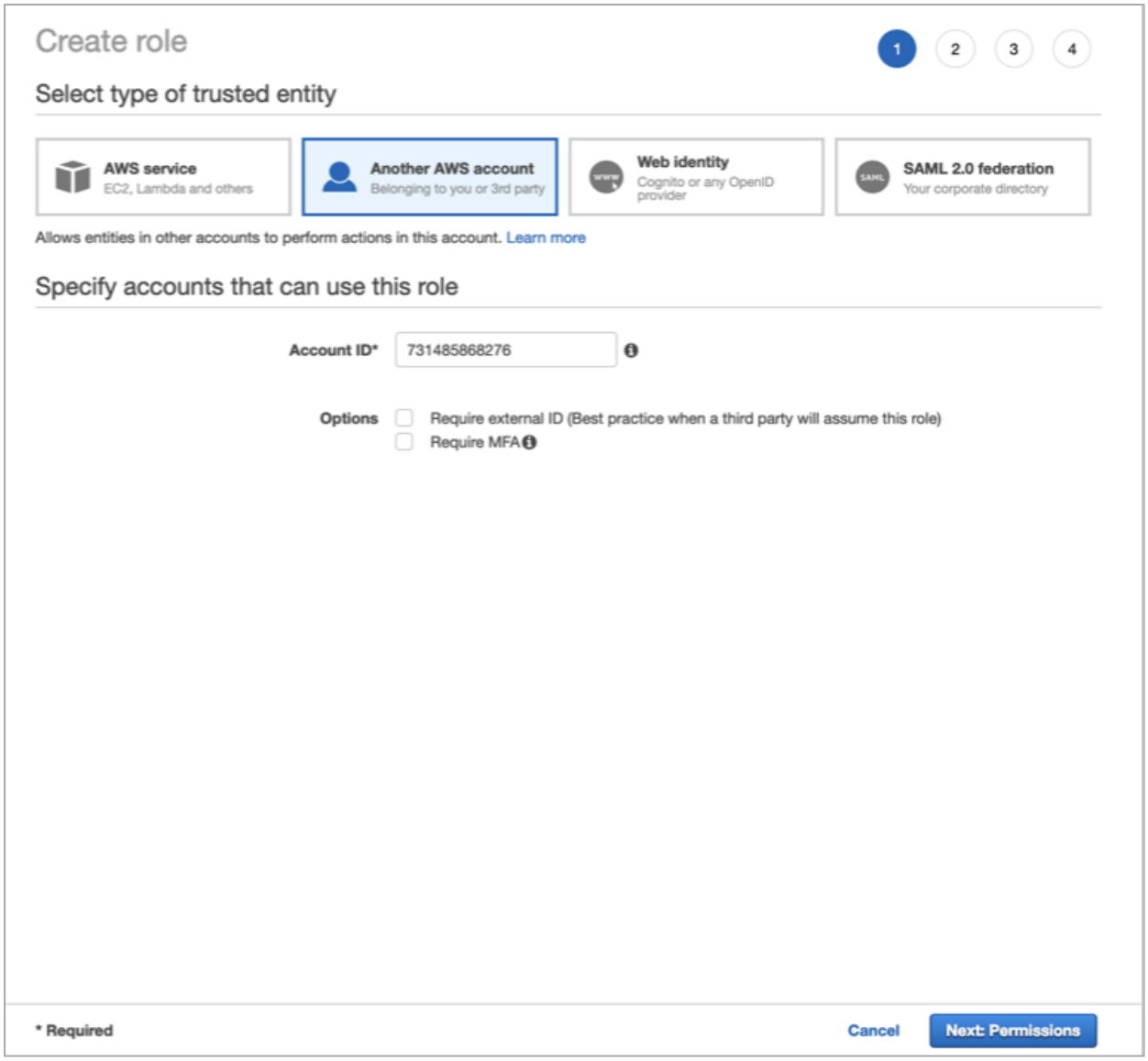
j. Confirm all the configurations and click **Create user**.



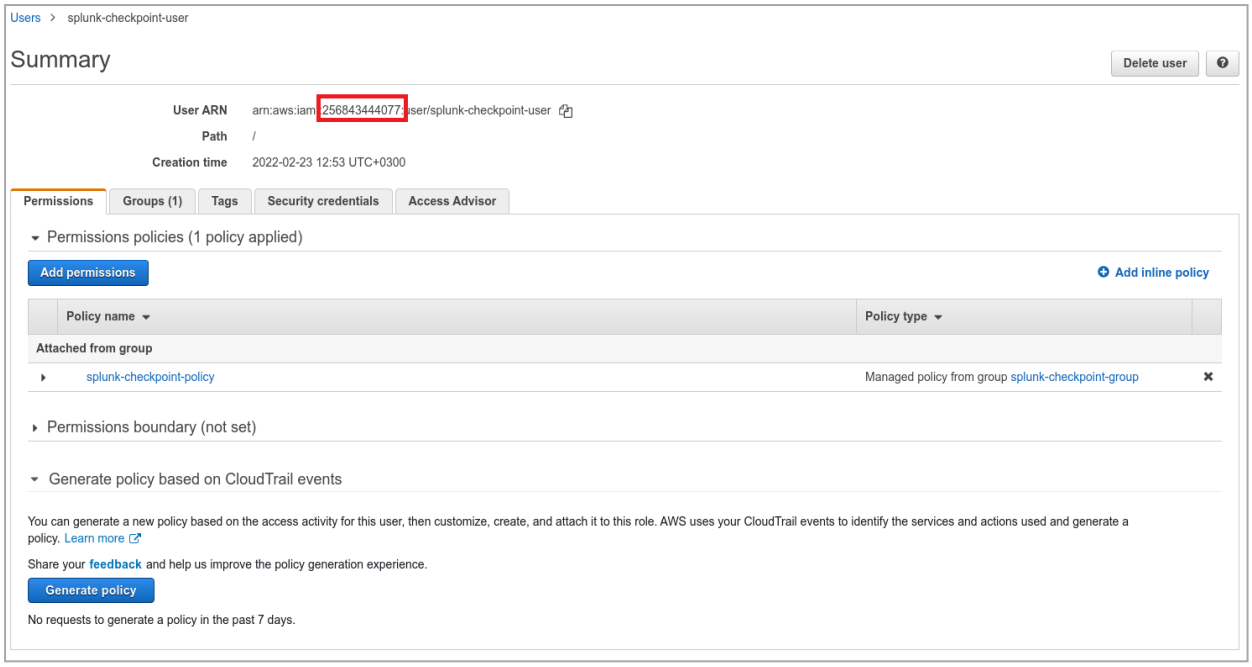
Note - Download the CSV file or copy the Access Key and Secret access key to a safe location. This information won't be available again.

k. Click **Close**.

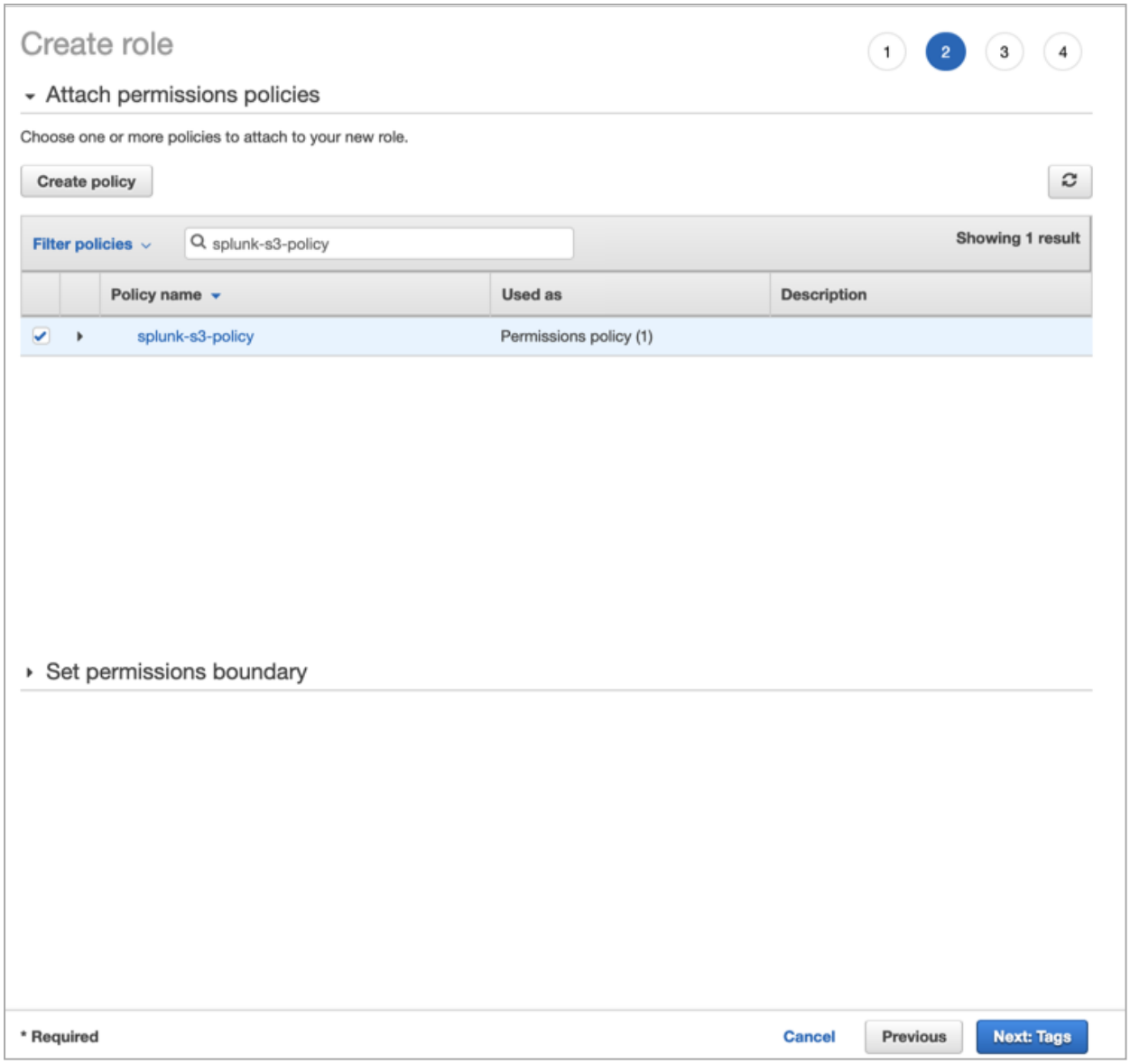
3. Click **Roles > Create Role**.
4. Select **Another AWS Account**.
5. Insert the 12 digit number of your account and click **Next: Permissions**.



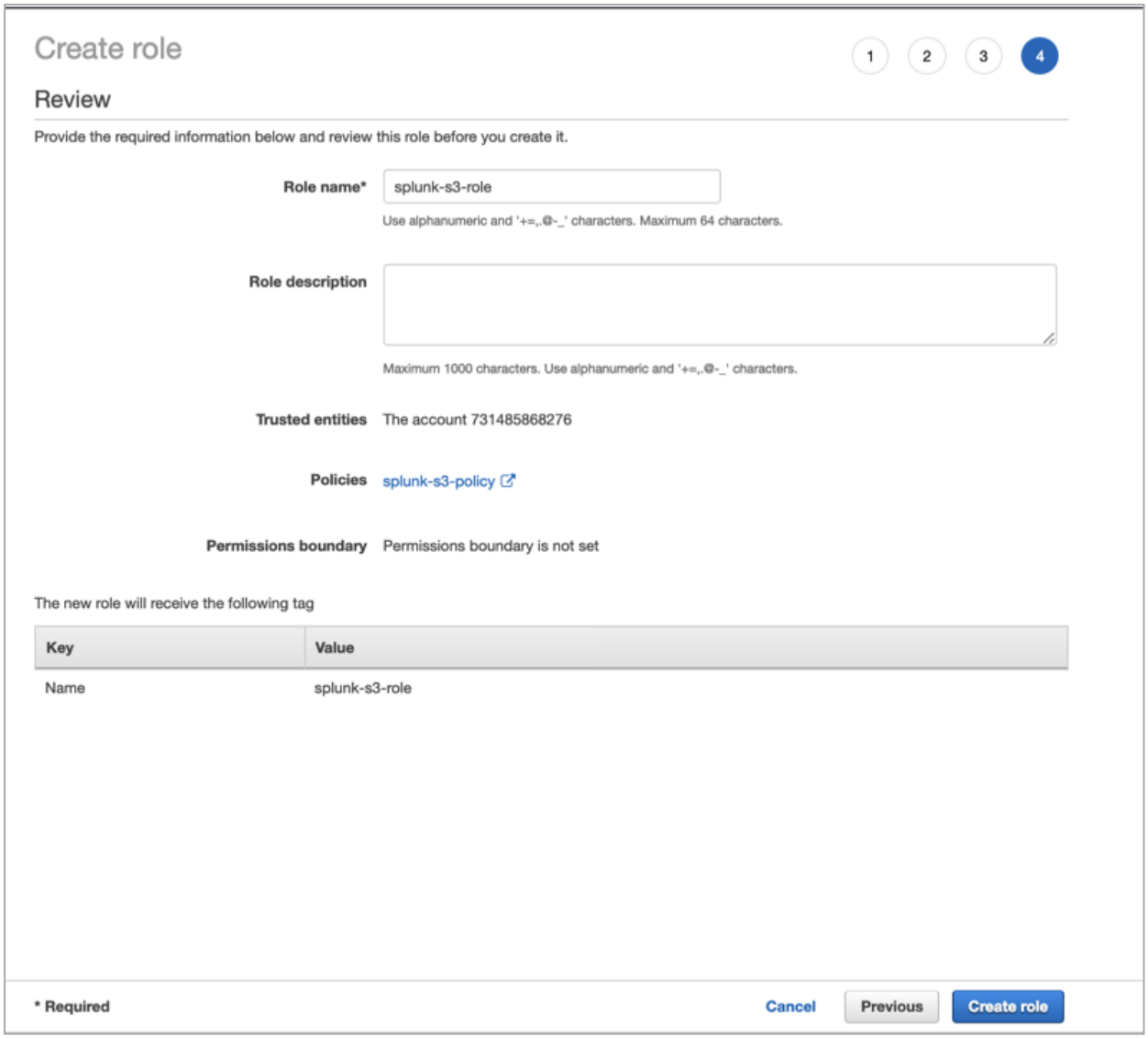
Note - To find the 12 digit number, open the user on another screen.



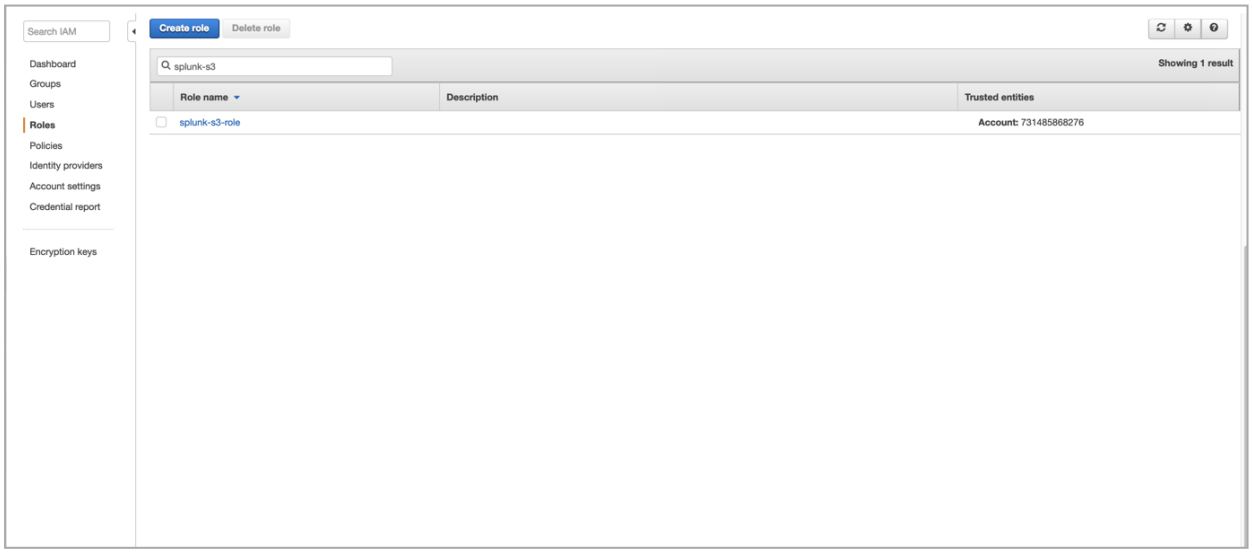
6. Select the policy created, and click **Next: Tags**.



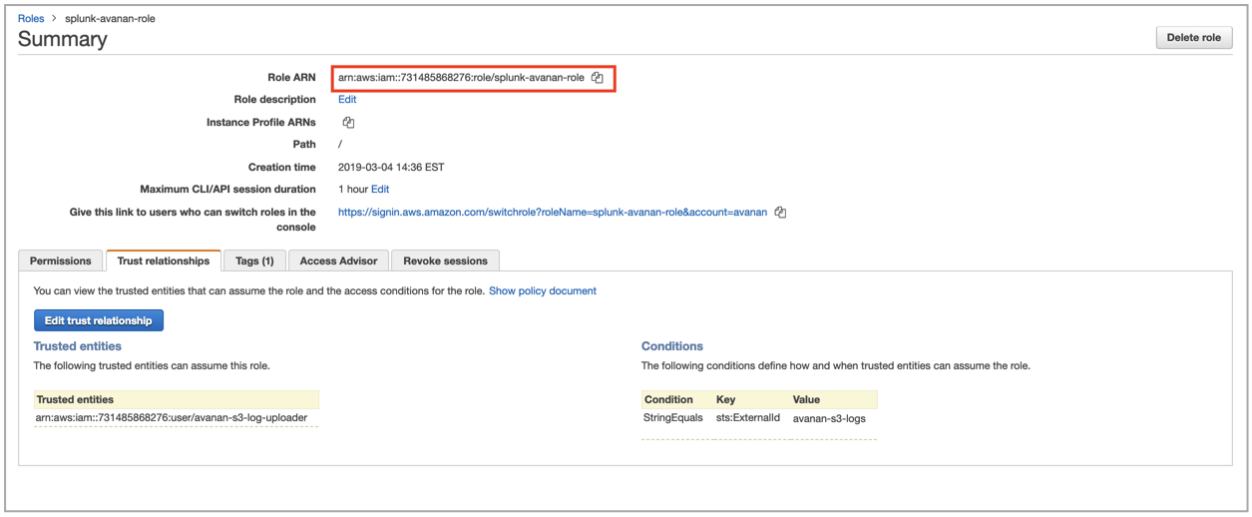
7. Add the necessary Tags (in accordance with your environment directives) and click on **Next: Review**.
8. Select a role name and click **Create Role**.



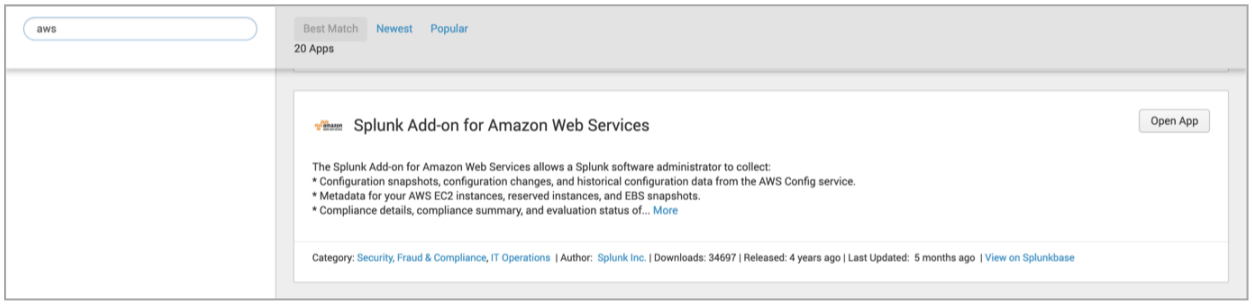
9. Search for the role you created and click on its name.



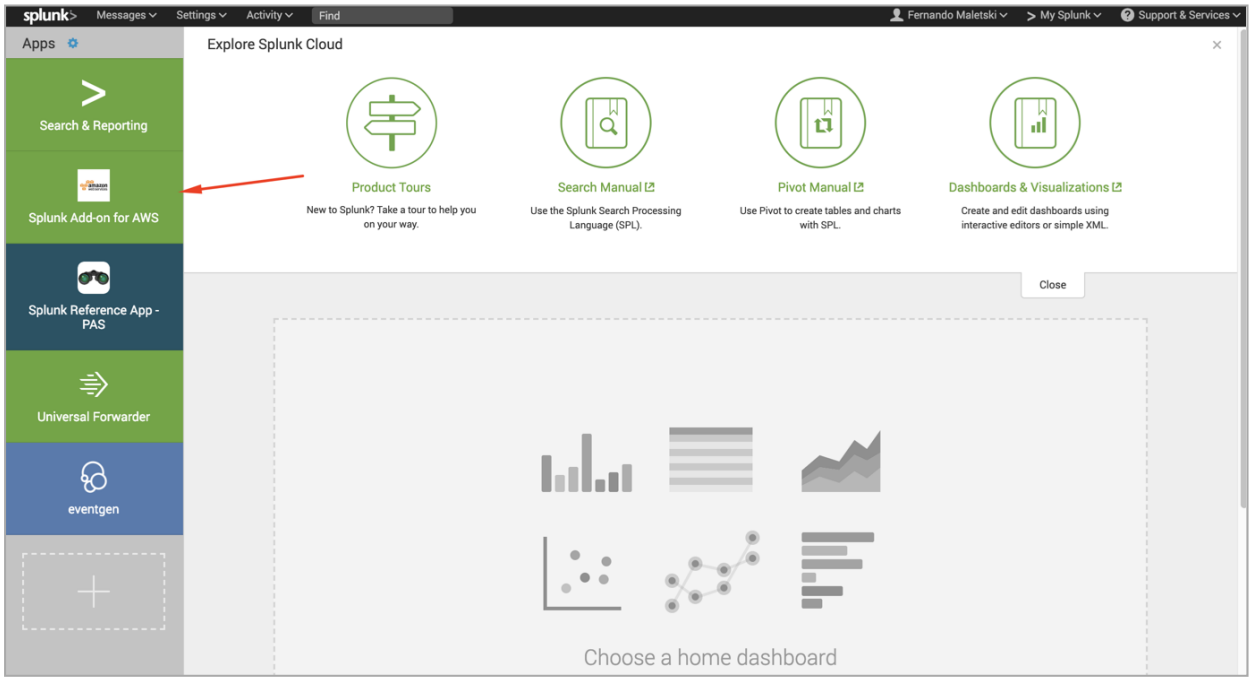
10. Copy the **Role ARN**.



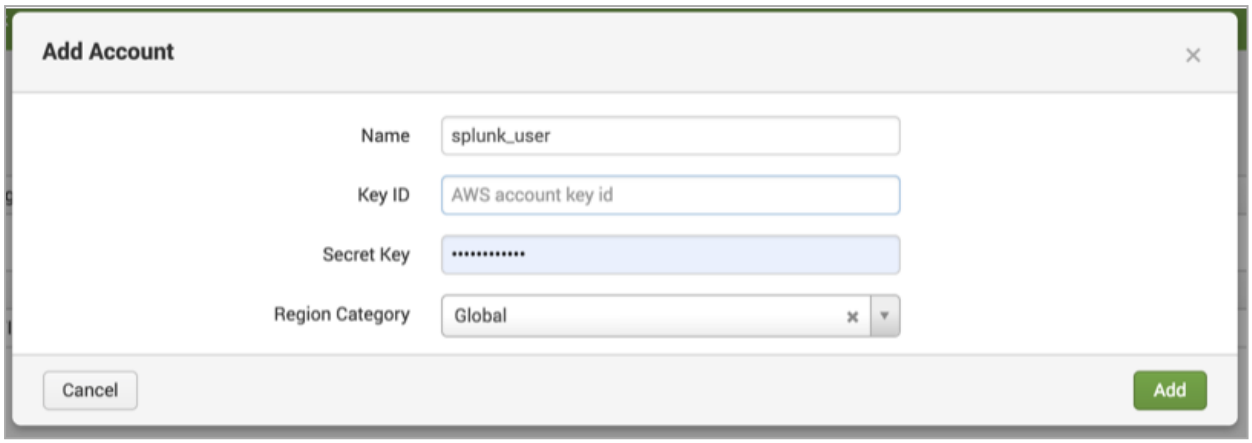
11. Open Splunk and install the **Splunk Add-on for Amazon Web Services**, if not already installed.



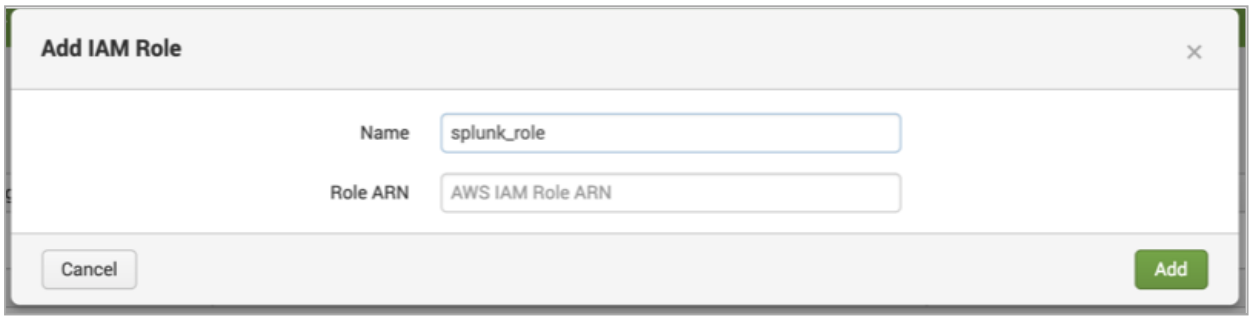
12. Open **Splunk Add-on for AWS**.



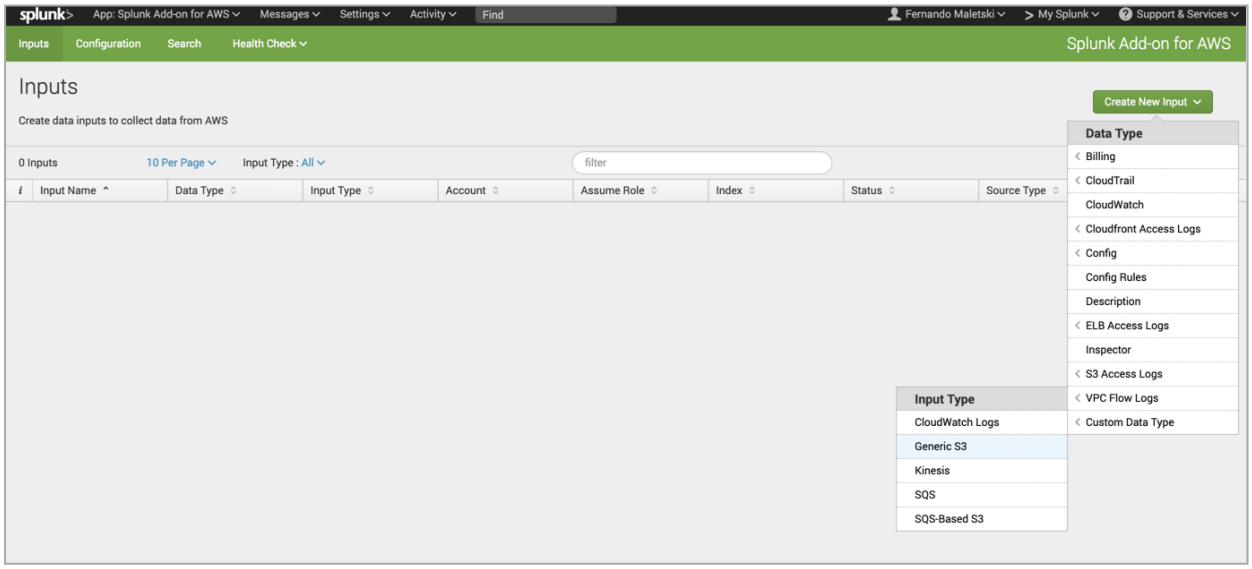
13. Click **Configuration > Account > Add** and enter the Key ID and Secret Key generated when the user was created and click **Add**.



14. Click **IAM Role > Add** and enter the **Role ARN**.



15. Click **Inputs > Create New Input > Custom Data Type > Generic S3**.

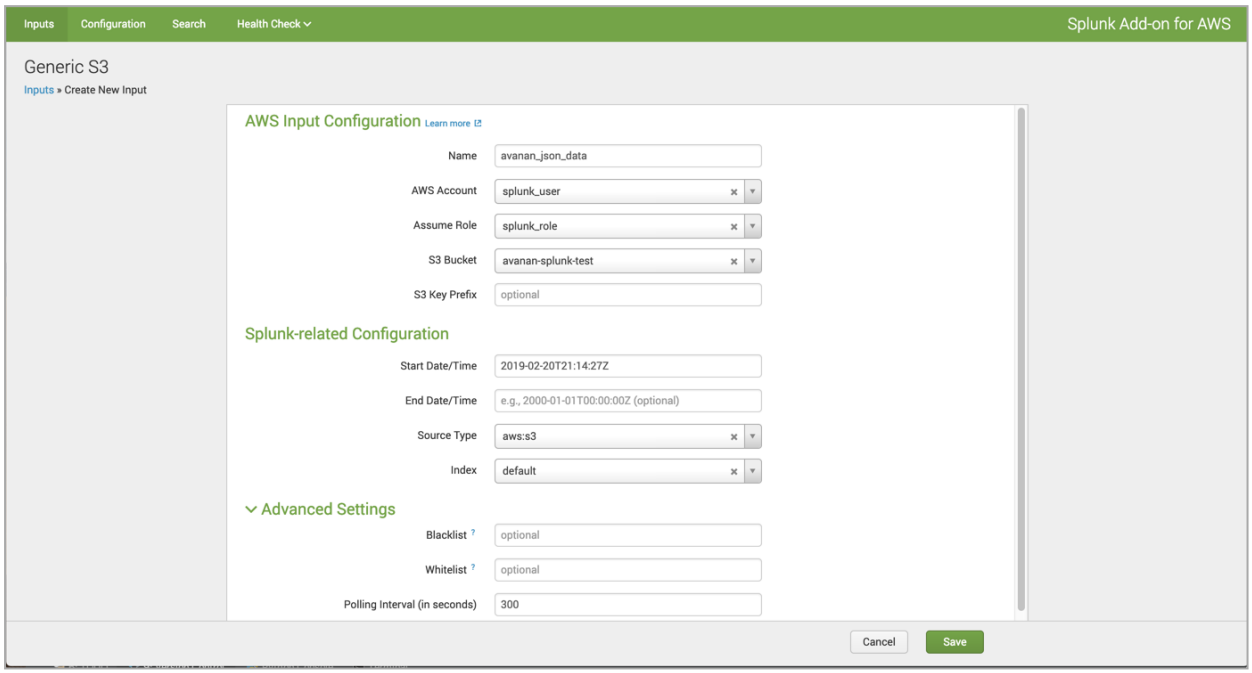


16. Select a name for the Input, the AWS Account and the Assume Role you configured above, the S3 Bucket Avanan is uploading the logs, a start datetime (ideally, a few minutes before you enabled Splunk on Avanan).

17. Under **Advanced Settings**, set the Polling Interval to 900 s (15 minutes) as Avanan uploads the logs every 15 minutes.

    Note - By default, Avanan uploads the logs even before the polling interval when they reach 5 MB.

18. Click **Save**.



Now, Splunk reads the logs from the S3 bucket while Avanan uploads them to the S3 bucket.

Recommended Configuration for known SIEM Platforms

Avanan can integrate with a large number of SIEM platforms.

Note - If you need help in configuring your SIEM platform to integrate with Avanan, contact *Avanan Support*.

These are the recommended configuration for some of the SIEM platforms.

SIEM Platform	Transport Method	Log Format
Splunk	Splunk HTTP Event Collector (HEC) ■ HTTP Event Collector Host / URI - Host or URI value from Splunk HEC configuration ■ HTTP Event Collector Token - value from Splunk HEC configuration	JSON (Splunk HEC/CIM compatible)

SIEM Platform	Transport Method	Log Format
Rapid7	AWS SQS ■ AWS SQS Queue URL - Contact *Avanan Support* to get this value	JSON (Rapid7, <8k characters)
Sumo Logic	HTTP Collector ■ HTTP Collector URL (HTTP/HTTPS) - value from Sumo Logic For example, *https://myconnector.mycompany.com*	JSON
Azure Log Workspace	Azure Log Workspace ■ Azure Log Workspace ID - value from Azure configuration ■ Azure Log Workspace Shared Key - value from Azure configuration	JSON
LogRhythm	AWS S3 For the fields required for AWS S3, see *"Supported Transport methods" on page 393*. If a new S3 Bucket is needed, you should follow specific instructions while configuring the S3 bucket. For more details, see *"Configuring AWS S3 to Receive Avanan Logs" on page 397*.	JSON
McAfee SIEM	AWS S3 For the fields required for AWS S3, see *"Supported Transport methods" on page 393*. If a new S3 Bucket is needed, you should follow specific instructions while configuring the S3 bucket. For more details, see *"Configuring AWS S3 to Receive Avanan Logs" on page 397*. To receive the logs from S3 bucket to McAfee SIEM, refer to Configuration of Amazon S3 upload feature and McAfee Documentation.	JSON
Other	Avanan can integrate with any SIEM platform. If you need help in configuring your SIEM platform to integrate with Avanan, contact *Avanan Support*.	

Configuring Integration with Cortex XSOAR by Palo Alto Networks

Avanan allows to integrate with Cortex XSOAR to automatically trigger playbooks based on detected security events and other criteria.

For more information about the integration, see Cortex XSOAR documentation.

Managing Quarantine

Avanan quarantines emails, files and messages based on the security policies and the settings of the different engines. In addition, using Attachment Cleaning (Threat Extraction), it modifies the email attachments and keeps their original copy in the solution's quarantine.

According to the policy, end users may be able to submit restore request both for quarantined emails and extracted (cleaned) attachments. Administrators then need to decide whether to approve restore requests or not.

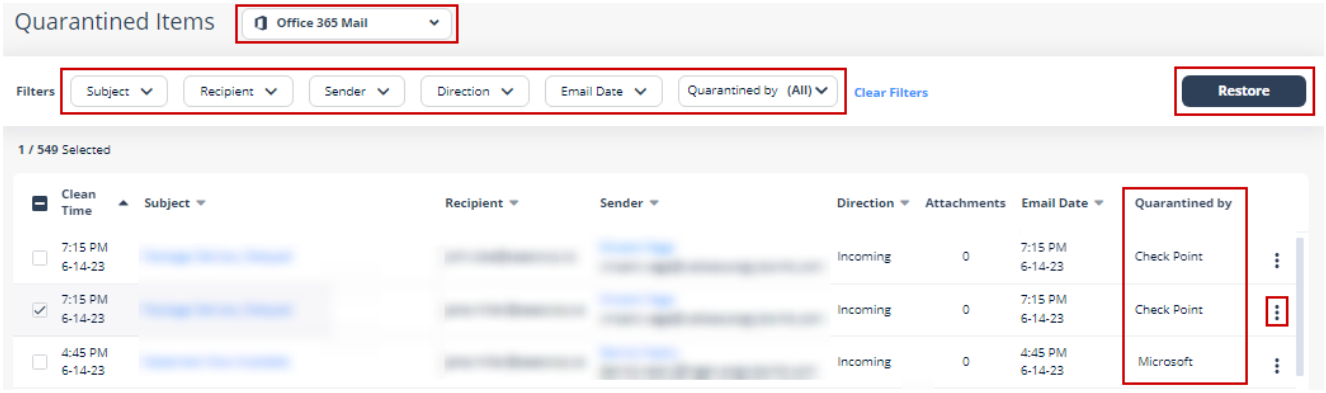
For more information about analyzing quarantined emails and other security events, see *"Events" on page 354*.

All Quarantined Emails (Admin View)

Under **User Interaction > Quarantined Items**, you will find all the quarantined items per protected application.

You can perform these actions from the **Quarantined Items** page.

- Filter the quarantined emails specific to a SaaS application.
- Search through the quarantined emails using **Subject**, **Recipient**, **Sender**, **Direction**, **Email Date**, and **Quarantined by** filters.
- Drill down to relevant quarantined emails for more information.
- Release (restore) emails from quarantine.



Emails with Modified Attachments

You can view these details in the **Emails with Modified Attachments** page.

- Emails with attachments, where the links in the attachments were replaced. See *"Click-Time Protection" on page 120*.
- Emails with attachments that were cleaned. See *"Attachment Cleaning (Threat Extraction)" on page 174*.

Note - The page does not show emails where links in the email body were replaced.

Sending the Unmodified Emails to End Users

To send the original email to the end-user, do one of these.

- From the **Modified Attachments** page.
  1. Go to **User Interaction** > **Modified Attachments**.
  2. To send a original email, click the ⋮ icon for the email from the last column of the request table and select **Send Original**.
  3. To send multiple emails at a time, select the emails and click **Send Original** from the top-right corner of the page.
  4. Click **OK**.
- From the Email profile page.
  1. Open the email profile page.
  2. In the **Email Profile** section, click **Send** for **Send Original Email**.
  3. Click **OK**.

Dedicated Quarantine Mailbox / Folder

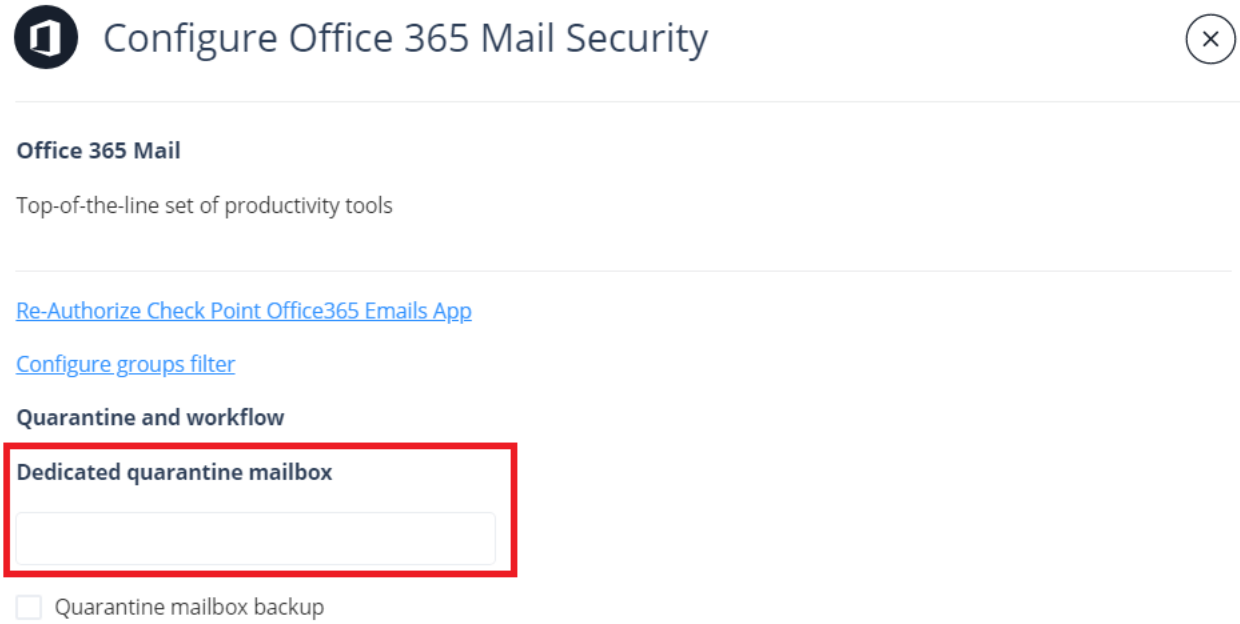
If you would like to store quarantined emails/files locally, you can configure a dedicated quarantine repository for every protected application. This repository is used to store every email / attachment / file that is quarantined automatically according to the policy or manually by administrators.

Specifying such a mailbox/folder is not mandatory, as Avanan stores a copy of quarantined items in an S3 bucket associated with the Avanan portal.

Office 365 Mail

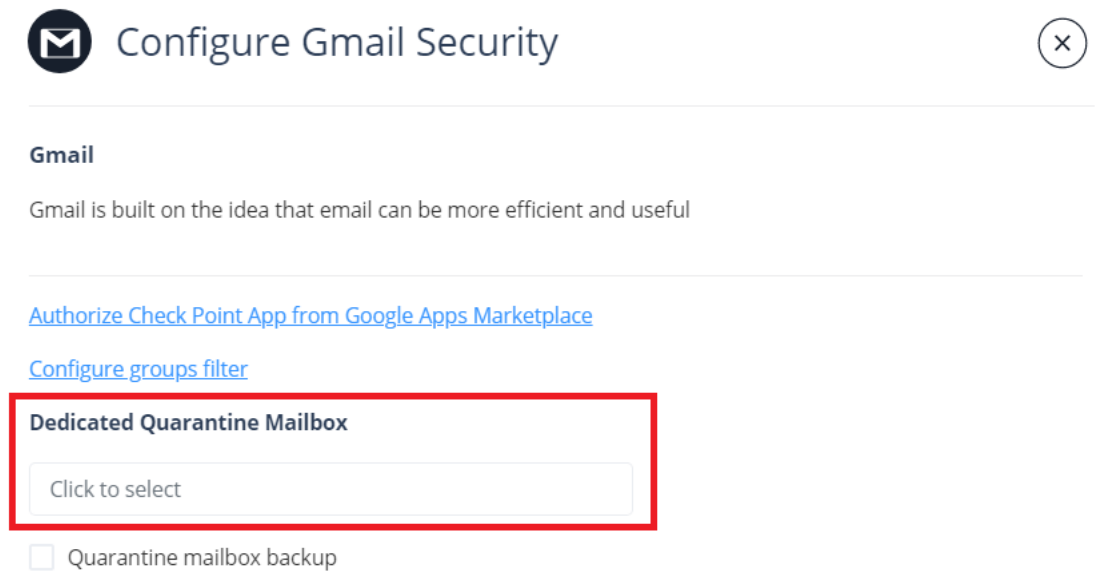
Note - The dedicated quarantine mailbox must be a full licensed mailbox and it cannot be a shared mailbox.

To configure the dedicated Office 365 Mail quarantine mailbox, click **Security Settings > SaaS Applications > Office 365 Mail > Configure**.



Gmail

To configure the dedicated Gmail quarantine mailbox, click **Security Settings > SaaS Applications > Gmail > Configure**.



End-User Daily Quarantine Report (Digest)

Daily Quarantine Report (Digest) allows you to send a email report daily to end-users about quarantined and junk/spam emails. The end-users get detailed report that has information about the emails sent to them and quarantined in the last 24 hours.

Global and targeted attacks can generate multiple phishing emails per day, and each one results in a quarantine notification email from Avanan based on the policy defined by the administrator. When the administrator activates the **Daily Quarantine Report (Digest)**, the user receives a single, aggregated email report per day for the quarantined emails.

The report includes:

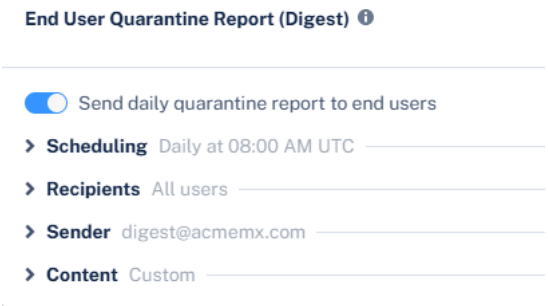
- **Quarantined emails** - Emails quarantined by Avanan and Microsoft based on the policy workflows. Each quarantined email has an associated user action:
  - **Request to release** – Sends a notification to the admin to release the email. After the administrator approves, the email gets delivered to the inbox. For more details, see *"Managing Restore Requests" on page 433*.
  - **Release** – Delivers the email to the inbox immediately.
- **Junk emails** (Optional) - Emails that were identified as junk/spam by the Anti-Phishing engine, Office 365 (Spam Confidence Level (SCL) >= 5) or Google. By default, these emails are sent to the Junk folder. Users can find any misclassified emails and move them to their inboxes, if required.
- **Link to generate quarantine report on demand** (Optional) - Adds a link at the bottom of the **Daily Quarantine Report (Digest)** email. The end users can click this link to generate a new quarantine report for the last 24 hours.

Notes:

- The report does not include quarantined emails that do not allow user action.
- If there are no events that happened in the last 24 hours, the user will not receive the **Daily Quarantine Report (Digest)** email.

Configuring Daily Quarantine Report (Digest)

1. Click **Security Settings** > **User Interaction** > **Quarantine**.
2. In the **End User Quarantine Report (Digest)** section, select **Send daily quarantine report to end users** toggle button.



3. In the **Scheduling**, select the time and time zone to send the report.

- In the **Daily at** section, select a specific time of the day to send the report.
  - To send the report multiple times a day, click **+ Add More** and select the required time.
  - If required, you can configure the report to be sent every hour, up to 24 times per day.
- In the **Time zone** section, select the required time zone.

4. In the **Recipients** section, select the users to send the daily quarantine report.
   - To send the report to all Office 365 and Google users in your organization, select **All Office 365 and Google Users**.
   - To send the report to all Google users in your organization and specific Office 365 users or groups, select **All Google users and specific Office 365 Users or Groups**.
     a. In the **Specific Users and Groups** section, select the required users or groups.
     b. Click **Add to Selected**.
   - For Office 365 users, to stop sending alerts for individual quarantined emails, select **Office 365 Users – Stop alerts on individual quarantined emails (recommended)** checkbox.
   - For Google users, to stop sending alerts for individual quarantined emails, select **Google Users - Stop alerts on individual quarantined emails (recommended)** checkbox.

     Note - Users who receive the daily quarantine report will no longer get notifications about individual phishing attacks, even if the policy is configured to send them.

5. In the **Sender** section, configure the required sender email address for the daily quarantine digest.
   - **Friendly-From name**
     - If no friendly-from name is required, select **None**.

       Note - Some email clients duplicate the sending address to the **Friendly-from name**.
     - To use a customized name, select **Custom** and enter the sender name.

- **From address**
  - To use the default email address, select **Default**. The default email address is *no-reply@checkpoint.com*.
  - To use a custom email address, select **Custom** and enter the email address.

    Notes:
    - If you use the default sender or any email address under your domain, you must add the Avanan statement to the custom domain's DNS to prevent SPF and DMARC failures.
      `include:spfa.cpmails.com`
    - The custom domain must be one of the protected domains in your Infinity Portal tenant.
- **Reply-to address**
  - To use **From address** as the Reply-to address, select **Same as From address**.
  - To use a custom email address, select **Custom** and enter the email address.

6. In the **Content** section, configure the content for daily quarantine report to end users:
   - To include spam emails sent to the Junk folder in the report, select the **Include spam emails that are sent to the Junk folder** checkbox.
   - To allow end users to generate a new quarantine report for the last 24 hours, select the **Allow end users to generate a quarantine report on demand** checkbox.

     This option adds a link at the bottom of the **End User Quarantine Report (Digest)** email, enabling end users to generate a new quarantine report for the last 24 hours.
7. In the **Email subject and body** section, configure the subject and the body of the daily quarantine digest email.
   - In the **Subject** field, enter the email subject for the daily quarantine digest email notification.

- In the **Body** field, enter the required information in the email notification.

  To add links to the email footer:

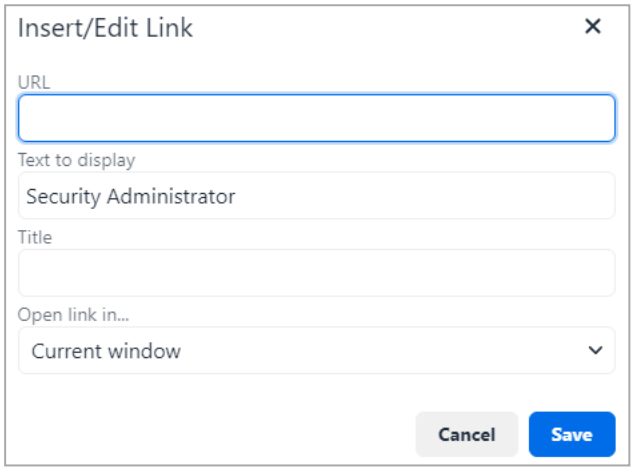
  a. Place the cursor where you want to add the link.

  b. Click the icon.

  or

  Right-click and select Link.

  c. In the **URL** field, enter the URL.



  d. In the **Text to display** field, enter the text that should appear for the link.

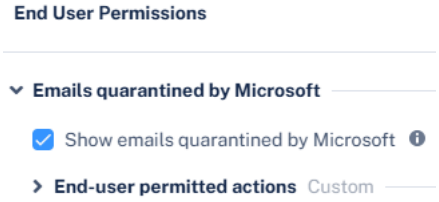
  e. If required, enter a **Title** for the link.

  f. In the **Open link in** list, select **Current window** or **New window**.

  g. Click **Save**.

8. To select the actions end users can perform on Microsoft quarantined items in the daily quarantine report:

   a. Go to **End User Permissions**.



   b. In the **Emails quarantined by Microsoft** section, select **Show emails quarantined by Microsoft** checkbox.

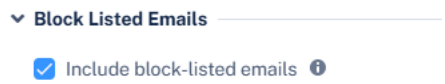
c. In the **End-user permitted actions** section, you can specify the actions end users can perform on emails quarantined by Microsoft for the following threats:

- Malware
- High Confidence Phishing
- Phishing
- High Confidence Spam
- Spam
- Bulk
- Data Loss Prevention
- Transport Rule

d. Select the supported actions for each type of threat:

- Can restore on their own
- Cannot restore
- Can request a restore (admin needs to approve)

e. To include blocklisted emails in the daily quarantine report, select the **Include block-listed emails** checkbox in the **Block Listed Emails** section.



Note - Emails quarantined due to a blocklist appear in the daily quarantine report and the End User Portal, where end users can take action on them like non-blocklisted emails.

9. Click **Save and Apply**.

To manage end user authentication on web browser, see *"Authentication for Email Notifications" on page 448*.

End-User Portal (Email Security Portal)

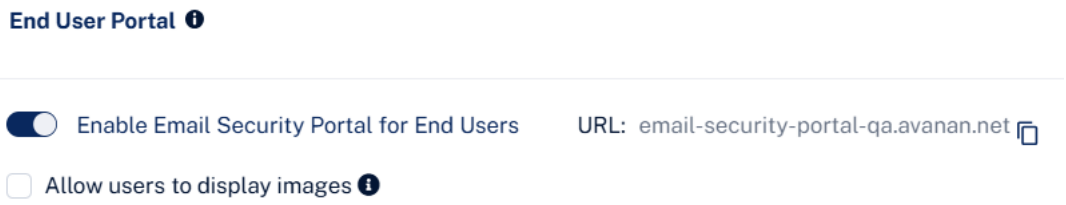
Avanan offers an **Email Security Portal** for end users to access all quarantined emails. In this portal, end users can preview the quarantined emails, restore them, or submit a restore request for them - all in accordance with the defined organization's policies.

Notes:

- The **Email Security Portal** only shows the quarantined emails that users can act on - either restore directly or request to restore.
- The email's availability in the **Email Security Portal** depends on its metadata retention period.
- The availability of action buttons (Restore / Request Restore) and email body depends on the raw email's retention period. For more information, see *"Appendix E: Data Retention Policy" on page 622*.
- For Microsoft quarantined emails:
  - Taking action might fail if the email is no longer retained in Microsoft's quarantine.
  - Once restored, the email body will not be visible.

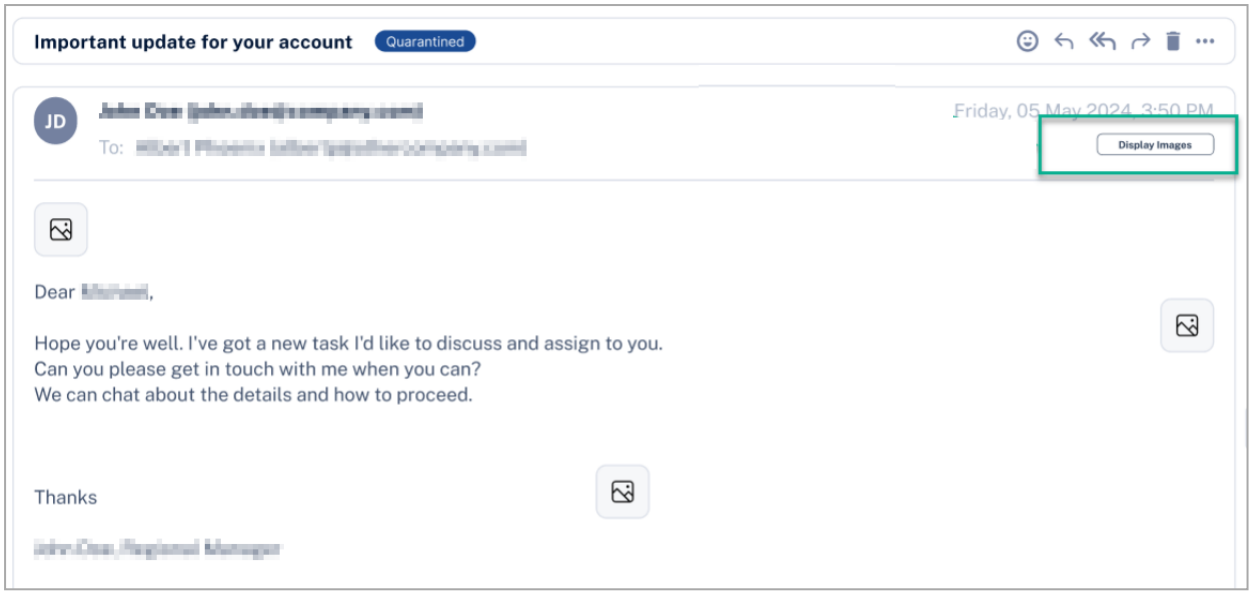
To enable the Email Security Portal for End Users:

1. Go to **Security Settings** > **User Interaction** > **Quarantine**.
2. In the **End User Portal** section, select the **Enable Email Security Portal for End Users** toggle button.



3. To allow end users to view images in the quarantined emails in the End User Portal, select the **Allow users to display images** checkbox.

   End users can now see the **Display Images** button when they preview quarantined emails in the End User Portal.



4. Click **Save and Apply**.

After enabling the **Email Security Portal**, all the end users can access it from this link: https://email-security-portal.avanan.net.

To limit access to specific users, see Limiting End User Portal Access to Specific Users.

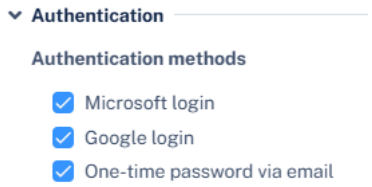
Authentication Methods for Accessing the Email Security Portal

Administrators can enable end users to log in to the Email Security Portal using these authentication methods:

- **Microsoft login**
- **Google login**
- **One-time password login**

To enable or disable an authentication method, do these:

1. Access the Avanan Administrator Portal and click **Security Settings**.
2. Go to **User Interactions** > **Quarantine** > **End User Portal**.
3. In the **Authentication** section, select or deselect the required authentication methods:
    - **Microsoft login**
    - **Google login**
    - **One-time password via email**



4. Click **Save and Apply**.

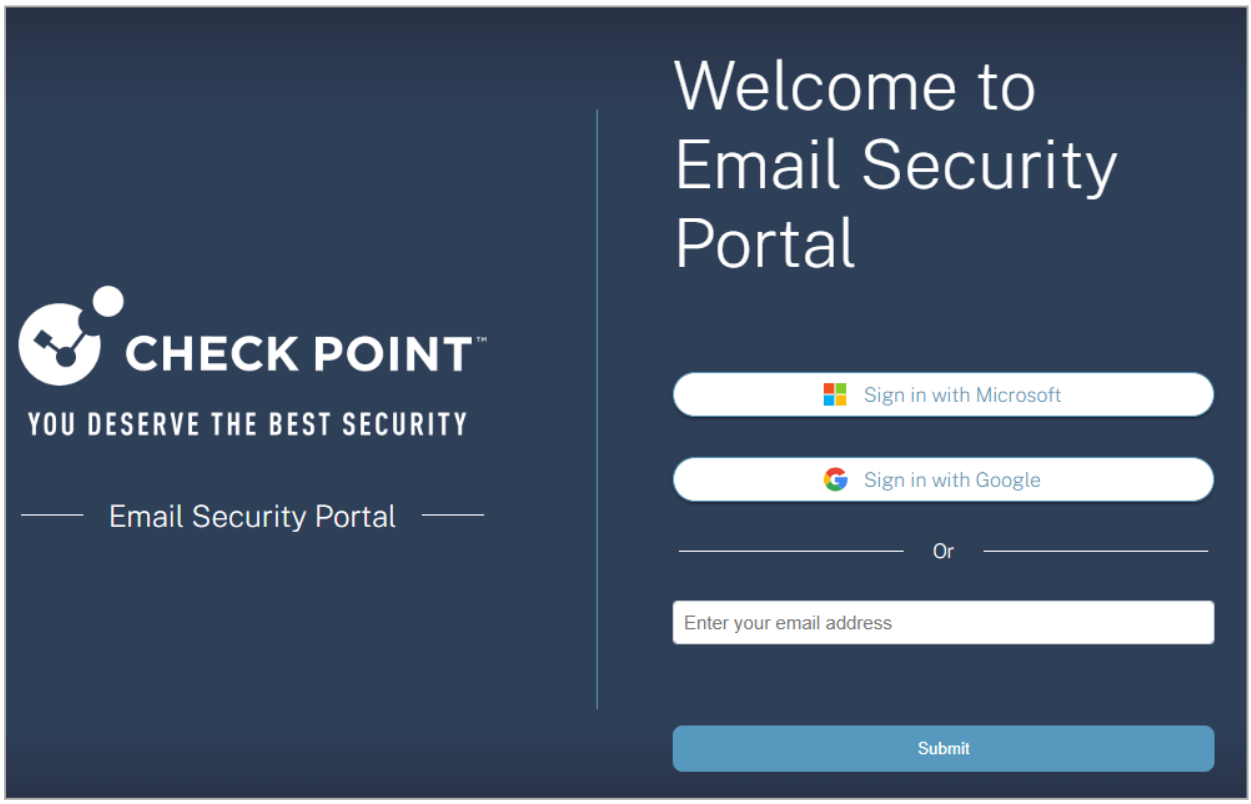
Note - After enabling the authorizing method (google/microsoft), an administrator must authorize the login for the entire organization by granting the necessary permission. For more information, see *"Authorizing Login Access for the Organization" below*.

Authorizing Login Access for the Organization

Avanan allows users to log in to the End User Portal (Email Security Portal) with Microsoft/Google credentials. To enable this option, the administrator must authorize the login for the entire organization by granting the necessary permissions.

To authorize Microsoft/Google login permissions:

1. Access the Email Security Portal using https://email-security-portal.avanan.net.
2. To allow end users to sign in using Microsoft credentials, select **Sign in with Microsoft**.



3. To allow end users to sign in using Google credentials, select **Sign in with Google**.
4. Enter the admin credentials.

The **Permissions requested** pop-up appears for **End User Portal HEC - prod** application and requests for the necessary permissions. See *"Required Permissions for Microsoft/Google Login Authorization" below*.

5. To allow end users to sign in using Microsoft/Google credentials, select the **Consent on behalf of your organization** checkbox.
6. Click **Accept**.

   End users can now sign in to the Email Security Portal using the organization's Microsoft/Google credentials.

Required Permissions for Microsoft/Google Login Authorization

Permissions required from Microsoft/Google	Functions performed by Harmony Email & Collaboration
Sign you in and read your profile	Allows users to sign in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Maintain access to data you have given it access to	Allows the app to view and update the signed-in user data even when you are not currently using the app.

Limiting End User Portal Access to Specific Users

By default, Avanan provides all users with access to the End User Portal.

To limit access to specific users or groups:

1. Access the Avanan Administrator Portal.
2. Go to **Security Settings** > **User Interactions** > **Quarantine**.
3. In the **Allowed Users** section, select the users you want to allow access to the End User Portal.
   - To allow access to all users in your organization, select **All Users**.
   - To allow access to specific users or groups, select **Select Users**.
     a. In the **Specific Users and Groups** section, select the required users or groups.
     b. Click **Add to Selected**.
4. Scroll-down and click **Save and Apply**.

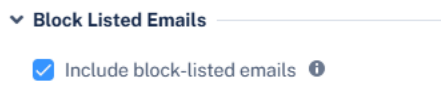
Note - If Microsoft or Google login is configured in the authentication methods (see Authentication Methods for Accessing the Email Security Portal), administrators can also restrict end users access through Microsoft or Google.

Including Blocklisted Emails in the End User Portal

Administrators can control the visibility of blocklisted emails in the End User Portal.

To include blocklisted emails in the End User Portal:

1. Access the Avanan Administrator Portal.
2. Go to **Security Settings** > **User Interactions** > **Quarantine** > **End User Permissions**.
3. In the **Block Listed Emails** section, select the **Include block-listed emails** checkbox.



4. Scroll-down and click **Save and Apply**.

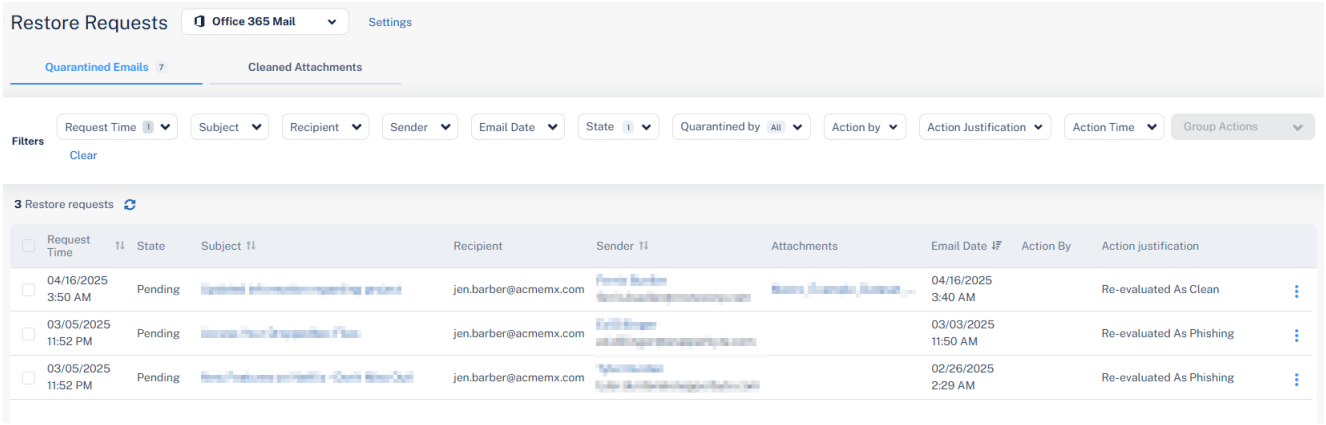
Note - Emails quarantined due to a blocklist appear in the End User Portal, where users can take action on them like non-blocklisted emails.

Managing Restore Requests

Quarantine Restore Requests

The **Restore Requests** dashboard shows requested restore emails from the end users. Whenever a user requests the restoration of a quarantined or clean email, a new entry is created in the dashboard. This allows the administrator to review and take the relevant actions.

To view user requested restore emails, navigate to **User Interaction** > **Restore Requests**.



Automatic Handling of Quarantined Restore Requests

Avanan allows you to automate the handling of quarantined restore requests, significantly reducing the administrator's workload.

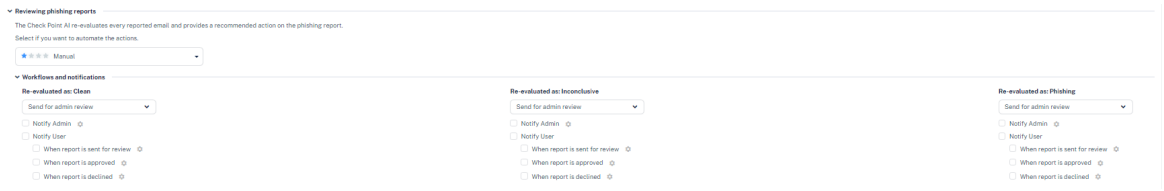
Whenever a user requests to restore an email from quarantine, Avanan re-evaluates the email and provides a re-evaluated verdict (clean, phishing, or inconclusive).

Administrators can configure a workflow for each re-evaluated verdict and customize notifications for administrators and end users. To do that:

1. Go to **Security Settings** > **User Interaction** > **Quarantine**.
2. In the **Reviewing Phishing Reports** drop-down, select one of these options:
    a. **Manual** - The administrator manually reviews every report.
        - Clean: Send for admin review
        - Inconclusive: Send for admin review
        - Phishing: Send for admin review
    b. **Semi-automatic** - Automated actions for some updated verdicts and manual review for others.
        - Clean: Approve request. Restore the email
        - Inconclusive: Send for admin review
        - Phishing: Decline request. Email remains in quarantine

c. **Automatic** - Automatic recommendation is performed.

- Clean: Approve request. Restore the email
- Inconclusive: Approve request. Restore the email
- Phishing: Decline request. Email remains in quarantine



3. Expand the **Workflows and notifications** section and select the required workflows.

Re-evaluated Verdict	Available Workflows
Re-evaluated as: Clean	■ **Send for admin review** ■ **Approve request. Restore the email**
Re-evaluated as: Inconclusive	■ **Send for admin review** ■ **Approve request. Restore the email** ■ **Decline request. Email remains in quarantine**
Re-evaluated as: Phishing	■ **Send for admin review** ■ **Decline request. Email remains in quarantine**

4. Select whom to notify:

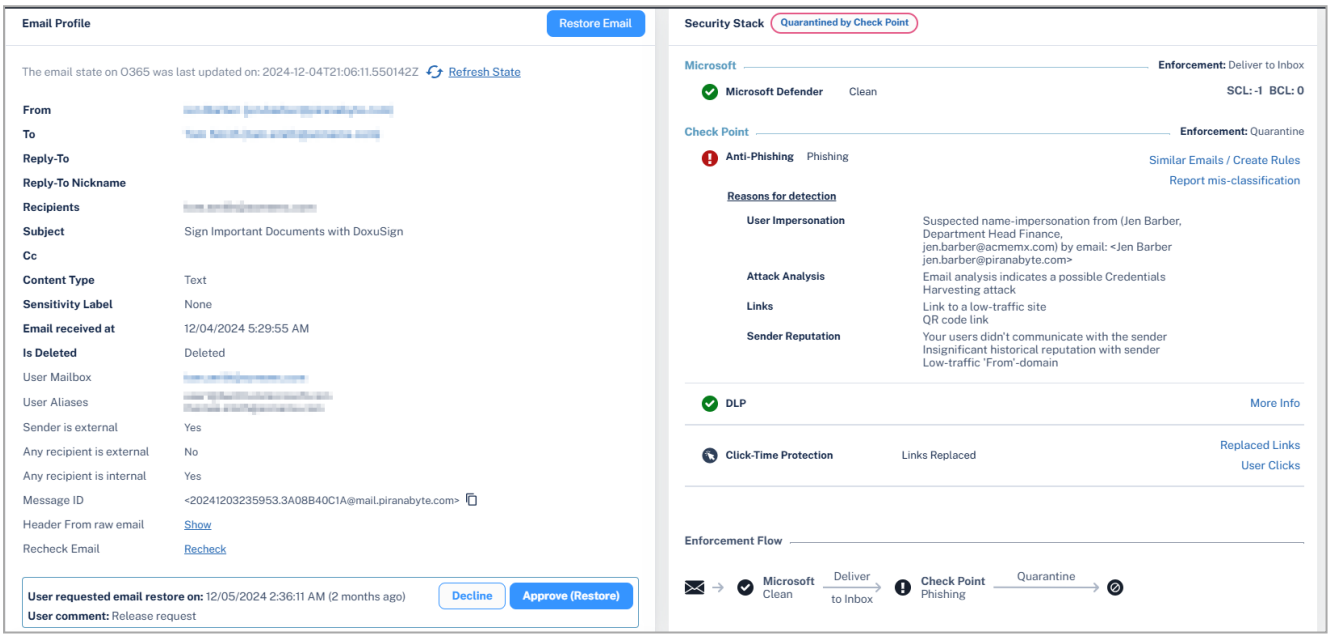
- **Notify Admin** - The administrator receives an email notification when the request is sent for their review.
- **Notify User**:
  - **When report is sent for review** - The system sends a notification to the end user when it sends the request for review.
  - **When report is approved** - The end user receives an email notification when the request is approved.
  - **When report is declined** - The end user receives an email notification when the request is declined.

Note - The availability of these options depends on the workflow selected.

5. To customize an email notification (subject and body), click ⚙ next to the specific notification, make the necessary changes, and then click **Save**.
6. Click **Save and Apply**.

Re-evaluated Verdict of Quarantined Restore Requests- Administrator Experience

When Avanan receives an end user's restore request, it re-evaluates the email, shows the updated verdict under the **Security Stack**, and takes the configured action.



Requesting a Restore from Quarantine - End-User Experience

Note - This procedure is applicable only when the email is sent to individual recipients or distribution lists. For the procedure to request to restore a quarantined email sent to groups, see *"Restore Requests for Emails Sent to Groups - End-User Experience" on the next page*.

Using the link in the email end-users can request to release the quarantined email or attachment if a false positive is suspected.

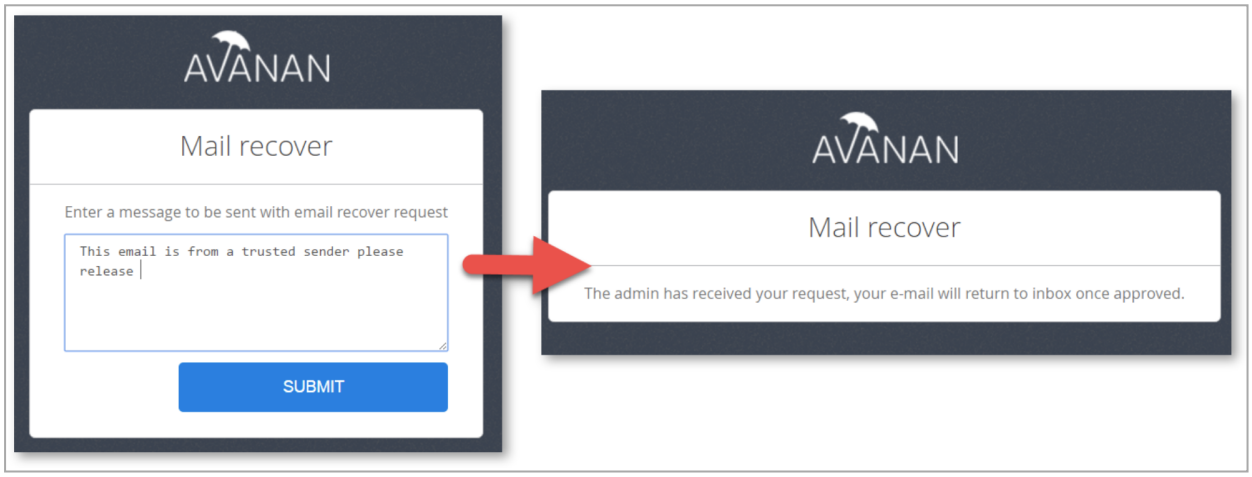
To request for restore from quarantine:

1. Click on the link in the email you received.
2. On the **User Verification** page that appears, do these:
   a. Enter your email address and click **Submit**.

      Avanan sends a verification code to your email address.

   b. Enter the verification code you received and click **Submit**.

      Note - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days.
3. Enter the reason for your request to release the email from quarantine and click **Submit**.



   You will receive a notification that the request is sent to the administrator.
4. If the request is approved by the administrator, the original message gets delivered to all the recipients of the restored email.

Restore Requests for Emails Sent to Groups - End-User Experience

This procedure is applicable when these conditions are met:

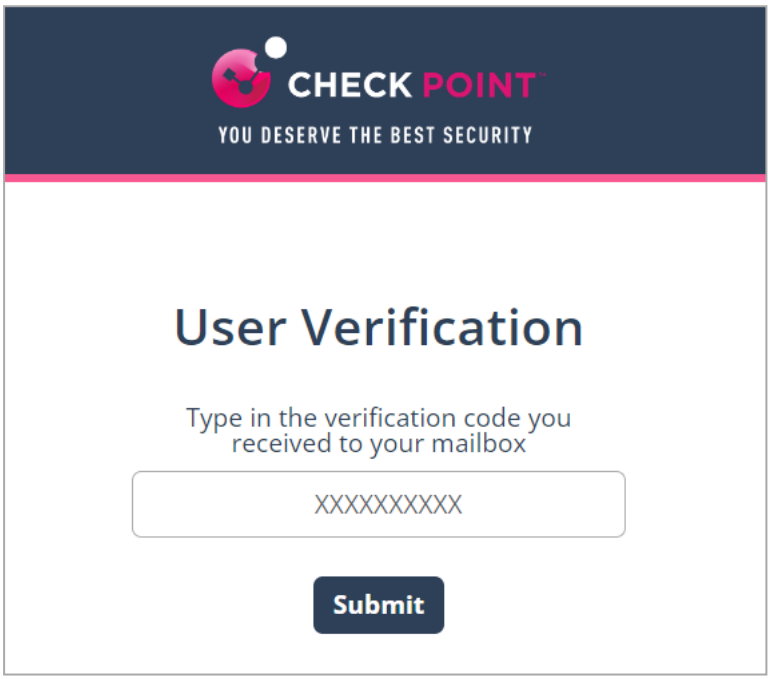
- Threat detection policy the email is matched on is in **Prevent (Inline)** protection mode.
- Email is sent to groups containing multiple users (not individual recipients or distribution lists).
- Email is quarantined or its attachments are cleaned.

End-user experience to request to restore a quarantined or cleaned email:

1. Click on the link in the email notification you received for the quarantined or cleaned email.
2. On the **User Verification** page that appears, do these:
   a. Enter your email address and click **Submit**.

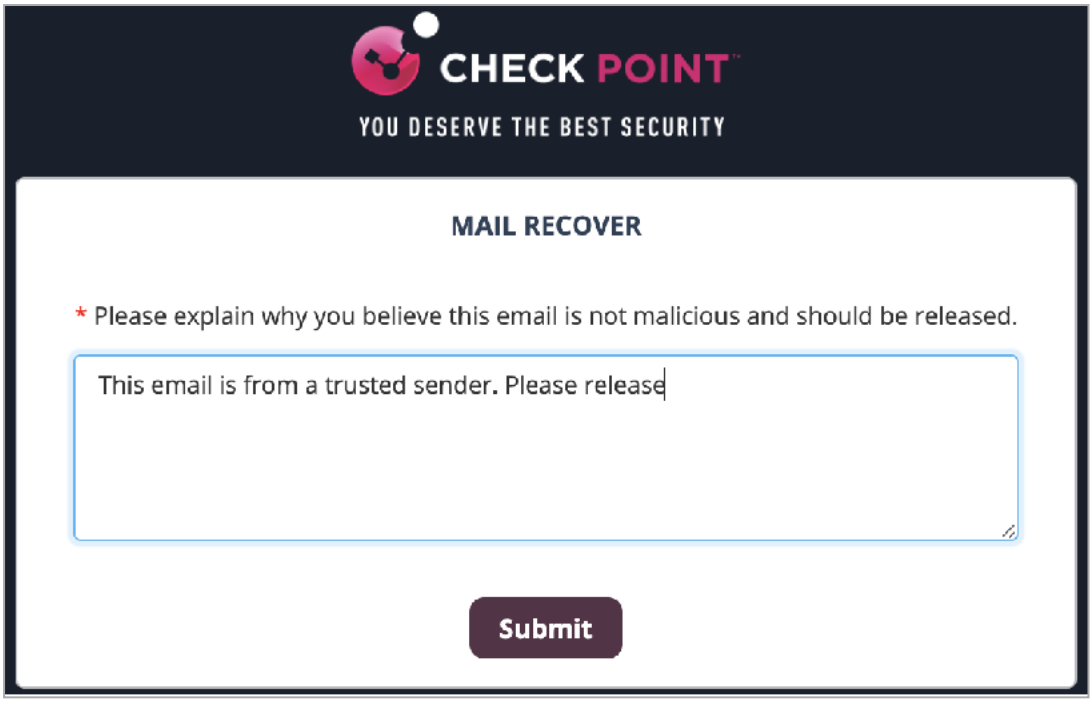
      Avanan sends a verification code to your email address.

   b. Enter the verification code you received and click **Submit**.

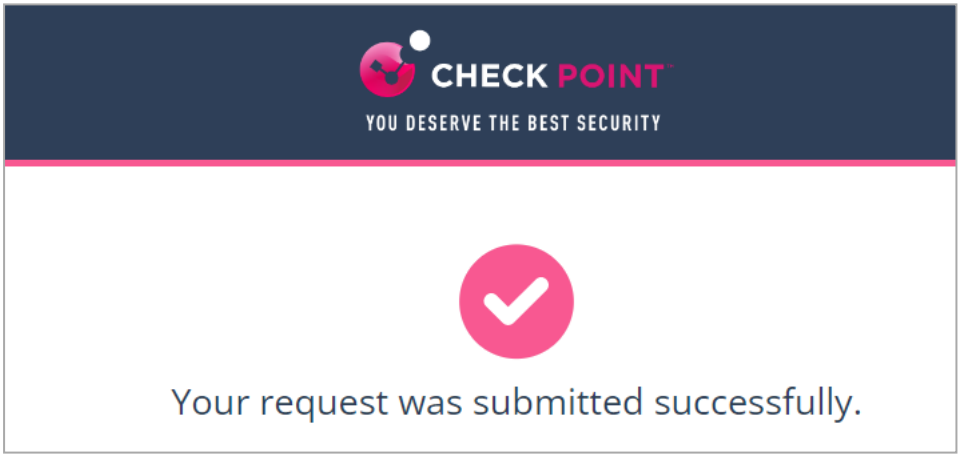


Note - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days.

3. Enter the reason for your request to restore the original email and click **Submit**.



The system shows the request status and the email is delivered to the mailbox in a couple of minutes.



Note - The email received time is the restore time of the email, and not the original email sent time.

Restoring Emails Without Administrator Approval - End-User Experience

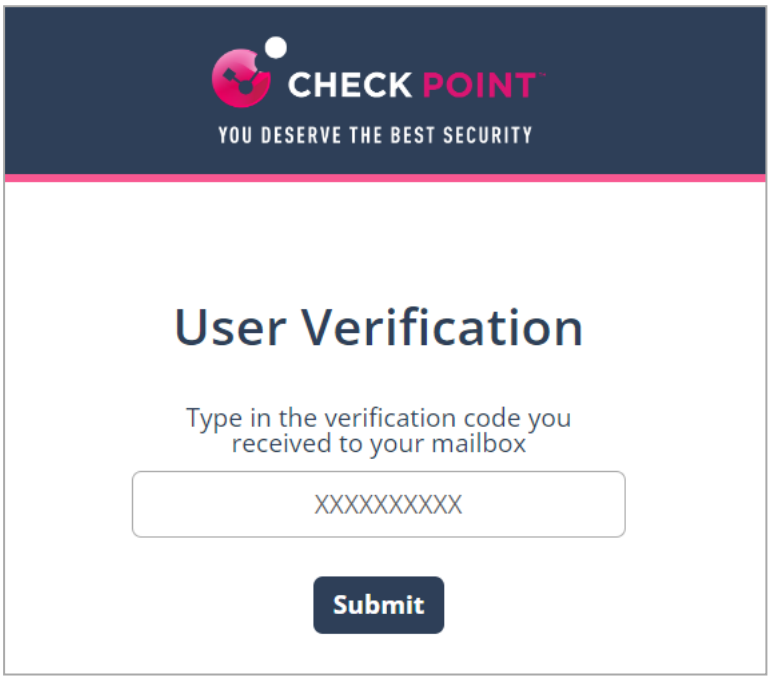
This procedure is applicable for emails where the policy is configured such that the end-user can restore the email without the administrator's approval **(Quarantine. User is alerted and allowed to restore the email**).

User experience to restore a quarantined email:

1. Click on the link in the email notification you received for the quarantined email.
2. On the **User Verification** page that appears, do these:
   a. Enter your email address and click **Submit**.

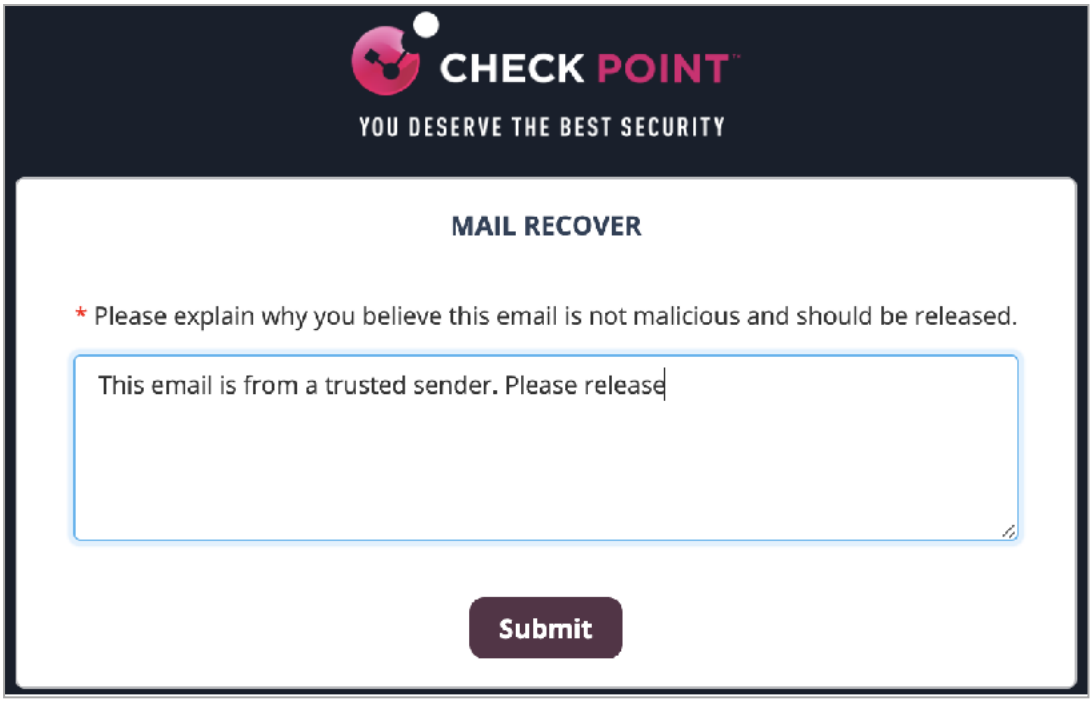
      Avanan sends a verification code to your email address.

   b. Enter the verification code you received and click **Submit**.

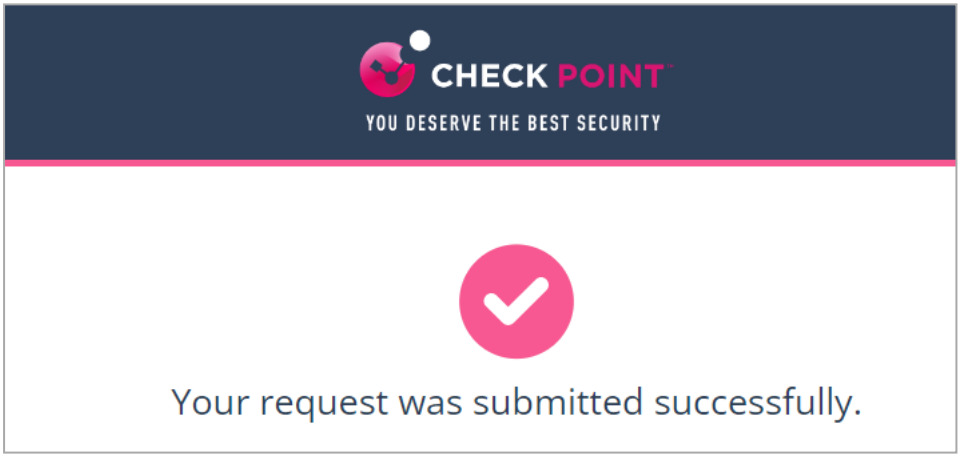


Note - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days or until the cookies are cleared, whichever is earlier.

3. Enter the reason for your request to restore the original email and click **Submit**.



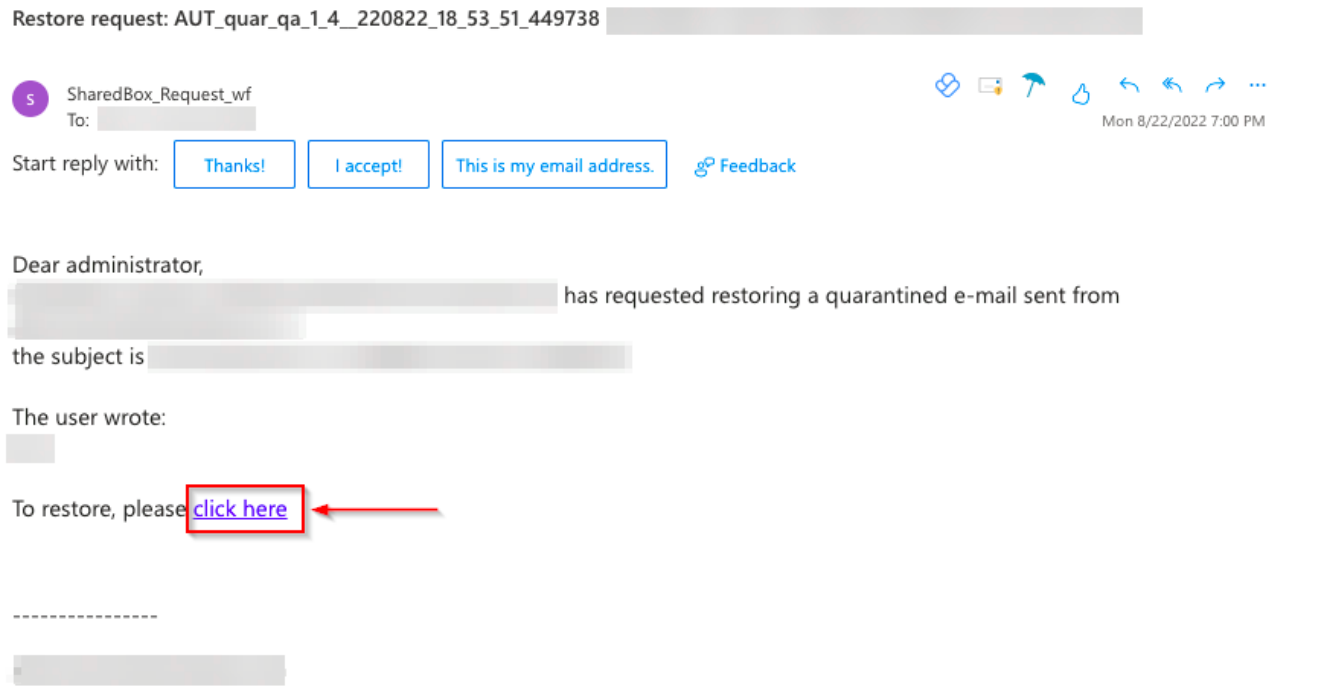
The system shows the request status and the email gets delivered to the mailbox in a couple of minutes.

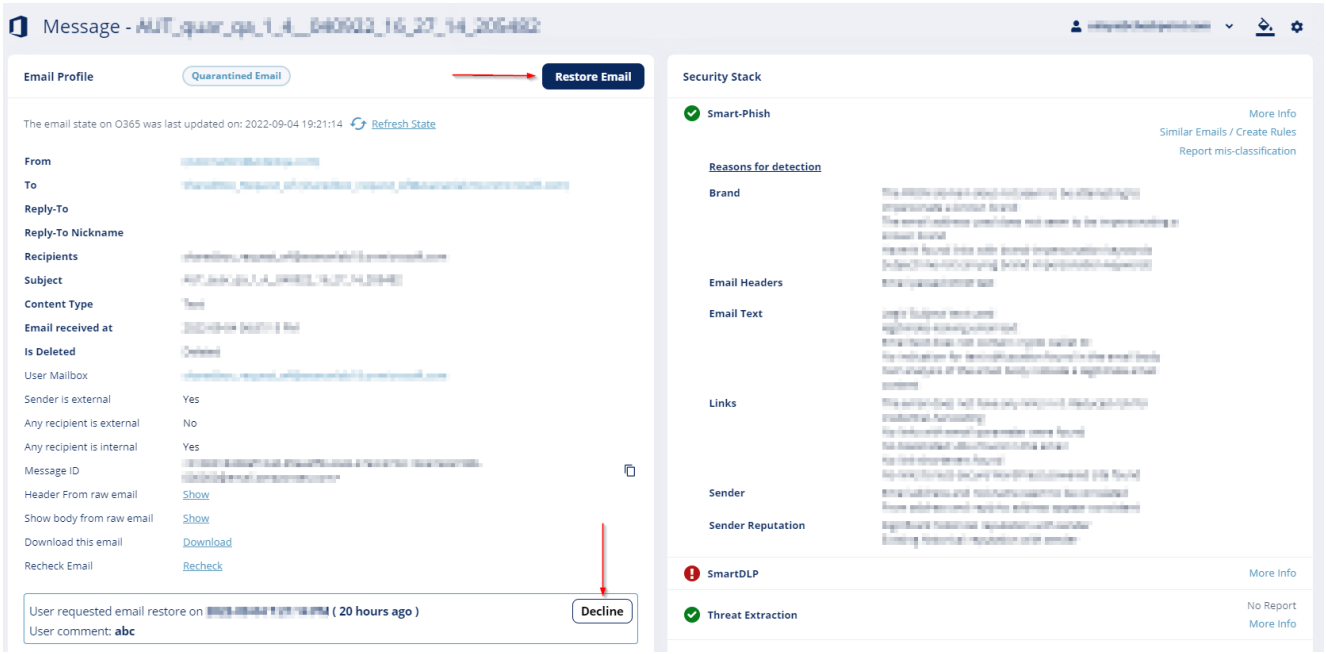


Note - The email received time is the restore time of the email, and not the original email sent time.

Admin Quarantine Release Process

When the end-user requests to release an email, the administrator is notified via email to the configured **Restore requests approver** email address. The email contains a direct link to the email profile in the Avanan portal. The administrator can do a full security review of the malware from the Avanan portal and can restore the email or decline the release request.





Cleaned Attachments Restore Requests

To view all the user requests currently pending to restore original email attachments:

1. Go to **User Interaction** > **Restore Requests**.
2. Select **Clean Attachments** tab.

Note - For emails in Office 365 that are quarantined, the senders flagged with a red icon are external users.

To approve or decline a request, do one of these:

- Click the ⋮ icon in the last column of the request table and select **Send Original/Decline**.
- To approve or decline multiple requests at a time, select the request and click **Send Original/Decline** at the top-right corner of the page.

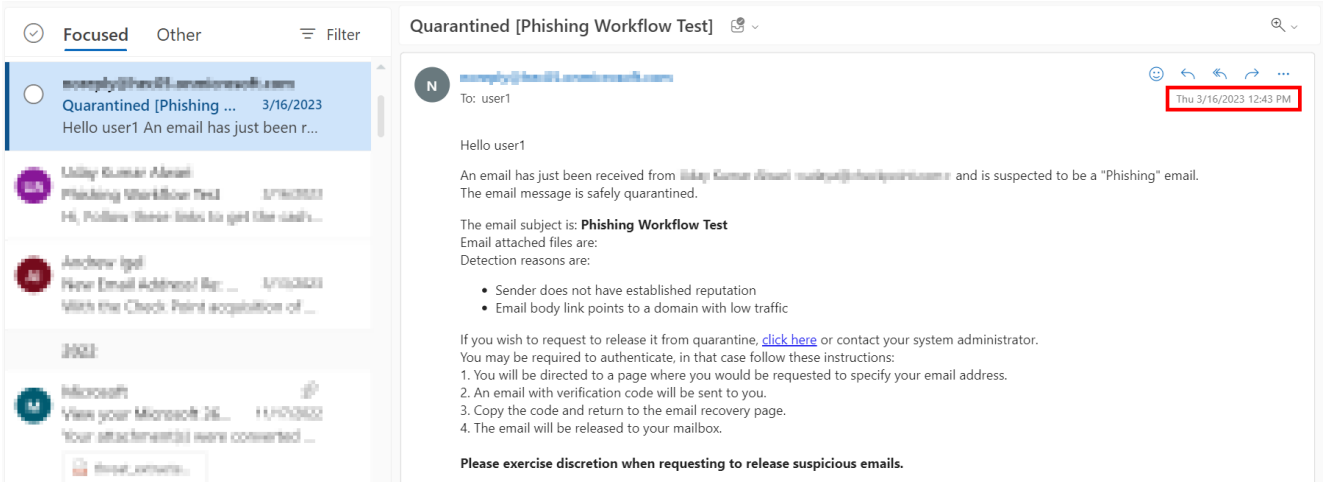
Note - When the original email is sent, it replaces the previously modified email in the user's mailbox.

Restoring Quarantined Emails - End-User Experience

After the administrator approves an end-user request to restore an email from quarantine, Avanan performs these actions:

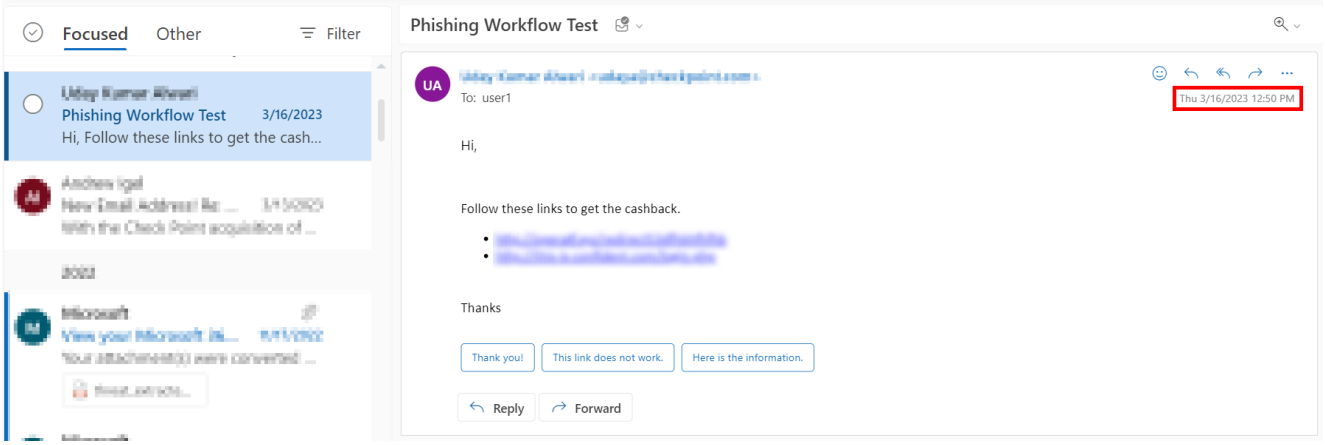
- Removes the quarantine/clean email notifications received for the quarantined email from the end-user mailbox.
- Adds the original email to the end-user mailbox, where the email received time is the restore time of the email from quarantine, but not the original email sent time.

This example shows the initial email received by the end-user.



This example shows the same email received by the end-user after the administrator approved the restore request.

Note - The initial email received by the end-user is removed and the restored email gets delivered as a new email to the end-user mailbox. The email received time is the restore time of the email by the administrator, but not the original email sent time.



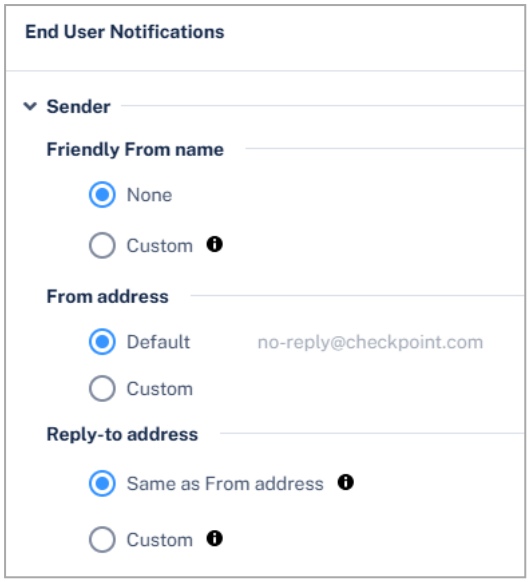
Who Receives the Emails Restored from Quarantine

- Emails quarantined by Avanan:
  - Depending on the configured workflow, Avanan delivers the email only to the requesting user or to all the original recipients.
    - If the user restores the email without administrator approval, Avanan delivers the email only to the requested user.
    - If the administrator releases the email from quarantine, Avanan delivers the email to all the original recipients of the email.
- Emails quarantined in Microsoft:
  - Avanan delivers the restored emails to all the original recipients regardless of whether it is restored by the user or the administrator.

Notifying End Users about Rejected Restore Requests

To notify end users when their quarantine restore requests are rejected:

1. Go to **Security Settings** > **User Interaction** > **Quarantine**.
2. In the **End User Notifications** section, configure the required sender email address for notifications.



3. To configure the sender email address for notifications, do these:
   - Friendly-From name
     - If no friendly-from name is required, select **None**.
     - To use a customized name, select **Custom** and enter the sender name.
   - From address
     - To use the default email address, select **Default**. The default email address is *no-reply@avanan-mail.net*.
     - To use a custom email address, see *"Customizing the From address for Email Notifications" on page 227*.
   - Reply-to address
     - To use **From address** as the Reply-to address, select **Same as From address**.
     - To use a custom email address, select **Custom** and enter the email address.
4. Click **Save and Apply**.

Note - This will also enable end user notifications for approved and rejected phishing reports. See *"Automatic Ingestion of End User Reports" on page 362*.

To configure the notification subject and body:

1. Go to **Security Settings** > **SaaS Applications**
2. To configure the notification for Office 365 Mail, click **Configure** for Office 365 Mail.
3. To configure the notification for Gmail, click **Configure** for Gmail.
4. Scroll-down to **Advanced** and edit these templates:

- Decline message subject
- Decline message body

Restore Requests - Notifications and Approvers

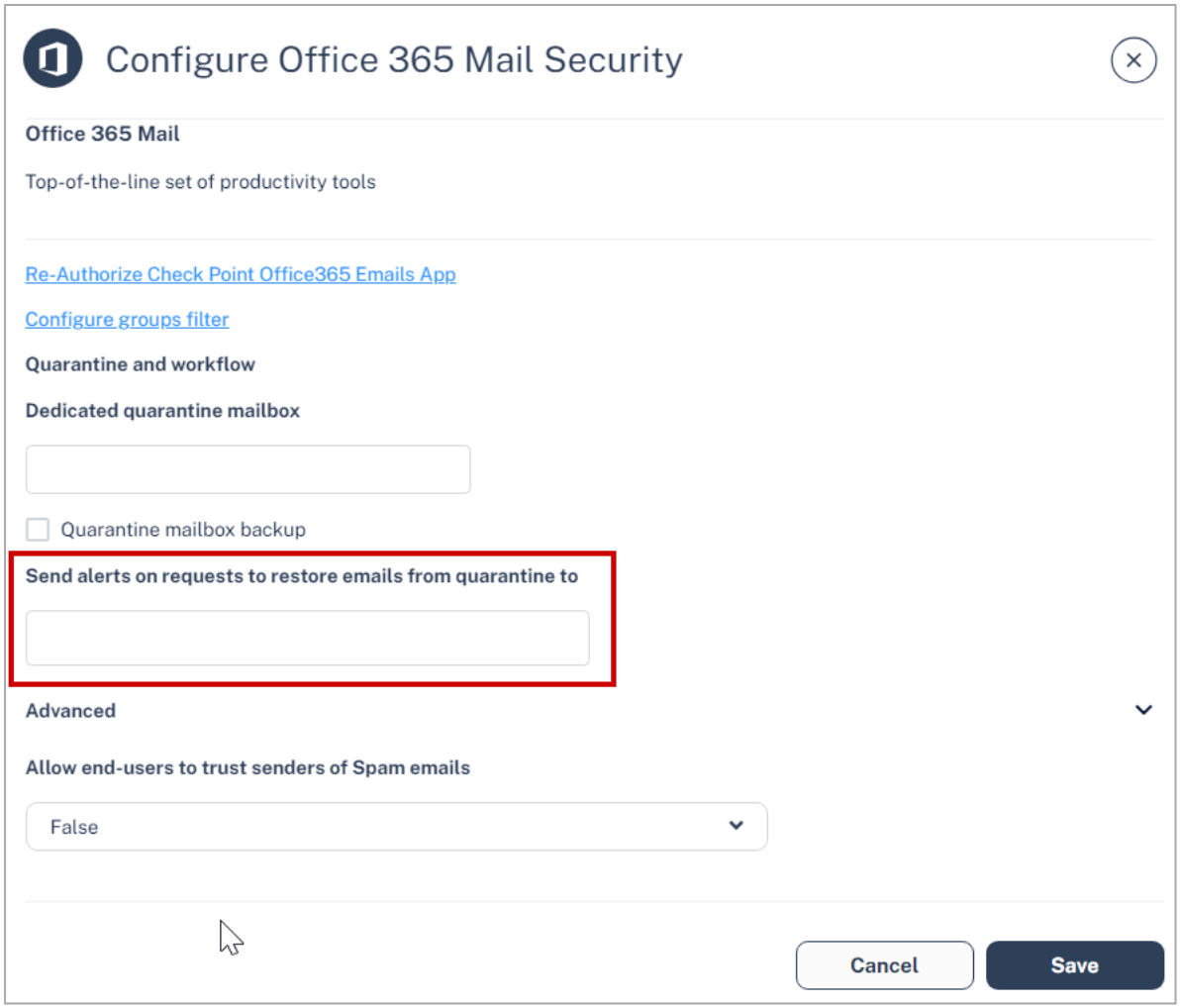
When a user requests to release an email from quarantine, Avanan sends email notifications to the email accounts configured in the **Send alerts on requests to restore emails from quarantine to** field.

Note - This field does not determine the restore requests approver. To approve a request, the approver must have **Admin** or **Help Desk** role.

Office 365 Email

To add email accounts to the **Send alerts on requests to restore emails from quarantine to** field:

1. Go to **Security Settings** > **SaaS Applications**.
2. Click **Configure** for Office 365 Mail.
3. In the **Send alerts on requests to restore emails from quarantine to** field, enter the email addresses.

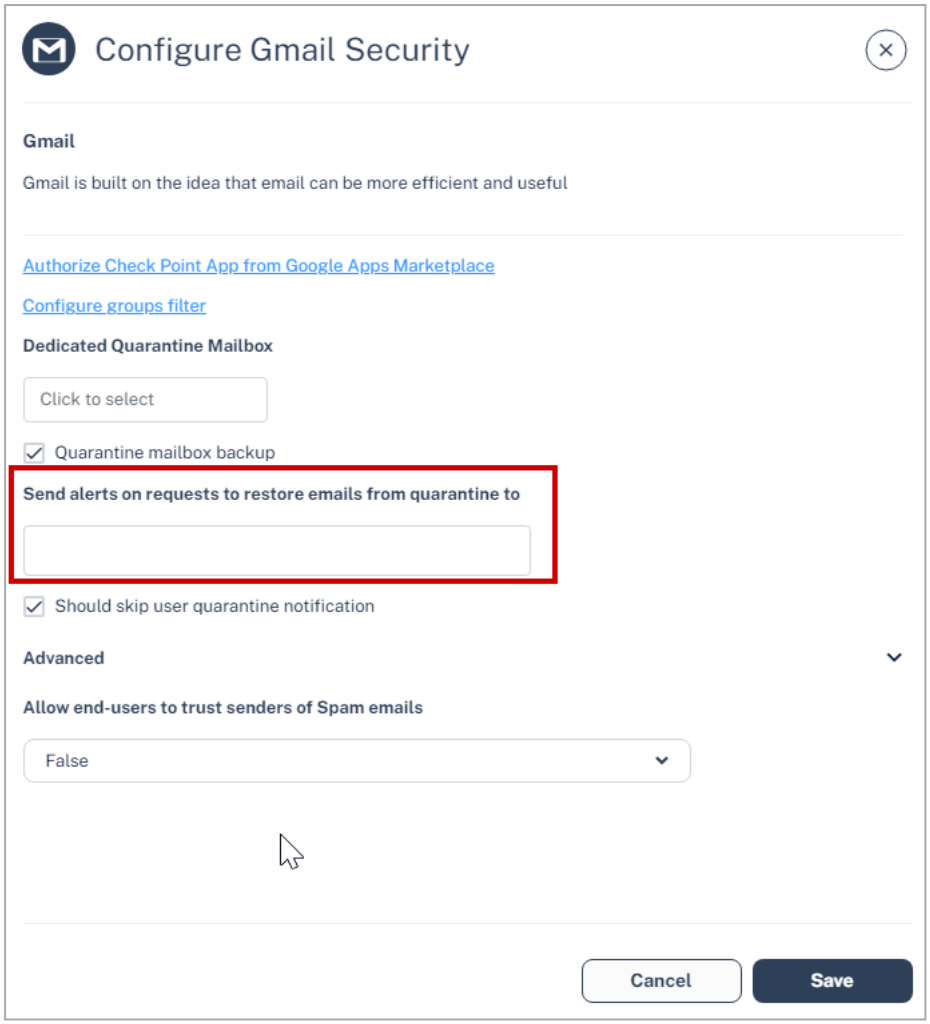


4. Click **Save**.

Gmail

To add email accounts to the **Send alerts on requests to restore emails from quarantine to** field:

1. Go to **Security Settings** > **SaaS Applications**.
2. Click **Configure** for Gmail.
3. In the **Send alerts on requests to restore emails from quarantine to** field, enter the email addresses.



4. Click **Save**.

Authentication for Email Notifications

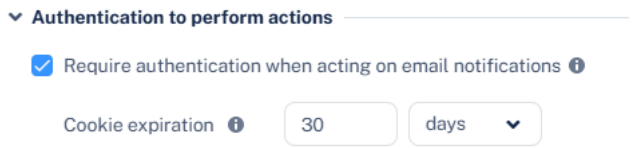
Avanan allows administrators to select the authentication methods requirements for end users interacting with the links in the email notifications, such as restoring quarantined emails.

If you enable authentication for email notifications, Avanan requests that all users authenticate before proceeding with the request. After successful authentication, Avanan adds a cookie to the user's browser, with an option to configure its expiration period.

For example, if you configure the **Cookie expiration** period as 2, Avanan does not request the user to authenticate after successful authentication in the same browser for the next two days.

To enable the authentication for email notifications:

1. Go to **Security Settings** > **User Interactions** > **Quarantine** > **End User Permissions**.
2. In the **Authentication to perform actions** section, select **Require authentication while acting on email notifications** checkbox.



3. Select the time frame for **Cookie expiration**.
4. Click **Save and Apply**.

Note - If you allow end users to restore quarantined emails without authentication, the email security solutions might mistakenly trigger the restore link during the automated scanning process. You must make sure that only authorized users can restore the quarantined emails.

Customization

Dark Mode

Administrators can switch the theme of the Avanan Administrator Portal to **Dark mode**. It provides a dark background (instead of white) across the UI.

To enable or disable Dark mode:

1. Access the Avanan Administrator Portal.
2. Go to **System Settings > Customization**.
3. Under **General**, toggle **Dark mode** to **On/Off**.
4. Click **Save and Apply**.

Note - Turning **Dark mode** on/off does not impact the end-users and it is specific to the signed-in administrator. Each administrator can turn the **Dark mode** on/off for themselves.

Custom Logo

You can replace the Avanan logo to show your organization logo in the browser pages, email notifications, and reports Avanan sends to the administrators and users.

To add a custom logo:

1. Access the Avanan Administrator Portal.
2. Go to **System Settings > Customization**.
3. Select the **Custom Logo** checkbox.

   Note - The logo must have these properties.

   - File type is PNG
   - File size is less than 2 MB
   - Logo dimensions ratio is 1/2.5 px, 72 dpi (Horizontal version)
4. Upload the required logo(s).
   - To upload the logo compatible with dark backgrounds, under **Logo for dark background**, click **Browse** and select the relevant logo.

- To upload the logo compatible with white backgrounds, under **Logo for white background**, click **Browse** and select the relevant logo.

Notes:

- If you upload only one logo, Avanan uses the same logo for dark and white backgrounds.
- To have a clear logo compatible with the background, Avanan recommends using separate logos for dark and white backgrounds.

5. Select where you want to replace the Avanan logo:
   - To replace the logo in the Security Checkup report, enable the **Security Checkup Report** checkbox.
   - To replace the logo in the Daily Quarantine report, enable the **Daily Quarantine Report** checkbox.
   - To replace the logo in the browser pages presented to the administrators and users, enable the **Browser pages** checkbox.
   - To replace the logo in the email notifications, select the required option:
     - To replace the logo in all the email notifications sent to administrators and end users, enable the **Admins and end users** checkbox.
     - To replace the logo in all the email notifications sent only to administrators, enable the **Admins only** checkbox.
     - To replace the logo in all the email notifications sent only to end users, enable the **End users only** checkbox.
6. Click **Save and Apply**.

Adding a branded header to admin email notifications

You can add your organization logo and contact information to the header and footer for the email notifications that Avanan sends to the administrators.

To add a branded header and footer to email notifications:

1. Go to **Security Settings** > **Customization**.
2. Under **General**, select **Add a branded header to admin email notifications** toggle button.
3. Scroll down to the end of the page and click **Save and Apply**.

Now that the toggle is enabled, all email notifications sent to administrators will include the following:

- Header: Avanan logo or the custom logo (if configured).
- Footer: Avanan contact information.

Customize Time Zone

Avanan allows you to customize the time zone for email notifications and reports sent to administrators and end users, ensuring that timestamps are consistent with the selected time zone.

However, the Avanan Administrator Portal and End User Portal display time according to the user's browser time zone, reflecting their local time.

To customize the time zone for email notifications and reports:

1. Go to **Security Settings** > **Customization**.
2. Under **General**, select the **Customize Time Zone** toggle button.
3. Select the required time zone.

   Note - By default, the time zone is set to (UTC +00:00) UTC.

4. Scroll down to the end of the page and click **Save and Apply**.

Customizing Retention Period of Emails

Avanan allows you to customize the email retention period based on the verdict of the security engines.

Default Retention Period of Emails

Verdict and Enforcement	Raw Email (Original email with attachments)	Email Meta Data (Attributes and data detected from the security scan)
Clean emails (Includes emails with re-written links in the email body)	14 days	14 days
Emails with modified attachments and emails that have cleaned (sanitized) attachments, removed as password-protected attachments, and re-written links	14 days	180 days

Verdict and Enforcement	Raw Email (Original email with attachments)	Email Meta Data (Attributes and data detected from the security scan)
Emails containing threats but not quarantined (includes emails with phishing /spam / malware / DLP detection that are not quarantined)	14 days	180 days
Quarantined emails (includes manually quarantined emails)	180 days	180 days
Emails quarantined by Microsoft	180 days	180 days

Custom Retention Periods

To configure custom retention periods for raw emails:

1. Go to **Security Settings** > **Customization**.
2. Under **Email Retention Settings**, select **Custom**.
3. Based on the security engines' verdict and quarantine state, select the number of days you need to retain an email.
4. Click **Save and Apply**.

Notes:

- Any changes to the retention period take effect within 24 hours and apply only to new emails.
- Emails get deleted at the end of the day (UTC time zone) of each retention period. Sometimes, it may take extra time for the delete action to be completed.

For details about the actions available during and after the retention period, see *"Available Actions on Emails During and After the Retention Period" on page 623*.

Auditing

Avanan audits all the changes to the retention period and adds them to the **System Logs** (**System Settings** > **System Logs**).

Incident Response as a Service (IRaaS)

Incident Response as a Service (IRaaS) is the Avanan offering in which an Avanan analyst assesses and responds to end-user reports and requests on your organization's behalf, relieving your SOC/Help Desk team of these responsibilities. This service provides uninterrupted 24/7 coverage and adheres to a concise SLA, ensuring a prompt response.

Activating IRaaS

After your purchase order is processed, Avanan automatically initiates IRaaS. Subsequently, an Avanan analyst analyzes all your end-user reports and takes preventive actions.

To purchase IRaaS, contact your Avanan representative.

Acting on End User Reports

The Avanan analysts review the email for the end-user reports, determine if they are malicious or benign, and then take actions if required:

- **Phishing emails reported by the end users**
  - Malicious email - The analyst approves the user report, and the reported email is removed from the user's mailbox.

    To remediate the entire campaign, similar emails are also removed from other users' mailboxes. For more information, see *"Automatically Quarantining Entire Phishing Campaigns" on the next page*.
  - Benign emails - The analyst rejects the user report, and the email remains in the user's mailbox.
  - Inconclusive - If the analyst cannot determine if the email is malicious or benign, the user report will be approved and the email will be treated as malicious.
- **Quarantined email restore requests by the end users**
  - Malicious email - The analyst rejects the request, and the email remains in quarantine.
  - Benign emails - The analyst approves the request, and the email is restored to the user's mailbox.

- Inconclusive - If the analyst cannot determine if the email is malicious or benign, the user request will be approved and the email will be restored to the user's mailbox.

Automatically Quarantining Entire Phishing Campaigns

When the Avanan analyst approves a user reported phishing email, Avanan detects all the emails in the phishing campaign and quarantines them.

Avanan considers an email as part of a phishing campaign when all these characteristics of the email are identical to the reported email.

- Subject
- From address
- Reply-to address
- SPF result
- Location in the email thread - If the email has multiple responses between the sender and the recipient, then the serial number of the response must be identical.

  For example, consider an employee of a protected organization received an email (number 1), replied to it (number 2), and then received another response (number 3) from the sender. Now, if the employee reported this response (serial number 3) as phishing, then only other emails that are 3rd in the thread gets quarantined.

Feedback to End Users

The Avanan analysts add a justification for every decision they make. The administrators can configure Avanan to send email notifications containing the justification for rejected quarantine restore requests and approved or rejected phishing reports.

To configure Avanan to send end-user notifications, see *"Sending Email Notifications to End Users" on page 225*.

Feedback to Administrators

After activating Incident Response as a Service (IRaaS), the administrators receive a daily email containing a summary of all the reports managed by the Avanan analysts.

The report consists of two sections: one for requests to release emails from quarantine and another for phishing emails reported by the user. These sections show various analyzed emails, along with the analyst's justification.

Finding Reports Handled by Avanan Analysts

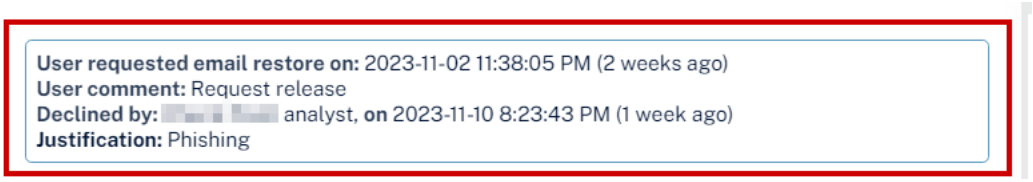
To view the emails the Avanan analysts managed, go to **User Interaction** and access **Restore Requests** or **User Reported Phishing**. You'll find:

- The **Action by** column with the value **Avanan analyst** are the emails the Avanan analysts handled.
- The **Action Justification** column shows the analyst's reason for the action (approve/decline).

From the **Events** page, you can view the user-reported phishing events. To filter all events resolved by Avanan analysts:

1. Go to **Events**.
2. Apply the filter **Avanan analyst** for the **Remediated by** field.

After opening the security event of an email that was handled by a Avanan analyst, the **Email Profile** card shows the user comment, action taken and additional details.



Handling Issues with IRaaS

For any issue with IRaaS, contact *Avanan Support*.

DMARC Management

Organizations use SPF, DKIM and DMARC to ensure attackers cannot launch phishing attacks impersonating to senders from their domain.

Emails from the organization’s domains are not sent only from the organization itself (for example, their Microsoft 365 tenant), but also from many other sending sources like Salesforce, Marketo and others.

To ensure the business is not harmed by partners/customers blocking legitimate emails from the organization’s domains, you should make sure your SPF and DKIM records are properly maintained and include all legitimate sending sources.

Avanan provides **DMARC Management** as an add-on that helps to manage DMARC and SPF.

DMARC Management helps organizations make sure all legitimate senders are allowed so that you can confidently apply a restrictive policy tag in your organization's DMARC DNS record.

- *"DMARC Management" on page 458*
- *"SPF Management" on page 468*

DMARC Management

Introduction

Avanan provides **DMARC Management** as an add-on that helps to manage DMARC and SPF.

DMARC Management helps organizations make sure all legitimate senders are allowed so that you can confidently apply a restrictive policy tag in your organization's DMARC DNS record.

- *"DMARC Management" above*
- *"SPF Management" on page 468*

The organization's DMARC DNS record – specifically the **p** tag - states what should be done with emails that fail authentication checks.

Three possible values to the p tag in the DMARC record:

- none – recipients should report failures but should also deliver emails allegedly from the domain even if they fail authentication.
- quarantine – recipients should quarantine emails that fail authentication. They would usually be marked as spam.
- reject – recipients should not even accept the email and never deliver it to their end users.

Since this is usually a difficult task, most organizations do not have a DMARC policy (**p**) tag at all or assign the value **none** to it.

Benefits

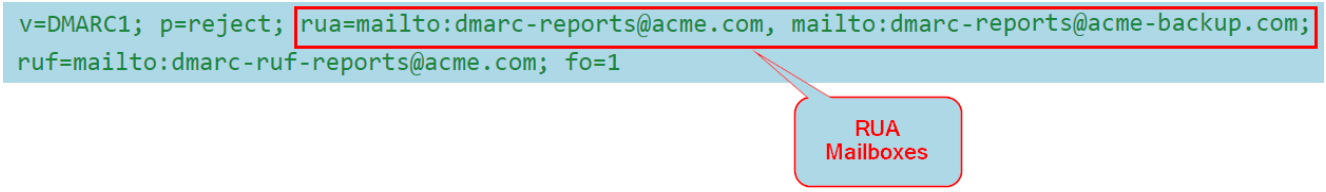
DMARC Management helps you safely transition to a restrictive DMARC policy. It includes:

- Visibility to all the services sending emails on behalf of your domains and subdomains
- Search all DMARC failed emails sent on the organization's behalf
- Actionable DMARC record change recommendations.

Prerequisites

Periodically, email receivers send aggregated reports containing information on all emails they received from your domain, the IP address from which they received the emails, and the authentication results (SPF and DKIM) for each IP address. These reports are sent to the email addresses (RUA mailbox) defined in your domain's DNS DMARC record with the **rua** tag.

Sample DMARC record content:



Avanan needs to get the aggregated DMARC RUA reports. To do that, you must configure the **rua** tag of your DMARC record:

Notes:

- The internal mailbox must be part of the scanned (protected) mailboxes.
- Avanan supports both IPv4 and IPv6 for DMARC exploration.

Present RUA value	Change to
An internal mailbox	Avanan reads the value from the DNS record and monitors the internal mailbox.
A hosted mailbox	If you wish to use a hosted mailbox, you must add a Avanan hosted mailbox to your **rua** tag. For more information, see *"RUA Mailbox Hosted by Avanan" below*.

RUA Mailbox Hosted by Avanan

Organizations that send large amounts of emails to external recipients often get a lot of DMARC RUA reports in a short period of time. The amount is so large, that Microsoft and Google often reject some of them, to meet their maximum allowed incoming emails rate.

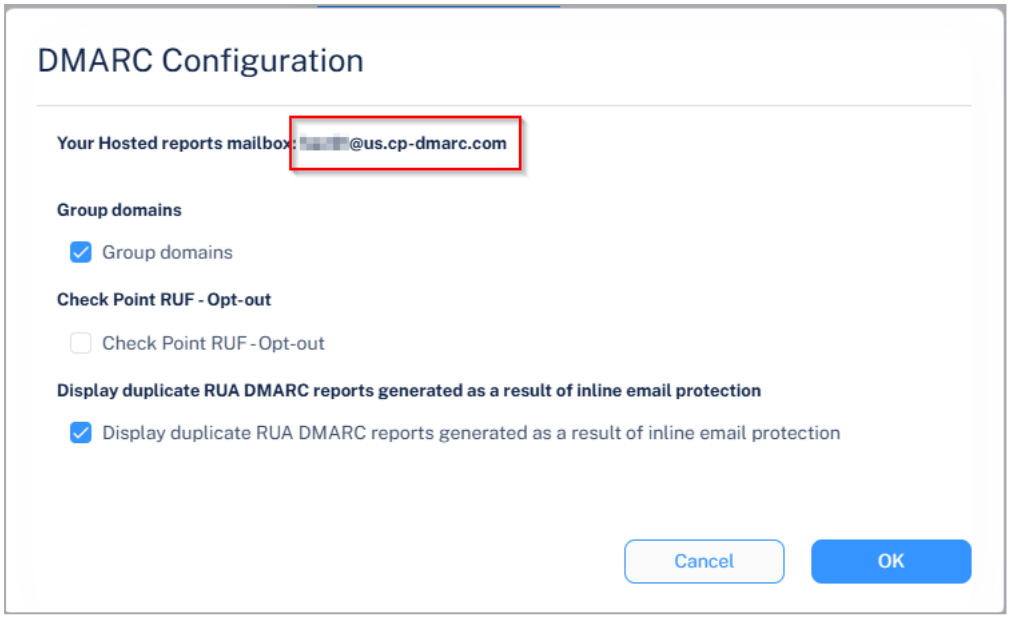
Avanan automatically creates a dedicated RUA mailbox for every tenant (account) in the Avanan Administrator Portal.

Note - The hosted RUA Mailbox is compliant with RFC 7489, section-7.1.

To use the dedicated RUA mailbox:

1. Access the Avanan Administrator Portal and click **DMARC** > **Overview**.
2. From the top of the page, click **Configuration**.

   The **DMARC Configuration** pop-up appears..
3. From the **Your Hosted reports mailbox** field, copy the dedicated RUA mailbox created for your tenant (account).



4. Click **OK**.
5. Add the RUA mailbox to the list of email addresses for the **rua** tag in your DMARC DNS record.

   Note - DNS changes might take up to 24 hours to reflect in the Avanan Administrator Portal.

External Reporting Authorization Record

To make sure that the DMARC records for your domain are accepted by Avanan, after you add the Avanan hosted mailbox to your DMARC record, Avanan automatically adds an External Reporting Authorization Record.

It creates a domain name in the format: `<your_domain>.com._report._dmarc.dmarc-cp.com`. In this domain, a TXT record is added with this content: "v=DMARC1":

Text	Description
TXT	<your_domain>.com._report._dmarc.dmarc-cp.com

Note - This process could take a couple of hours after Avanan detects the update to your DMARC record.

Overview

To view the **Overview** page, access the Avanan Administrator Portal and click **DMARC** > **Overview**.

To add a new domain to the monitored domains list:

1. Click **Add Domain** at the top of the page.
2. In the pop-up that appears, enter the domain name in the **New Domain** section.
3. Click **OK**.

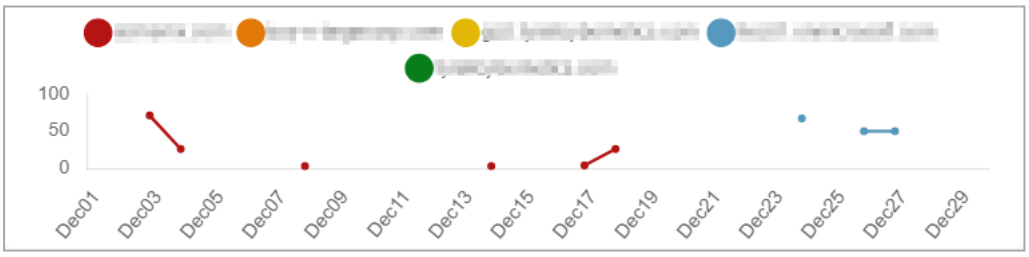
Note - It may take up to 24 hours for the system to start monitoring the domain.

The **Overview** page displays the following graphs for the selected time frame:

Top Domains Success

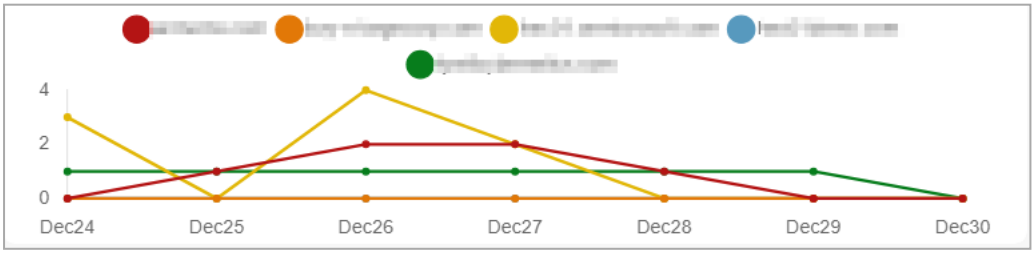
The **Top Domains Success** widget shows the domains with the highest success rate within your organization for the selected timeframe.

Top Domains Failures



The **Top Domains Failures** widget shows the domains with the highest failure rates within your organization for the selected timeframe.

Top Sending Domains



The **Top Sending Domains** widget shows the domains that have sent the most number of emails within your organization for the selected timeframe.

Reviewing the DMARC Status of your Domains

The **Overview** page shows a list of all the organization's protected domains and subdomains.

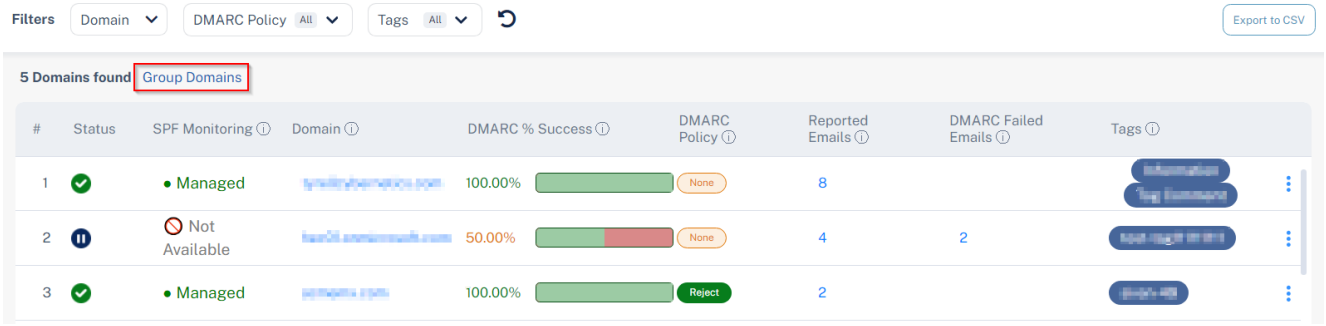
To view the **Overview** page, click **DMARC** > **Overview**.

Column	Description
Status	Monitoring status of the domain. ■ - DMARC policy is in place and the reports are being received properly. ■ - DMARC policy is in place but no reports were received in the last 72 hours. ■ - DMARC policy is in place, trying to receive the first report. ■ - No DMARC policy is in place and cannot monitor the domain.
Domain	Domain name.
DMARC % Success	The percentage of emails that pass DMARC (DKIM and SPF) out of the total numbers of reported emails sent by the domain.
SPF Monitoring	Monitoring status of the domain. ■ **Managed** - Avanan manages your SPF. ■ **Pending** - The Avanan SPF is not yet active. To activate it, update your domain's SPF record in your DNS to include Avanan's SPF entry. **Note** - DNS records may take some time to propagate across the internet. ■ **Not Managed** - The Avanan does not host your domain's SPF record yet, but the necessary settings are configured and ready to be deployed. ■ **Not Available - SPF management** is unavailable for `onmicrosoft.com` sub-domains, as Microsoft controls these DNS settings centrally to ensure consistency and security. For full DNS and email authentication control, use a custom domain.

Column	Description
DMARC Policy	The recommended enforcement on emails that failed DMARC sent on behalf of the sub domain. It is a description of the value defined in the policy (**p**) tag in the subdomain DMARC record. ■ Reject ■ None ■ Quarantine ■ No DMARC Record
Reported Emails	The total number of reported emails for the domain.
DMARC Failed Emails	The total number of failed DMARC emails for the domain.
Tags	Custom annotation tags added to the domain.

Changing View to Top Level Domains

By default, the **Overview** page shows the status of different subdomains. To change the DMARC status view to aggregate the results based on top level domains, click **Group Domains**.



While viewing the aggregated results based on top level domains, to clear the aggregated results and view the status of different sub domains, click **Ungroup Domains**.

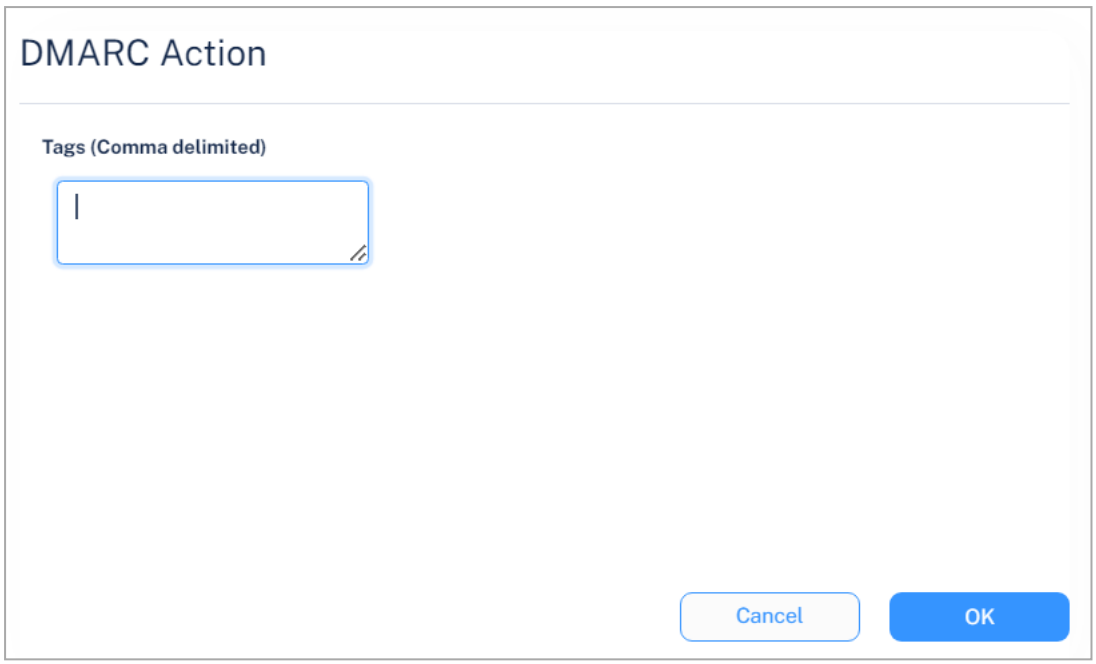
Annotating / Tagging Domains and Sending Sources

While analyzing the subdomains, administrators need to annotate domains to differentiate between them.

To add a custom tag to a domain or subdomain:

1. Click the ⋮ icon in the last column of the domain.
2. Click **Update Tags**.

3. In the **Tags** field, enter one or more tags separated by a comma.



4. Click **OK**.

Note - Annotating / tagging domains does not impact the DMARC status of the domain and does not change the domain's DNS.

Investigating the DMARC Status of Domains

The **Overview** page allows you to drill down to domains and analyze the sources sending emails on the organization's behalf.

To analyze the DMARC status of a domain, click the domain from the table. The system shows these details describing the different sending sources:

Column	Description
New	Indicates if the source has recently started sending emails on behalf of the domain. ■ [Empty] - If the domain is not detected recently. ■ New - If the domain in detected recently. To see the first instance of the domain sending emails on behalf of the domain, hover over the source name / IP address.
Sent via Source	The service provider used to send the email. To investigate the IP addresses from which the sending source sent emails on behalf of the domain, see *"Investigating a Specific Sending Source" on the next page*.

Column	Description
Reported Emails	The number of reported emails sent from this source on behalf of the domain.
Reported Failed Emails	The number of emails sent from this source, which failed DMARC authentication.
DMARC % Failures	The percentage of emails that failed DMARC out of the total numbers of reported emails sent from the source.
SPF % Failures	The percentage of emails that failed SPF out of the total numbers of reported emails sent from the source.
DKIM % Failures	The percentage of emails that failed DKIM out of the total numbers of reported emails sent from the source.
SPF Not Aligned	The percentage of the emails whose SPF is not aligned out of the total numbers of reported emails sent from the source.
DKIM Not Aligned	The percentage of the emails whose DKIM is not aligned out of the total numbers of reported emails sent from the source.
Number of Reporters	The number of unique servers that reported emails being sent from this source.
Distinct IP Addresses	The number of unique IP addresses used by the source to send emails.
Tags	Tags assigned to the source. See *"Annotating / Tagging Domains and Sending Sources" on page 463*.

Investigating a Specific Sending Source

You can drill down to a specific sending source for a particular domain to investigate the IP addresses from which the sending source sent emails on behalf of the domain.

To do that, after you drilled down to the specific domain, click on one of the source names in the **Sent via Source** column. The system shows these details:

Column	Description
IP Address	IP address of the sending source. For more information about the IP address, see *"Investigating a Single Sending IP Address" on the next page*.
Location	The geo-location of the IP address.

Column	Description
Reported Emails	The number of reported emails sent from this IP address by the source.
Reported Failed Emails	The number of emails sent from this IP address, which failed DMARC authentication.
DMARC % Failures	The percentage of emails that failed DMARC out of the total numbers of emails sent from the IP address.
SPF % Failures	The percentage of emails that failed SPF out of the total numbers of emails sent from the IP address.
DKIM % Failed	The percentage of emails that failed DKIM out of the total numbers of reported emails sent from the IP address.
Number of Reporters	The number of unique organizations that reported emails being sent from this IP address.
Number of Envelope	The number of unique envelop to values in emails sent from this IP address.

Investigating a Single Sending IP Address

To view more information about the IP address of a specific sending source, click the IP address from the table. The system shows these details for the IP address:

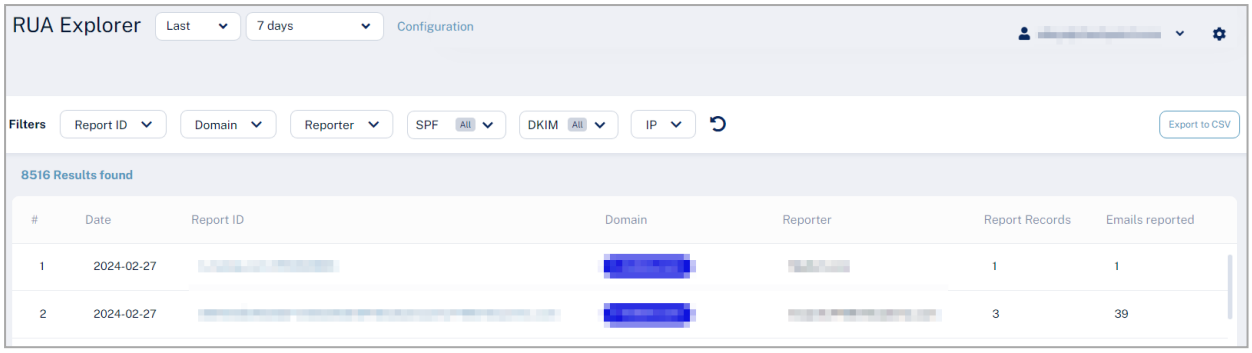
Column	Description
IP	IP address
Host name	Host name
Location	The geo-location of the IP address.
ASN	Autonomous System Number (ASN) of the IP address.

Viewing Specific RUA Reports

To view a specific RUA report:

1. Click **DMARC** > **RUA Explorer**.

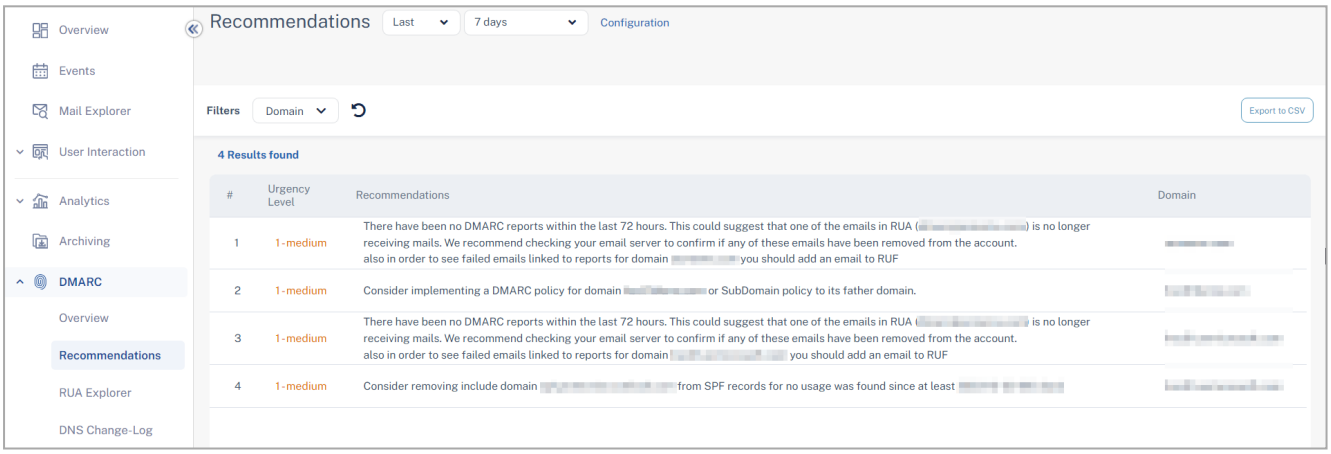
   The system shows a table with all the RUA reports received.



2. Click on the link in the **Report ID** column to view its raw XML content.

Improving your Domains' DMARC Enforcement

The **Recommendations** page shows a list of actionable recommendations to safely configure a restrictive DMARC policy for your domains and helps to maintain SPF and DKIM hygiene.



To view the **Recommendations** page, click **DMARC** > **Recommendations**.

To export the data in CSV format, click **Export to CSV**.

Possible recommendations:

- Adding IP addresses to SPF
- Properly configuring RUA mailboxes for your domains
- Implementing a DMARC policy where p=none
- Implementing a restrictive policy for certain domains
    - This is done when the percentage of DMARC failures is below 3%
- and so on.

Monitoring SPF and DMARC Changes

The **DNS Change-Log** page shows changes to the SPF records and the DMARC policies of your domains.

Note - The system synchronizes and updates SPF records every hour to keep them up to date.

To view the **DNS Change-Log** page, click **DMARC** > **DNS Change-Log**.

Column	Description
Date	The date and time of the change.
Domain	The domain whose SPF / DMARC record has changed.
Type	The record type that was changed. ■ DMARC ■ SPF
Current Value	The value after the change.
Changes	The previous value and the new value.
Comments	The custom comments added for the change.

Annotating / Commenting on SPF and DMARC Changes

You and your team can add custom comments to every change. This is helpful in investigating or auditing a specific event.

To add comments to a specific change:

1. Click the ⋮ icon in the last column of the change.
2. Click **Update Comment**.

   The **DMARC Action** pop-up appears.
3. In the **Comments** field, enter the comments.
4. Click **OK**.

SPF Management

SPF Management is included as part of the **DMARC** add-on.

SPF records ensure emails are sent from an authorized server by comparing the sender's IP address with the domain's DNS records.

Benefits

- Overcome SPF limitations with simplified management.
- Configure SPF settings directly in your Avanan Administrator Portal.

- Seamlessly integrate with the DMARC solution for ongoing monitoring and issue resolution.

High-Level Procedure

1. Add the authorized sending sources through the Avanan Administrator Portal. See *"Adding New Source to SPF Records" on the next page*.
2. Activate **SPF Management** by updating the DNS SPF record with the required include statement. See *"Activating SPF Management" on the next page*.
3. Avanan manages authorized sending sources for each domain.
4. Modify sending sources as needed through the Avanan Administrator Portal. See *"Managing Sending Sources" on page 472*.
5. Avanan ensures seamless operation beyond SPF limitations.

Reviewing the SPF Status of your Domains

The **SPF Management** page shows a list of all the organization's protected domains and sub-domains.

To view the **SPF Management** page, access the Avanan Administrator Portal and click **DMARC** > **SPF Management**.

Column	Description
Domain	Domain name.
SPF Monitoring	Monitoring status of the domain. ■ **Managed** - Avanan manages your SPF. ■ **Pending** - The Avanan SPF is not yet active. To activate it, update your domain's SPF record in your DNS to include Avanan's SPF entry. **Note** - DNS records may take some time to propagate across the internet. ■ **Not Managed** - The Avanan does not host your domain's SPF record yet, but the necessary settings are configured and ready for deployment. ■ **Not Available** - **SPF management** is unavailable for `onmicrosoft.com` sub-domains, as Microsoft controls these DNS settings centrally to ensure consistency and security. For full DNS and email authentication control, use a custom domain.
SPF% Success	The percentage of emails that pass SPF out of the total number of reported emails sent by the domain.
Managed sources	Number of managed sources in the domain.

Column	Description
Last Updated	The date and time of the last update.
Hosted Domain	Name of the hosted domain.

Activating SPF Management

Avanan uses the SPF Macro Mechanism, which allows an unlimited number of SPF entries to be defined.

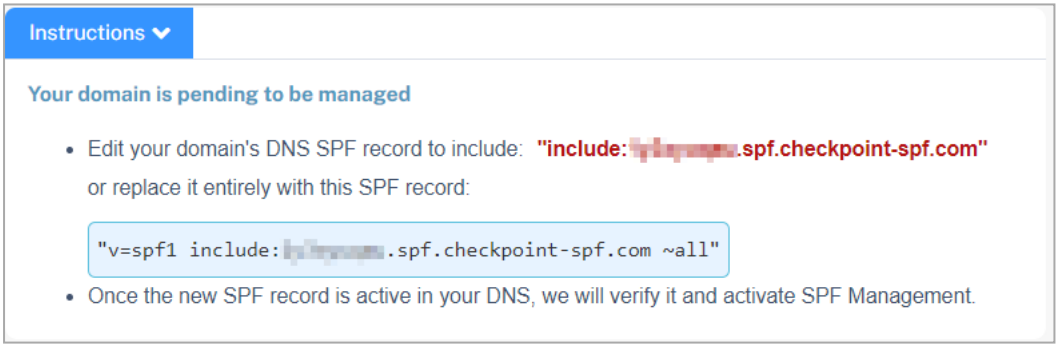
To activate the SPF Management for Avanan, edit your organizational domain's DNS SPF record to include this statement:

```
include:{code}.spf.checkpoint-spf.com
```

or replace it entirely with this SPF record:

```
v=spf1 include:{code}.spf.checkpoint-spf.com ~all
```

where `{code}` is the unique code specific to your organization. You can find the code from the **Instructions** widget.



Once the new SPF record is active in your DNS, Avanan verifies it and activates **SPF Management**.

Adding New Source to SPF Records

To manually add a new source to your SPF record:

1. On the **SPF Management** page, click the domain to which you need to add a source.
2. Click **Insert Source** next to the **Instructions** at the top of the page.
3. In the pop-up that appears, select the mechanism from the **Mechanism** list.
    - **ip4**: Matches specified IPV4 or IPV6 addresses
    - **ip6**: Matches specified IPV4 or IPV6 addresses

- **include**: Use SPF rules from another domain
- **a**: Matches domain's A or AAAA records
- **mx**: Matches domain's MX records
- **exists**: Matches if a DNS query returns a result

4. In the **Value** field, enter the value relevant to the selected **Mechanism**.

   Examples of **Value** for different **Mechanisms**:

   - **ip4**:
     - Single IP: 192.0.2.1
     - Subnet: 192.0.2.1/16
   - **ip6**:
     - Single IP: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
     - Subnet: 2001:db8::/32
   - **include**: _spf.example.com
   - **a**: Specify a domain or leave it blank
   - **mx**: Specify a domain or leave it blank
   - **exists**: %{i}._spf.example.com
5. In the **Notes** field, enter the description as required.
6. Click **OK**.

To add a new source to your SPF record from a list of known sources:

1. On the **SPF Management** page, click the domain to which you need to add a source.
2. Click **Add Source from List** next to the **Instructions** at the top of the page.
3. In the **Source** section, select the required source and click **OK**.

Configuring the SPF Record

By using these SPF qualifiers in the SPF record, you can define the action for emails sent from unauthorized sources.

- **Fail (-all)**: Rejects the email (Recommended).
- **SoftFail (~all)**: Flags the email as a SoftFail and may be rejected.

- **Allow (+all)**: Allows the email.

  Important - Avanan recommends avoiding this qualifier, as it allows any IP address to send emails on behalf of your domain.

- **None**: It defines no specific action.

  Note - Ensure that your domain has a default SPF policy.

Defining the SPF Record

You should configure the main SPF record with the appropriate policy in your DNS settings.

Note - Since SPF is managed at the DNS level, you do not need to configure the policy in the Avanan Administrator Portal. These settings will not impact the SPF evaluation result.

Managing Sending Sources

You can manage your authorized sending sources as required. To do that, click the ⋮ icon from the last column of the Sending Sources table.

- To insert the source, click **Insert Source Above / Below**. In the pop-up that appears, select the required options and click **OK**.

  You can also click **Insert Source** directly next to the **Instructions** at the top of the page. In the pop-up that appears, select the required options and click **OK**.

- To delete a source, click **Delete Source**. In the confirmation pop-up that appears, click **OK**.

- To update the source, click **Update Source**. In the pop-up that appears, make the necessary changes and click **OK**.

- To modify the prefix of the **all** element in your SPF record, click **Update Prefix**. In the **Update Prefix** pop-up that appears, make the necessary changes and click **OK**.

  Note - This option is available only for sources with a preconfigured prefix.

After making the changes, click **Save & Update** to generate the SPF record based on the configured sources.

Column	Description
Status	Status of the sending source. ■ ✔ - Active ■ ⏸ - Non-Active

Column	Description
Prefix	Action for the email source.
Type	Type of the element.
Value	Value of the mechanism.
Notes	Description of the sending source.
Warnings	Description of the warnings, if any.

DKIM Management

DKIM Management is included as part of the **DMARC** add-on.

DKIM records ensure emails are cryptographically signed to verify their authenticity and integrity.

Benefits

- Prevents email spoofing.
- Simplify DKIM management without needing to update records at your DNS provider every time.
- Configure DKIM settings directly in your Avanan Administrator Portal.
- Seamlessly integrate with the DMARC solution for ongoing monitoring and issue resolution.

High-Level Procedure

1. Add the required selectors through the Avanan Administrator Portal. See *"Adding New DKIM Selector to your Domain" on page 475*.
2. Activate **DKIM Management** by updating the domain's DNS NS record with the required value. See *"Activating DKIM Management" on the next page*.
3. Avanan manages selectors for each domain.
4. Modify selectors as needed through the Avanan Administrator Portal. See *"Managing Selectors" on page 475*.
5. Avanan ensures seamless operation, eliminating the need to update DKIM records in your DNS every time.

Reviewing the DKIM Status of your Domains

The **DKIM Management** page shows a list of all the organization's protected domains and sub-domains.

To view the **DKIM Management** page, access the Avanan Administrator Portal and click **DMARC** > **DKIM Management**.

Column	Description
Domain	Domain name.
DKIM Monitoring	Monitoring status of the domain. ■ **Managed** - Avanan manages your DKIM. ■ **Pending** - The Avanan DKIM is not yet active. To activate it, update your domain's NS record in your DNS. **Note** - DNS records may take some time to propagate across the internet. ■ **Not Managed** - The Avanan does not host your domain's DKIM record yet.
DKIM% Success	The percentage of emails that pass DKIM out of the total number of reported emails sent by the domain.
Managed Selectors	Number of managed selectors in the domain.
Last updated	The date and time of the last update.
Hosted Name Servers	Names of the hosted servers.

Activating DKIM Management

Avanan allows an unlimited number of DKIM entries to be defined.

To activate DKIM Management for Avanan:

1. Add all your selectors to the domain's DKIM Management page. See *"Adding New DKIM Selector to your Domain" on the next page*.
2. If required, insert DNS NS records for your subdomains.
3. Click **Save & Update** to activate the selectors.

   Once the selectors are activated, the system shows your Name Servers.
4. Avanan verifies the updated DNS NS record and activates **DKIM Management**.

Adding New DKIM Selector to your Domain

To manually add a new DKIM selector to your domain:

1. On the **DKIM Management** page, click the domain to which you need to add a selector.
2. Click **Insert Selector** next to the **Instructions** at the top of the page.
3. In the pop-up that appears, enter a unique selector name in the **Selector** field.
4. In the **Type CNAME/TXT** field, select the required option from the list.
   - **CNAME**: URL to another domain
   - **TXT**: DKIM public key
5. In the **Value** field, enter the value relevant to the selected **Type CNAME/TXT**.
6. (Optional) In the **Notes** field, enter the description as required.
7. In the **Service** field, enter the service that the selector is used for.
8. (Optional) Select the **t=s?** checkbox to support only exact domain signing.

   If you select this checkbox, the DKIM signature is valid only for the exact domain in the record.

   For example, if you select this checkbox and the domain is *example.com*, any email sent from *sales.example.com* will not pass DKIM validation using the existing key for *example.com*. To enable DKIM for *sales.example.com*, you must add a separate DKIM record.
9. Click **OK**.

Managing Selectors

You can manage your authorized selectors as required. To do that, click the ⋮ icon from the last column of the Selectors table.

- To insert the selector, click **Insert selector Above / Below**. In the pop-up that appears, select the required options and click **OK**.

  You can also click **Insert Selector** directly next to the **Instructions** at the top of the page. In the pop-up that appears, select the required options and click **OK**.
- To delete a selector, click **Delete Selector**. In the confirmation pop-up that appears, click **OK**.
- To update the selector, click **Update Selector**. In the pop-up that appears, make the necessary changes and click **OK**.

After making the changes, click **Save & Update** to generate the DKIM record based on the configured selectors.

Column	Description
Status	Status of the selector. ■ - Active ■ - Non-Active
Selector	Unique name of the selector.
Type	Type of the element.
Value	Value of the CNAME/TXT.
Notes	Description of the selector.
Service	Name of the service.
t=s	Status of the selector to support only exact domain signing. ■ True ■ False
Warnings	Description of the warnings, if any.

Security Awareness Training

The **Security Awareness Training** feature in Avanan helps organizations create awareness among employees on essential security skills. It includes awareness of phishing simulation emails reflecting recent attacks and interactive training modules.

Note - The **Security Awareness Training** is supported only for **Exchange Online** (Microsoft 365 cloud) mailboxes.

Creating Security Awareness Training Policy

To create a security awareness training policy:

1. Access the Avanan Administrator Portal.
2. From the left navigation panel, click **Security Training** > **Policy**.
3. Click **Create New Policy Rule**.
4. Make sure the **Rule state** is **Running**.
5. (Optional) In the **Rule name** field, enter a name for the policy.
6. Click **Save**.

   Note - By default, the security awareness training policy is applied to all the Microsoft 365 users in your organization.

Customizing Security Awareness Training Policy

To customize the security awareness training policy:

1. Click on the security awareness training policy you want to customize.
2. In the **Users and groups** section, select the users and/or group of users for whom the policy is applicable:
   - To apply the policy to all users and groups in your organization, select **All Office 365 users**.
   - To apply the policy to specific users or groups, select the users/groups and click **Add to Selected**.
3. Select a **Phishing Simulation Strategy**:

- **Prioritize the past attack types of the user** - Sends phishing simulation emails that reflect recent attack types faced by the users in your organization.
- **None, do not perform simulations** - No simulation emails are sent to the users.

4. (Optional) To view the phishing email templates used to send simulation emails to users, click **Generated Phishing Simulations (samples)**.

   To view generated phishing simulation samples based on a user's recent communication patterns, enter the user's email address and click **Generate**.

5. In the **Frequency** section, select the required frequency of the simulation emails.
   - Daily
   - Weekly
   - Biweekly
   - Monthly
   - Quarterly
   - Yearly

   Note - By default, the frequency of the simulation emails is set to Biweekly.

6. In the **Send randomly on** section, select the days to randomly send simulation emails to users.
   - Monday
   - Tuesday
   - Wednesday
   - Thursday
   - Friday
   - Saturday
   - Sunday
7. In the **Time Range Start** section, select the start time to send emails on the selected days.
8. In the **Time Range End** section, select the end time to stop sending emails on the selected days.

   Note - By default, the time range is set to 9:00 AM to 18:00 PM.

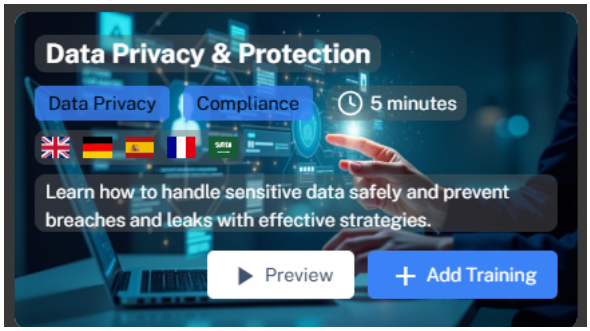
9. In the **Select Time Zone** section, select the required time zone.

Note - By default, the time zone is set to (UTC +00:00) UTC.

10. Select the **Training Modules**.
    i. Click **Select training modules**.

    The **Select Training Module** pop-up displays the available training modules.

    Each module provides the following details:



    - The training module name and key concepts in the module.
    - The time duration shows the time required to complete the module.
    - The flags represent the languages available for the training module.
    - (Optional) To view a preview of the training module, click **Preview**.

    ii. Click **Add Training** for the required modules.

    iii. Click **Save**.

Note - The deadline for completing each training is 14 days.

11. The **Selected training modules** section shows the order of the modules assigned to the user.
    - To arrange the training modules in the required order:
        a. Click the icon.
        b. Move the module to the desired position in the order and drop it.
    - To remove a selected training module, click the icon.
12. To configure settings for the training and reminders for the email notifications, click **Advanced settings** and do these:

a. In the **Training max frequency (days)** field, enter the number of days after which the system initiates a new training session.

b. In the **Training reminder interval** field, enter the number of days after which the system sends a reminder. For example, if you enter 2, the system sends reminder after every 2 days.

c. To configure email notifications for the training and reminders:

- In the **Training invitation subject** field, enter the subject for the training invitation email.
- In the **Training invitation body template** field, enter the body for the training invitation email.
- In the **Training remind subject** field, enter the subject for the training reminder email.
- In the **Training remind body template** field, enter the body for the training reminder email.

To view the supported placeholders, see *"Training and Reminder Emails - Supported Placeholders" on page 483*.

d. Click **Save**.

13. Click **Save**.

Note - Now that the security awareness training policy is configured, the end users receive an email with a link to access the training modules. To allow users to access the training modules, the administrator must authenticate by granting the necessary permissions.

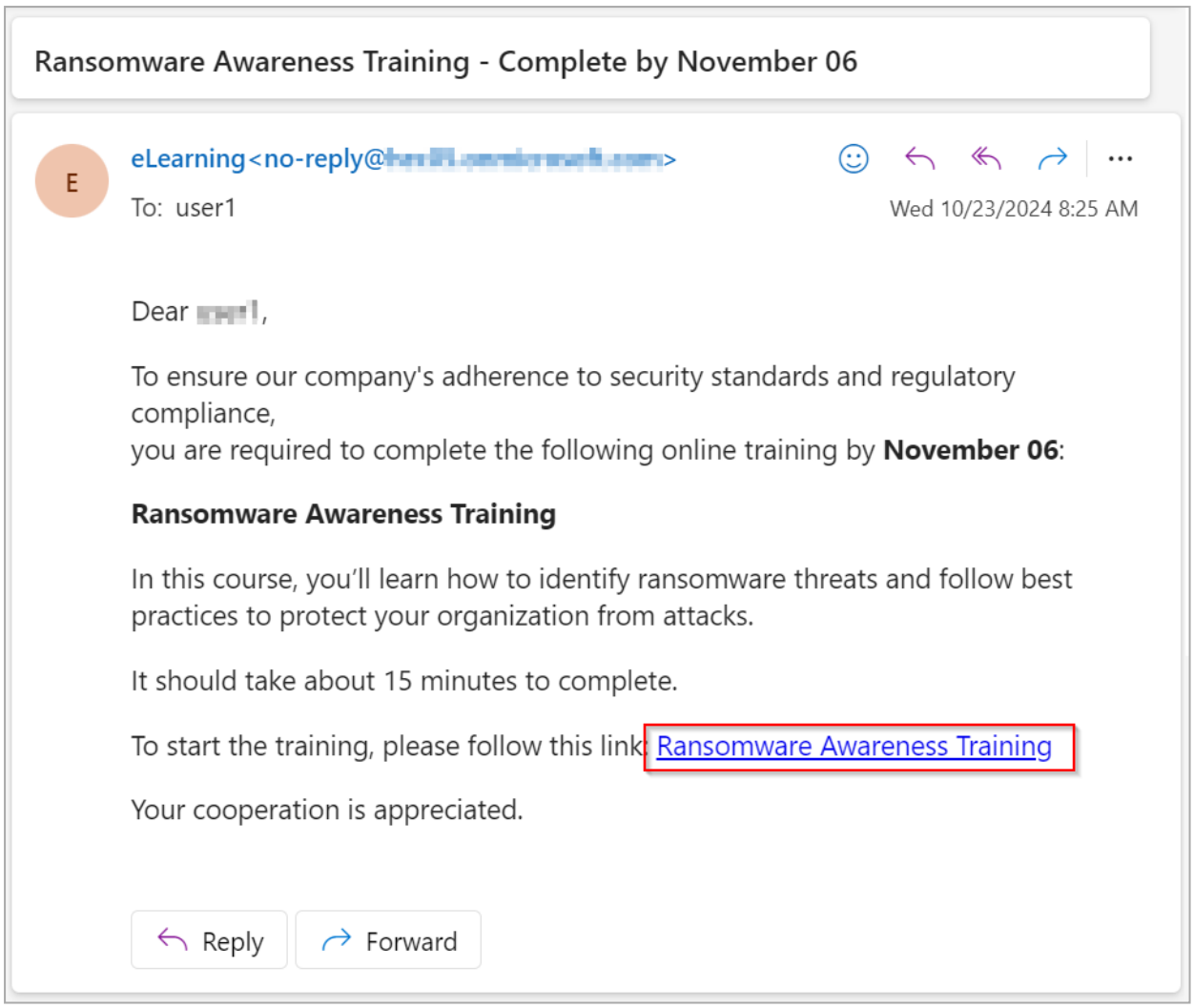
Authorizing Training Module Access for the Organization

Avanan allows users to access the training modules using the link provided in the email notification.

The administrator must authorize access for the entire organization by granting the necessary permissions.

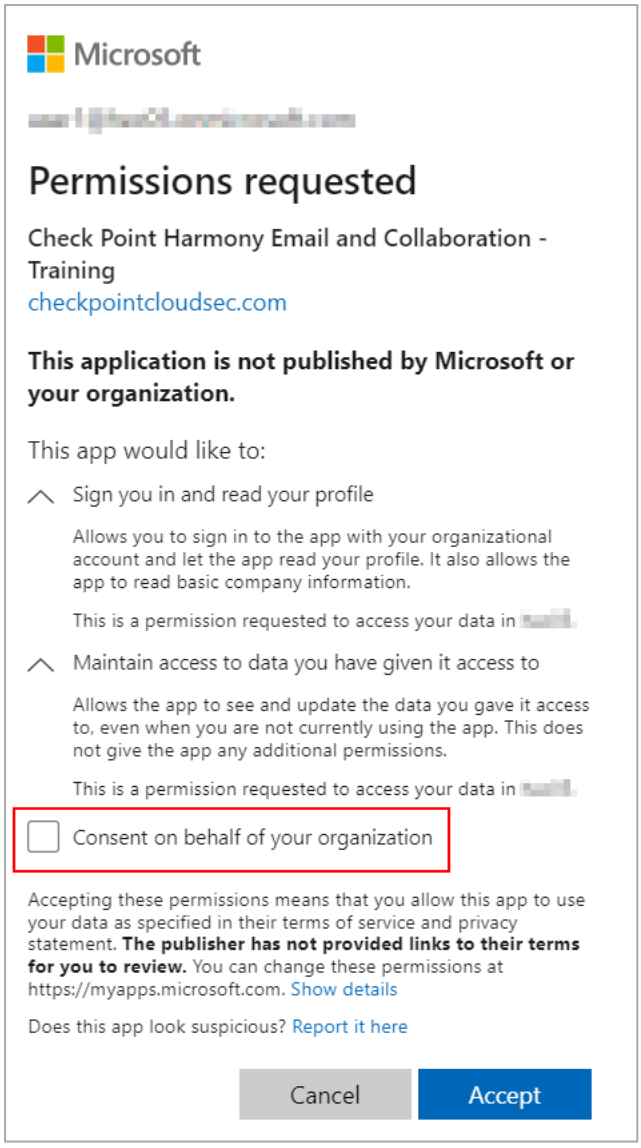
To authorize the Microsoft login permissions for training modules:

1. Click on the link provided in the email.



2. Click **Sign in with Microsoft**.
3. Enter the admin credentials and sign in.

   The **Permissions requested** pop-up appears for the **Avanan Avanan - Training** application and requests the necessary permissions. See *"Required Permissions for Microsoft Login Authorization" on the next page*.
4. To allow end users to sign in using Microsoft credentials, select the **Consent on behalf of your organization** checkbox.



5. Click **Accept**.

   End users can now sign in with their organization's Microsoft credentials using the link provided in the email to access the training modules.

Required Permissions for Microsoft Login Authorization

Permissions required from Microsoft/Google	Functions performed by Harmony Email & Collaboration
Sign you in and read your profile	Allows users to sign in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Maintain access to data you have given it access to	Allows the app to view and update the signed-in user data even when you are not currently using the app.

Training and Reminder Emails - Supported Placeholders

While configuring email notifications for training and reminders in **Security Awareness Training**, the administrators can use these placeholders to replace content dynamically.

Placeholder Name	Placeholder Value
Email recipient name	{recipient_name}
Training module name	{training_name}
Training module description	{training_description}
Date before which the training module must be completed	{training_due_date}
Length of the training mode in minutes or hours	{training_duration}
Number of days remaining to complete the training module	{training_days_left}

Branding the Security Awareness Training Web Page

To customize the training module interface and phishing simulation web pages to reflect your organization's branding:

1. Go to **Security Training** > **Policy**.
2. Click **Configuration** next to **Security training policies** from the top of the page.
3. In the **Branding of user interaction (landing pages, course screens)** section, select one of these:
   - To show the web pages and course screens that matches your organization's branding, select **Auto-brand pages with AI for my domain (recommended)**. Avanan uses AI and auto-brands the pages based on your organizational domain.
   - To use Check Point's branding, select **Use Check Point branding**.
4. Click **Save**.

Security Awareness Training Domains

While emails will be delivered, some URLs may be blocked upon clicking due to security tools. To prevent this, allowlist the following domains and their subdomains for both senders and links in your non-Avanan security solutions.

login-microsoftonline.co

- us.login-microsoftonline.co
- eu.login-microsoftonline.co
- au.login-microsoftonline.co
- me.login-microsoftonline.co
- ca.login-microsoftonline.co
- uk.login-microsoftonline.co
- in.login-microsoftonline.co

office356.co

- us.office356.co
- eu.office356.co
- au.office356.co
- me.office356.co
- ca.office356.co
- uk.office356.co
- in.office356.co

office356.email

- us.office356.email
- eu.office356.email
- au.office356.email
- me.office356.email
- ca.office356.email
- uk.office356.email
- in.office356.email

redeem-amazon.com

- us.redeem-amazon.com
- eu.redeem-amazon.com
- au.redeem-amazon.com

- me.redeem-amazon.com
- ca.redeem-amazon.com
- uk.redeem-amazon.com
- in.redeem-amazon.com

tracking-amazon.com

- us.tracking-amazon.com
- eu.tracking-amazon.com
- au.tracking-amazon.com
- me.tracking-amazon.com
- ca.tracking-amazon.com
- uk.tracking-amazon.com
- in.tracking-amazon.com

update-fedex.com

- us.update-fedex.com
- eu.update-fedex.com
- au.update-fedex.com
- me.update-fedex.com
- ca.update-fedex.com
- uk.update-fedex.com
- in.update-fedex.com

training-cp.com

- us.training-cp.com
- ca.training-cp.com
- eu.training-cp.com
- uk.training-cp.com
- au.training-cp.com
- me.training-cp.com
- in.training-cp.com

fedex.email

- us.fedex.email
- ca.fedex.email
- eu.fedex.email
- uk.fedex.email
- au.fedex.email
- me.fedex.email
- in.fedex.email

dnc.cloud

- us.dnc.cloud
- ca.dnc.cloud
- eu.dnc.cloud
- uk.dnc.cloud
- au.dnc.cloud
- me.dnc.cloud
- in.dnc.cloud

rnc.cloud

- us.rnc.cloud
- ca.rnc.cloud
- eu.rnc.cloud
- uk.rnc.cloud
- au.rnc.cloud
- me.rnc.cloud
- in.rnc.cloud

avnn.us

- us.avnn.us
- ca.avnn.us
- eu.avnn.us

- uk.avnn.us
- au.avnn.us
- me.avnn.us
- in.avnn.us

Monitoring User Interactions with Phishing Simulations

The **Security Training Dashboard** shows an overview of training completion and phishing simulation performance for organization members using widgets, charts, and tables. It also shows individual training statuses and user details, enabling administrators to analyze the organization's security awareness and readiness against phishing threats.

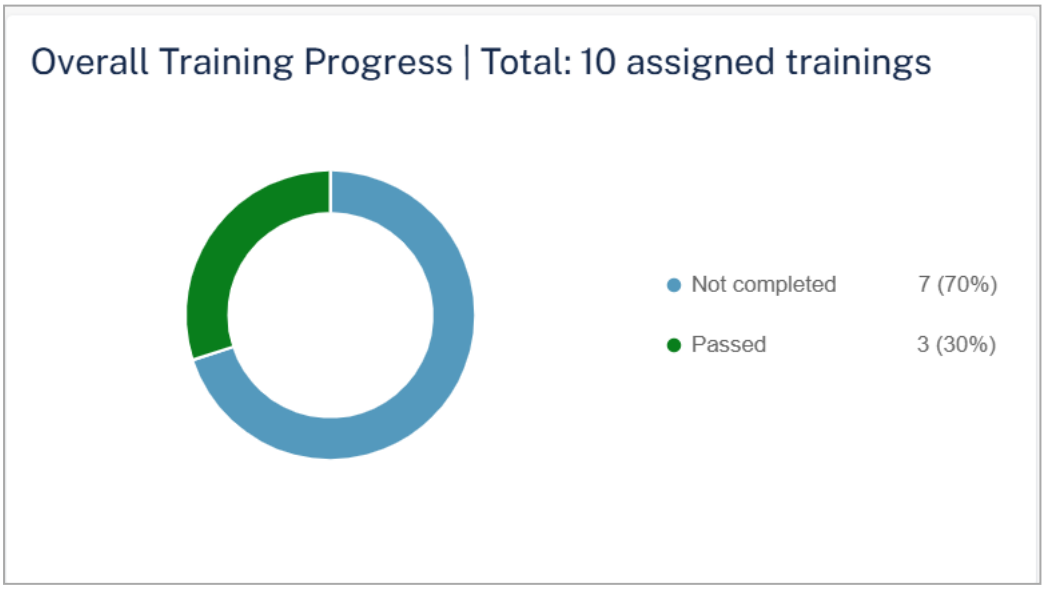
To view the **Dashboard** page, click **Security Training** > **Dashboard**.

To select a time frame for the **Dashboard**, select an option from the dropdown next to **Dashboard** at the top of the page.

- Last 24h
- Last 7 days
- Last 30 days
- Last 12 months
- Custom

To export the details to a PDF, click **Export to PDF**.

Overall Training Progress

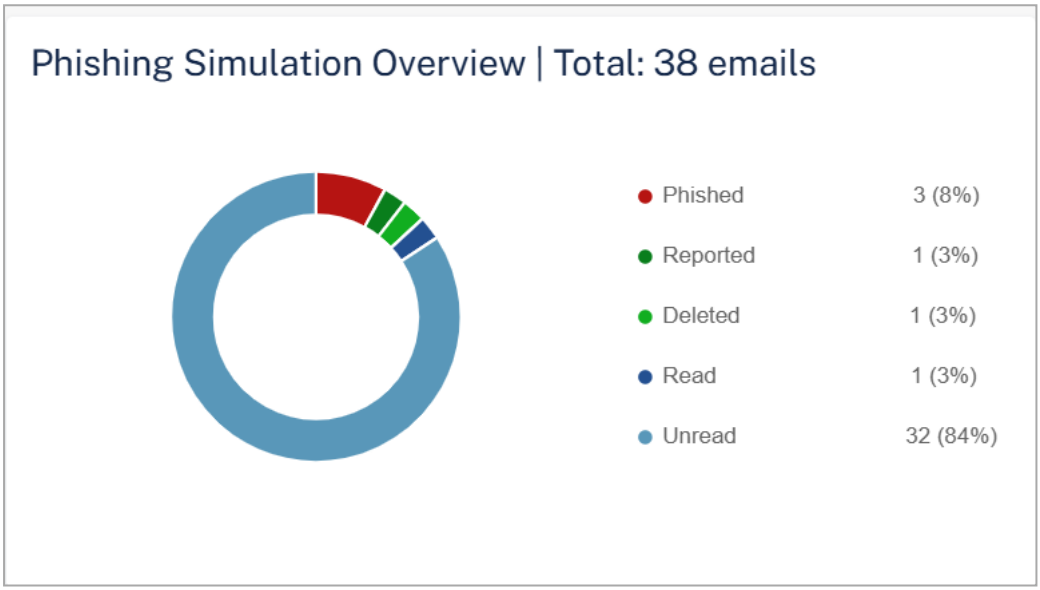


The **Overall Training Progress** widget shows the number of trainings assigned and their status in the selected time frame.

- Passed
- Failed
- Not Completed

To view specific assigned trainings, click the relevant field in the widget, and the system shows the filtered trainings on the Users page.

Phishing Simulation Overview



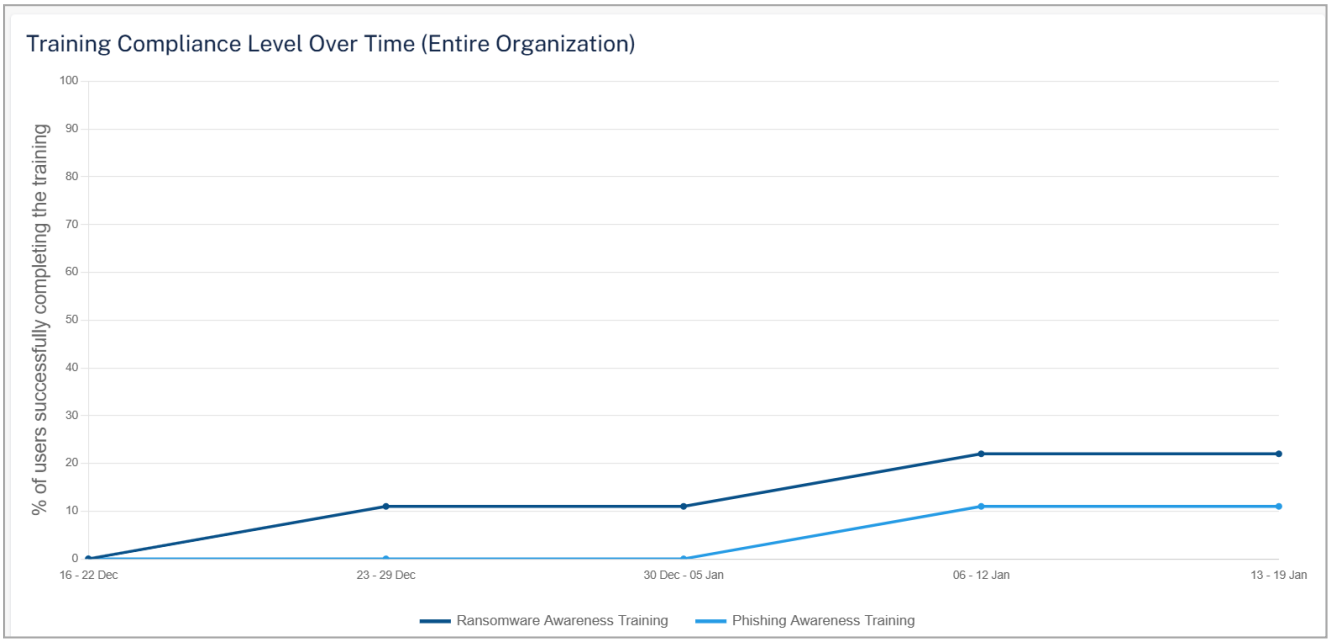
The **Phishing Simulation Overview** widget shows the number of phishing simulation emails sent and their status in the selected time frame.

- Unread
- Read
- Deleted
- Reported
- Phished
    - Clicked
    - Scanned QR Code
    - Replied
    - Forwarded
    - Opened attachment

- Called unknown number
- Shared data

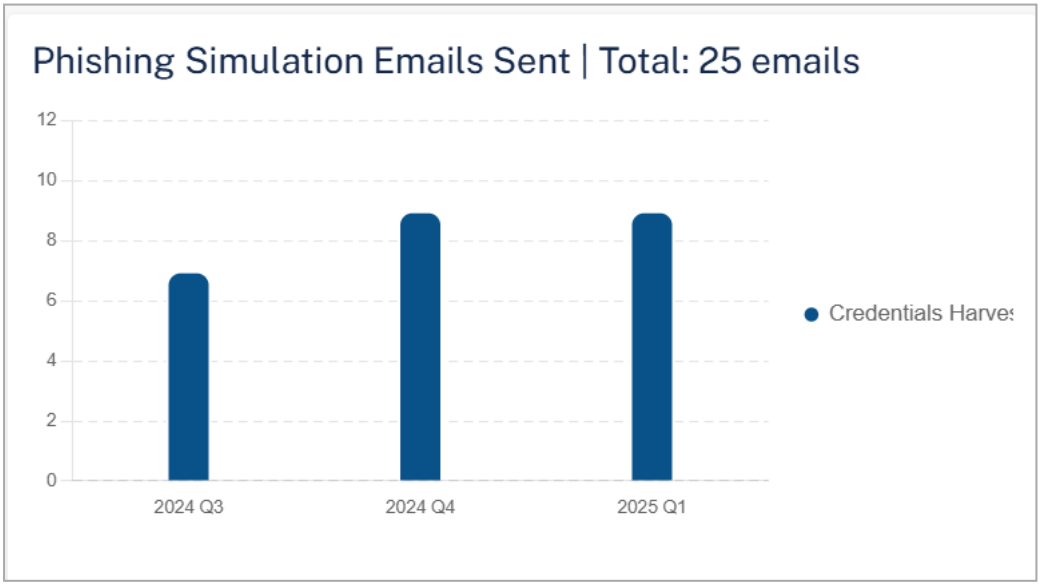
To view specific phishing simulations, click the relevant field in the widget, and the system shows the filtered phishing simulations on the Users page.

Training Compliance Level Over Time (Entire Organization)



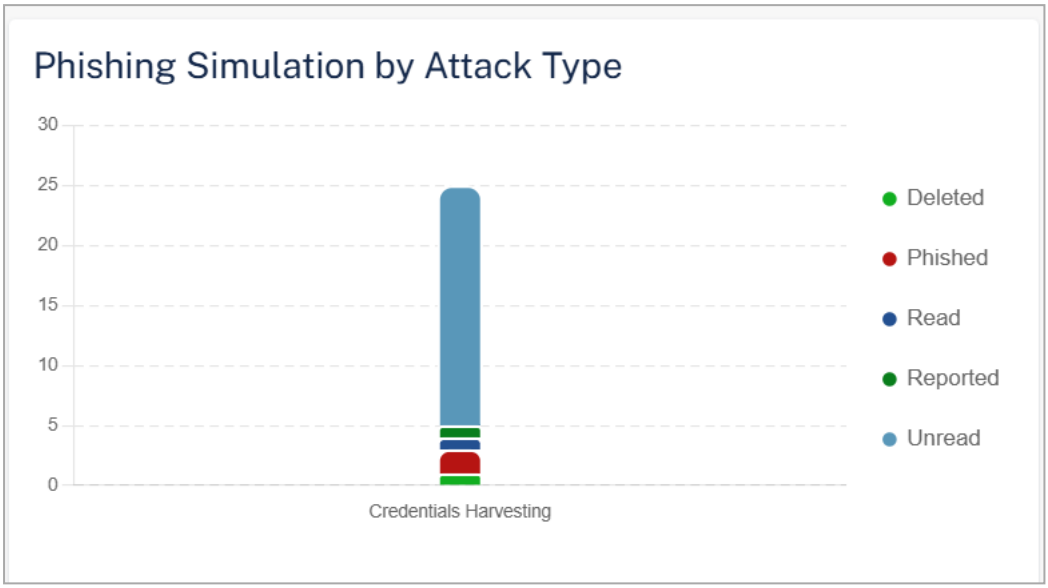
The **Training Compliance Level Over Time (Entire Organization)** widget shows the percentage of users in the organization who have completed the training in the selected time frame.

Phishing Simulation Emails Sent



The **Phishing Simulation Emails Sent** widget shows the total number of phishing simulation emails sent and their status in the selected time frame.

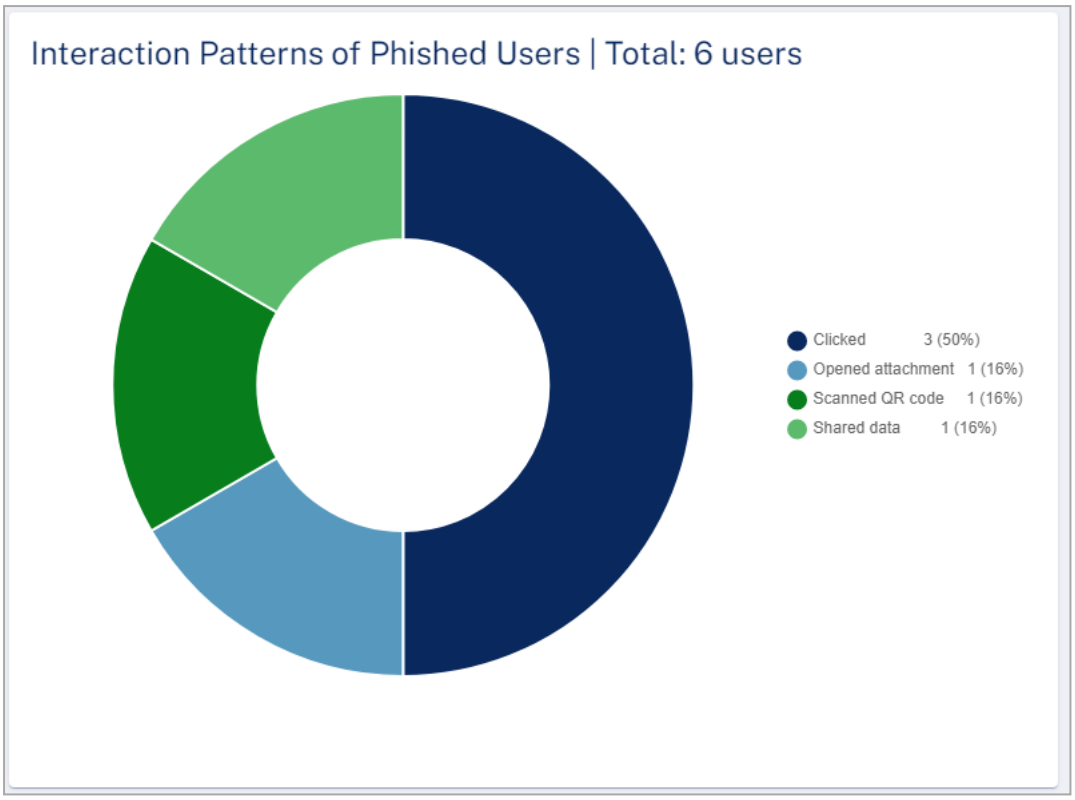
Phishing Simulation by Attack Type



The **Phishing Simulation by Attack Type** widget shows the number of phishing simulation emails sent based on the attack type in the selected time frame.

To view specific phishing simulation details based on the attack type, click the relevant field in the widget, and the system shows the filtered phishing simulations by attack type on the Users page.

Interaction Patterns of Phished Users



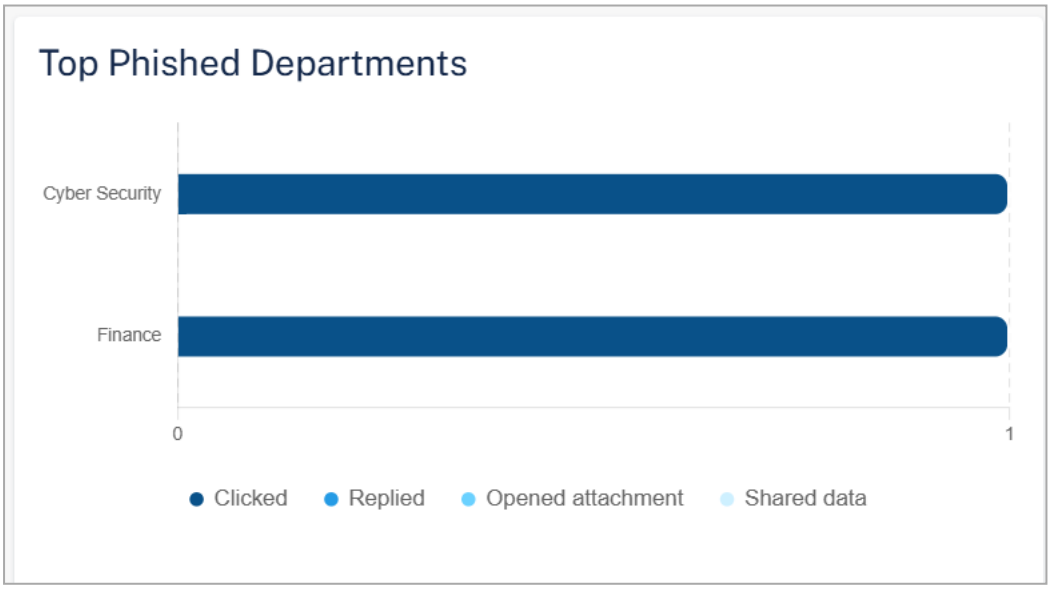
The **Interaction Patterns of Phished Users** widget shows the total number of phished emails and their interaction status in the selected time frame.

To view specific phished emails and their interactions, click the relevant field in the widget, and the system shows the filtered interactions of phished users on the Users page.

Phishing Simulation - Failure Rate Over Time

The **Phishing Simulation - Failure Rate Over Time** widget shows the percentage of emails that have failed the simulation in the selected time frame.

Top Phished Departments



The **Top Phished Departments** widget shows the top ten departments in the organization with the most phished users in the selected time frame.

To view specific department in the organization with the most phished users, click the relevant field in the widget, and the system shows the filtered departments on the Users page.

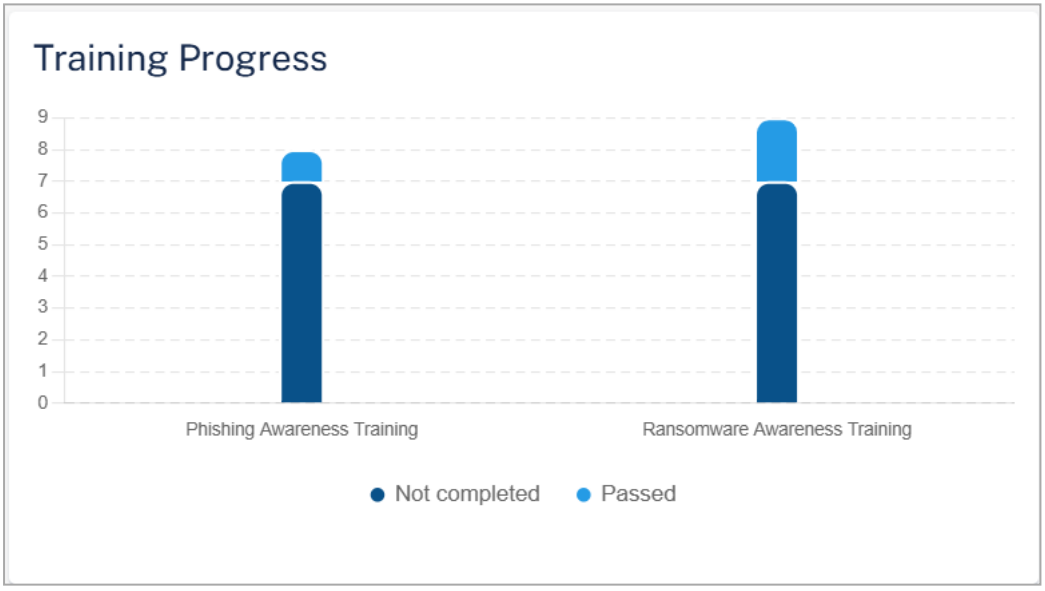
Top Phished Users

The **Top Phished Users** table shows the users that are phished more times in the selected time frame.

Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Failures	Number of phishing emails opened.

Monitoring User Training Progress

Training Progress



The **Training Progress** widget shows the training modules and their status in the selected time frame.

Training Status

The **Training Status** table shows the status of each training module.

Column	Description
Training	Training module name
Policy	Name of the policy.

Column	Description
Start Date	Date on which the training module is assigned to the users.
Training Status	Training status: ■ Not Started ■ In progress ■ Completed
Users	Users that are assigned the training module.
Passed	Percentage of users that have passed in the training module.
Failed	Percentage of users that have failed in the training module.
Not Completed	Percentage of users that have not started the training module.

Users

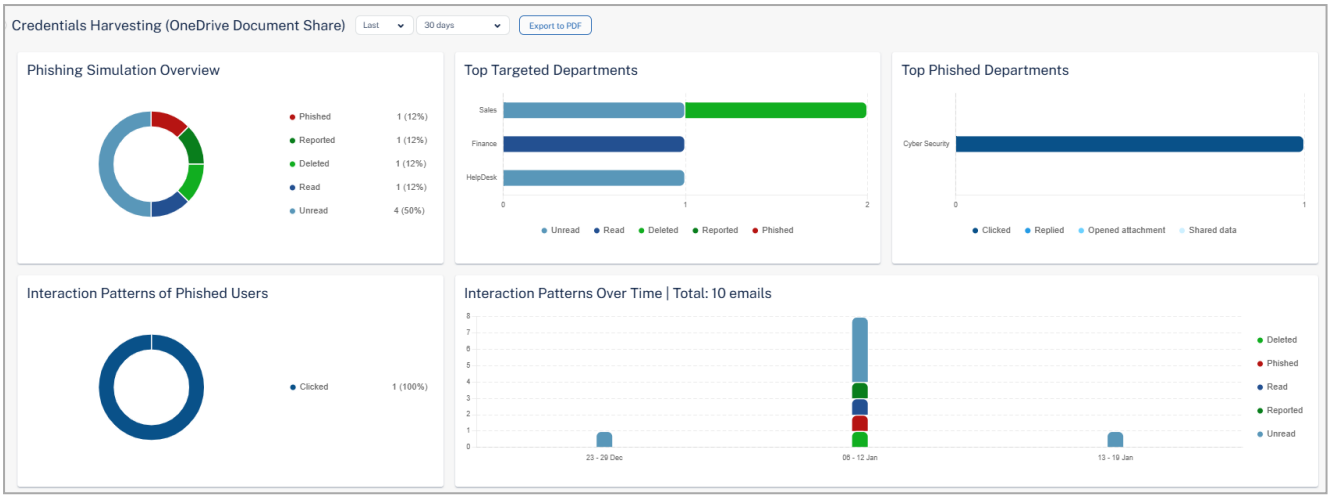
The **Users** table shows the phishing simulation emails sent to the users and their training status in the selected time frame.

Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Phishing Simulation	Type of simulation email sent to the user and their status. Click on the simulation name to view analytics filtered specifically for that simulation. See Monitoring Phishing Simulations.
Awareness Training	Training module name and their status. Click on the training module name to view analytics filtered specifically for that module. See Monitoring User Awareness Training Progress.

Monitoring Phishing Simulations

To view the details of a specific phishing simulation, click on the required phishing simulation name in the **Phishing Simulation** column of the **Users** table.

Avanan redirects you to the relevant phishing simulation dashboard.



To select a time frame for the phishing simulation, select an option from the drop-down next to the phishing simulation name at the top of the page.

- Last 24h
- Last 7 days
- Last 30 days
- Last 12 months
- Custom

To export the details to a PDF, click **Export to PDF**.

Phishing Simulation Overview

The **Phishing Simulation Overview** widget shows the number of phishing simulation emails sent and their status for the selected phishing simulation in the selected time frame.

- Unread
- Read
- Deleted
- Reported
- Phished
    - Clicked
    - Scanned QR Code
    - Replied
    - Forwarded
    - Opened attachment

- Called unknown number
- Shared data

Top Targeted Departments

The **Top Targeted Departments** widget shows the top ten targeted departments in the organization with the most phished users for the selected phishing simulation in the selected time frame.

Top Phished Departments

The **Top Phished Departments** widget shows the top ten departments in the organization with the most phished users for the selected phishing simulation in the selected time frame.

- Clicked
- Replied
- Opened attachment
- Shared data

Interaction Patterns of Phished Users

The **Interaction Patterns of Phished Users** widget shows the total number of phished emails and their interaction status for the selected phishing simulation in the selected time frame.

- Clicked
- Replied
- Opened attachment
- Shared data
- Scanned QR Code

Interaction Patterns Over Time

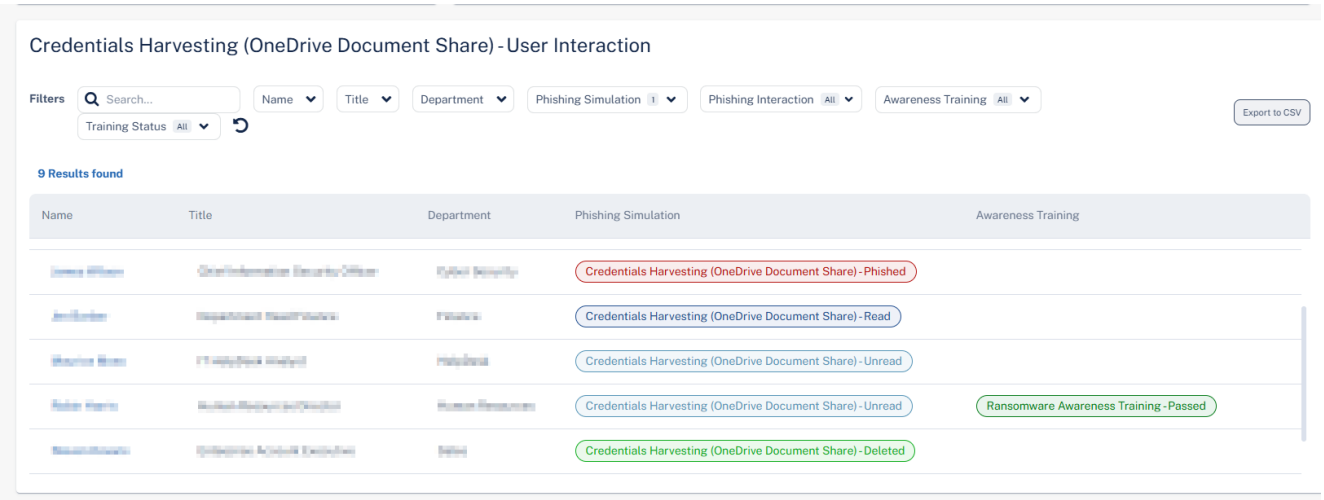
The **Interaction Patterns Over Time** widget shows the total number of phished emails sent to the users and their interaction status for the selected phishing simulation in the selected time frame.

- Unread
- Read
- Deleted
- Reported

- Phished
- Scanned QR Code

User Interaction

The **User Interaction** table shows the phishing simulation emails sent to the users and their training status in the selected time frame.



Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Phishing Simulation	Type of simulation email sent to the user and their status. Click on the simulation name to view analytics filtered specifically for that simulation. See Monitoring Phishing Simulations.
Awareness Training	Training module name and their status. Click on the training module name to view analytics filtered specifically for that module. See Monitoring User Awareness Training Progress.

Monitoring User Awareness Training Progress

To view the progress of a specific training module, click on the training module name in the **Awareness Training** column of the **Users** table.

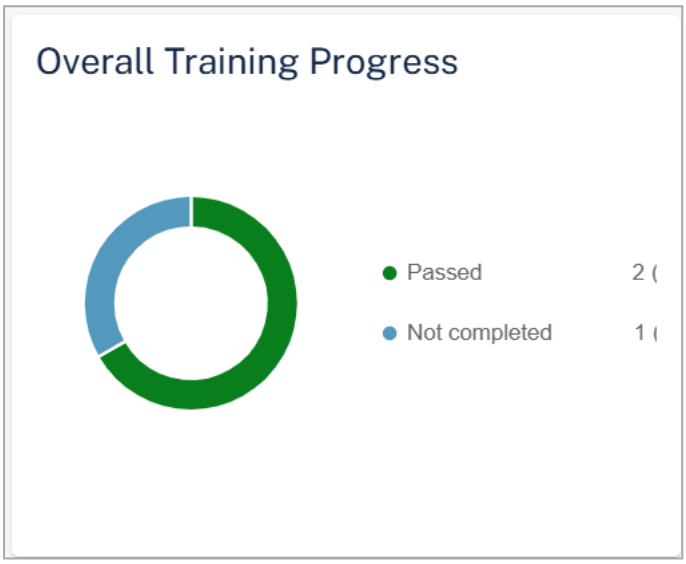
Avanan redirects you to the relevant awareness training module progress dashboard.

To select a time frame for the training module, select an option from the drop-down next to the awareness training module name at the top of the page.

- Last 24h
- Last 7 days
- Last 30 days
- Last 12 months
- Custom

To export the details to a PDF, click **Export to PDF**.

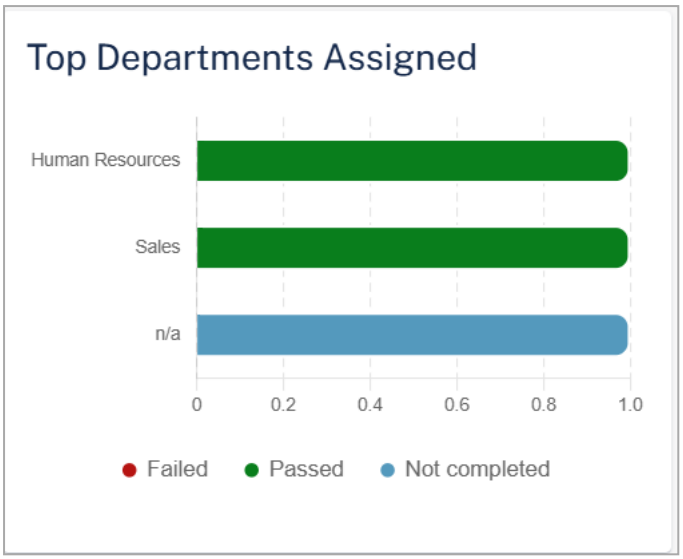
Overall Training Progress



The **Overall Training Progress** widget shows the number of training modules and their status for the selected training module in the selected time frame.

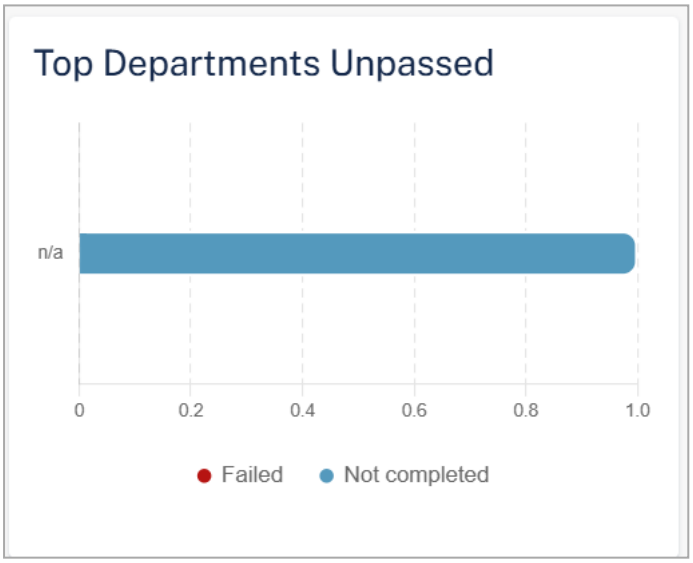
- Passed
- Failed
- Not Completed

Top Departments Assigned



The **Top Departments Assigned** widget shows the top ten departments in the organization assigned to the selected training module and their status in the selected time frame.

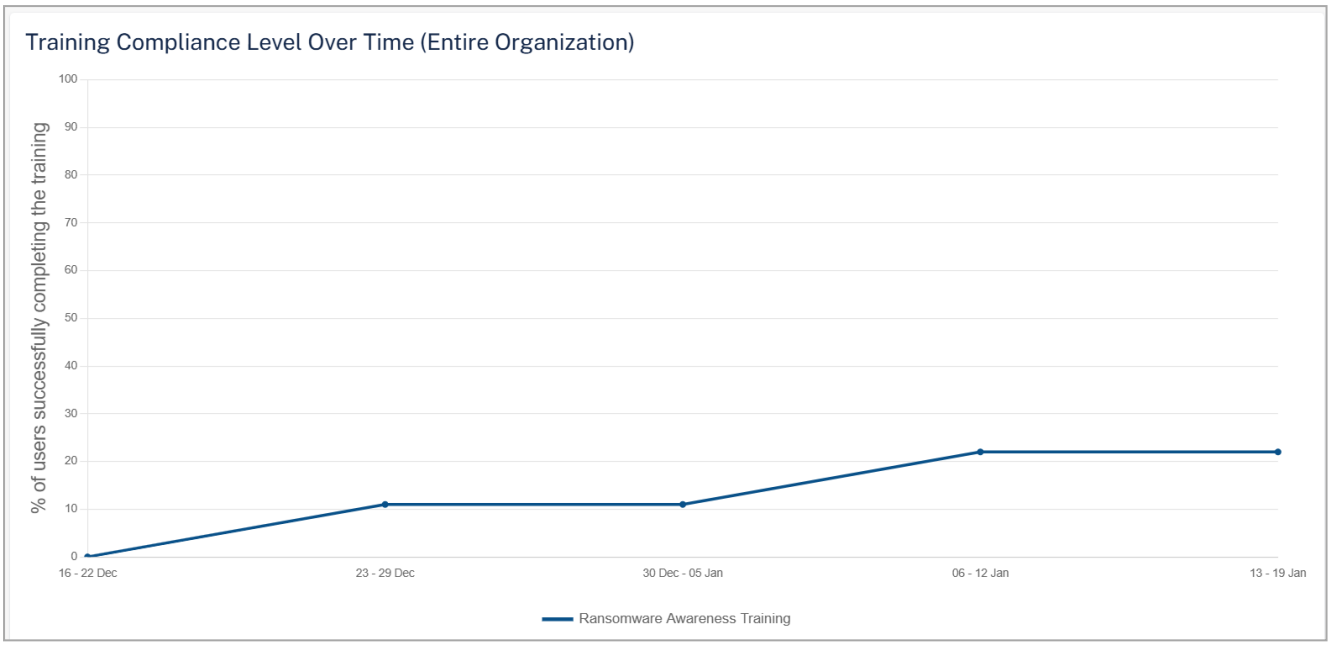
Top Departments Unpassed



The **Top Departments unpassed** widget shows the top ten departments in the organization that did not pass the selected training module in the selected time frame.

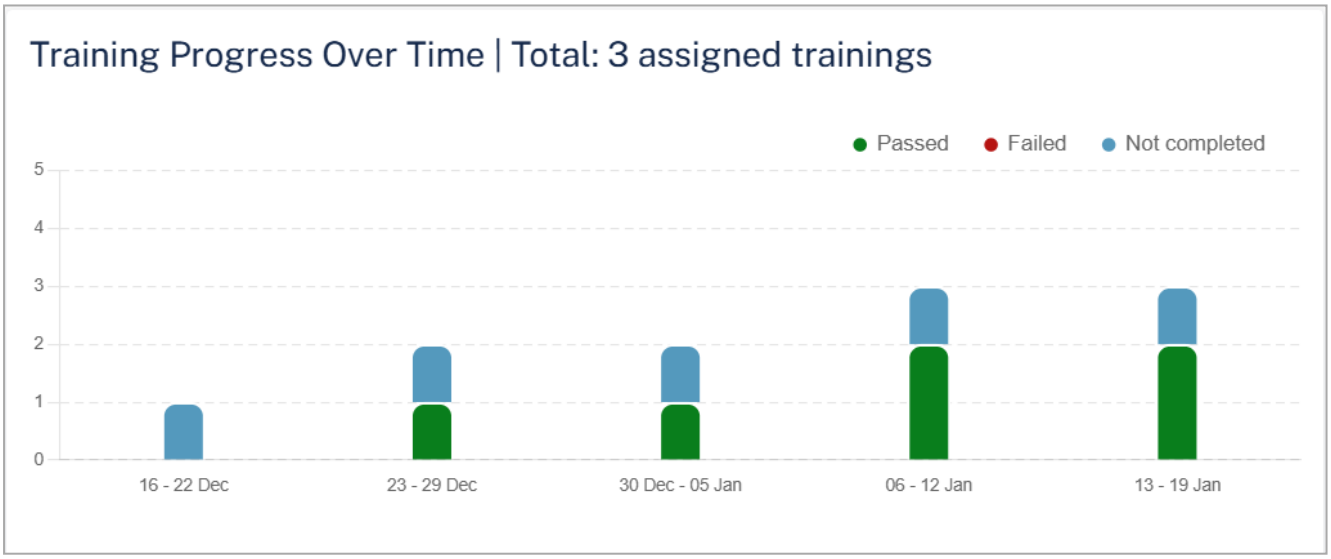
- Failed
- Not Completed

Training Compliance Level Over Time (Entire Organization)



The **Training Compliance Level Over Time (Entire Organization)** widget shows the percentage of users in the organization who completed the training for the selected training module in the selected time frame.

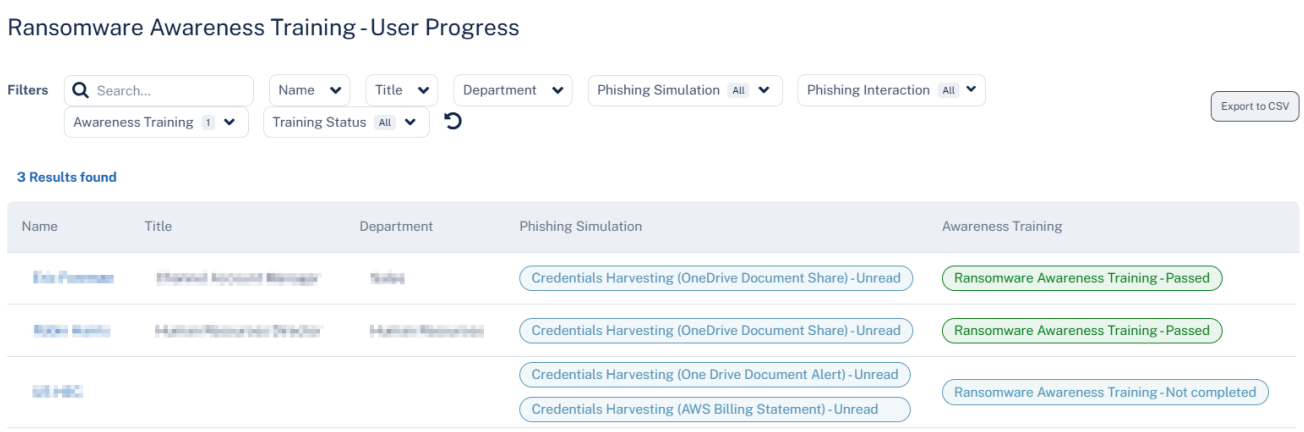
Training Progress Over Time



The **Training Progress Over Time** widget shows the number of trainings assigned and their status for the selected training module in the selected time frame.

User Progress

The **User Progress** table shows the phishing simulation emails sent to the users and their training status in the selected time frame.



Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Phishing Simulation	Type of simulation email sent to the user and their status.
Awareness Training	Training module name and their status.

Training Log

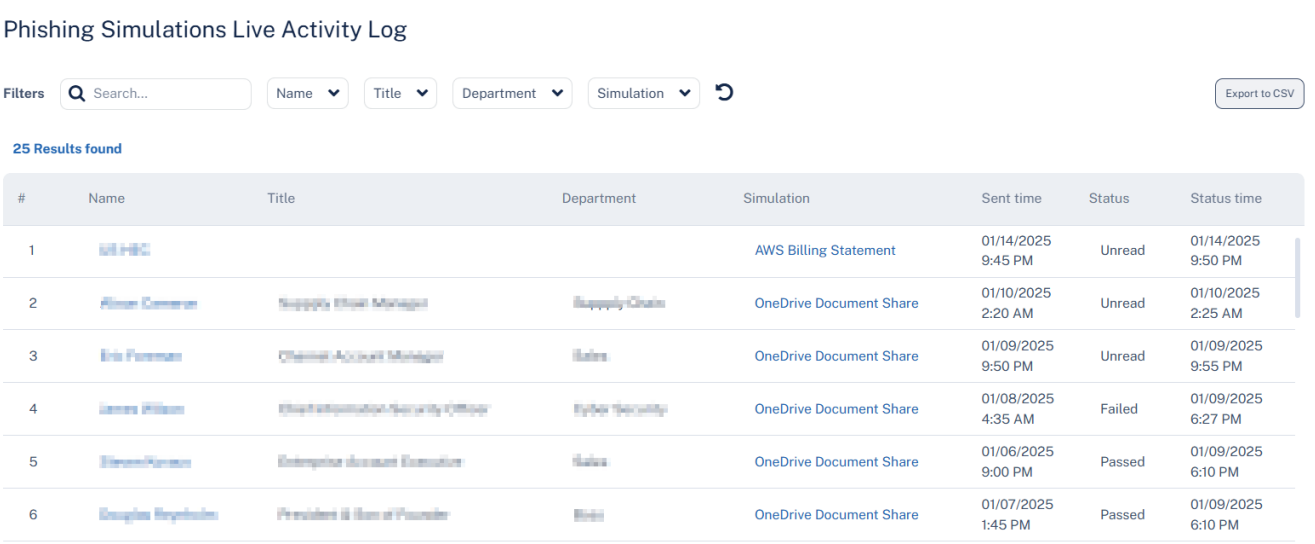
The **Training Log** table shows the users and their training status in the selected time frame.

Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Days Left	Number of days left to complete the training module.
Training	Name of the training module.
Status	Status of the training module. ■ Invited ■ In progress ■ Passed ■ Failed
Status Details	Detailed information about the status.

Column	Description
Time	Date and Time of the training started.

Phishing Simulations Live Activity Log

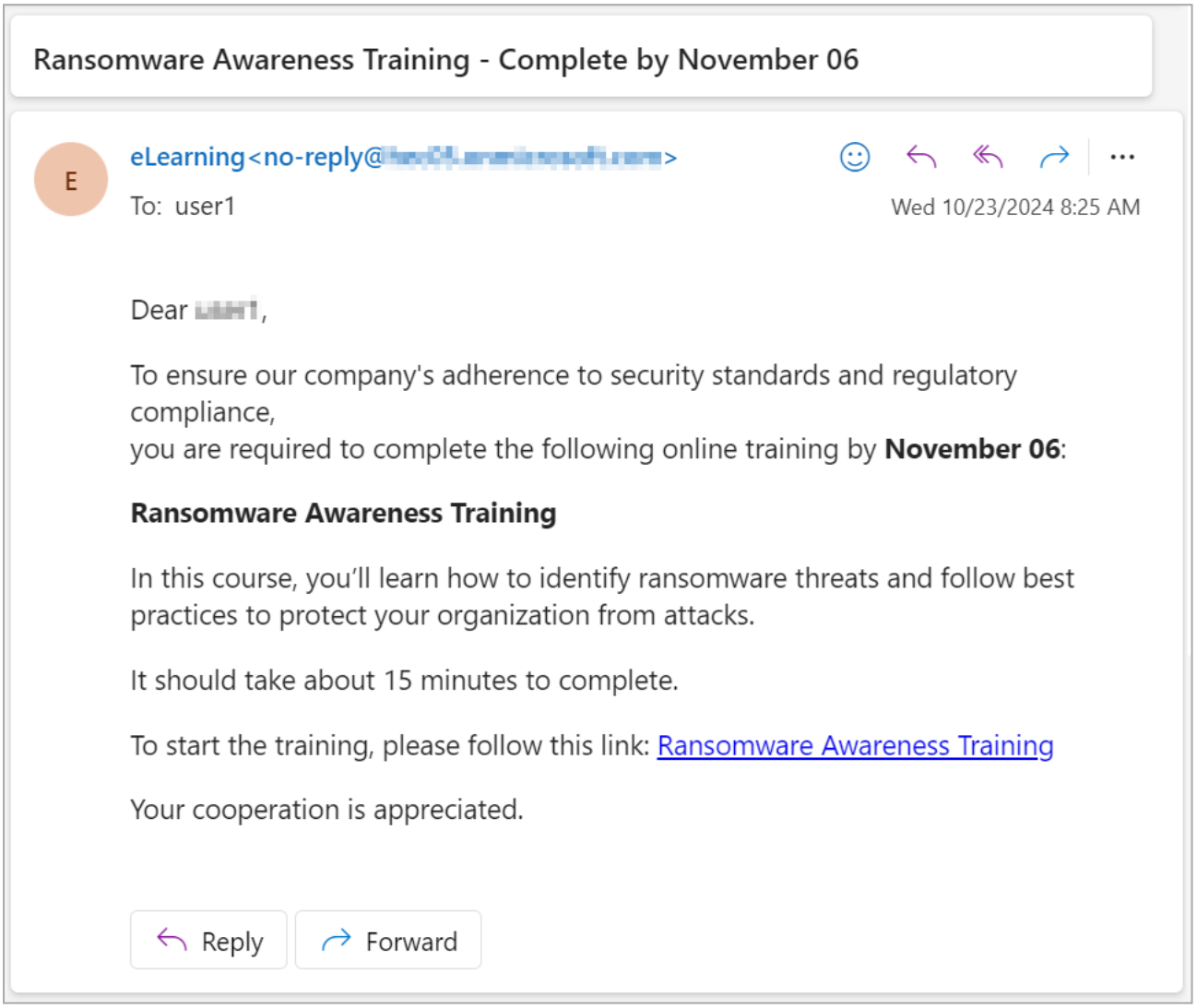
The **Phishing Simulations Live Activity Log** table shows the simulation emails sent to the users and their status.



Column	Description
Name	Name of the user in the organization.
Title	Job title of the user in the organization.
Department	Department the user belongs to within the organization.
Simulation	Type of simulation email sent to the user.
Sent time	Date and time at which the simulation email is sent.
Status	Status of the simulation email. ■ Unread ■ Passed ■ Failed
Status time	Time at which the status is received.

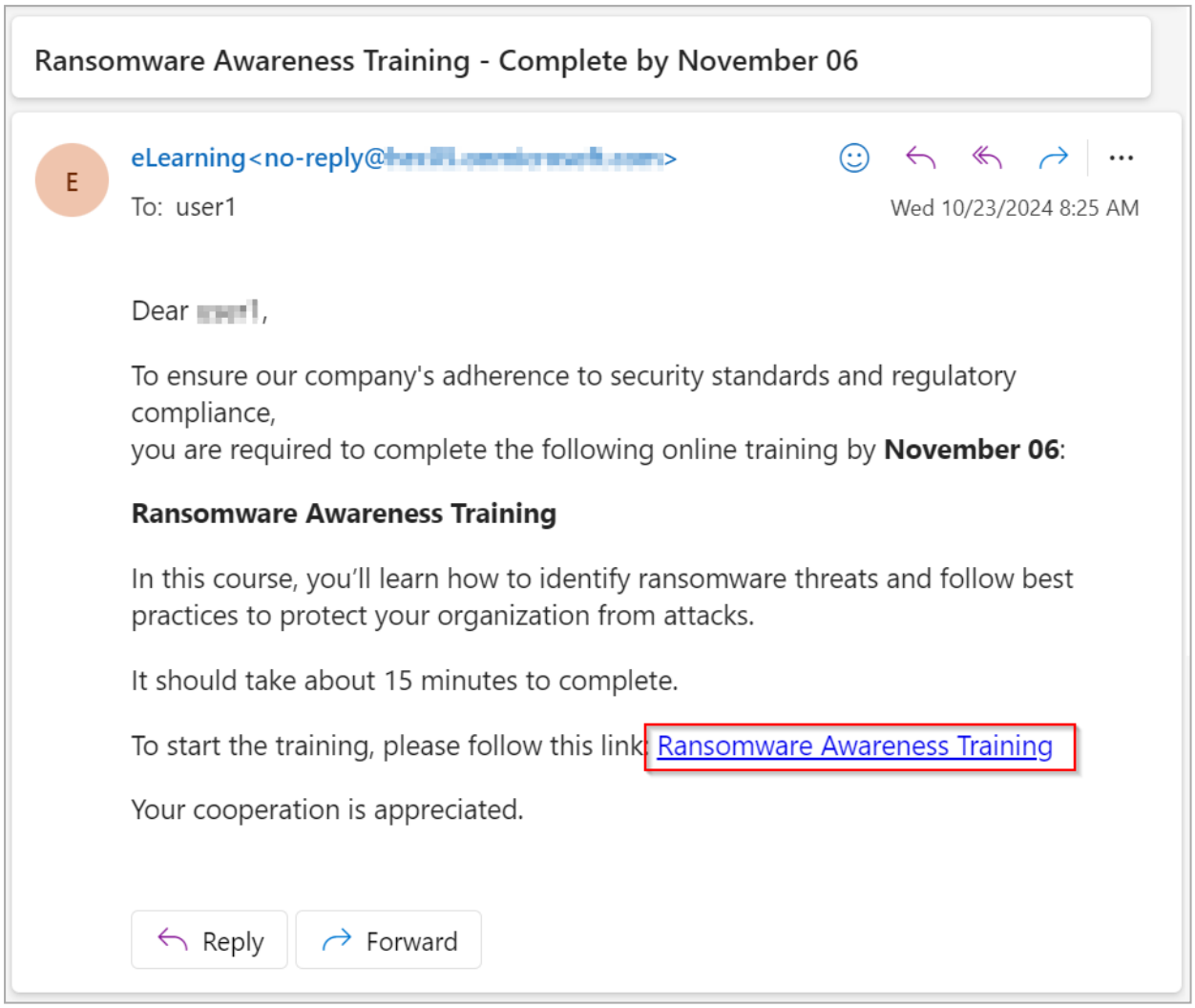
Security Awareness Training - End User Experience

As per the security training policy configured by the administrator, the end-user receives emails with the necessary training details. The emails contain the training module name, duration, due date, and a link to access the training module.



To start the training module:

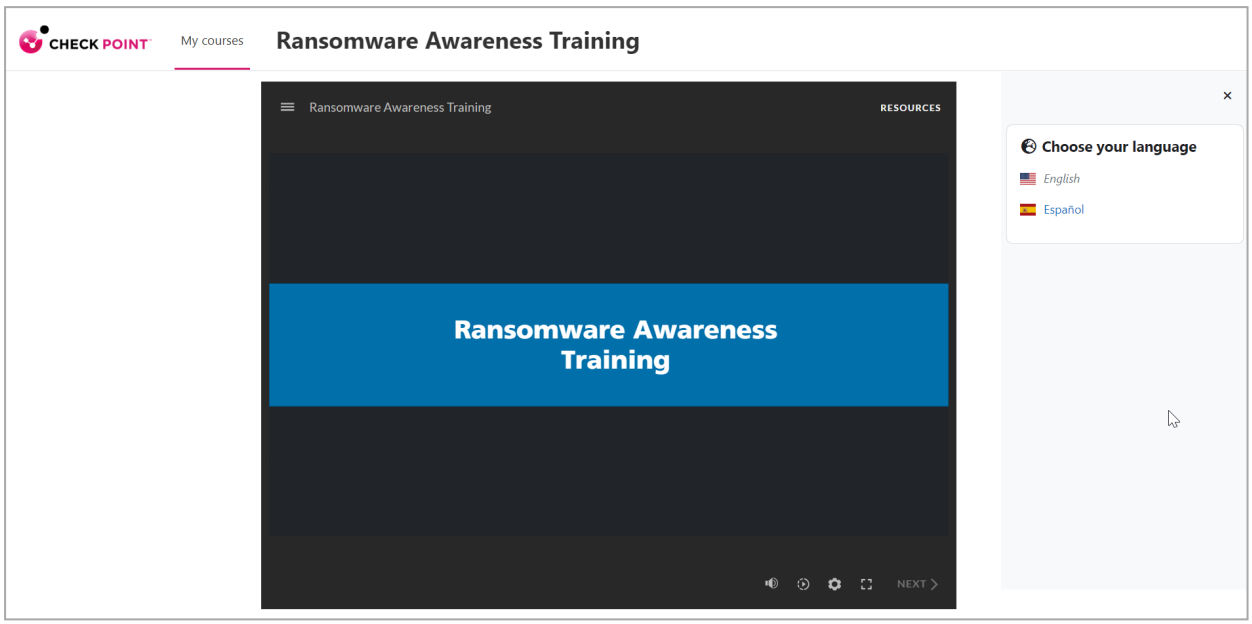
1. Click the link provided in the email.



The **Welcome to Security Awareness Training** page appears.

2. Click **Sign in with Microsoft**.
3. Enter your organization's Microsoft credentials and sign in.

   The training module page appears.



4. (Optional) If the training module is available in multiple languages, the **Choose your language** widget appears to the right of the screen. Select the required language.

   Note - The system determines the user's language for phishing simulation emails and training modules based on Microsoft account attributes:
   - **preferredLanguage**: If this attribute is set, the system uses it as the primary language (if supported).
   - **usageLocation**: If **preferredLanguage** is not defined. By default, the system selects the primary language of the country specified in **usageLocation**.

     For more information about supported languages, see *"Supported Languages for Phishing Simulations" below* and *"Supported Languages for Training Modules" on the next page*.

5. (Optional) To view the different sections in the training module, click the  icon.

   The **Menu** appears, displaying the different sections in the training module.

6. If required, click **Start** to begin the training.

The training includes a quiz with multiple questions to help understand the content. It also covers key use cases and provides strategies to protect against security threats.

Supported Languages for Phishing Simulations

Avanan supports these languages for phishing simulation emails:

- Arabic
- Czech
- English
- French
- German
- Greek
- Hebrew
- Polish
- Portuguese
- Russian
- Spanish
- Turkish

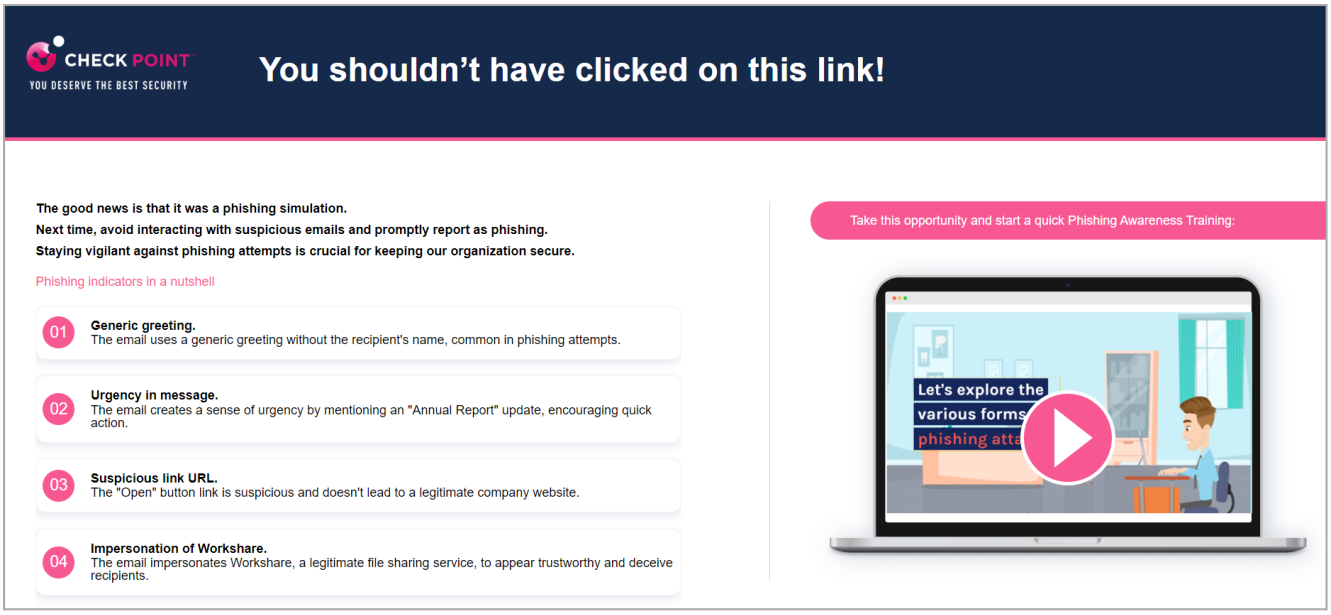
Supported Languages for Training Modules

Avanan supports these languages for training modules:

- Arabic
- English (US)
- French
- German
- Hebrew
- Spanish

Phishing Simulation Email - End User Experience

As per the security training policy configured by the administrator, the end-user receives phishing simulation emails periodically. When a user clicks a link in these emails, a web page displays the risk indicators relevant to the simulation and allows the user to take the Phishing Awareness Training.


CHECK POINT
YOU DESERVE THE BEST SECURITY
You shouldn't have clicked on this link!
The good news is that it was a phishing simulation.
Next time, avoid interacting with suspicious emails and promptly report as phishing.
Staying vigilant against phishing attempts is crucial for keeping our organization secure.
Phishing indicators in a nutshell
01
Generic greeting.
The email uses a generic greeting without the recipient's name, common in phishing attempts.
02
Urgency in message.
The email creates a sense of urgency by mentioning an "Annual Report" update, encouraging quick action.
03
Suspicious link URL.
The "Open" button link is suspicious and doesn't lead to a legitimate company website.
04
Impersonation of Workshare.
The email impersonates Workshare, a legitimate file sharing service, to appear trustworthy and deceive recipients.
Take this opportunity and start a quick Phishing Awareness Training:
Let's explore the
various forms
phishing atta

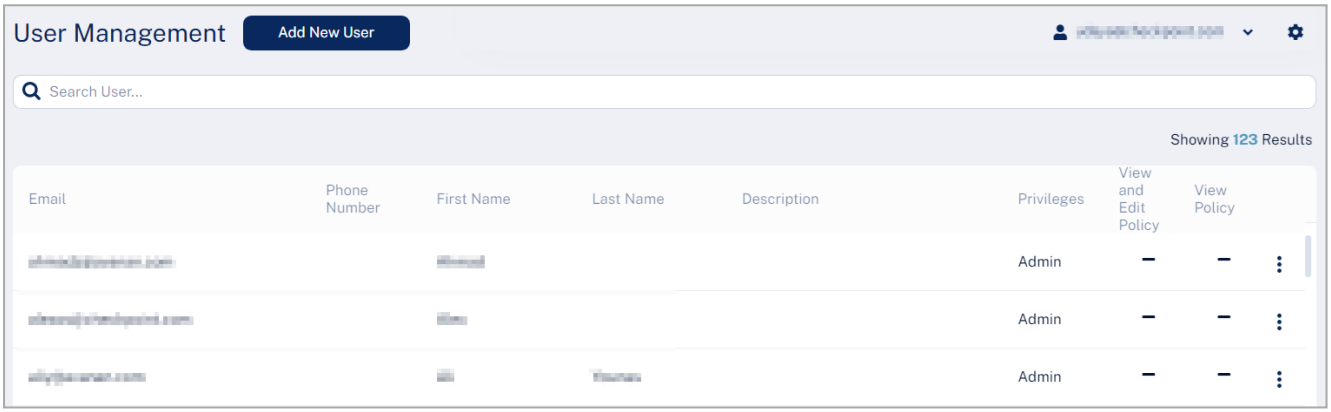
User Management

The **User Management** page allows you to manage Avanan Administrator Portal users. You can view and update user information, and add or delete users.

Note - You must have Admin privileges to access the **User Management** screen.

Viewing User Information

To view user information, click **System Settings** > **User Management**.



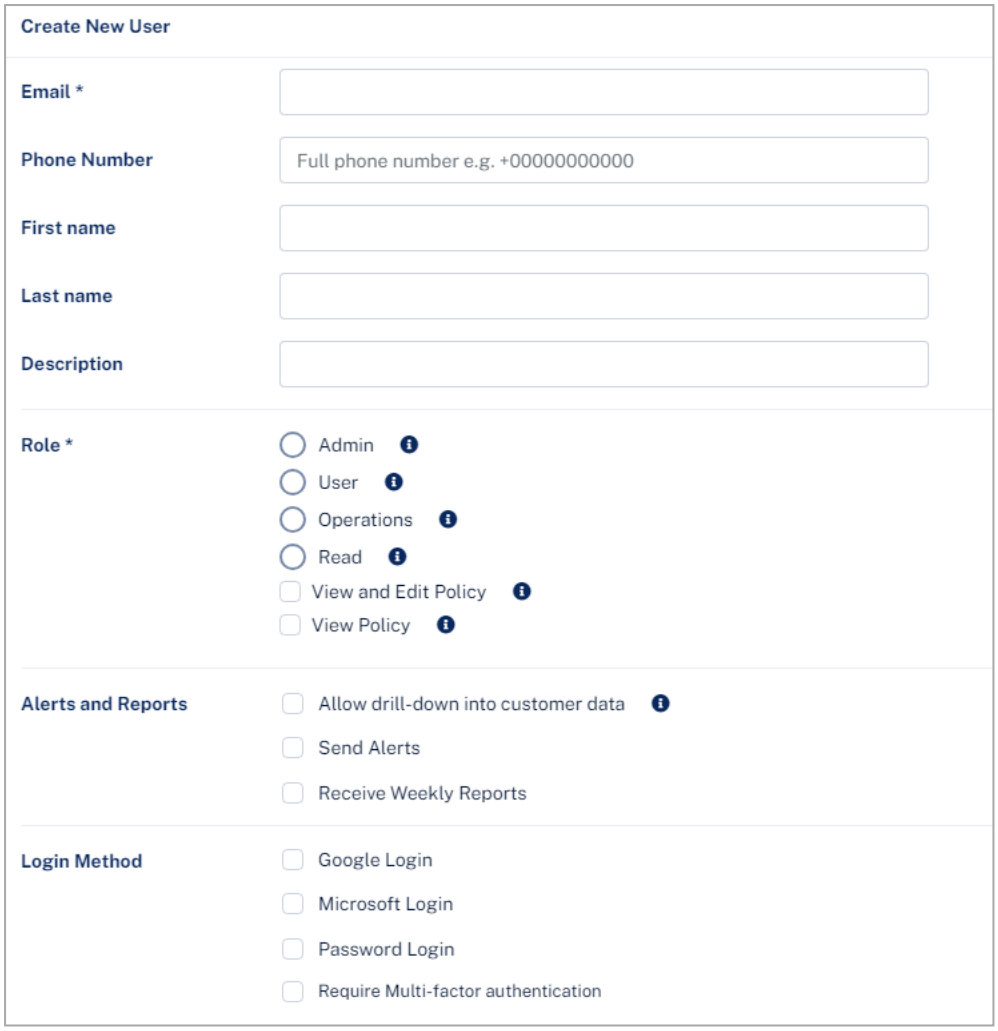
The **User Management** page shows this information:

Column	Description
Email	User email ID.
First name	User first name.
Last name	User last name.
Description	Brief description about the user.
Privileges	User privilege level. ▪ Admin ▪ User ▪ Operations ▪ Read
View Policy	Allows the user to view the policy rules and does not allow to edit the rules.
Google Login	Shows if login using Google credentials is enabled or not.

Column	Description
Microsoft Login	Shows if login using Microsoft credentials is enabled or not.
SAML Login	Shows if login using SAML credentials is enabled or not.
Password Login	Shows if login using email ID and password is enabled or not.
MFA	Shows if login using Multi-Factor Authentication (MFA) is enabled or not.
Allow Private Data Access	Shows if the user can access private data.
Send Alerts	Shows if the user can receive alerts.
Receive Periodic Alerts	Shows if the user can receive periodic alerts.
Last Login	Date and time when the user last logged in to the portal.

Adding a New User

1. Log in to the Avanan Administrator Portal.
2. Click **System Settings** > **User Management**.
3. Click **Add New User**.
4. In the **Email** field, enter the user email ID.



5. (Optional) Enter the details in these fields: **First name**, **Last name** and **Description**.
6. Select the privilege type for the user.

Privilege	Description
Admin	Can access all the pages and can perform all operations.
User	Similar privileges to the Admin role, but cannot access the **User Management** page or create new SaaS applications.
Operations	Can perform all operations except: ■ Start, stop or authorize SaaS applications. ■ Interact with policy rules ■ Perform actions on custom queries.
Read	Read-only access to the portal.

7. To allow the user to view the policy rules and not allow to edit the rules, select the **View Policy** checkbox.

8. To allow the user to view, create, and edit the policy rules, select the **View and Edit Policy** checkbox.
9. (Optional) Under Alerts and Reports, select the relevant options:
   - Allow drill-down into customer data.

     When selected, the user is allowed to access the email header, body, attachments, links to external resources, and text identified as DLP.
   - Send Alerts.
   - Receive Weekly Reports.

     When selected, the user receives a weekly report by email.

     Note - This option is also available in the **Analytics** section of the Avanan Administrator Portal.
10. (Optional) Select the relevant authentication methods.

    Note - You must enable at least one of the authentication methods:
    - Google Login
    - Password Login
    - Microsoft Login
    - SAML Login (see *"SAML Configuration" on the next page*)
    - *"Multi-Factor Authentication using Google Authenticator" on page 539*
11. Click **Create**.

Updating User Information

1. Log in to the Avanan Administrator Portal.
2. Click **System Settings** > **User Management**.
3. Click the ⋮ icon of the user you want to update and select **Edit**.
4. Continue from Step 4 of *"Adding a New User" on page 509*.
5. Click **Update**.

Deleting a User

1. Log in to the Avanan Administrator Portal.
2. Click **System Settings** > **User Management**.
3. Click the ⋮ icon of the user you want to delete and select **Delete User**.
4. Click **Delete**.

SAML Configuration

Avanan allows you to authenticate users using these Identity and Access Management (IAM) providers:

SAML Configuration for Azure

To set up an Microsoft Azure application as your Identity Provider to allow SAML authentication:

1. Log in to the Avanan Administrator Portal:
    a. Go to **Security Settings** > **Settings** and click **Configure SAML**.

    The **Configure SAML** window appears.

    b. To copy the SAML SSO url, in the **SAML SSO URL** field, click  .
2. Log in to the Microsoft Azure:
    a. Click **Enterprise applications** from the left navigation pane.
    b. Click **New application**.
    c. Select **Non-gallery application**.
    d. In the **Name** field, enter a name for the application.
    e. Click **Add**.
    f. Select **Set up single sign on**.
    g. Select **SAML**.
    h. In the **Identifier (Entity ID)** field, enter a unique string, for example, Avanan.
    i. In the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** fields, paste the url copied in step **1.b.**
    j. In the **Sign on URL** field, enter your Avanan Administrator Portal url.
    k. Click **Save**.

l. In the **User Attributes & Claims** field, click .

m. From the **Source attribute** field, select one of these:

- **user.mail**
- **user.userprincipalename**

Note - Make sure that **user.mail** is populated for all relevant users when making your selection, if not, authenticating users becomes impossible.

n. In the **SAML signing certificate** section, for **Federation Metadata XML**, click **Download**.

3. Log in to the Avanan Administrator Portal:

a. Go to **Security Settings** > **Settings** and click **Configure SAML**.

The **Configure SAML** window appears.

b. In the **Metadata Source** field, select **Import a metadata file** and upload the Federation Metadata XML file downloaded in step **2.n**.

c. Unselect the **Are you running Azure AD** checkbox.

d. In the **Identity Provider Entity ID** field, enter the enter a unique string entered in step **2.h**.

4. Log in to the Microsoft Azure Portal:

a. Go to **Manage** > **Users and groups**.

b. Click **Add user**.

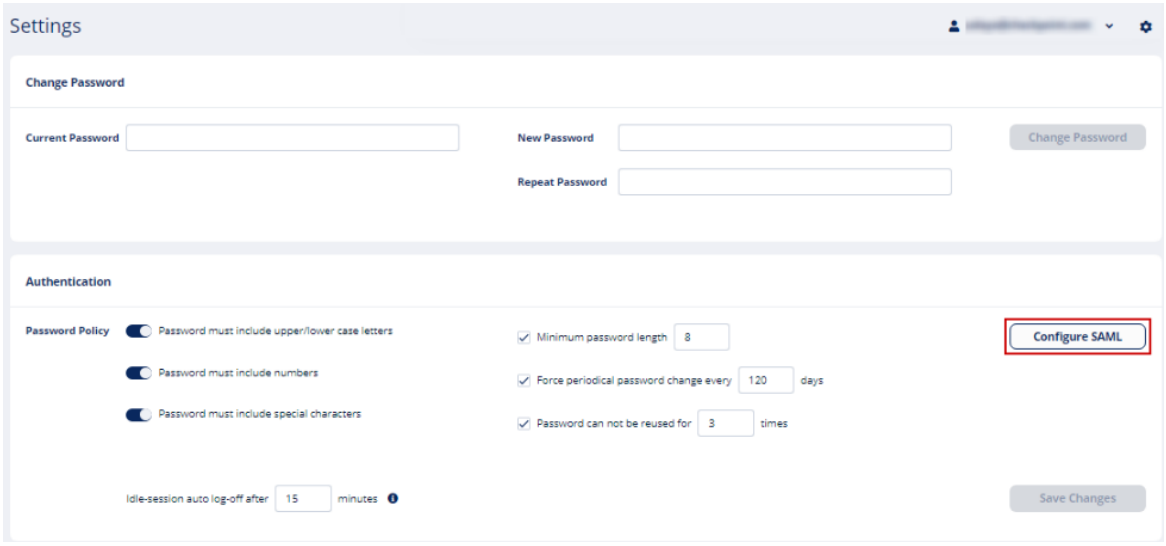
c. From the **Users and groups** list, select the user or group you want to grant access.

d. Click **Assign**.

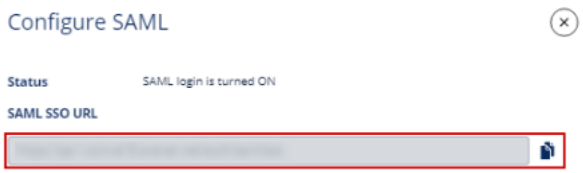
You are now able to login to the Avanan Administrator Portal with SAML.

SAML Configuration for Duo

1. Log in to the Avanan Administrator Portal:
   a. Go to **System Settings** > **Settings** and click **Configure SAML**.

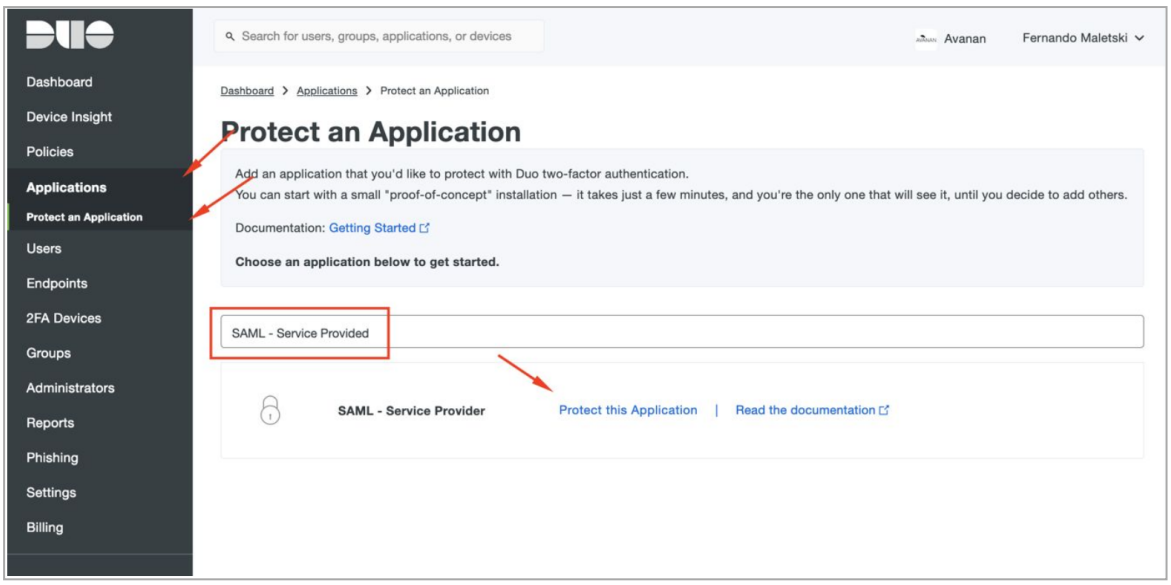


   The **Configure SAML** window appears.



   b. In the **SAML SSO URL** field, click to copy the SAML SSO URL.
2. Log in to your Duo Admin Portal:

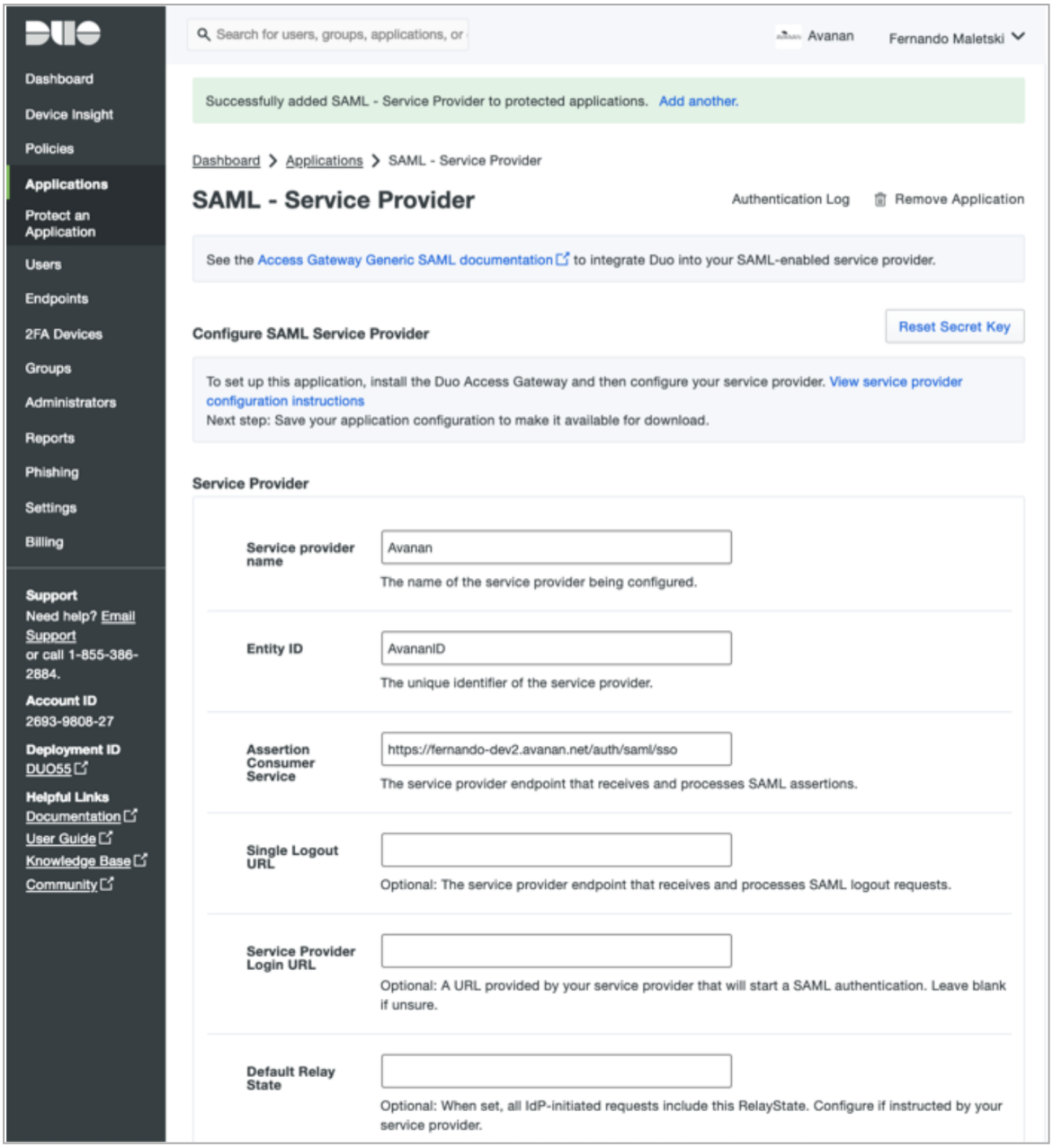
a. Go to **Applications** > **Protect an Application**.



b. In the search box, search for **SAML - Service Provider**.

c. Click **Protect this Application**.

The **SAML - Service Provider** page appears.

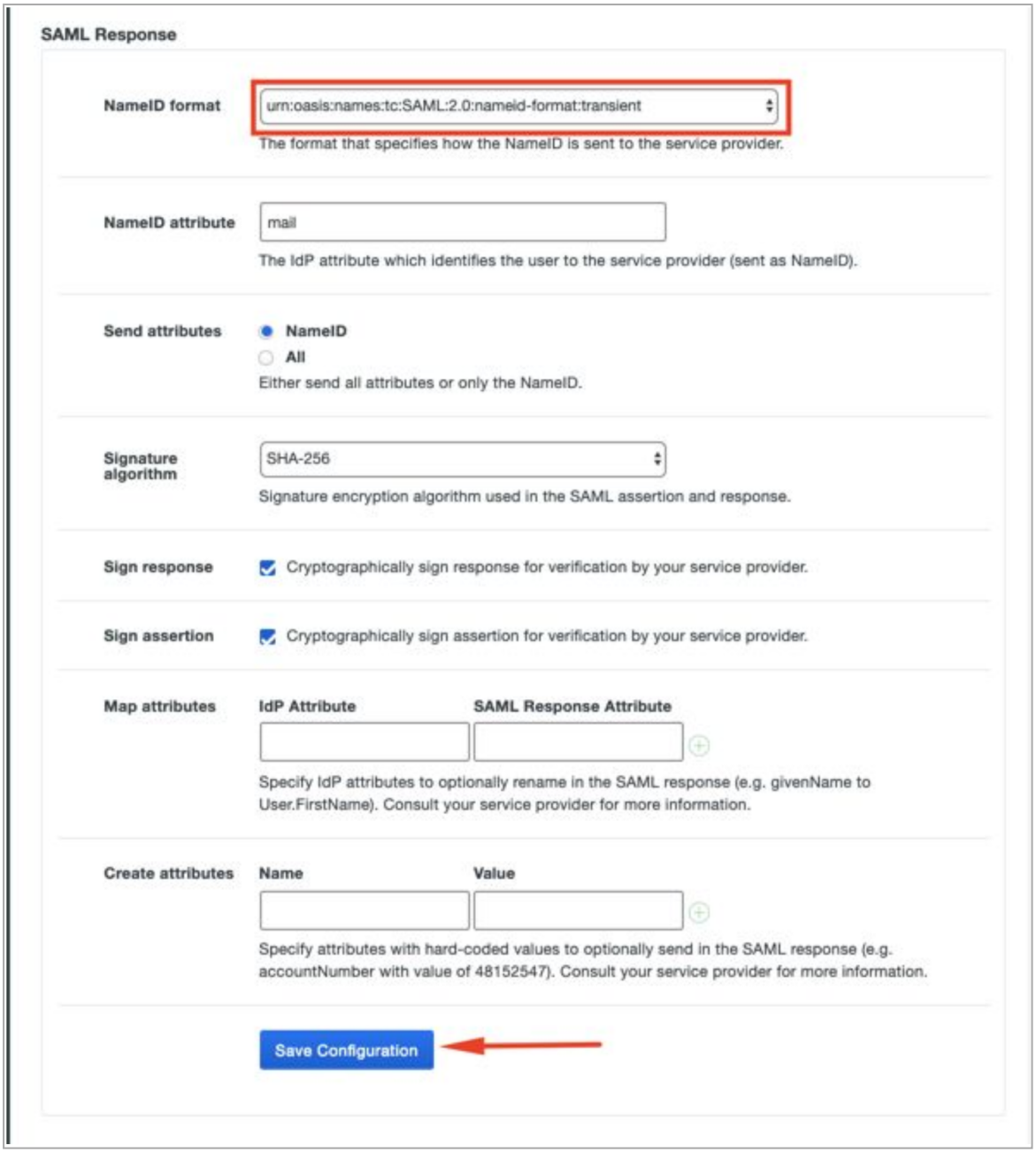


d. In the **Service provider name** field, enter a name for the application.

e. In the **Entity ID** field, enter a unique Entity ID.

f. In the **Assertion Consumer Service** field, enter the URL you copied in step **1.b**.

g. In the **NameID format** field, select transient.



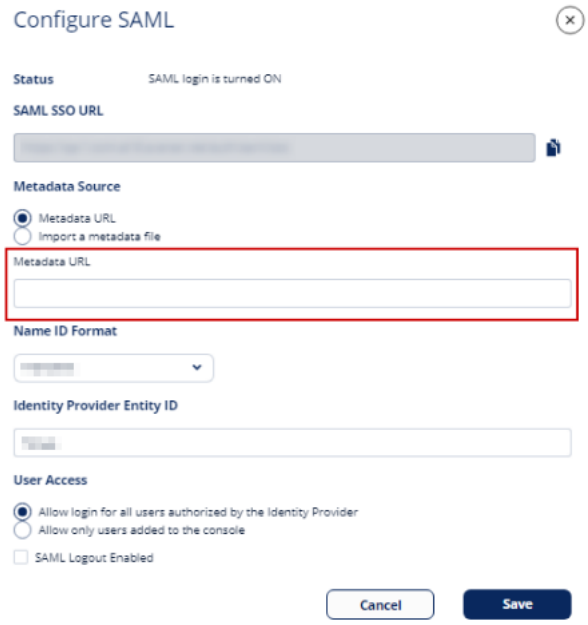
h. Click **Save Configuration**.

i. In the **Configure SAML Service Provider** section, click **Download your configuration file** and save the JSON file.

3. Log in to the Avanan Administrator Portal:

a. Go to **System Settings** > **Settings** and click **Configure SAML**.

   The **Configure SAML** window appears.



b. In the **Metadata Source** field, select **Import a metadata file** and upload the XML file downloaded in step **2.i**.

c. Select the **Are you running Azure AD** checkbox.

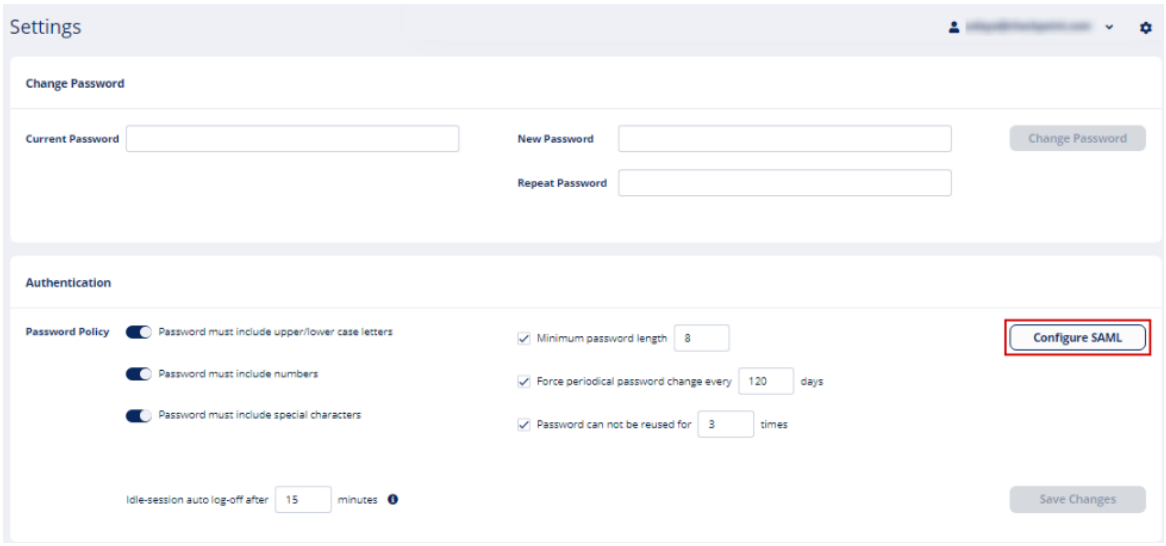
d. In the **Identity Provider Entity ID** field, enter the unique string entered in step **2.e**.

e. Click **Save**.

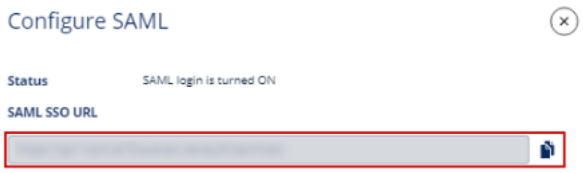
SAML Configuration for Idaptive

To set up an Idaptive application as your Identity Provider to allow SAML authentication:

1. Log in to the Avanan Administrator Portal:
    a. Go to **System Settings** > **Settings** and click **Configure SAML**.



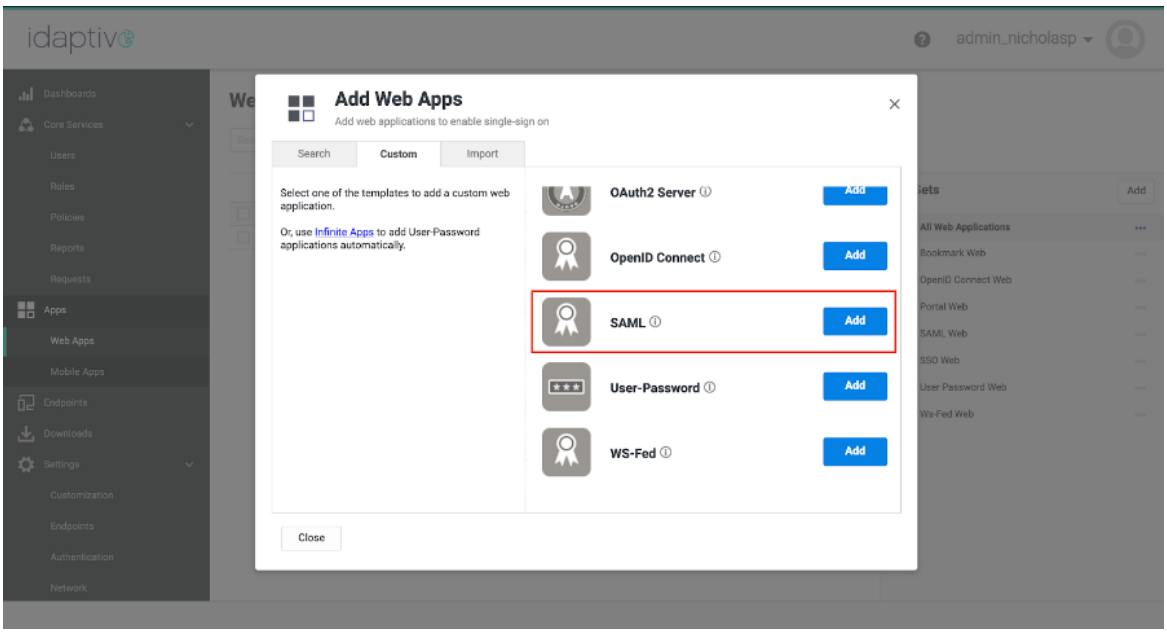
    The **Configure SAML** window appears.



    b. In the **SAML SSO URL** field, click  to copy the SAML SSO URL.

2. Log in to your Idaptive Admin Portal:
    a. Go to **Apps** > **Web Apps**.
    b. Click **Add Web Apps**.
    c. Click the **Custom** tab.

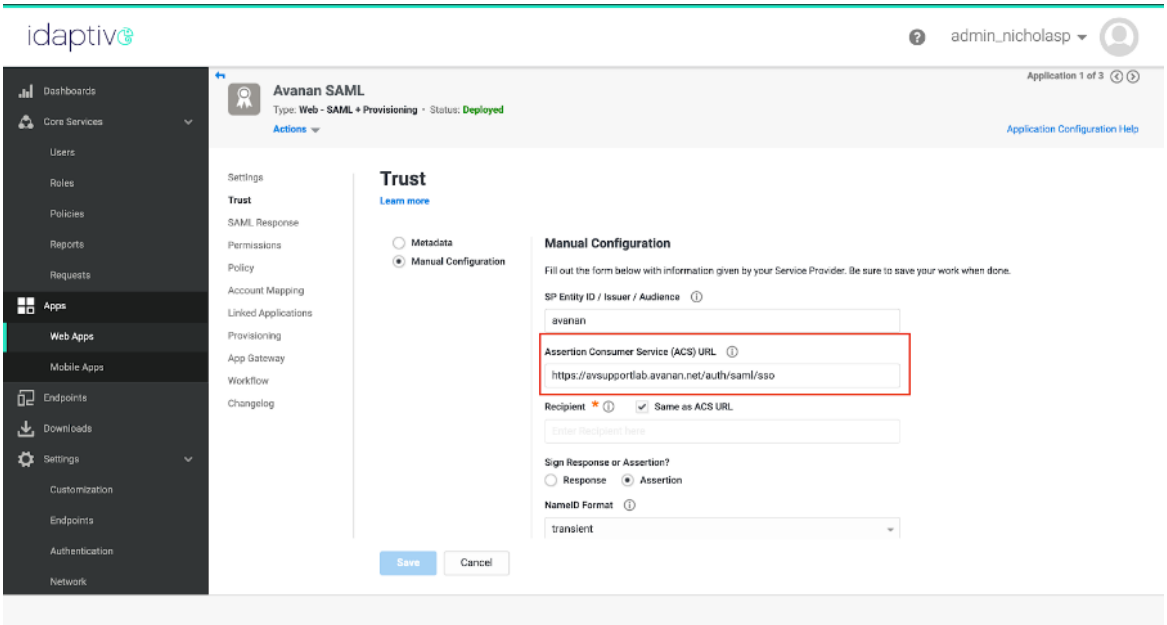
d. For SAML, click **Add**.



e. Click **Trust** and in the **Service Provide Configuration** section, select **Manual Configuration**.

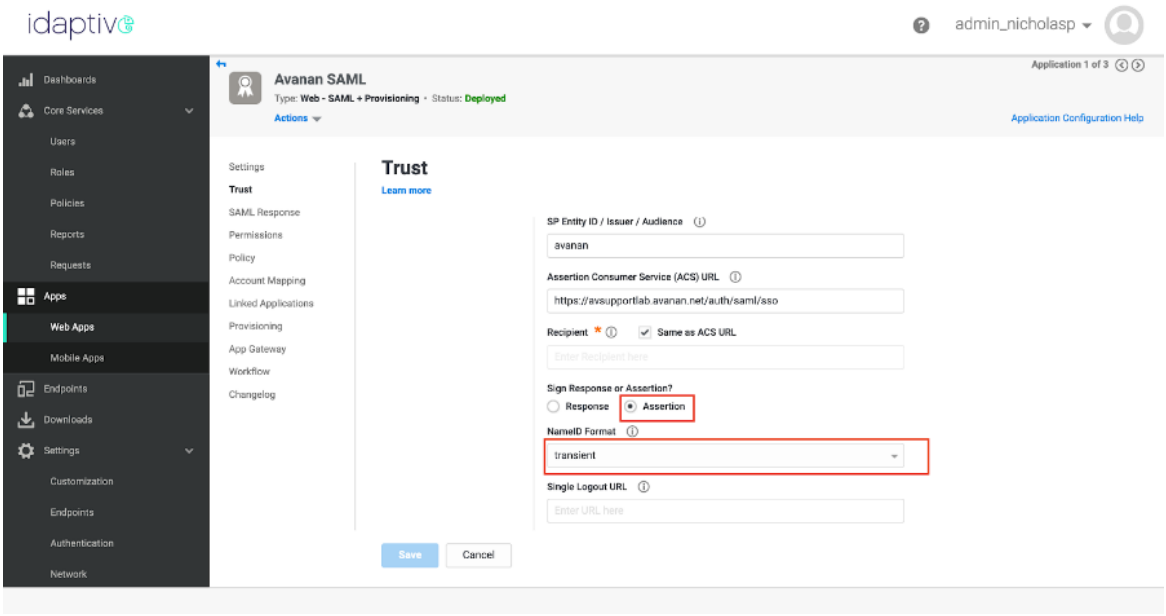
The **Manual Configuration** section appears.

f. In the **Assertion Consumer Service (ACS) URL** field, paste the url copied in step **1.b**.



g. From the **Sign Response or Assertion** options, select **Assertion**.

h. From the **NameID Format** list, select **transient**.



i. Click **Save**.

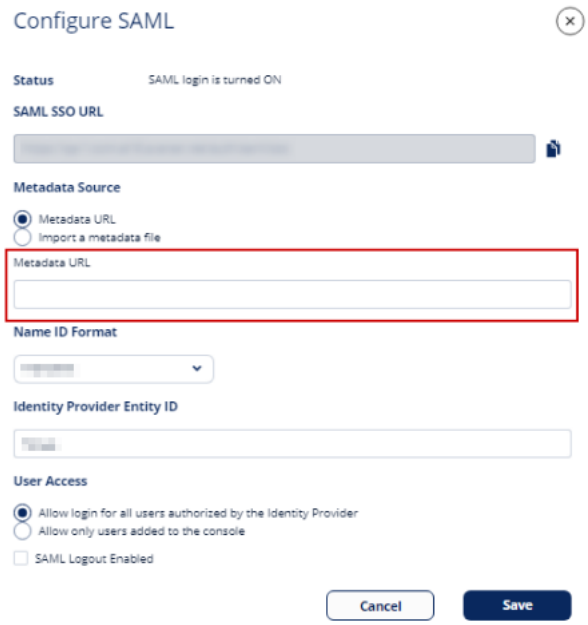
j. Scroll up to the **Metadata URL** field and click .

3. Log in to the Avanan Administrator Portal:

   a. Go to **System Settings** > **Settings** and click **Configure SAML**.

      The **Configure SAML** window appears.

b. In the **Metadata Source** field, select **Metadata URL** and paste the url copied in step **2.I**.



c. Clear the **Are you running Azure AD** checkbox.

d. Click **Save**.

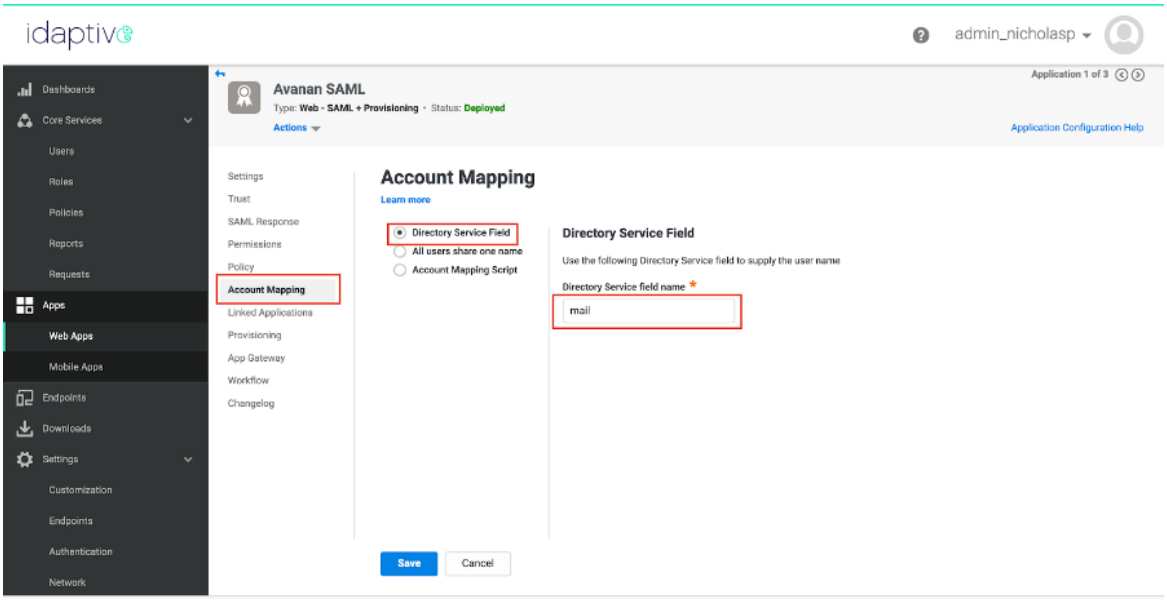
4. Log in to your Idaptive Admin Portal:

   a. Go to **Apps** > **Web Apps**.

   b. Click **Account Mapping** and select **Directory Service Field**.

      The **Directory Service Field** section appears.

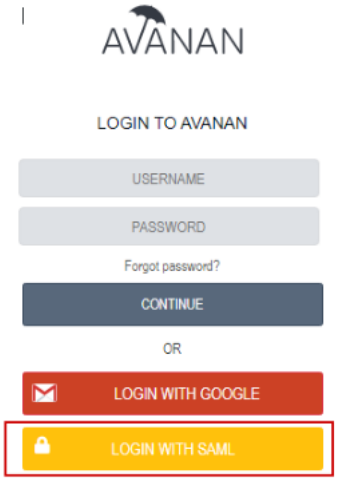
c. In the **Directory Service field name** field, enter **mail** as the directory service field name.



d. Click **Save**.

e. Make sure that you assign users to the newly created SAML application in Idaptive Admin portal.

You are now able to login to the Avanan Administrator Portal with SAML.



SAML Configuration for JumpCloud

1. Log in to the Avanan Administrator Portal:

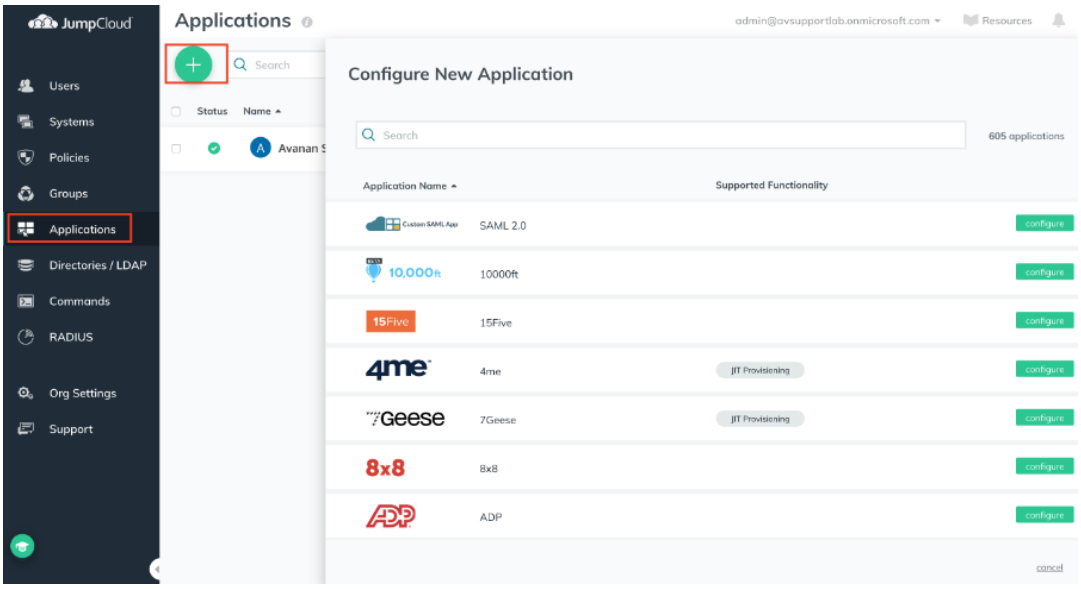
a. Go to **System Settings** > **Settings** and click **Configure SAML**.

   The **Configure SAML** window appears.

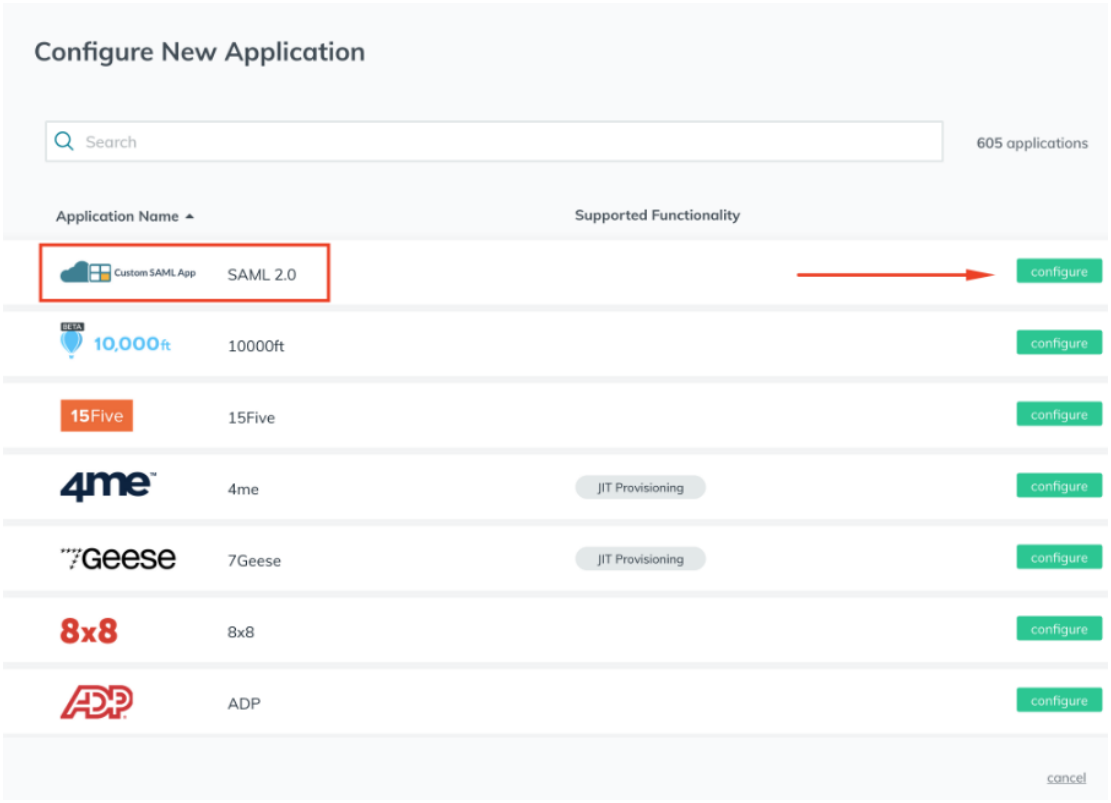
b. In the **SAML SSO URL** field, click  to copy the SAML SSO URL.

2. Log in to the JumpCloud Administrator Portal:

   a. Go to **Applications** and click  .



   The **Configure New Application** window appears.



b. For the **SAML 2.0**, click **Configure**.

c. Expand **General Info**.

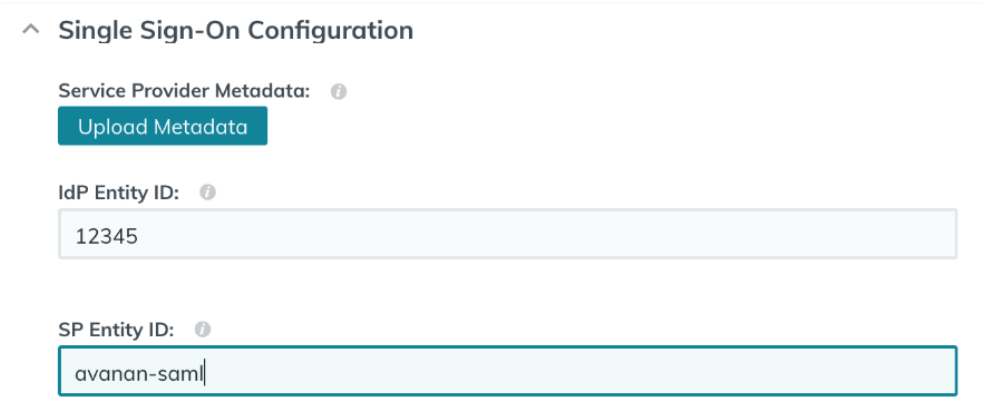
d. In the **Display Label** field, enter a name.

e. (Optional) In the **Description** field, enter a description.

f. Expand **Single Sign-On Configuration**.

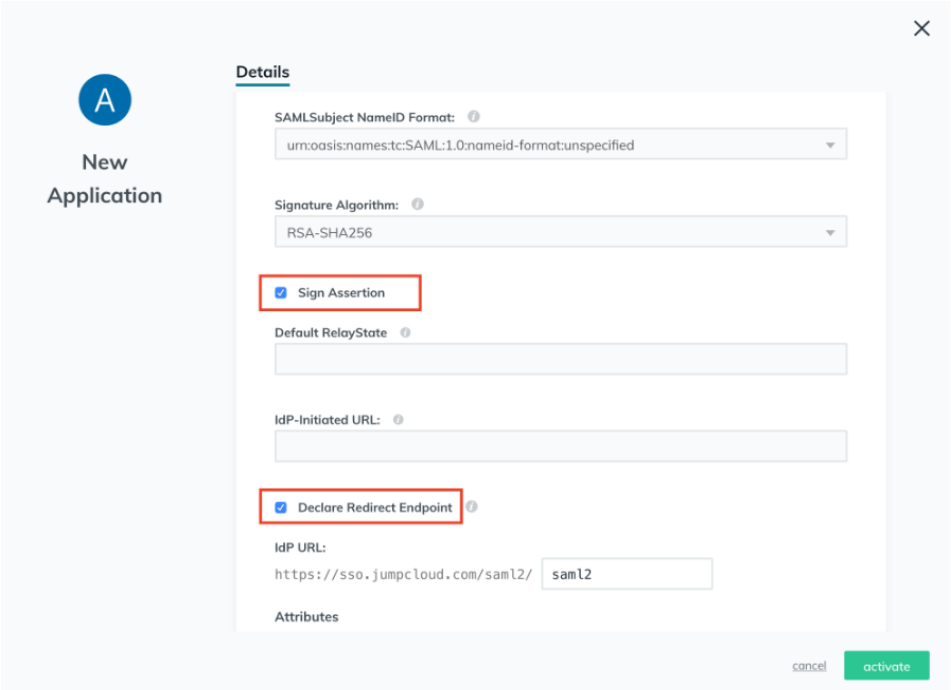
g. Specify these:

- **IdP Entity ID**
- **SP Entity ID** - Paste the url copied in step **1.b**.



h. Select these checkboxes:

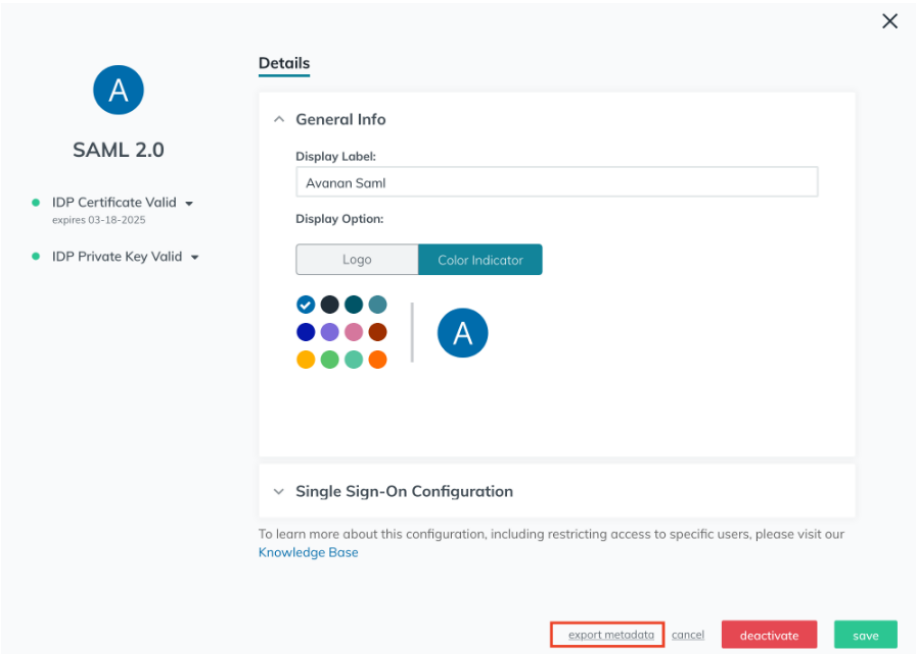
- **Sign Assertion**
- **Declare Redirect Endpoint**



i. Click **activate**.

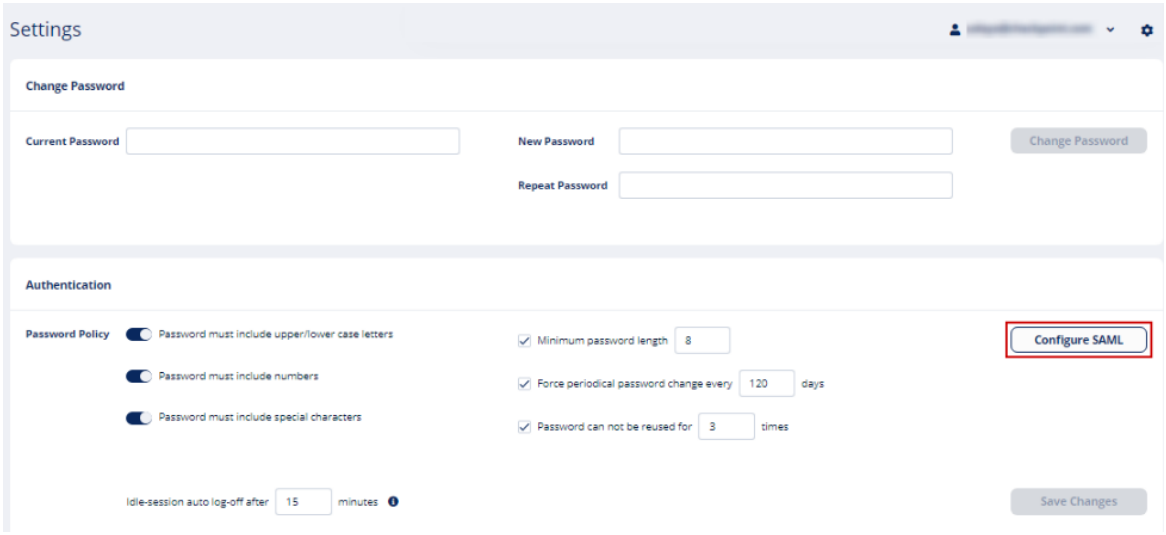
j. To export Metadata, go to **Applications** and select the newly created application.

k. Click **export metadata**.

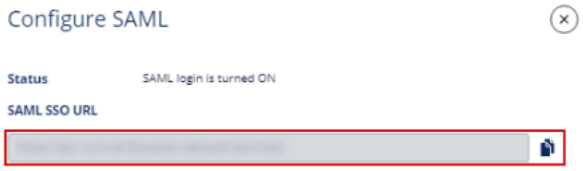


3. Log in to the Avanan Administrator Portal:

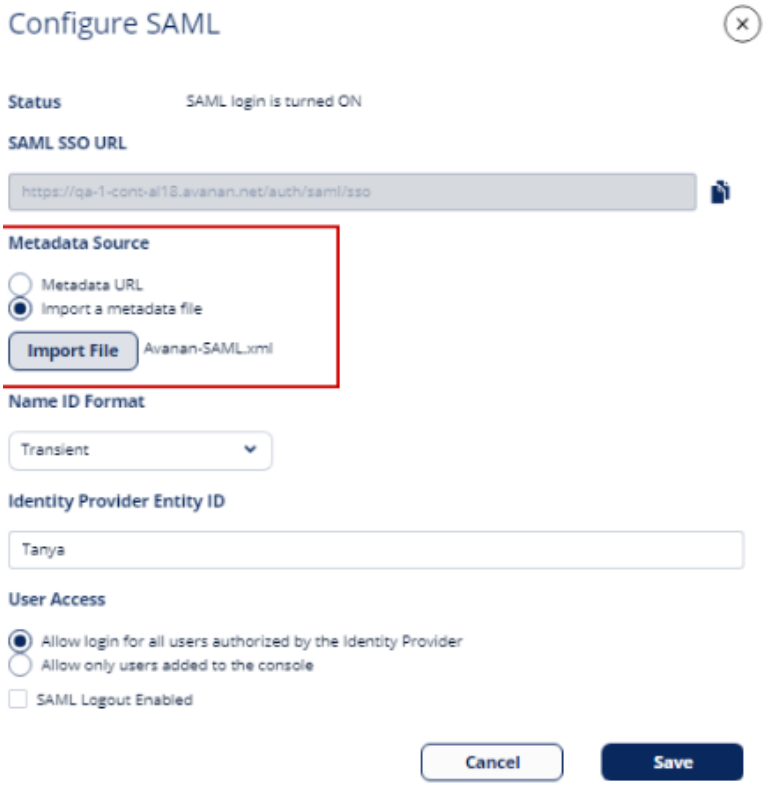
a. Go to **System Settings** > **Settings** and click **Configure SAML**.



The **Configure SAML** window appears.



b. In the **Metadata Source** field, select **Import a metadata file** and upload the XML file downloaded in step **2.k**.



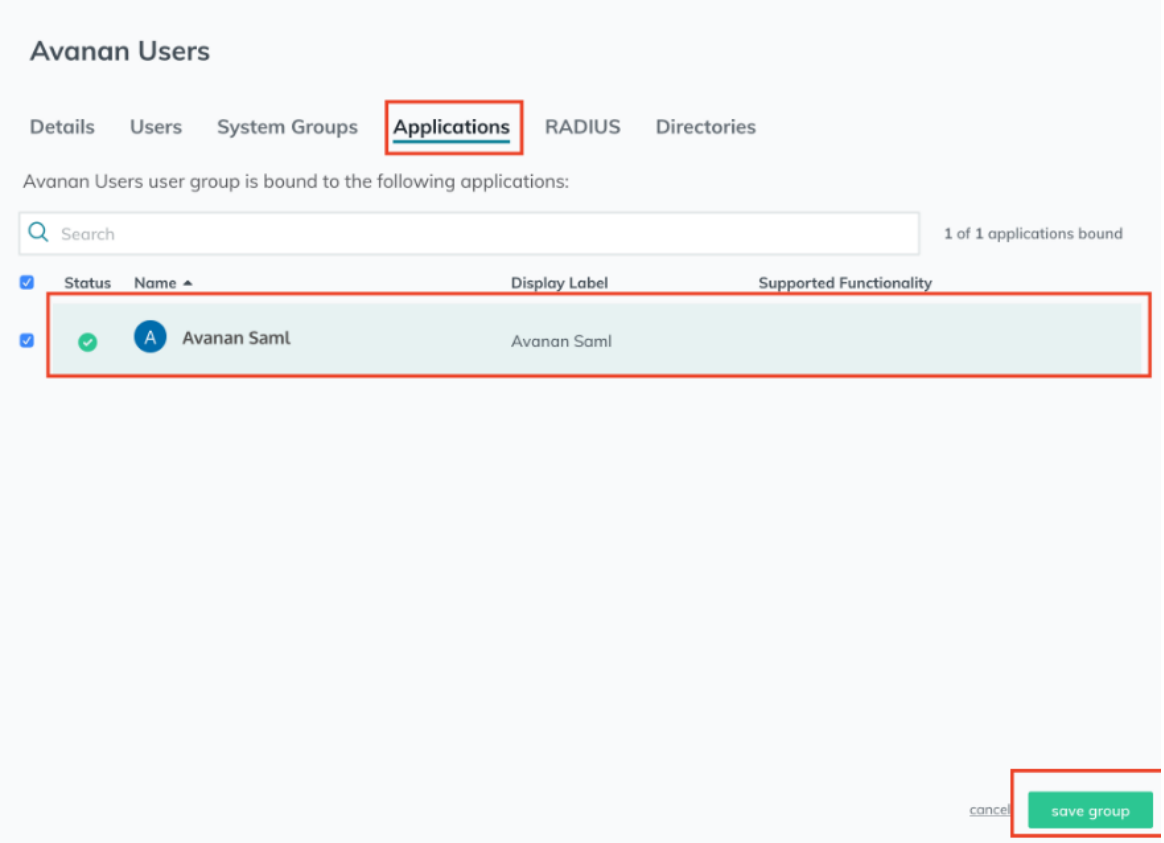
c. Clear the **Are you running Azure AD** checkbox.

d. Click **Save**.

4. To assign users to the newly created JumpCloud application, log in to the JumpCloud Administrator Portal:

   a. Go to **Groups** and select a user group.

   b. From the edit group window, click **Applications** and select the newly created application.



   c. Click **save group**.

   You are now able to login to the Avanan Administrator Portal with SAML.

For more information, see support.jumpcloud.com.

SAML Configuration for Okta

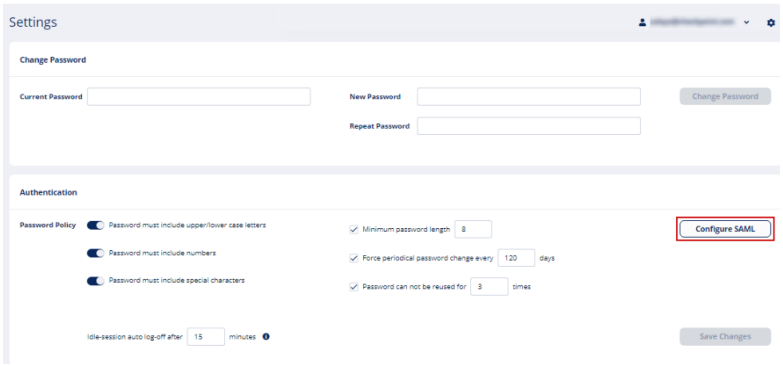
1. To set up SAML applications in Okta:

a. Make sure you have a Okta account, if not, create an account.

b. Log in to your Avanan Administrator Portal:

   i. Go to **System Settings** > **Settings**.

   ii. Click **Configure SAML**.

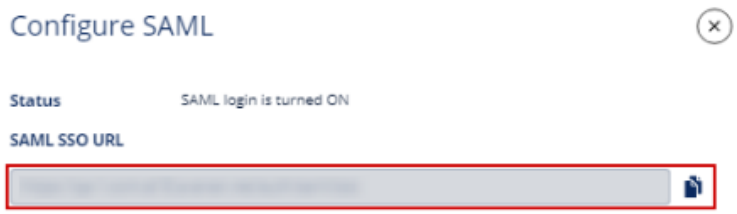


   The **Configure SAML** window appears.

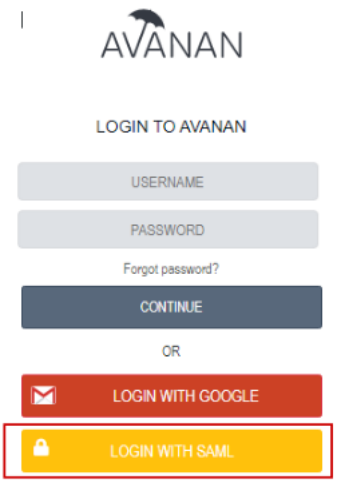
   iii. In the **SAML SSO URL** field, click  to copy the SAML SSO URL.

   iv. In the **Identifier Provider Entity ID** field, enter a unique string, for example, Avanan.

v. To create your private integration in Okta:
    i. Sign in to your Developer Edition org as a user with administrative privileges.
    ii. Go to **Applications** > **Applications** in the Admin Console.
    iii. Click **Create App Integration**.
    iv. Select **SAML 2.0** in the **Sign-in method** section.
    v. Click **Next**.
    vi. In the **General Settings** tab, enter a name for your integration and optionally upload a logo. You can also choose to hide the integration from your end user's Okta dashboard or mobile app.
    vii. Click **Next**.
    viii. In the **Configure SAML** tab, paste the url copied in step **1.b.iii**.
    ix. In the **Single sign on URL** field, enter the Assertion Consumer Service (ACS) URL.
    x. In the **Audience URI (SP Entity ID)** field, enter the value enter in the **Identifier Provider Entity ID** field in step **1.b.iv**.
    xi. From the **Name ID Format** field, select **Email Address**.
    xii. Click **Finish**.
vi. In the **SAML SSO URL** field, paste the URL copied from SSO provider.



You are now able to login to the Avanan Administrator Portal with SAML. You can also run the from Okta directly from `https://{domain}.oktapreview.com/app/UserHome`.


AVANAN
LOGIN TO AVANAN
USERNAME
PASSWORD
Forgot password?
CONTINUE
OR
LOGIN WITH GOOGLE
LOGIN WITH SAML

Email Archiving

Overview

Avanan Archiving is a cloud-based archiving solution for preserving email communications. Archiving provides organizations with a variety of tools for one or more of these reasons:

- Business continuity and disaster recovery
- Email backup and recovery of emails deleted by end-users or because of technical malfunction
- Regulatory compliance and records management
- Litigation and legal discovery
- Prove chain of custody and keep the authenticity of emails.

Activating Email Archiving

After your purchase request is processed, **Archiving** gets activated automatically.

After activation, **Archiving** starts archiving all the emails sent from and received by the protected user's mailboxes (users that are assigned Avanan license). For more information on assigning licenses, see *"Managing Licenses" on page 39*.

Note - Though **Archiving** starts archiving the emails immediately, it might take up to 48 hours for these emails to be available in the **Archive Search** (**Archiving** > **Archive Search**).

If required, administrators can import the archived emails from an external source. See *"Importing Emails to Archive" on page 537*.

For more information on assigning licenses, contact *Avanan Support*.

Deactivating Email Archiving

To deactivate **Archiving** or to delete the archive storage, contact *Avanan Support*.

Archived Emails

After activating **Archiving**, all the internal, outgoing, and incoming emails (sent or received) from protected users will be archived.

For users not licensed for Avanan, the emails will not be archived.

Emails that were sent before activating **Archiving** are not archived. To import historical emails to the **Archiving**, see *"Importing Emails to Archive" on the next page*.

Emails will be stored for a period of seven years and will be automatically deleted afterwards.

Avanan encrypts and stores the archived emails in the same region as your tenant in the Avanan portal.

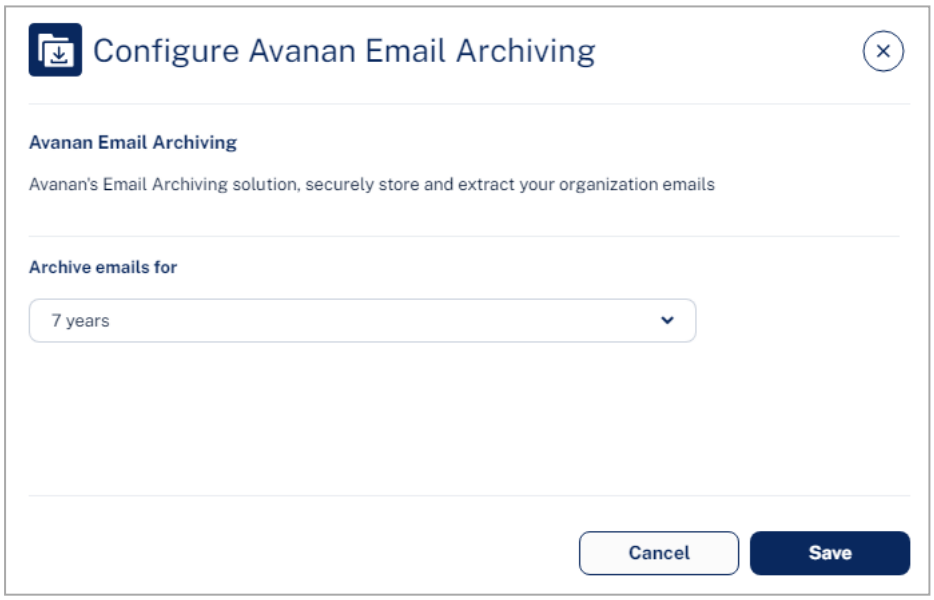
Customizing the Retention Period of Archived Emails

By default, the archived emails are stored for a period of seven years and will be automatically deleted afterwards.

To customize the retention period of archived emails:

1. Click **Security Settings** > **Security Engines**.
2. Click **Configure** for Avanan Email Archiving.

   The **Configure Avanan Email Archiving** pop-up appears.



3. In the **Archive emails for** dropdown, select the number of years to retain the emails.
   - 1 year
   - 2 years
   - 3 years
   - 5 years

- 7 years (default)
- 10 years

4. Click **Save**.

Note - Change in the retention period applies retroactively to all the archived emails. For example, if you change the retention period to one year, Avanan deletes the emails older than one year from the archive.

Viewing Archived Emails

From the **Archive Search** screen, administrators can use filters and search for the required emails. The **Archive Search** screen gives a detailed view of all the archived emails (whether they have been archived or imported from an external source).

Note - After the emails are archived, it takes up to 48 hours for the archived emails to appear in the **Archive Search**.

Importing Emails to Archive

Administrators can import emails from the email archiving solutions they used in the past or from other sources.

Supported Archiving import file format and size:

Before importing the existing email archive to the Avanan Archiving, do these:

1. Export the existing emails as EML files with a maximum size of 150 MB per file.
2. Group your EML files and compress them into ZIP files with a maximum size of 15 GB per ZIP file.
3. Follow the procedure below to import emails to Archiving.

Notes:
- To import the emails to Archiving, the combined size of all uploaded ZIP files must be less than 150 GB.
  For example, you can upload up to 10 ZIP files, each with a maximum size of 15 GB, or alternatively, upload 50 ZIP files, each with a maximum size of 3 GB.
- You can follow the same procedure multiple times to upload ZIP files totaling up to 300 GB, 450 GB, and so on. If you need to upload an archive significantly larger than that, contact *Avanan Support*.

To import emails to Archiving:

1. Click **Archiving** > **Archive Search**.
2. Click **Import archive**.

3. In the **Import Emails to Archive** window that appears, click **Get credentials** to receive credentials to a temporary upload path.

   Note - This upload path and credentials are valid only for 7 days.

4. Use the path and credentials (Host name, user name and password) to log in to SFTP.
5. Upload the ZIP file(s) to the uploads folder.
6. After uploading all the files, click **Done uploading**.
7. Click **Confirm** to initiate the import.

   Note - After importing the emails, it takes up to 48 hours for the archived emails to appear in the **Archive Search**.

Exporting Emails from Archive

If required, administrators can export the archived emails from the **Archive**. Each archive export creates encrypted ZIP file(s), which includes EML files. If the export file size exceeds 10 GB, then the export is divided into multiple ZIP files, with each file size not exceeding 10 GB.

To export archived emails:

1. Click **Archiving** > **Archive Search**.
2. Using filters, refine the search criteria for the required emails.
3. Select the emails to export, and click **Export**.
4. In the **Export Archive Emails** window that appears, enter the required **Export Name** and **Passphrase** for the archive export.
5. Click **OK**.

   Note - The export process could take several hours. After it is complete, the administrator who initiated the export process receives an email notification.

6. To download the archive export file(s), click **Archiving** > **Archive Export**.
7. Click **Download** for the required export file(s).

   Note - The link to download the exported file(s) will only be available for 7 days after the export is completed.

Auditing

Avanan audits all the archive search, archive import, archive export, and archive download actions and adds them to the **System Logs** (**System Settings** > **System Logs**).

Multi-Factor Authentication using Google Authenticator

Multi-Factor Authentication (MFA) is key to a healthy security and identity protection posture. Users can log into the Avanan portal using MFA in one of these ways.

- Log in via Microsoft / Google – then in the Google/Microsoft directory, set the relevant MFA settings. For more information, see *"User Management" on page 508*.
- Log in via a standard password and add Google Authenticator confirmation on top of it.

Prerequisites

- Users must download and install the Google Authenticator app on their mobile phones. For more information, see https://support.google.com/accounts/answer/1066447.
- To allow administrators to configure MFA login via Google Authenticator, contact *Avanan Support*.

High-Level Procedure

1. Administrator enforces MFA for the user
2. User enables MFA

Enforcing MFA for the User

The Administrators must enforce the MFA for the user.

1. Access the Avanan Administrator Portal.
2. Click **System Settings** > **User Management**.
3. Click the ⋮ icon in the last column for the user you want to update and select **Edit**.
4. Under **Login Method**, select the **Require Multi-factor authentication** checkbox.

   Note - You must select at least one of the login methods; Google, Password, Microsoft, or SAML.

5. Click **Update**.

   A pop-up window appears and shows that the user has been updated successfully.

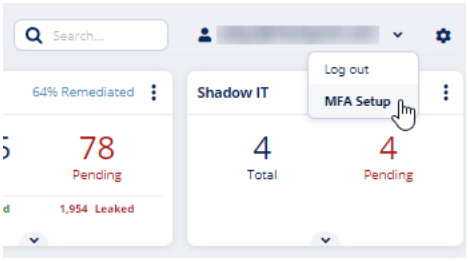
6. Click **OK**.

Note - If you don't see these options in your Avanan portal, contact *Avanan Support*.

Enabling MFA by a User

After the administrator enforces MFA, the user must enable the MFA.

1. Access the Avanan Administrator Portal.
2. In the **Overview** page, open the menu under your user name in the top right corner and select MFA Setup.



   The MFA Setup screen appears that shows the QR code.

3. Open the Google Authenticator app on your device and scan the QR code.

   The Avanan portal is added to the Google Authenticator app and shows the authentication code.

4. In the **Enter the Auth Code** field, enter the authentication code.
5. Click **Enable MFA**.
6. Click **OK**.

   The screen shows the authentication status.

Logging in via Google Authenticator - End User Experience

1. Log in to the Avanan portal with the configured password.
2. Open the Google Authenticator app and copy the six-digit authentication code for the Avanan portal.

   Note - The six-digit authentication code is valid only for 30 seconds. After 30 seconds, a new code is generated.

3. Enter the authentication code from the Google Authenticator app in the **MFA Code** field in the Avanan portal.
4. Click **Submit**.

After successful authentication, the user is logged into the Avanan portal.

Appendix

Appendix A: Avanan Manual Integration with Office 365

This topic describes how to perform a manual on-boarding and configuration process for Avanan where customers bind their Office 365 environment to Avanan.

Note - **Automatic mode** for onboarding allows for better maintenance, management, and smoother user experience. Avanan recommends only using **Manual mode** as a last resort. Before using the **Manual mode**, contact *Avanan Support* to help resolve any issues raised with the **Automatic mode** for onboarding.

After you select to bind Avanan to your Office 365, the **Office 365 Install Mode** window opens.

Select one of these modes:

- **Automatic mode** - Avanan automatically configures Office 365 emails to operate in Detect modes (**Monitor only** and **Detect and Remediate**) and/or **Protect (Inline)** mode. You only need to authorize the Avanan app during the wizard and all configuration changes are applied automatically.
- **Manual mode** - You must manually perform the necessary configurations in the Office 365 Admin Exchange Center before you bind the application.

This topic explains the various settings that need to be configured for **Manual mode** in the Office 365 Exchange Admin Center.

We recommend that you review if any of these scenarios listed below apply to you:

- You want to choose automatic mode but first want to learn the configuration changes that are automatically applied to Office 365.
- You want to choose manual mode and need to know what the initial configuration should be.
- You are already using one of the Detect modes and moving to **Protect (Inline)** mode (in this case skip to *"Introduction - Protect (Inline) Mode" on page 562*). Or, you are already in **Protect (Inline)** mode but changing the scope of the policy groups it applies to (In this case, skip to *"Step 9 - Transport Rules (Protect (Inline) Mode)" on page 565*). Make the changes in the Protect rule).

Note - In this guide, **{portal}** refers to your portal name. The portal name can be found in the **Office 365 Install** window. For more information, see *"Portal Identifier of Avanan Tenant" on page 36*.

If you have any queries about how to apply these changes in the configuration, contact the *Avanan Support* for assistance.

Note - Manual deployment does not support user blocking or provide visibility into the Microsoft Quarantine. For more information, see *"Unified Quarantine for Manual Mode of Onboarding" on page 577*.

Manual Integration with Office 365 Mail - Required Permissions

You can choose **Manual mode** of integration when you do not want Avanan to automatically add and manage Mail Flow rules, connectors, and other Microsoft configurations for your organization.

As these configurations are not managed by Avanan, **Manual mode** require less permissions when compared with **Automatic mode**.

Permissions required from Office 365 for manual integration	Functions performed by Avanan
AuditLog.Read.All	Used to detect anomalous user behavior and trigger workflows for compromised accounts.
Contacts.Read	Used to protect contacts and scope policies for users.
Domain.Read.All	Collect protected domains to: ■ Secure domains. ■ Skip inspection and avoid returning emails from other domains to Microsoft. ■ Allow DMARC Management for these domains. ■ Automatically apply branding to the Security Awareness Training end user experience.
Group.Read.All	Used for mapping users to groups to properly assign policies to users.
InformationProtectionPolicy.Read.All	Read Microsoft Sensitivity Labels to use them as part of the Check PointDLP policy.
Mail.ReadWrite	Used for these: ■ Enforcing Detect and Remediate policy rules, where emails are quarantined or modified post-delivery. ■ Allowing administrators to quarantine emails that are already in the users' mailboxes. ■ Allowing administrators to restore emails to users' mailboxes. ■ Baselining communication patterns as part of **Learning Mode**.

Permissions required from Office 365 for manual integration	Functions performed by Avanan
MailboxSettings.ReadWrite	Used for these: ■ Read mailbox rules to detect compromised accounts. ■ Add a mailbox rule as part of the Greymail workflow.
Member.Read.Hidden	Used to collect hidden group members to support policy assignment, policy enforcement, and user-based reporting.
RoleManagement.Read.Directory	Used to collect users and their roles to scope policies, enforce them, and generate user-specific reports.
User.Read.All	Used to collect all users for the purposes of protection and policy scoping.
Directory.ReadWrite.All (Azure AD Graph)	Used for these: ■ Read users, groups, and other directory data during onboarding. ■ Read updates from Active Directory daily to influence policy assignments and other per user functions and configurations.
full_access_as_app (Office 365 Exchange Online)	Required to allow the execution of other Microsoft Exchange APIs.
Mail.ReadWrite (Office 365 Exchange Online)	Used for these: ■ Enforcing Detect and Remediate policy rules, where emails are quarantined or modified post-delivery. ■ Allowing administrators to quarantine emails that are already in the users' mailboxes. ■ Allowing administrators to restore emails to users' mailboxes. ■ Baselining communication patterns as part of **Learning Mode**.
ActivityFeed.Read (Office 365 Management APIs)	Collecting user login events, Microsoft defender events and Active Directory hierarchy changes to detect compromised accounts and maintain an up-to-date user hierarchy.

Permissions required from Office 365 for manual integration	Functions performed by Avanan
Send mail as any user	Used to send notifications to end users in scenarios where Microsoft does not support other delivery methods.

Policy Modes

These are the policy modes:

- **Monitor only** - Monitors the emails and creates the relevant event.
- **Detect and Remediate** - Creates an event, and also performs retroactive enforcement for Inbound emails already delivered to users.
- **Protect (Inline)** - All emails are reviewed before delivery to the user.

Monitor only and **Detect and Remediate** have the same configuration and are sometimes referred to as **Detect modes** in this document.

Best Practice - We recommend that you start with the configuration for **Detect modes** and later change to **Protect (Inline)**. If you are already in one of the Detect modes and want to start with Protect (Inline) mode, skip to *"Introduction - Protect (Inline) Mode" on page 562*.

Note - For the system to work properly, you must follow the steps in the order they appear.

Step 1 - Authorize the Manual Integration Application

1. From the **Getting Started Wizard**, click **Start** for Office 365 Mail.

   or

   From the left panel, go to **Security Settings** > **SaaS Applications**.
2. Click **Start** for Office 365 Mail.
3. Select **Manual mode** of operation.
4. In the **Office 365 Authorization** window that appears, sign in with your Microsoft Global Administrator credentials.
5. In the authorization screen, click **Accept** to grant permissions for **Avanan Cloud Security Platform - Emails - Manual Mode** application.

   For more information, see *"Permissions required from Office 365 for manual integration" on page 544*.

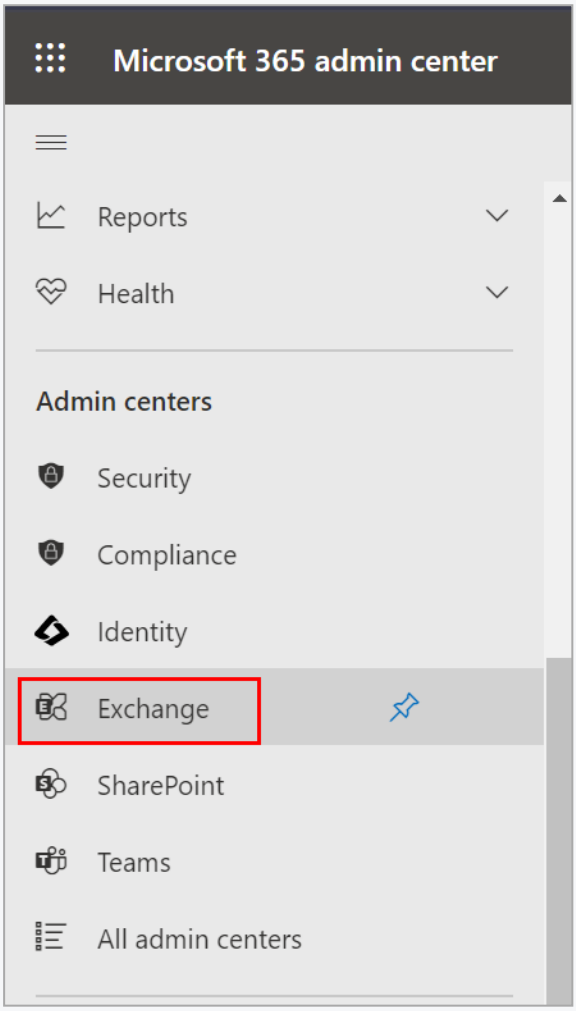
Step 2 - Avanan Contact

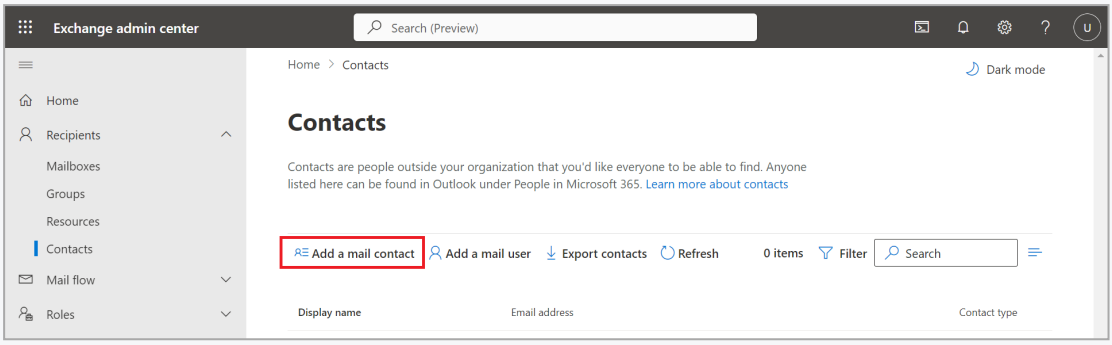
In the **Manual mode** of integration, you have to add a dedicated Avanan Contact.

This contact is used for the **Undeliverable Journal Reports** under **Journal Rules** in *"Step 3 - Journal Rule" on page 550*.

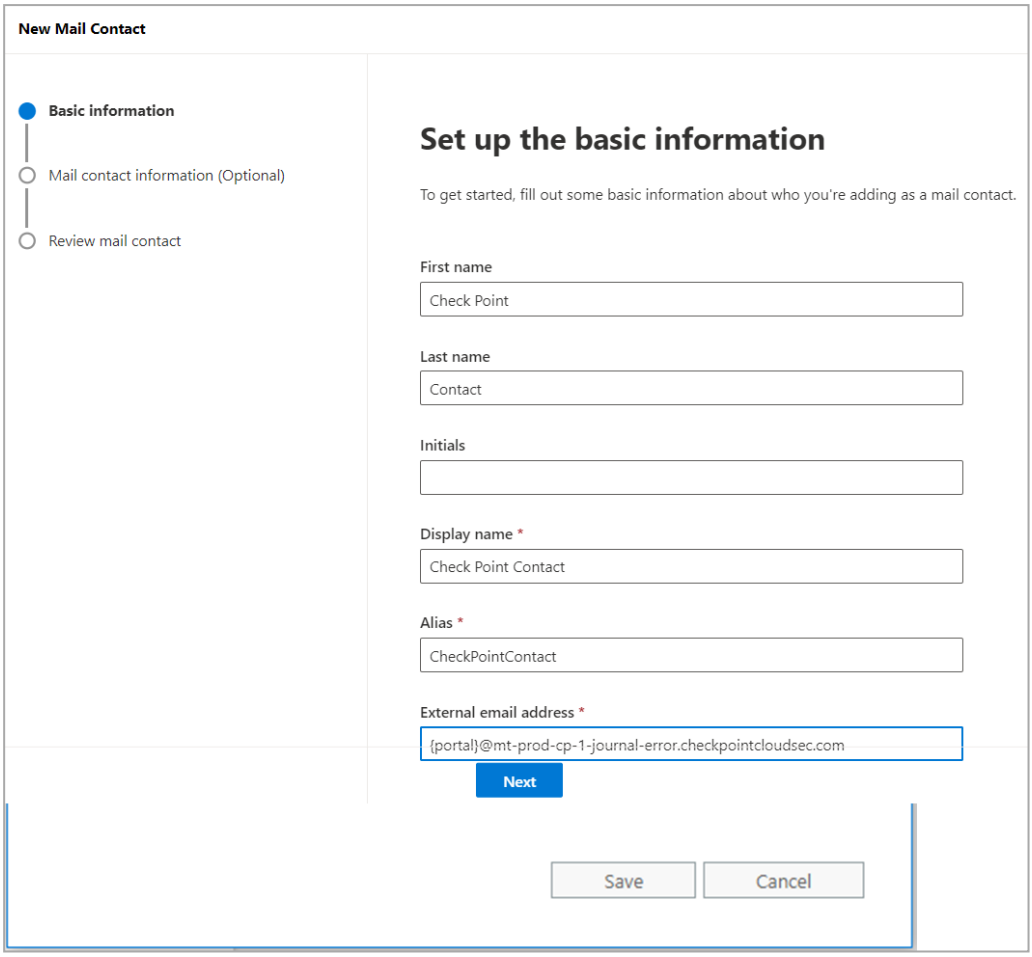
If you already configured a recipient for undeliverable journal rules, skip this step.

To add a contact

Step	Instructions
1	Log in to your Microsoft 365 admin account.
2	In the **Microsoft 365 admin center**, select **Exchange**. 
3	In the **Exchange admin center**, go to **Recipients** > **Contacts**.

Step	Instructions
4	Click **Add a mail contact**. 

Step	Instructions
5	In the **New Mail Contact** window, enter this information: ■ **First name** - Avanan (Optional) ■ **Initials** (Optional) ■ **Last name** - Contact (Optional) ■ **Display name** - Avanan Contact ■ **Alias** - AvananContact ■ **External email address**: • If your data residency is in the **United States** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-1-journal-error.checkpointcloudsec.com` • If your data residency is in **Australia** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-au-4-journal-error.checkpointcloudsec.com` • If your data residency is in **Canada** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-ca-1-journal-error.checkpointcloudsec.com` • If your data residency is in **Europe** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-eu-1-journal-error.checkpointcloudsec.com` • If your data residency is in **India** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-aps1-1-journal-error.checkpointcloudsec.com` • If your data residency is in **United Arab Emirates** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-mec1-1-journal-error.checkpointcloudsec.com` • If your data residency is in **United Kingdom** use (replace "`{portal}`" with your portal name): `{portal}@mt-prod-cp-euw2-1-journal-error.checkpointcloudsec.com`

Step	Instructions
	
6	Click **Next**.
7	(Optional) Enter the details about the Company and click **Done**.

Step 3 - Journal Rule

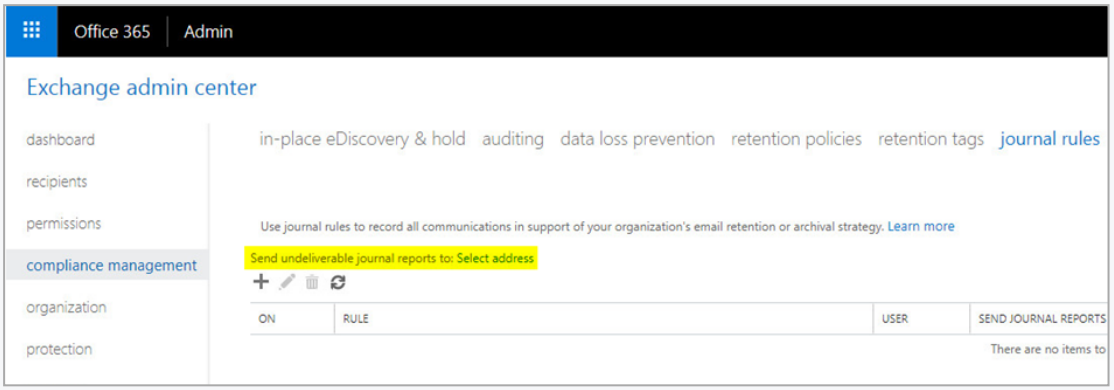
The **Journal rule** is used only for **Detect** modes (**Monitor only** or **Detect and Protect**).

The Journal rule configures Office 365 to send a copy of all scoped emails to the journaling mailbox used by Avanan for inspection.

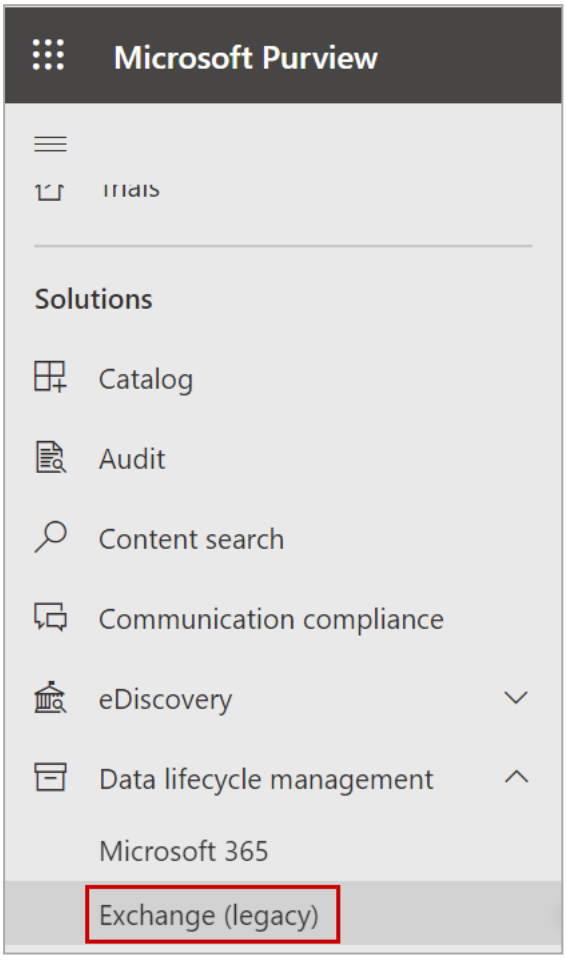
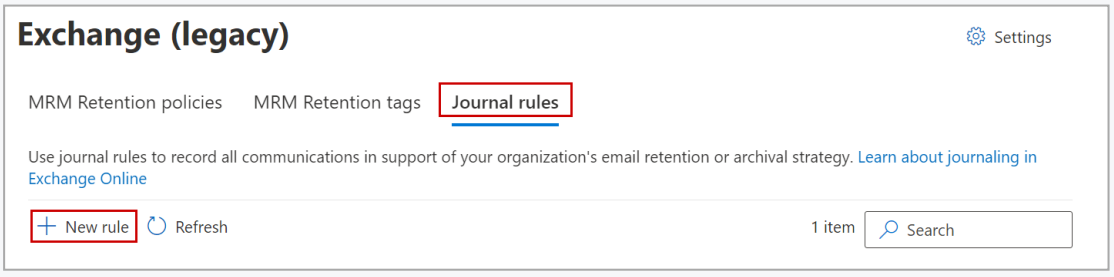
Notes -

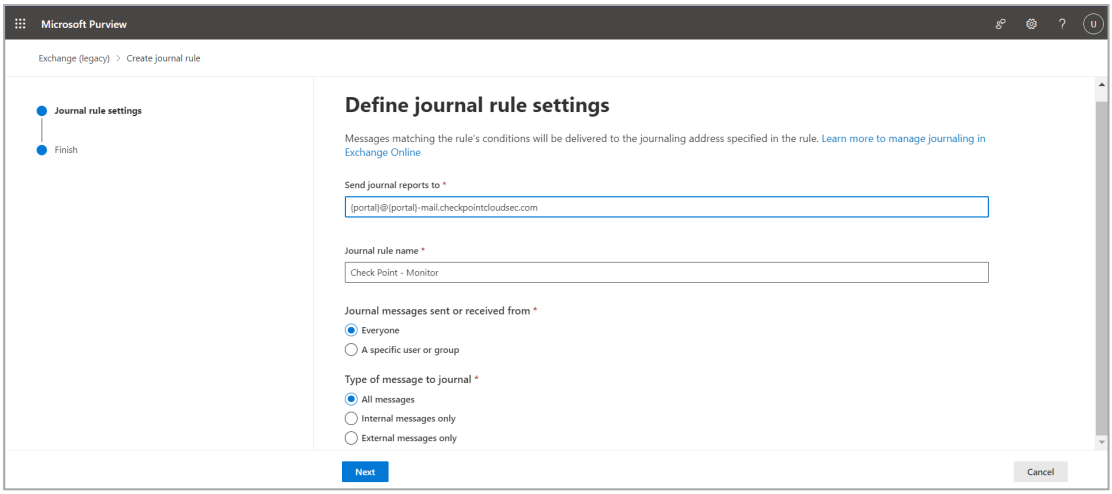
- Before you create a Journal rule, you must specify a mailbox to receive the Undeliverable journal report. If you already configured a mailbox for this purpose, skip this step and define only the journal rule.

To define an address for Undeliverable journal reports

Step	Instructions
1	In the **Exchange admin center**, go to **Compliance management** > **Journal rules**.
2	Click **Select address**. 
3	Click **Browse** and add the **Avanan Contact** created in *"Step 2 - Avanan Contact" on page 546*.

To configure the Journal rule

Step	Instructions
1	In the **Microsoft Purview**, from the left navigation pane, go to click **Data lifecycle management** > **Exchange (legacy)**. 
2	Click the **Journal rules** tab and click **New rule**. 

Step	Instructions
3	Enter this information in the **Define journal rule settings** window:  ■ For **Send journal reports to**, enter (replace "`{portal}`" with your portal name): `{portal}@{portal}-mail.avanan.net` ■ For **Name**, enter: Avanan - Monitor For **If the message is sent to or received from...**, select **(Apply to all messages)**. **Note** - If you plan to use group filters in your setup, select the group you want to include in your policy. ■ For **Journal the following messages...**, select **All messages**.
4	Click **Next**.
5	Review the settings and click **Submit**.

Step 4 - Connectors

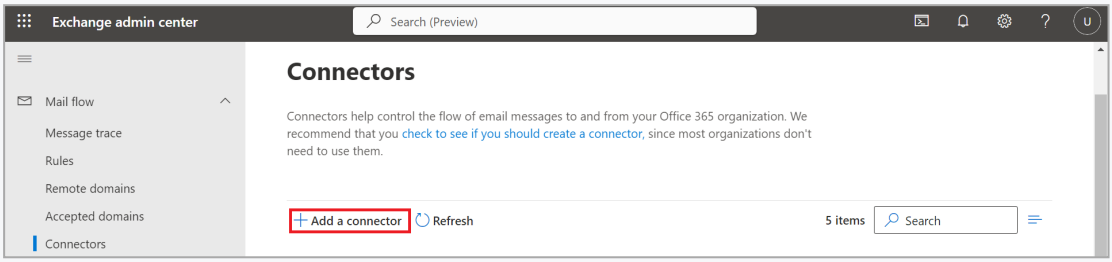
In this step, you define two connectors:

- **Inbound connector** - For all modes.
- **Journaling Outbound** - For Detect modes.

These connectors send traffic to and receive traffic from the cloud.

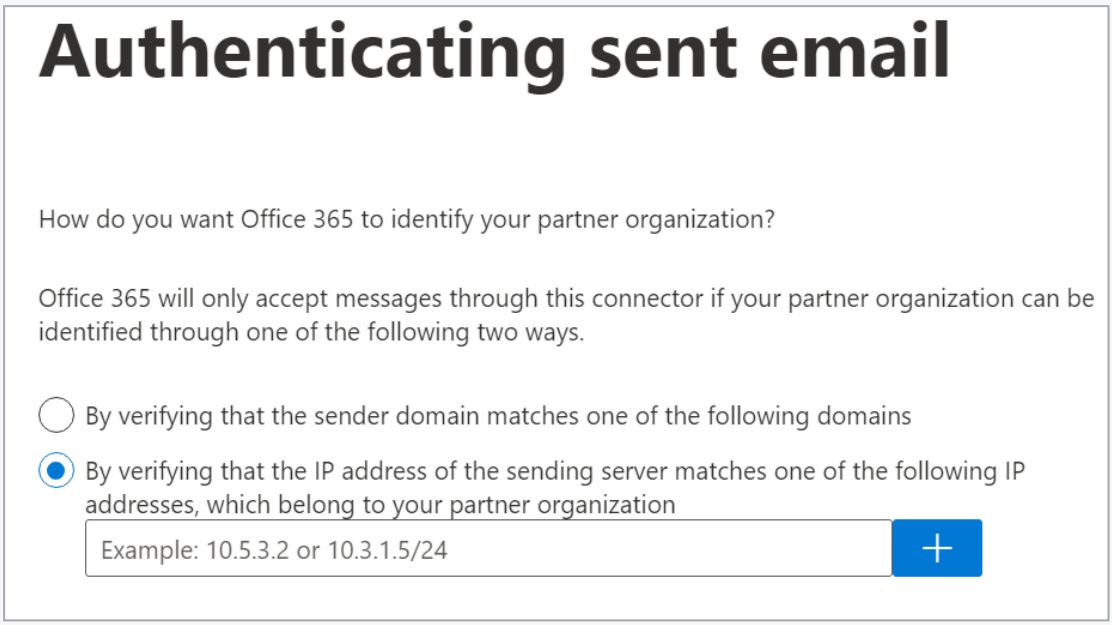
Note - These connectors are used for Detect modes. For information on the configuration for **Protect (Inline)** mode, see *"Introduction - Protect (Inline) Mode" on page 562*.

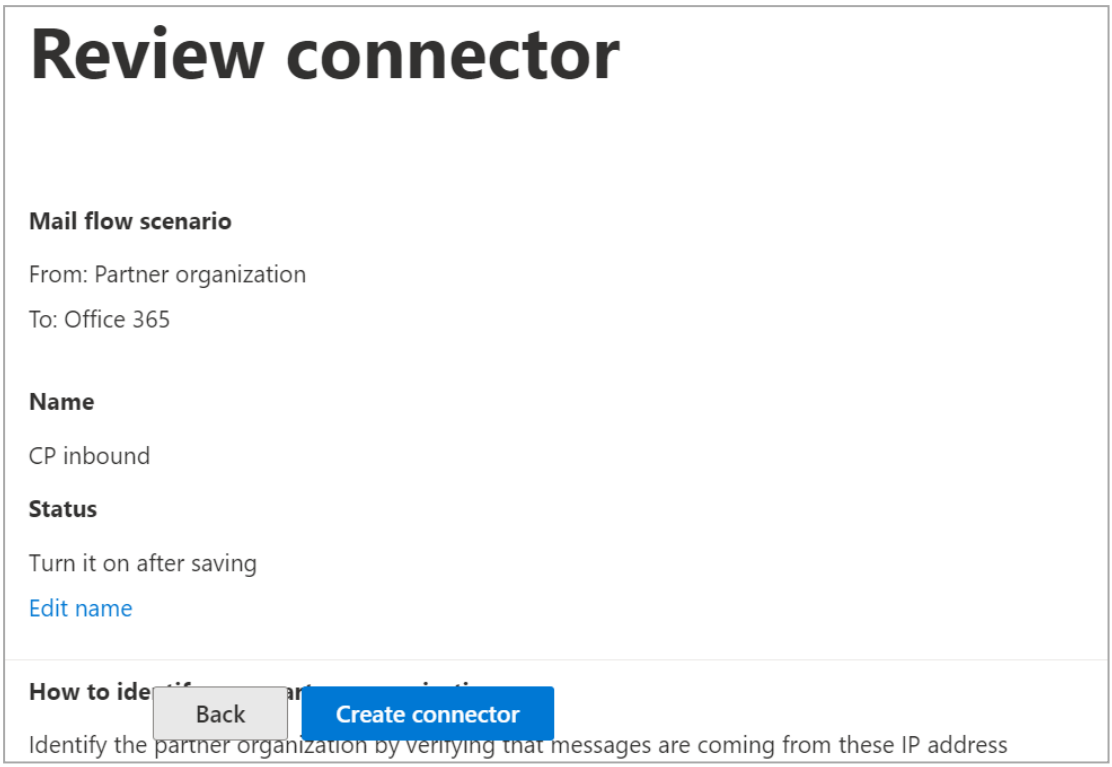
To create a new connector

Step	Instructions
1	In the **Exchange admin center**, from the left navigation pane, click **Mail flow** > **Connectors**.
2	To create a new connector, click **Add a connector**. 

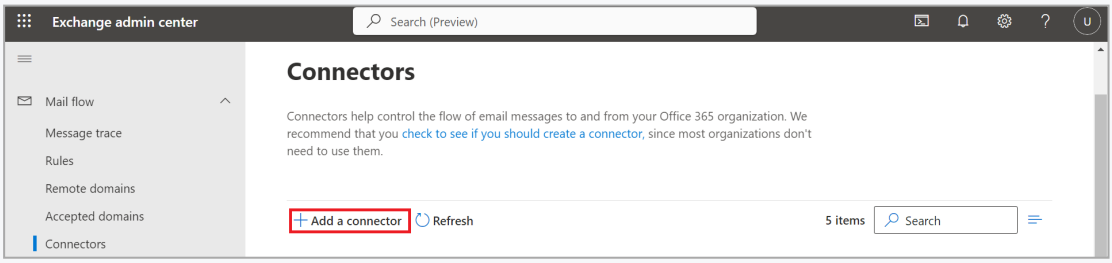
To configure the Avanan Inbound connector

Step	Instructions
1	For **From**, select **Partner organization**.
2	For **To**, select **Office 365**.
3	Click **Next**.
4	For **Name**, enter Avanan Inbound.
5	For **Description**, enter Avanan Inbound Connector.
6	For **What do you want to do after the connector is saved?**, select **Turn it on**.
7	Click **Next**.

Step	Instructions
8	For **How do you want to identify the partner organization**, select **By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your organization address**. 
9	Enter the IP address relevant to your region and click **+**. ■ If your data residency is in the **United States**, enter this IP address: `35.174.145.124` ■ If your data residency is in **Europe**, enter this IP address: `52.212.19.177` ■ If your data residency is in **Australia**, enter this IP address: `13.211.69.231` ■ If your data residency is in **Canada**, enter this IP address: `15.222.110.90` ■ If your data residency is in **India**, enter this IP address: `3.109.187.96` ■ If your data residency is in **United Arab Emirates**, enter this IP address: `3.29.194.128` ■ If your data residency is in **United Kingdom**, enter this IP address: `13.42.61.32`
10	Click **Next**.
11	For **What security restrictions do you want to apply?**, select **Reject email messages if they are not sent over TLS**.
12	Click **Next.**

Step	Instructions
13	In the **Review connector** window, verify the settings and click **Create connector**. 

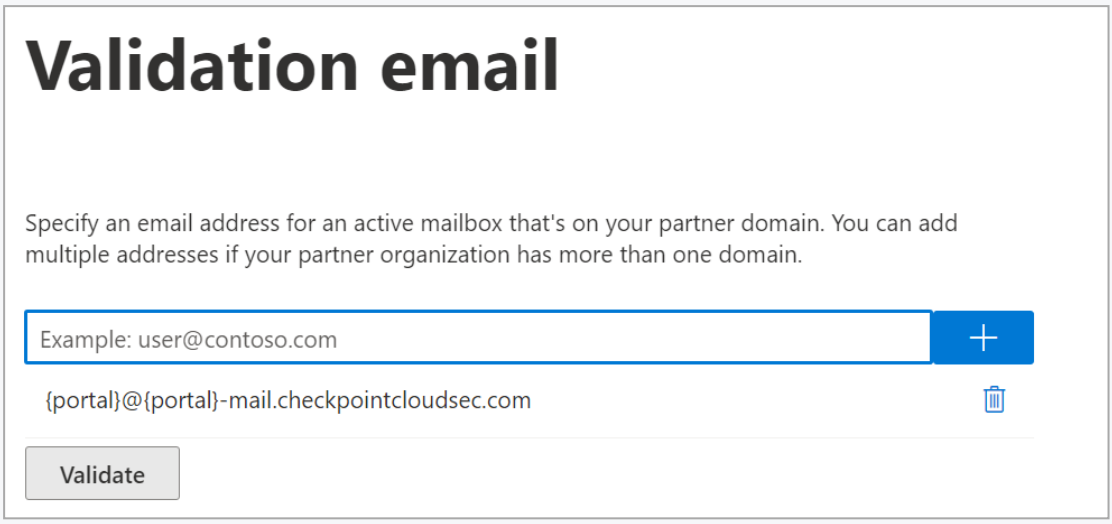
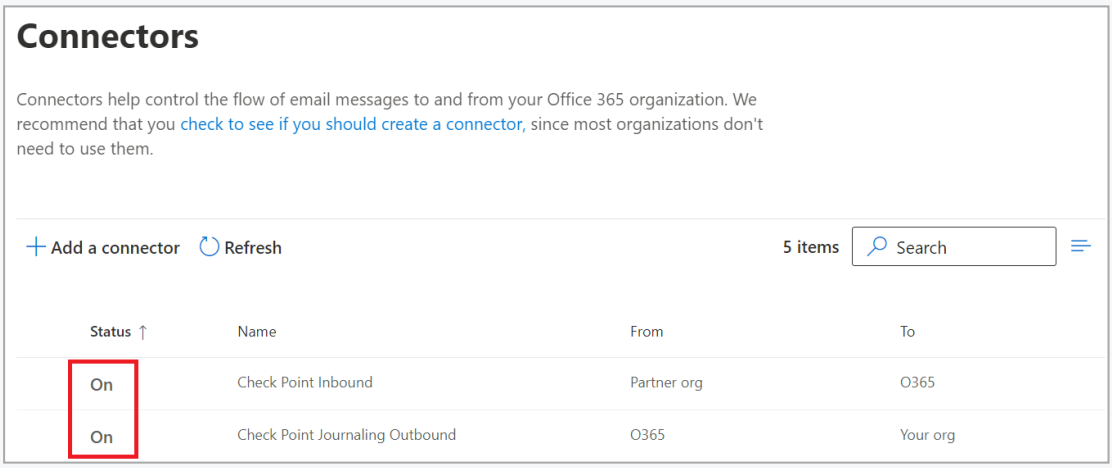
To create the Journaling Outbound connector

Step	Instructions
1	In the **Exchange admin center**, from the left navigation pane, click **Mail flow** > **Connectors**.
2	To create a new connector, click **Add a connector**. 

To configure the Journaling Outbound connector

Step	Instructions
1	For **From**, select **Office 365**.

Step	Instructions
2	For **To**, select **Partner organization**.
3	Click **Next**.
4	For **Name**, enter: `Avanan Journaling Outbound`
5	For **Description** (Optional), enter: `Avanan Journaling Outbound connector`
6	For **What do you want to do after connector is saved?**, select **Turn it on**.
7	Click **Next**.
8	For **When do you want to use this connector?**, select **Only when email messages are sent to these domains**.
9	Add the new domain: `{portal}-mail.avanan.net` (replace "`{portal}`" with your portal name) and then click **+**.
10	Click **Next**.
11	For **How do you want to route email messages?**, select **Route email through these smart hosts**.
12	Enter the host domain name: `{portal}-mail.avanan.net` (replace "`{portal}`" with your portal name) and then click **+**.
13	Click **Save** and then **Next**.
14	For **How should Office 365 connect to your partner organization's email server?**, select **Always use Transport Layer Security (TLS) to secure the connection**.
15	For **Connect only if the recipient's email server certificate matches this criteria**, select **Any digital certificate, including self-signed certificates**.
16	Click **Next**.
17	Check your settings before validation and click **Next**.

Step	Instructions
18	Click the **+** icon and Enter this email address: `{portal}-mail.avanan.net` (replace "`{portal}`" with your portal name) and click **+**. 
19	Click **Validate**.
21	Verify that the status of both the connectors are **On**. 

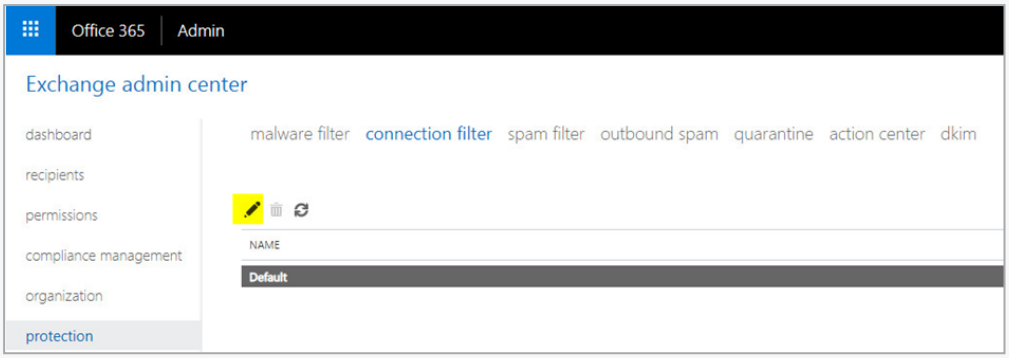
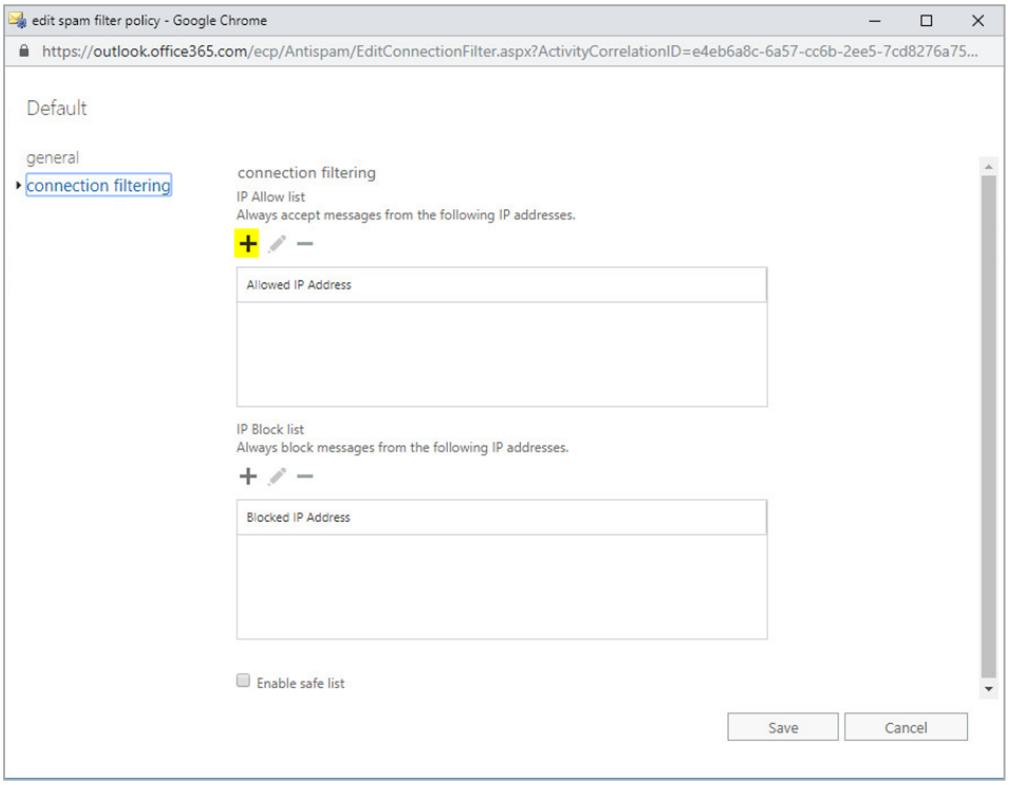
Step 5 - Connection Filter (All Modes)

Update the **Connection Filter** to Allow-list emails from Avanan.

This goes hand-in-hand with the Avanan Inbound Connector created in *"Step 4 - Connectors " on page 553*.

To configure the connection filter

Step	Instructions
1	In the **Exchange admin center**, go to **Protection** > **Connection filter**.

Step	Instructions
2	Click the icon to edit the default rule. 
3	Under **Connection filtering** > **IP Allow list**, click the **+** icon. 

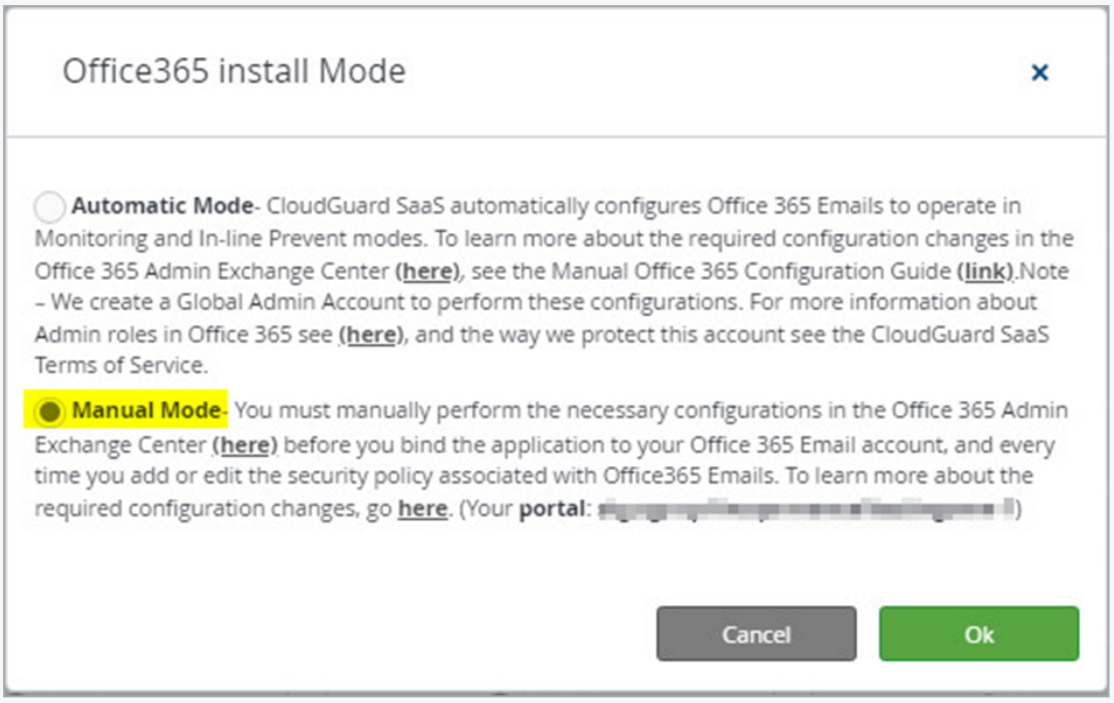
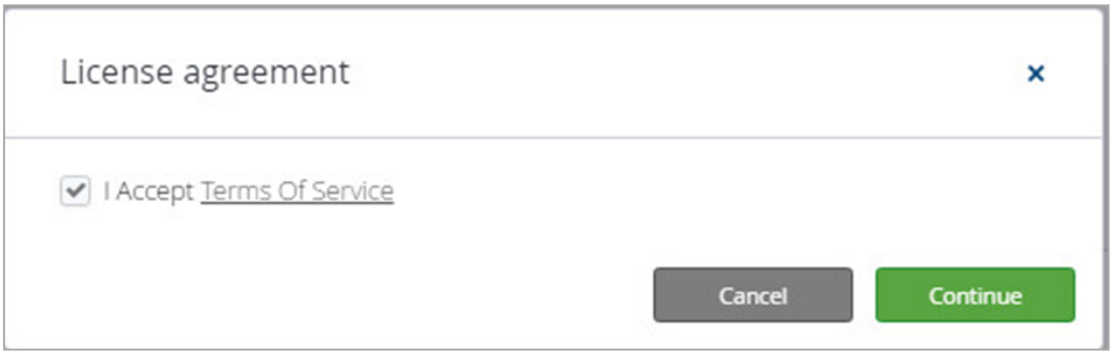
Step	Instructions
4	Under **Add allowed IP address**: ■ If your data residency is in the **United States**, enter this IP address: `35.174.145.124` ■ If your data residency is in **Europe**, enter this IP address: `52.212.19.177` ■ If your data residency is in **Australia**, enter this IP address: `13.211.69.231` ■ If your data residency is in **Canada**, enter this IP address: `15.222.110.90` ■ If your data residency is in **India**, enter this IP address: `3.109.187.96` ■ If your data residency is in **United Arab Emirates**, enter this IP address: `3.29.194.128` ■ If your data residency is in **United Kingdom**, enter this IP address: `13.42.61.32`

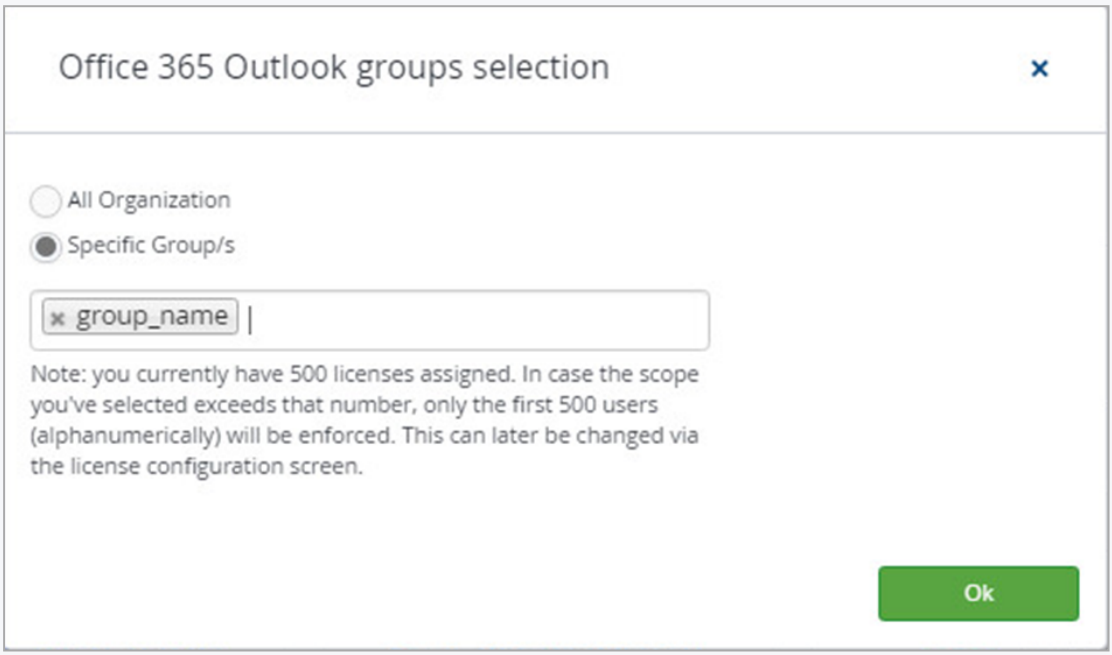
Step 6 - On-boarding (Monitor only & Detect and Remediate)

In this step, you are ready to integrate Avanan with Office 365 for **Monitor only** and **Detect and Remediate** modes.

To integrate Avanan with Office 365

Step	Instructions
1	Log in to Avanan and select the relevant tenant.
2	Click **Let's get started**.
3	Select the Office 365 service and click **Start**.

Step	Instructions
4	Select the **Manual Mode** checkbox. 
5	Accept the License agreement and click **Continue**. 
6	Authorize Office 365 event monitoring - click **Continue**.
7	Enter your Office 365 admin credentials and click **Accept**.

Step	Instructions
8	Authorize Office 365 security - click **Continue** and accept the terms. ■ If you selected **Apply to all messages** in *"Step 3 - Journal Rule" on page 550*, select **All Organization** in the window below. ■ If you specified a group, enter the group's name and click **OK**. **Note** - The group's name must be identical to the one that appears on Office 365. 
9	Move to step 2: Click **Next** and then **Start Now**.

Step 7 - Protect (Inline) Policy Configuration on Avanan

Introduction - Protect (Inline) Mode

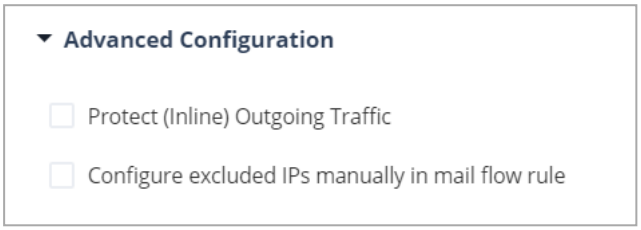
In **Protect (Inline)** mode, the system inspects all emails in scope before delivery to the users.

In manual mode, you must change the policy to **Protect (Inline)** before moving to Office 365 configurations.

To configure **Protect (Inline)** mode, follow Steps 7-9 below.

Note - To return to detect modes, disable the transport rules in *"Step 9 - Transport Rules (Protect (Inline) Mode)" on page 565*.

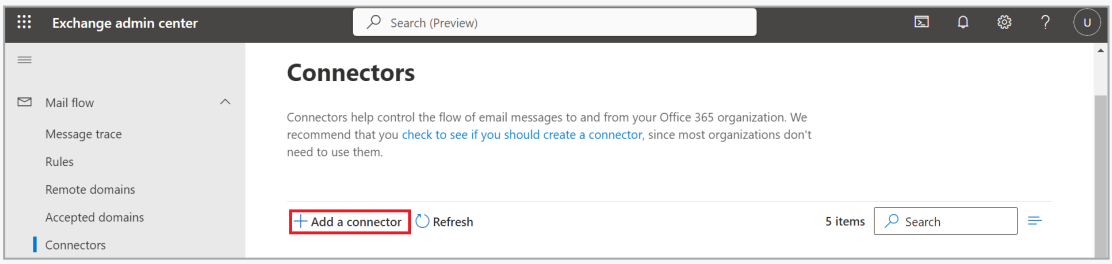
To configure the Protect (Inline) policy

Step	Instructions
1	Go to **Policy**.
2	In **Office 365 Emails**, change the **Mode** to **Protect (Inline)**.
3	Under **Advanced Configuration** select **Configure excluded IPs manually in mail flow rule**. 
4	Click **Save and apply**.

Step 8 - Connectors (Protect (Inline) Mode)

In this step, you define the outbound connector for **Protect (Inline)** mode.

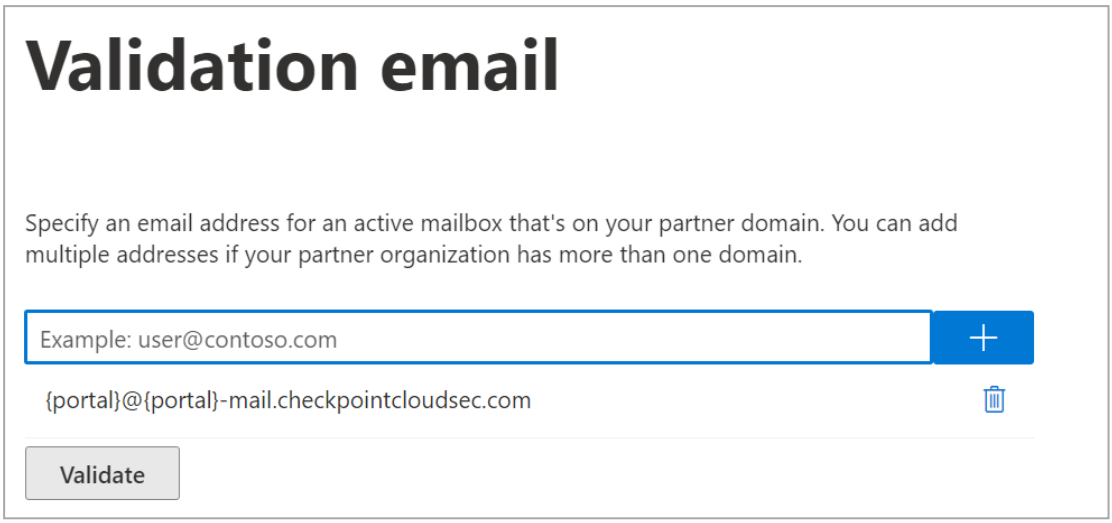
To create the Avanan Outbound connector

Step	Instructions
1	In the **Exchange admin center**, from the left navigation pane, click **Mail flow** > **Connectors**.
2	To create a new connector, click **Add a connector**. 

To configure the Avanan Outbound connector:

Step	Instructions
1	For **From**, enter: `Office 365`
2	For **To**, enter the partner organization.
3	Click **Next**.

Step	Instructions
4	For **Name**, enter: `Avanan Outbound`
5	For **Description** (Optional), enter: `Avanan Outbound Connector`
6	For **What do you want to do after connector is saved?**, select **Turn it on** and click **Next**. To enable Inline protection for Microsoft 365 Mail, you must select the **Retain internal Exchange email headers** checkbox in the Check Point DLP Outbound Connector.
7	For **When do you want to use this connector?**, select **Only when I have a transport rule to set up that redirects messages to this connector** and then click **Next**.
8	For **How do you want to route email messages?**, select **Route email through these smart hosts**.
9	Add a smart host: `{portal}-host.avanan.net` (replace "`{portal}`" with your portal name) and then click **+**.
10	Click **Next**.
11	For **How should Office 365 connect to your partner organization's email server?**, select **Always use Transport Layer Security (TLS) to secure the connection**.
12	For **Connect only if the recipient's email server certificate matches this criteria**, select **Any digital certificate, including self-signed certificates** and click **Next**.
13	Confirm your settings before validation and click **Next**.
14	Enter this email address: `{portal}-host.avanan.net` (replace "`{portal}`" with your portal name) and then click **+**.

Step	Instructions
15	Click **Validate**. 
16	Verify that the **Status** of the connector is **On**.

Step 9 - Transport Rules (Protect (Inline) Mode)

The purpose of the transport rule is to implement the inline mode for the users that need to be inline. Every time you change the scope of the inline policy (add or remove users/groups) you need to edit the scope of the transport rule accordingly.

Note - If any mail flow rules already exist, the Avanan rules must be prioritized.

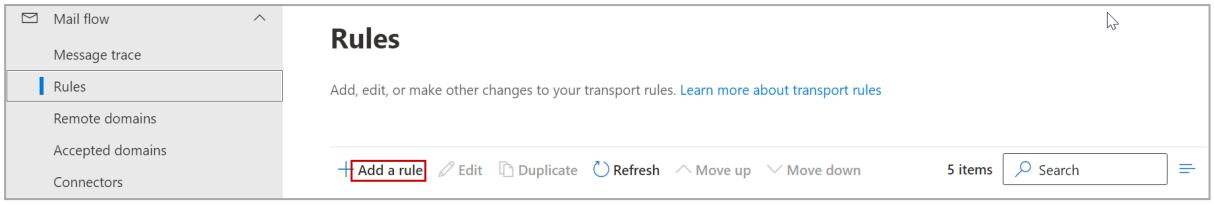
These are the Avanan rules:

1. *"Avanan - Protect Internal" below*
2. *"Avanan - Protect" on page 568*
3. *"Avanan - Allow-List" on page 572*
4. *"Avanan - Junk Filter" on page 573*

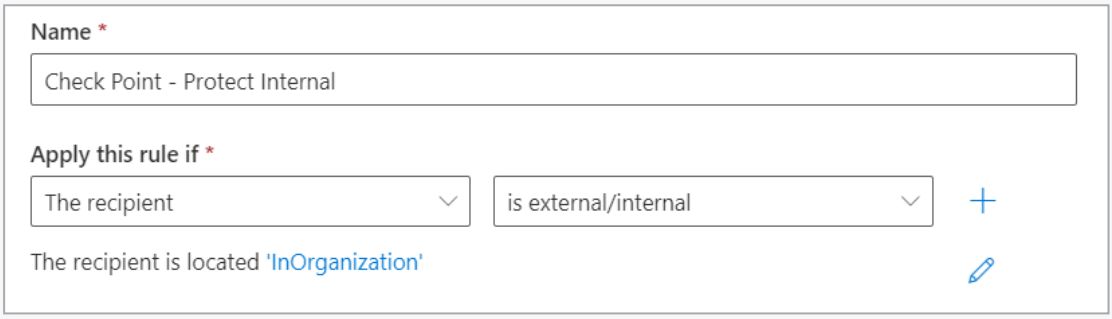
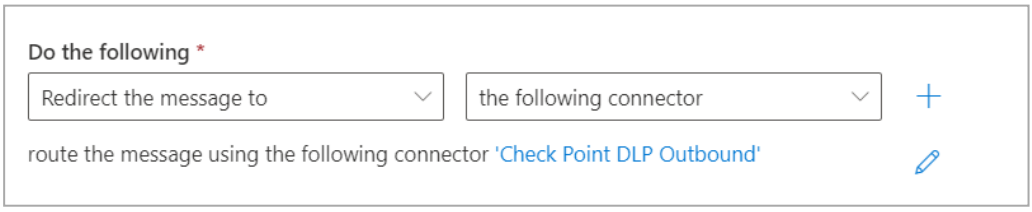
Avanan - Protect Internal

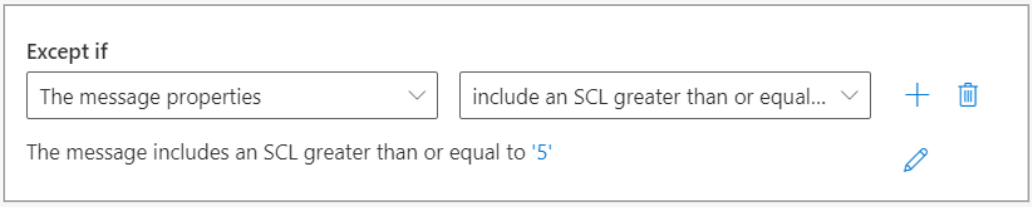
To create the Avanan - Protect rule

1. In the **Exchange admin center**, Click **Mail flow** > **Rules**.
2. To add a rule, click **Add a rule** and select **Create a new rule**.



To configure the Avanan - Protect rule as the first mail-flow rule

Step	Instructions
1	For **Name**, enter Avanan - Protect Internal.
2	For **Apply this rule if...**, add this condition: The sender is located outside the organization. 
3	For **Do the following...**, add these two actions: 1. Modify the message properties: a. In the first field, select **Modify the message heading**. b. In the next field, select **set the message header**. c. Click the first **Enter text** and enter `X-CLOUD-SEC-AV-Info` d. Click the second **Enter text** and enter this value: `{portal}, office365_emails, inline` (replace "`{portal}`" with your portal name) 2. Redirect the message to:**Use the following connector**, select **Avanan DLP Outbound** connector.  a. In the first field, select **Redirect the message to**. b. In the next field, select **the following connector**. c. Select **Avanan DLP Outbound** connector and click **Save**.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>For Except if..., add these two exceptions:
The message has an SCL greater than or equal to 5.
 

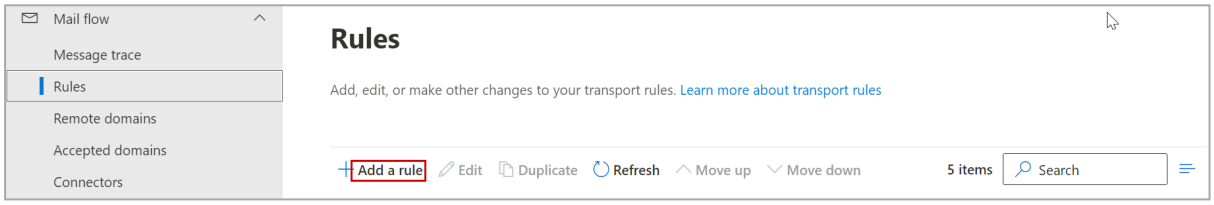
<ol type="a">
In the first field, select The message properties.
In the next field, select include an SCL greater than or equal to.
From the dropdown, select 5 and click Save.
Sender's IP address is in the range:<ol type="a">
In the first field, select The sender.
In the next field, select IP address is in any of these ranges or exactly matches.
Enter the IP address, click Add and then click Save.
If your data residency is in the United States, enter this IP address:
<code>35.174.145.124</code>
If your data residency is in Europe, enter this IP address:
<code>52.212.19.177</code>
If your data residency is in Australia, enter this IP address:
<code>13.211.69.231</code>
If your data residency is in Canada, enter this IP address:
<code>15.222.110.90</code>
If your data residency is in India, enter this IP address:
<code>3.109.187.96</code>
If your data residency is in United Arab Emirates, enter this IP address:
<code>3.29.194.128</code>
If your data residency is in United Kingdom, enter this IP address:
<code>13.42.61.32</code>
Note - If you have other inbound connectors using IP addresses, add their IP addresses to this list.</td></tr>
<tr><td>5</td><td>Click Next.</td></tr>
<tr><td>6</td><td>In the Rule mode, select Enforce.</td></tr>
</table>

Step	Instructions
7	Select the **Stop processing more rules** checkbox.
8	In the **Match sender address in message** field, select **Header**.
9	Click **Finish**.

Avanan - Protect

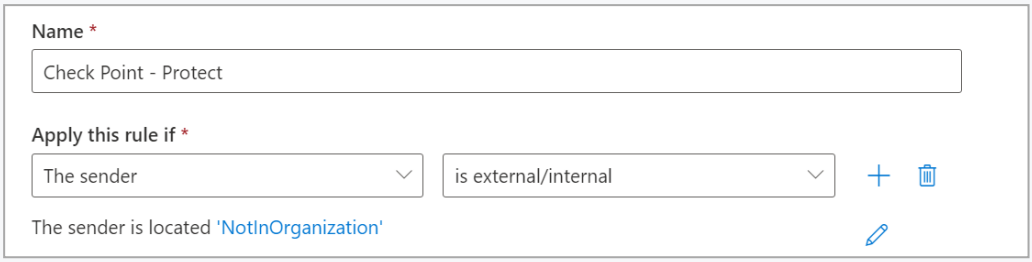
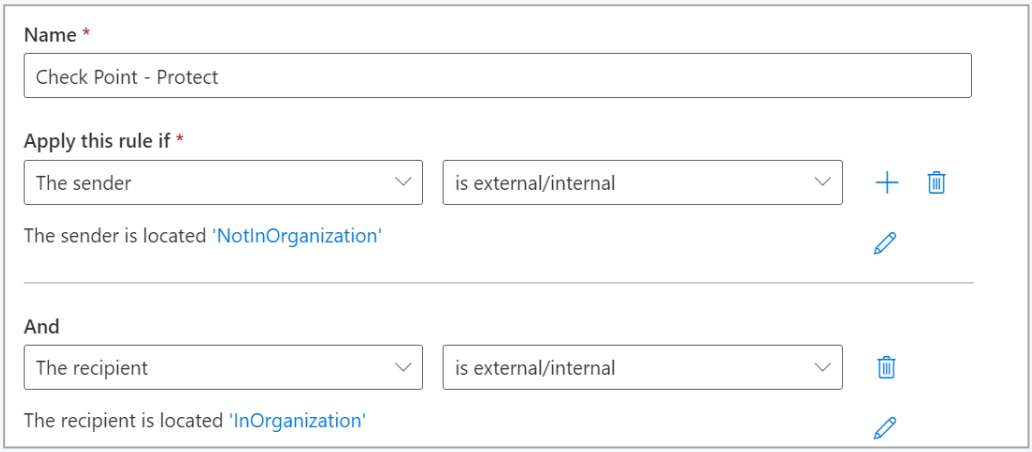
To create the Avanan - Protect rule

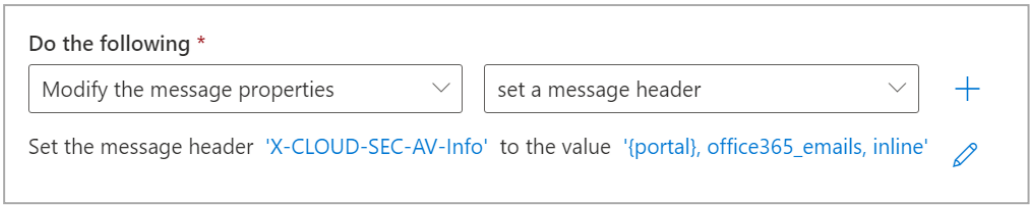
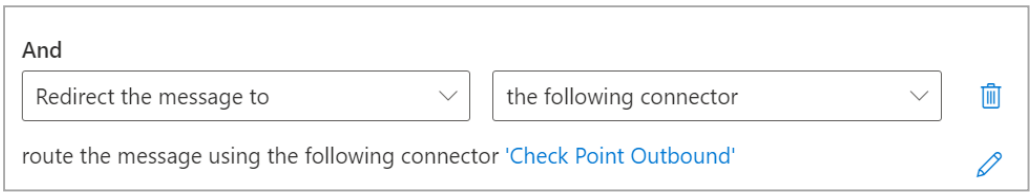
1. In the **Exchange admin center**, Click **Mail flow** > **Rules**.
2. To add a rule, click **Add a rule** and select **Create a new rule**.

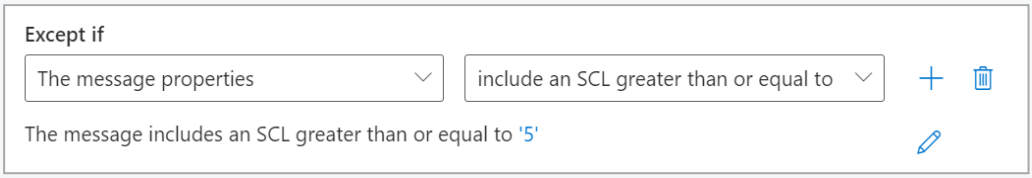


To configure the Avanan - Protect rule as the first mail-flow rule

Step	Instructions
1	For **Name**, enter Avanan - Protect.

Step	Instructions
2	For **Apply this rule if...**, add two conditions: 1. The sender is located outside the organization.  2. The recipient is located inside the organization.  If necessary, add another condition and specify the groups that should be inline.

Step	Instructions
3	For **Do the following...**, add these two actions: 1. Modify the message properties:  a. In the first field, select **Modify the message heading**. b. In the next field, select **set the message header**. c. Click the first **Enter text** and enter `X-CLOUD-SEC-AV-Info` d. Click the second **Enter text** and enter this value: `{portal}, office365_emails, inline` (replace "`{portal}`" with your portal name) 2. Redirect the message to:**Use the following connector**, select **Avanan Outbound** connector.  a. In the first field, select **Redirect the message to**. b. In the next field, select **the following connector**. c. Select **Avanan - Outbound** connector and click **Save**.

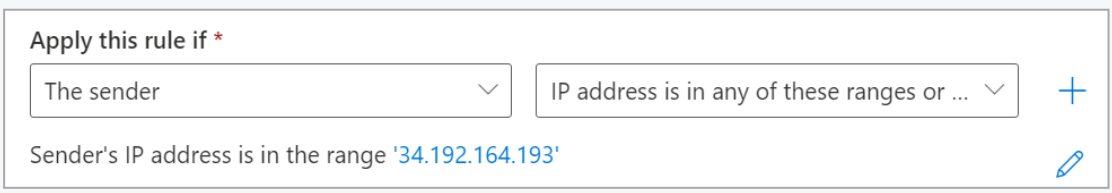
<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>For Except if..., add these two exceptions:
The message has an SCL greater than or equal to 5.
 

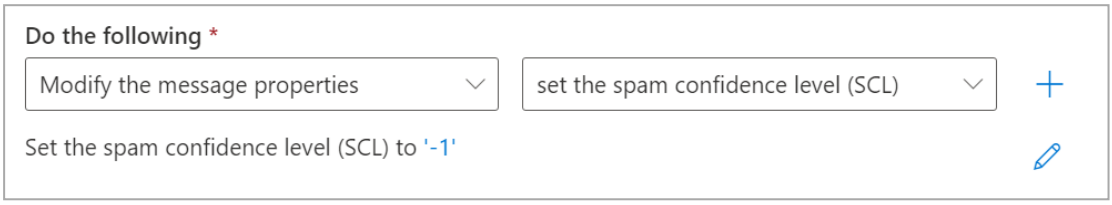
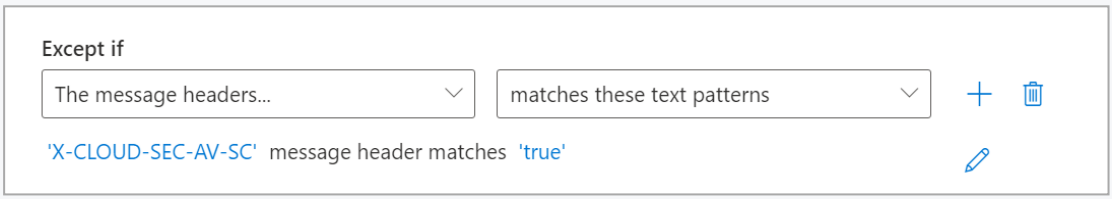
<ol type="a">
In the first field, select The message properties.
In the next field, select include an SCL greater than or equal to.
From the dropdown, select 5 and click Save.
Sender's IP address is in the range:<ol type="a">
In the first field, select The sender.
In the next field, select IP address is in any of these ranges or exactly matches.
Enter the IP address, click Add and then click Save.
If your data residency is in the United States, enter this IP address:
<code>35.174.145.124</code>
If your data residency is in Europe, enter this IP address:
<code>52.212.19.177</code>
If your data residency is in Australia, enter this IP address:
<code>13.211.69.231</code>
If your data residency is in Canada, enter this IP address:
<code>15.222.110.90</code>
If your data residency is in India, enter this IP address:
<code>3.109.187.96</code>
If your data residency is in United Arab Emirates, enter this IP address:
<code>3.29.194.128</code>
If your data residency is in United Kingdom, enter this IP address:
<code>13.42.61.32</code>
Note - If you have other inbound connectors using IP addresses, add their IP addresses to this list.</td></tr>
<tr><td>5</td><td>Click Next.</td></tr>
<tr><td>6</td><td>In the Rule mode, select Enforce.</td></tr>
</table>

Step	Instructions
7	Select the **Stop processing more rules** checkbox.
8	In the **Match sender address in message** field, select **Header**.
9	Click **Finish**.

Avanan - Allow-List

To configure the Avanan Allow-List rule

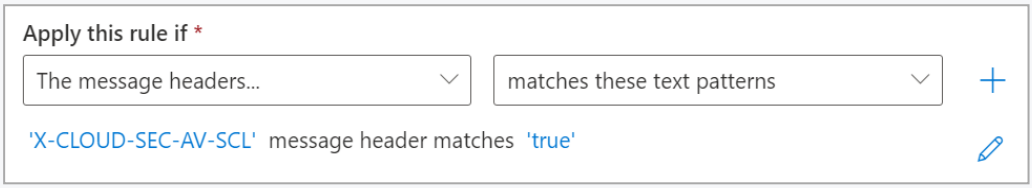
Step	Instructions
1	In the **Name** field, enter `Avanan - Allow-List`
2	In the **Apply this rule if...** field, sender's IP address: 1. In the first field, select **The sender**. 2. In the next field, select **IP address is in any of these ranges or exactly matches**. 3. Enter the IP address, click **Add** and then click **Save**. • If your data residency is in the **United States**, enter this IP address: `35.174.145.124` • If your data residency is in **Europe**, enter this IP address: `52.212.19.177` • If your data residency is in **Australia**, enter this IP address: `13.211.69.231` • If your data residency is in **Canada**, enter this IP address: `15.222.110.90` • If your data residency is in **India**, enter this IP address: `3.109.187.96` • If your data residency is in **United Arab Emirates**, enter this IP address: `3.29.194.128` • If your data residency is in **United Kingdom**, enter this IP address: `13.42.61.32` 

Step	Instructions
3	For the **Do the following...** field, select **set the spam confidence level (SCL) to... > Bypass spam filtering**. 1. In the first field, select **The message properties**. 2. In the next field, select **set the spam confidence level (SCL)**. 3. Select **Bypass spam filtering** and click **Save**. 
4	For the **Except if...** field, select **A message header matches these text patterns**.  1. In the first field, select **The message header**. 2. In the next field, select **matches these text patterns**. 3. Click the first **Enter text**, enter `X-CLOUD-SEC-AV-SCL` and click **Save**. 4. Click the second **Enter text**, enter the value **true**, click **Add** and then click **Save**.
5	Click **Next**.
6	In the **Rule mode**, select **Enforce**.
7	Select the **Stop processing more rules** checkbox.
8	In the **Match sender address in message** field, select **Header**.
9	Click **Finish**.

Avanan - Junk Filter

To configure the Avanan Junk filter rule

Step	Instructions
1	In the **Name** field, enter `Avanan - Junk Filter`

Step	Instructions
2	For the **Apply this rule if...** field, add these two conditions: 1. **The message header matches these patterns**: a. In the first field, select **The message header**. b. In the next field, select **matches these text patterns**. c. Click the first **Enter text**, enter `X-CLOUD-SEC-AV-SCL` and click **Save**. d. Click the second **Enter text**, enter the value **true**, click **Add** and then click **Save**.  2. **Senders IP address is in the range**: a. In the first field, select **The sender**. b. In the next field, select **IP address is in any of these ranges or exactly matches**. c. Enter the IP address, click **Add** and then click **Save**. • If your data residency is in the **United States**, enter this IP address: `35.174.145.124` • If your data residency is in **Europe**, enter this IP address: `52.212.19.177` • If your data residency is in **Australia**, enter this IP address: `13.211.69.231` • If your data residency is in **Canada**, enter this IP address: `15.222.110.90` • If your data residency is in **India**, enter this IP address: `3.109.187.96` • If your data residency is in **United Arab Emirates**, enter this IP address: `3.29.194.128` • If your data residency is in **United Kingdom**, enter this IP address: `13.42.61.32`

Step	Instructions
3	For the **Do the following...** field, do these: 1. In the first field, select **The message properties**. 2. In the next field, select **set the spam confidence level (SCL)**. 3. Select **9** for Bypass spam filtering and click **Save**. 
4	Click **Next**.
5	In the **Rule mode**, select **Enforce**.
6	Select the **Stop processing more rules** checkbox.
7	In the **Match sender address in message** field, select **Header**.
8	Click **Finish**.

Transport Rules

Office 365 Transport rules automate actions on emails-in-traffic based on custom policies. In most enterprise environments, every transport rule falls under either Delivery Rule or Modification Rule.

Delivery Rule: A transport rule that modifies the delivery of the email

- Quarantine emails from "abc.com"
- Allow-List emails coming from IP 111.111.111.111
- Mark emails with Nickname = "John" as Spam (SCL)
- Send emails to Connector XYZ
- Forward emails sent to X to Y

Modification Rule: A transport rule that modifies the content of the email

- Add "[EXTERNAL]" to the subject if sender is Outside Organization
- Add disclaimer to the email body footer

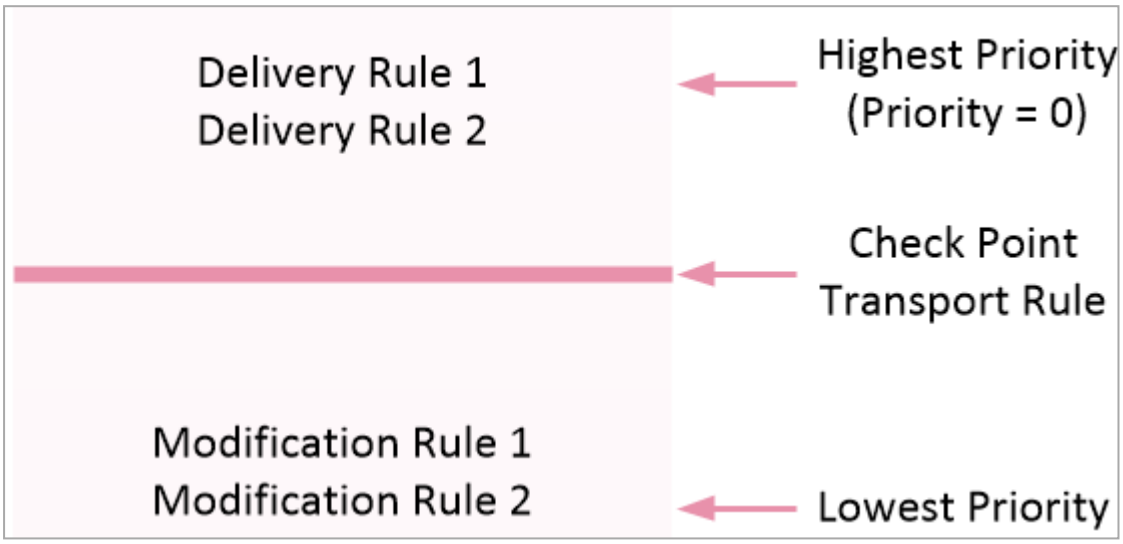
Avanan Transport Rule Optimal Priority

The Avanan Protect policy for Office 365 Exchange automatically creates a transport rule with the name of "Avanan - Protect" with default priority of 0 (highest priority).

Unless you have a reason to keep your rules in a specific order, keep the Delivery Rules on top of the Modification Rules. Place the Avanan Protect Rule between the Delivery Rules and the Modification Rules.

Contact *Avanan Support* if one of these is true:

- There is a 3rd party integration that receives the mail-flow.
- The rules only function is a specific order.

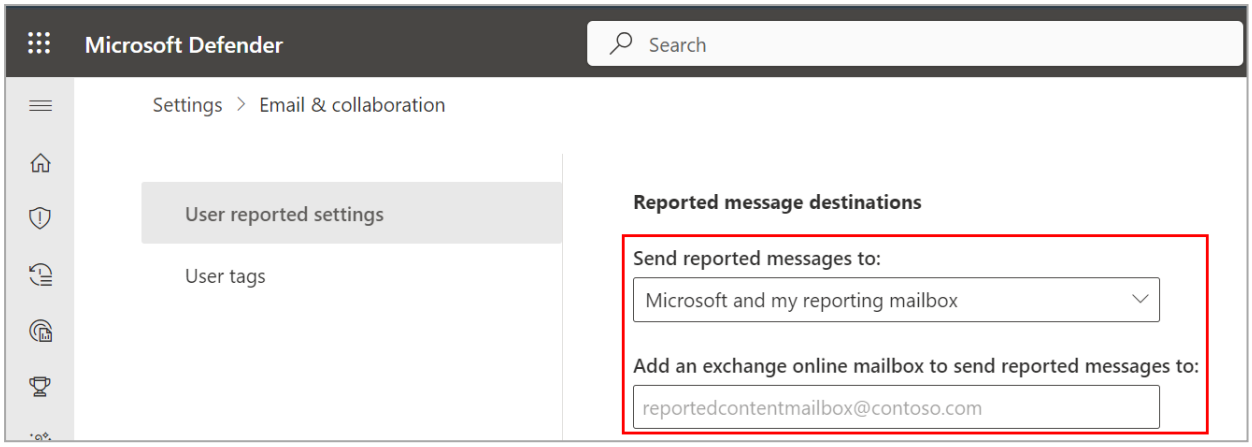


Step 10 - Sending User Reported Phishing Emails to an Internal Mailbox

To handle phishing reports effectively, Avanan requires that reports sent through the Microsoft Report Phishing / Report Message add-in are also sent to an internal mailbox. This mailbox can be an existing dedicated mailbox or a new shared mailbox that does not require a Microsoft license.

To send user reported phishing emails to an internal mailbox:

1. Log in to the Microsoft Defender portal.
2. Click **Settings** > **Avanan** > **User reported settings**.
3. Scroll down to the **Reported message destinations** section and do these:



a. In the **Send reported messages to:** field, select **Microsoft and my reporting mailbox**.

b. In the **Add an exchange online mailbox to send reported messages to:** field, enter the dedicated mailbox email address.

4. Click **Save**.

Reverting Manual Onboarding / Switching to Automatic Onboarding

To switch the onboarding from **Manual mode** to **Automatic mode** or to disconnect Avanan from your Office 365 account, follow these steps:

1. Navigate to **Security Settings > SaaS Applications**.
2. Click **Stop** for all the Office 365 SaaS applications.
3. Follow all the steps in *"Appendix A: Avanan Manual Integration with Office 365" on page 543*, and remove every rule and object you created.
4. Contact *Avanan Support* so that Avanan support finalizes the process in the backend.

   After the confirmation from *Avanan Support*, the reverting process is complete.
5. To start the onboarding in **Automatic mode**, follow the procedure in *"Activating Office 365 Mail" on page 47*.

Unified Quarantine for Manual Mode of Onboarding

Some organizations prefer **Manual mode** of onboarding for these reasons:

- The permissions required by the **Avanan Cloud Security Platform - Emails V2** enterprise application for **Automatic mode** are too high for the organization.
- The organization prefers that Avanan do not automatically change mail flow rules, connectors, transport rules, and so on in their Microsoft Azure cloud platform.

However, to get visibility on emails quarantined by Microsoft (Unified Quarantine) and act on them, Avanan requires permissions that are requested only by the **Avanan Cloud Security Platform - Emails V2** application in the **Automatic mode** of onboarding.

For customers using Avanan in **Manual mode** who agree to grant the necessary permissions (see *"Required Roles and Permissions" on page 49*) to the **Avanan Cloud Security Platform - Emails V2** application, but prefer not to have Avanan manage mail flow rules, connectors, transport rules, and other configurations in their Microsoft Azure, can still use Unified Quarantine.

To do that:

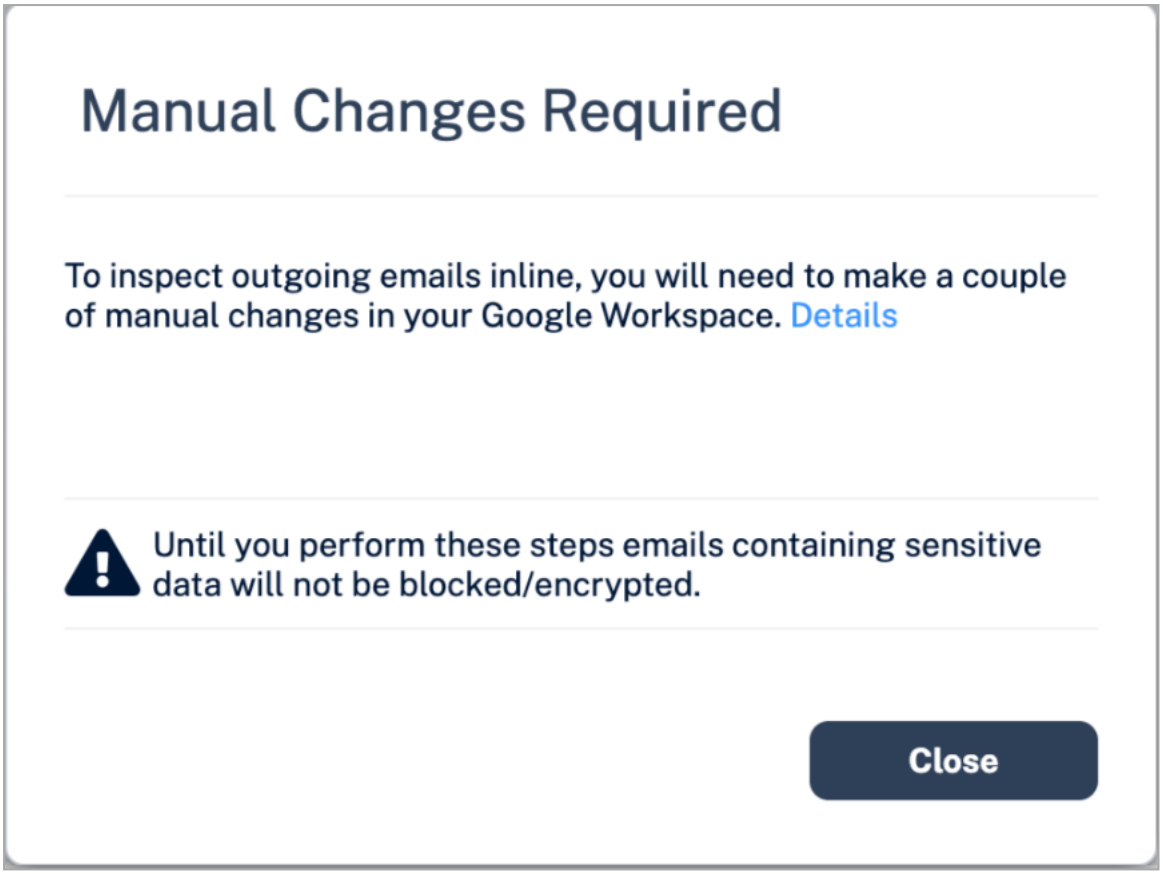
1. Contact *Avanan Support* with the request.
2. After approval from the support representative, re-authorize the Office 365 Mail application with Microsoft administrator credentials.
    a. Click **Security Settings** > **SaaS Applications**.
    b. Click **Configure** for Office 365 Mail.
    c. Click **Re-Authorize Avanan Office 365 Email App**.
    d. Follow the onscreen instructions and authorize the Microsoft 365 application.

    You can see that Avanan is using a different application requiring more permissions.

Unified Quarantine is enabled and the application will not make any changes to your Microsoft 365 configuration.

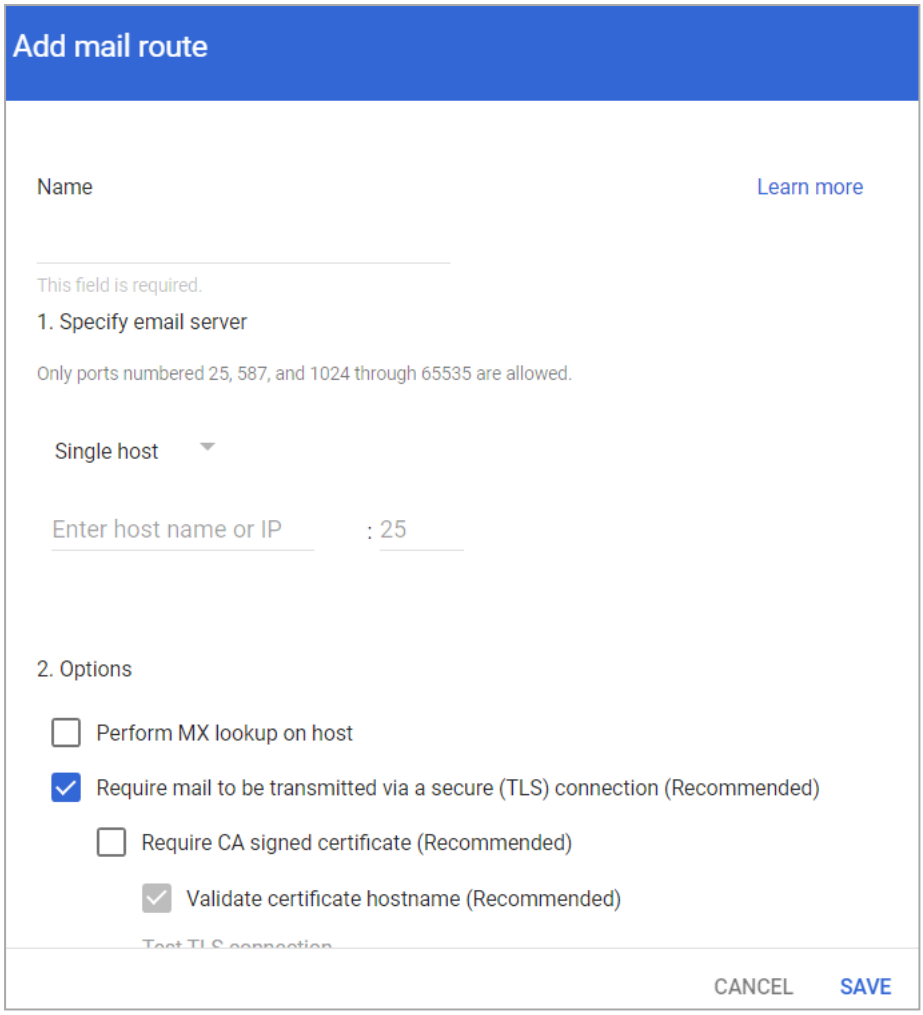
Appendix B: Manual Steps for Enabling Gmail Prevent (Inline) DLP Policy

If you receive the **Manual Changes Required** message while creating a **Prevent (Inline)** DLP policy for Gmail, you must make these changes in the Google Admin Console.



Step 1: Adding a Host

1. Sign in to the Google Admin Console.
2. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
3. Click **Hosts**.
4. Click **Add Route**.
5. Under **Name**, enter **CLOUD-SEC-AV DLP Service**.



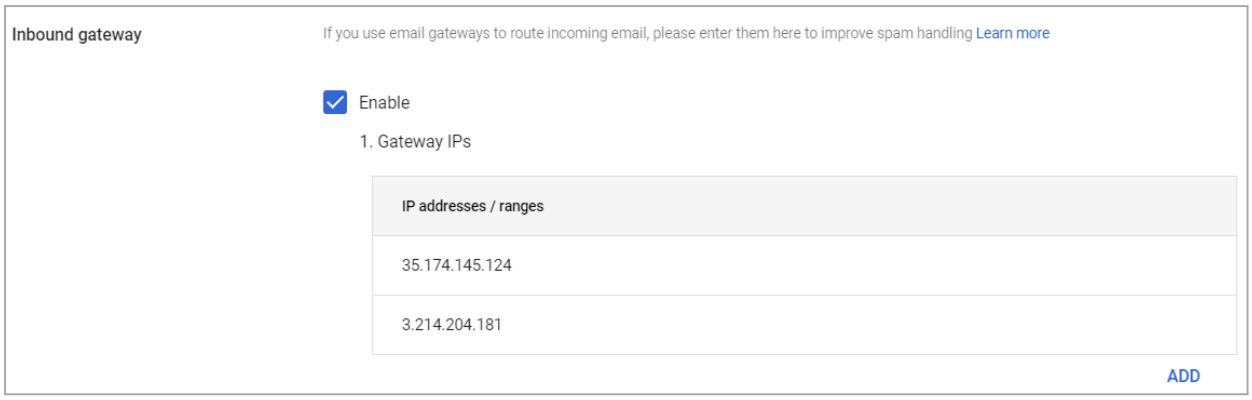
6. Under **Specify email server**, select **Single host**.
7. Enter the host name as **[portal identifier]-dlp.avanan.net**.

   To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.
8. Enter the port number as **25**.
9. Under **Options**, clear the **Require CA signed certificate** checkbox.
10. Click **Save**.

Step 2: Updating Inbound Gateway

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll down and click **Spam, Phishing and Malware**.
3. Click **Inbound gateway**.
4. Select **Enable** and under **Gateway IPs**, click **Add** and enter the IP address or IP address range relevant to your Avanan tenant (account) region.

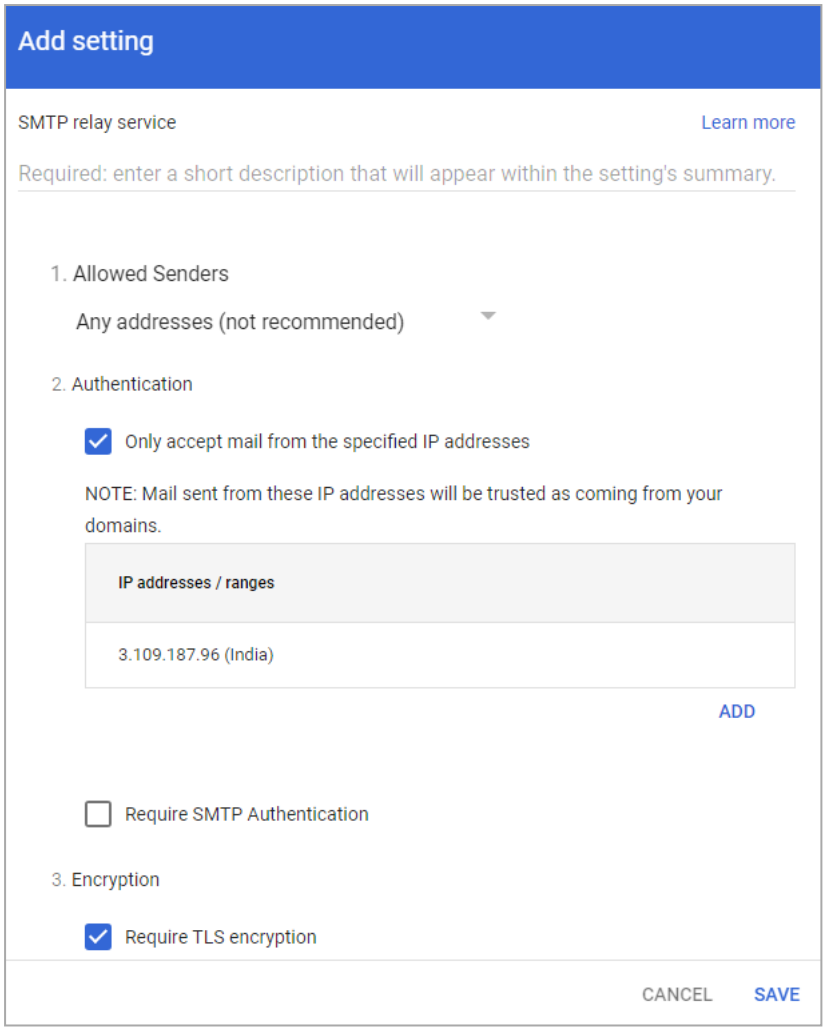
For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 591*.



5. Click **Save**.

Step 3: Adding SMTP Relay Host

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll-down and click **Routing**.
3. Under **SMTP relay service**, click **Add Another Rule**.
4. Enter a description for the rule.



5. In the **Allow Senders** list, select **Any Addresses** checkbox.
6. Under **Authentication**, do these:

a. Select the **Only accept mail from the specified IP addresses** checkbox.

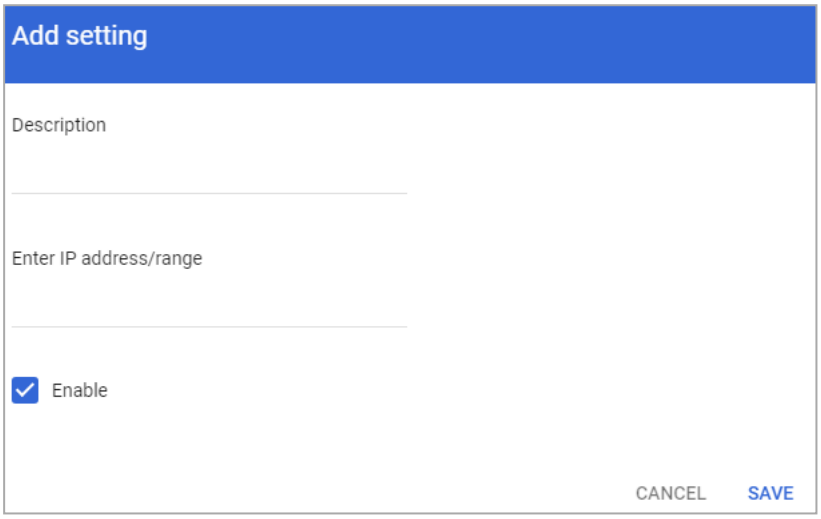
b. Add all the IP addresses relevant to your Avanan tenant (account) region.

For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 591*.

To add an IP address:

i. Click **Add**.

ii. Enter a **Description** for the IP address.



iii. Enter the IP address.

iv. Select the **Enable** checkbox.

v. Click **Save**.

c. Clear the **Require SMTP Authentication** checkbox.

7. Under **Encryption**, select the **Require TLS encryption** checkbox.

8. Click **Save**.

Step 4: Add Groups

You must create two groups.

- avanan_inline_outgoing_policy
- avanan_monitor_outgoing_policy

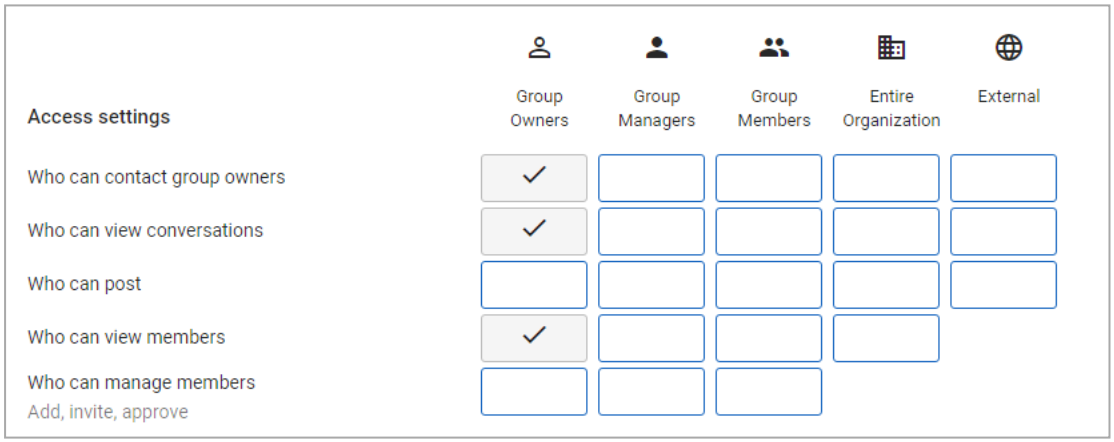
Note - If you use GCDS (Google Cloud Directory Sync) to synchronize your user groups on-premises and in the cloud, the synchronization triggers the deletion of these Avanan groups. Though this will not impact the email delivery, Avanan cannot scan the emails, and no security events get generated.

Before activating Google Workspace, you must create exclusion rules for these user groups. Select the exclusion type as **Group Email Address**, match type as **Exact Match**, and the group email address should be in the *groupname@[domain]* format.

For example, the group email addresses should be **avanan_inline_outgoing_policy@mycompany.com** and **avanan_monitor_outgoing_policy@mycompany.com**, where mycompany is the name of your company.

To create a group:

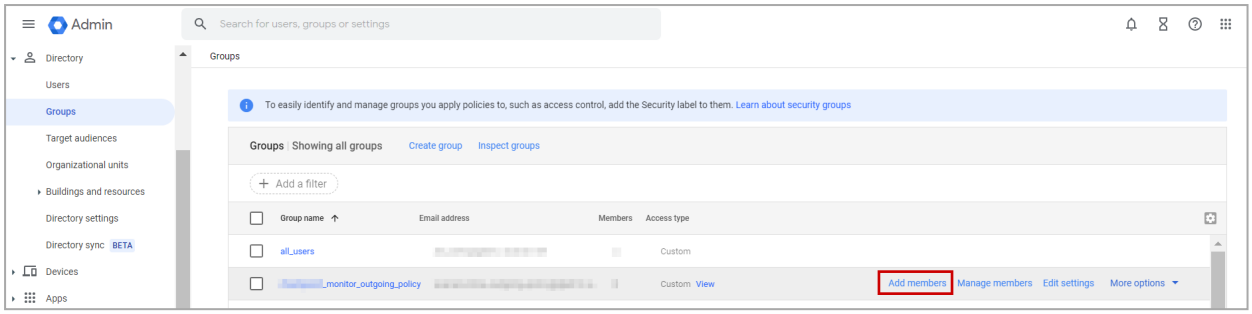
1. From the left navigation panel, click **Directory** > **Groups**.
2. Click **Create Group**.
3. In **Group name** field, enter the group name. For example, **avanan_inline_outgoing_policy**.
4. In **Group email** field, enter the group email. For example, **avanan_inline_outgoing_policy**.
5. Click **Next**.
6. In **Access Settings**, clear everything except the default settings.



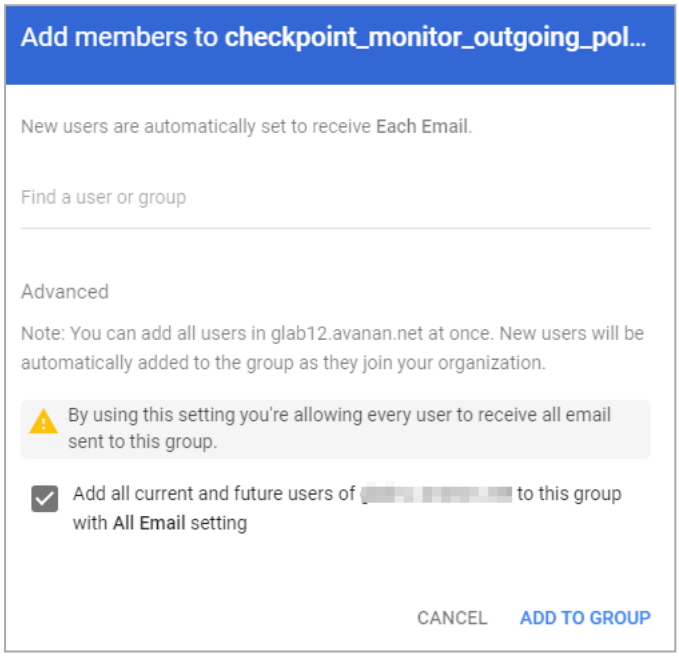
7. In **Who can join the group**, select **Anyone in the organization can join**.
8. Click **Create Group**.
9. Repeat the same procedure and create a group with **Group name** and **Group email** as **avanan_monitor_outgoing_policy**.

After creating the groups, you must do these to the **avanan_monitor_outgoing_policy** group.

1. From the left navigation panel, click **Directory** > **Groups**.
2. Hover over the **avanan_monitor_outgoing_policy** group you created and click **Add members**.



3. Click **Advanced** and select the **Add all current and future users of {domain} to this group with All Email setting** checkbox.



4. Click **Add to Group**.

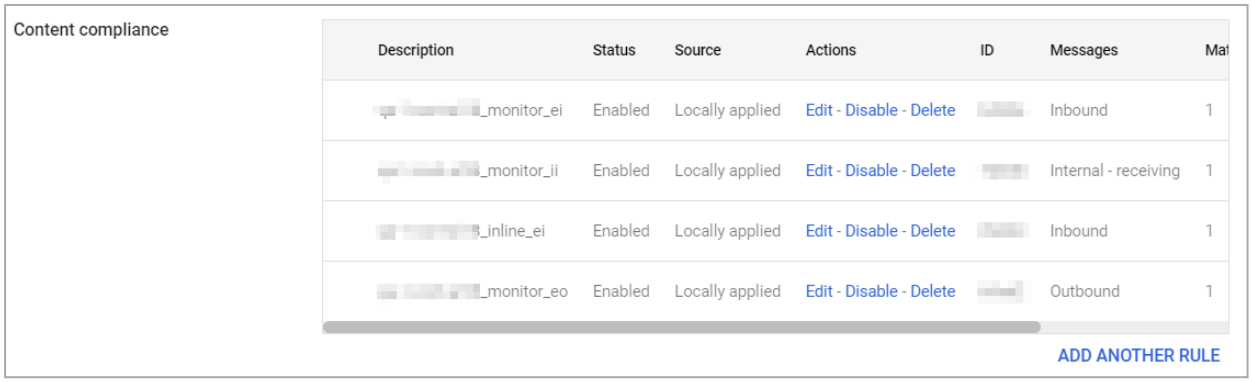
Step 5: Create a Compliance Rule

1. From the left navigation panel, click **Apps** > **Google Workspace** > **Gmail**.
2. Scroll-down and click **Compliance**.

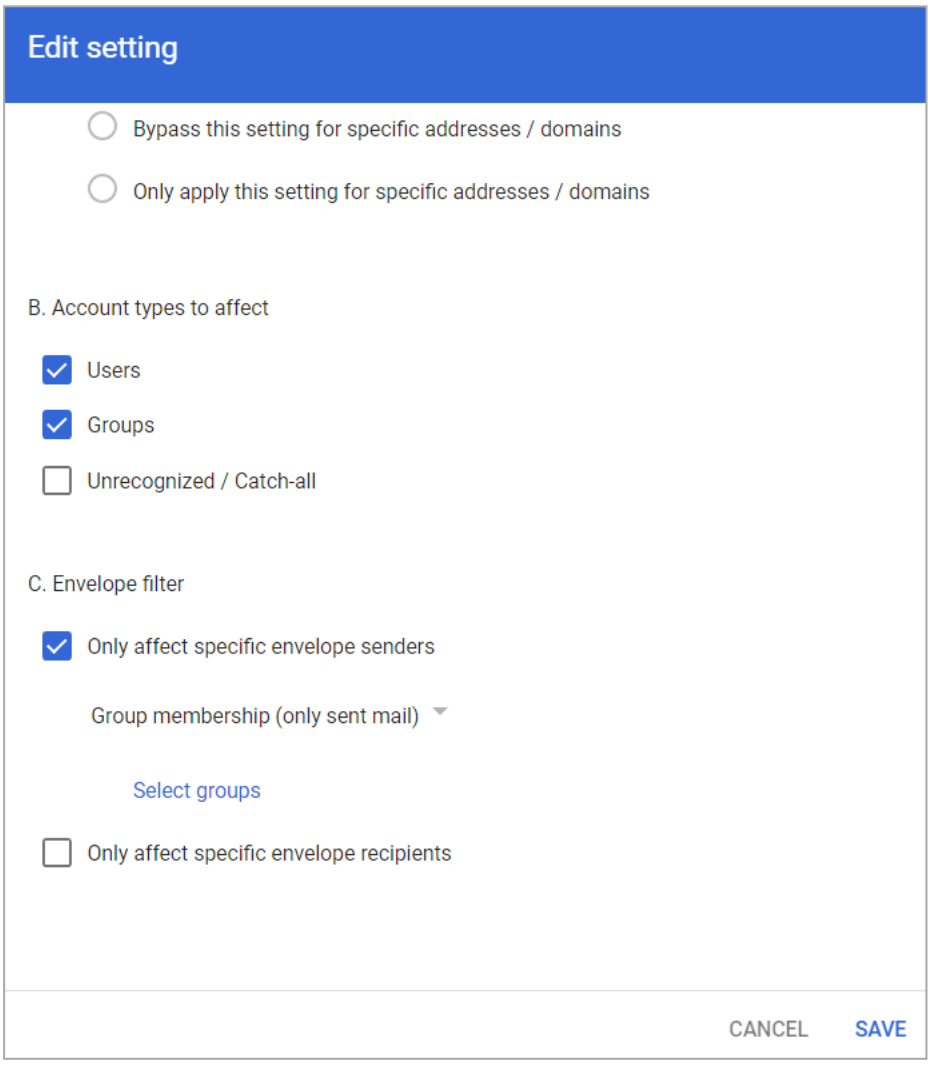
   By default, the system shows these rules in **Content compliance**:

   - [portal identifier]_monitor_ei
   - [portal identifier]_monitor_ii
   - [portal identifier]_monitor_eo
   - [portal identifier]_inline_ei

   To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.



3. Update the settings for **[portal identifier]_monitor_eo** rule.
   a. For **[portal identifier]_monitor_eo** rule, click **Edit**.
   b. Scroll-down to the end of the **Edit setting** pop-up and click **Show options**.
   c. Under **Envelope filter**, select the **Only affect specific envelope senders** checkbox.



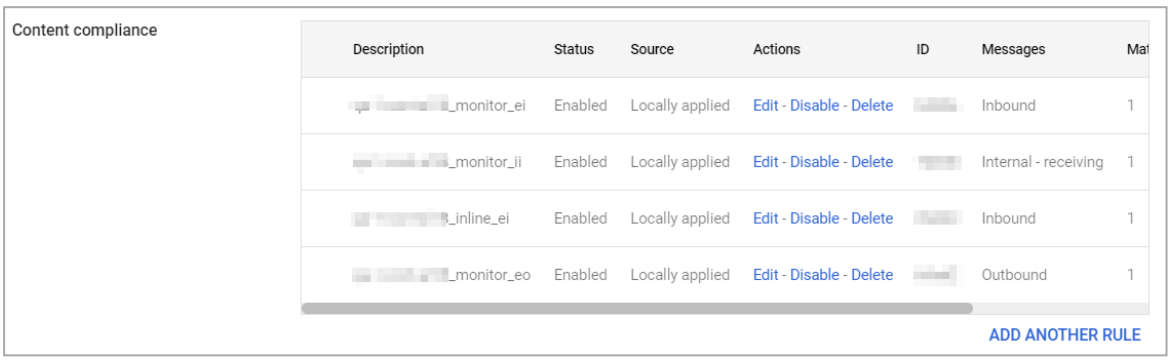
d. From the list, select **Group membership (only sent mail)**.

e. Click **Select groups** and select **avanan_monitor_outgoing_policy**.

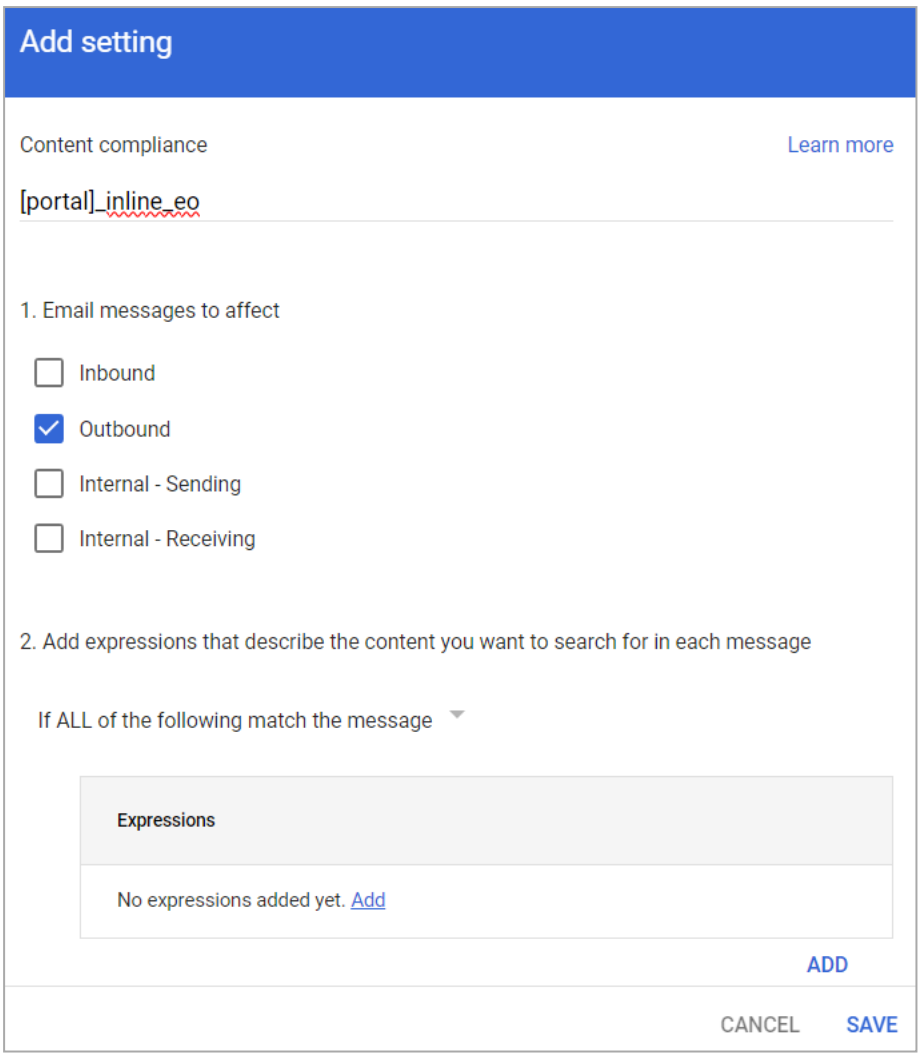
f. Click **Save**.

4. Create the **[portal identifier]_inline_eo** rule with these settings:

   a. From the **Content compliance** rules, click **Add Another Rule**.



b. Enter the **Content compliance** rule name as **[portal identifier]_inline_eo**.



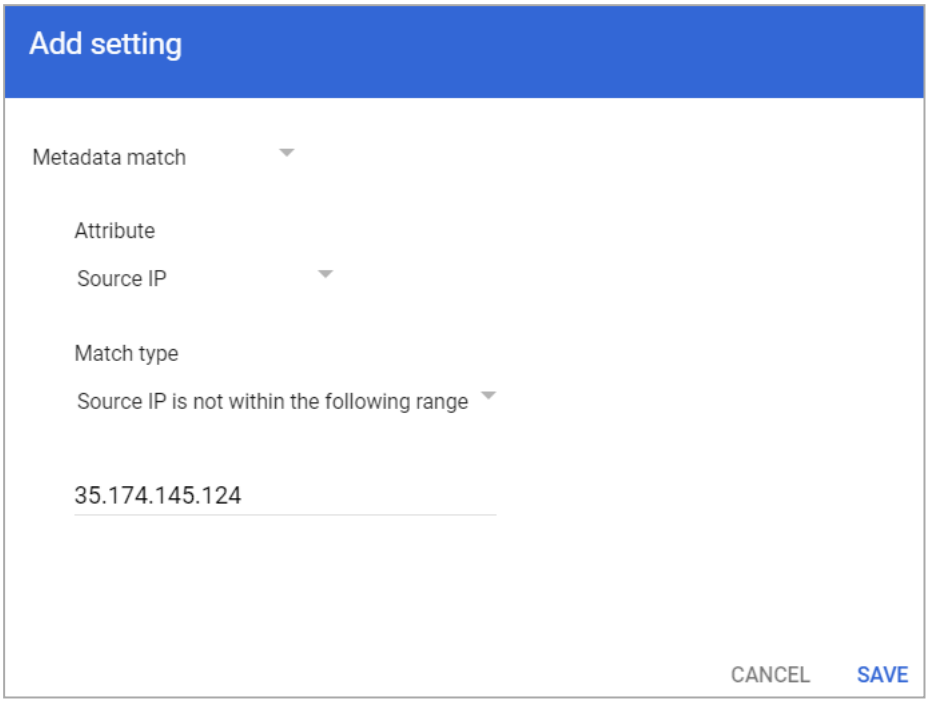
To find the portal identifier, see *"Portal Identifier of Avanan Tenant" on page 36*.

c. Under **Email messages to affect**, do these:

i. Select **Outbound** checkbox.

ii. In **Add expressions that describe the content you want to search for in each message**, select **If ALL of the following match the message**.

iii. Click **Add**.



iv. In the **Add setting** pop-up, select **Metadata match**.

v. Under **Attribute**, select **Source IP**.

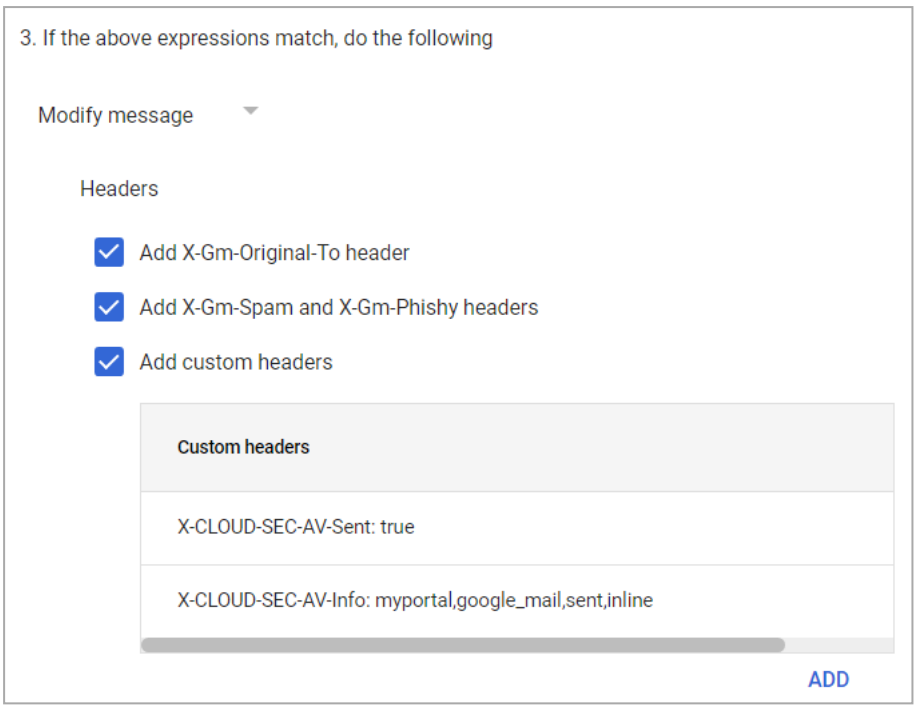
vi. Under **Match type**, select **Source IP is not within the following range**.

vii. Enter all the IP addresses relevant to your data region.

For the list of supported IP addresses, see *"IP Addresses Supported Per Region" on page 591*.

viii. Click **Save**.

d. Under **If the above expressions match, do the following**, do these:



i. Select **Modify message**.

ii. Under **Headers**, do these:

i. Select **Add X-Gm-Original-To header** checkbox.

ii. Select **Add X-Gm-Spam and X-Gm-Phishy headers** checkbox.

iii. Select **Add custom headers** checkbox and add custom headers with these values.

Header Key	Header Value
CLOUD-SEC-AV-Sent	true
CLOUD-SEC-AV-Info	[portal],google_mail,sent,inline

To add a custom header:

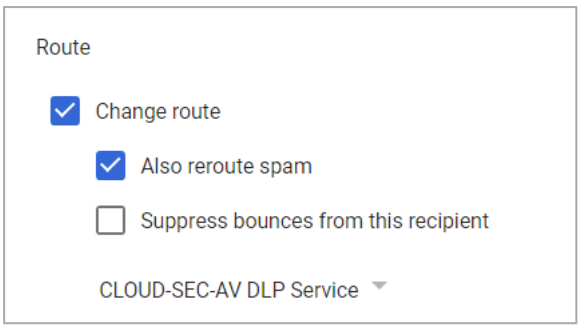
i. Click **Add**.

ii. In **Header key**, enter the header key.

iii. In **Header value**, enter the header value.

iv. Click **Save**.

iii. Under **Route**, do these:



i. Select the **Change route** checkbox.

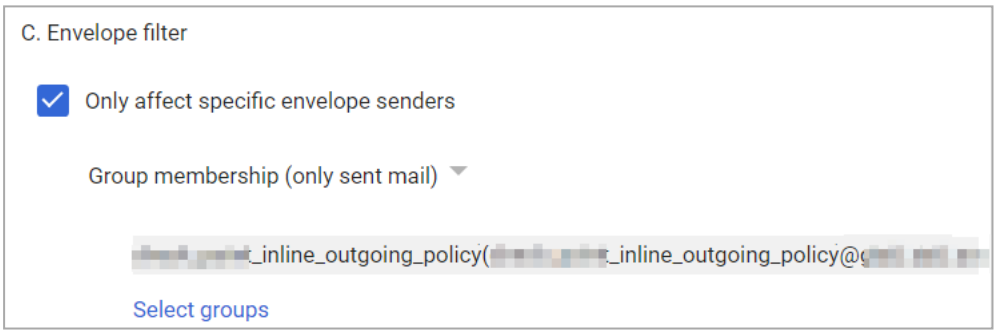
ii. Select the **Also reroute spam** checkbox.

iii. In the list, select **CLOUD-SEC-AV DLP Service**.

e. Scroll-down to the end of the page and click **Show options**.

f. Under **Account types to affect**, select **Users** and **Groups** checkbox.

g. Under **Envelope filter**, do these:



i. Select the **Only affect specific envelope senders** checkbox.

ii. From the list, select **Group membership (only sent mail)**.

iii. Click **Select groups** and select **avanan_inline_outgoing_policy**.

iv. Click **Save**.

IP Addresses Supported Per Region

- **United States**
  - 35.174.145.124
  - 3.214.204.181
  - 44.211.178.96/28
  - 44.211.178.112/28
  - 3.101.216.128/28

- 3.101.216.144/28

- **Australia**
  - 13.211.69.231
  - 3.105.224.60
  - 3.27.51.160/28
  - 3.27.51.176/28
  - 18.143.136.64/28
  - 18.143.136.80/28
- **Canada**
  - 15.222.110.90
  - 52.60.189.48
  - 3.99.253.64/28
  - 3.99.253.80/28
  - 3.101.216.128/28
  - 3.101.216.144/28
- **Europe**
  - 52.212.19.177
  - 52.17.62.50
  - 3.252.108.160/28
  - 3.252.108.176/28
  - 13.39.103.0/28
  - 13.39.103.23/28
- **India ***
  - 3.109.187.96
  - 43.204.62.184
  - 43.205.150.240/29
  - 43.205.150.248/29
  - 18.143.136.64/28

- 18.143.136.80/28

These regions are relevant only for tenants created using the Avanan MSP Portal.

- **United Arab Emirates**
  - 3.29.194.128/28
  - 3.29.194.144/28
- **United Kingdom**
  - 13.42.61.32
  - 13.42.61.47
  - 13.42.61.32/28
  - 13.42.61.47/28
  - 13.39.103.0/28
  - 13.39.103.23/28

Appendix C: DLP Built-in Data Types and Categories

DLP Data Types

DLP Data Types represent the data being looked for in emails, attachments, files, and messages.

Each DLP Data Type is assigned a geographical region that it fits in. All the DLP Data Types are either Global or relate to a specific country.

These are the built-in DLP Data Types in Avanan.

Global Data Types

The Global built-in Data Types for Avanan DLP are as follows.

Data Type Name	Description
Advertising identifier	Identifiers used by developers to track users for advertising purposes. These include Google Play Advertising IDs, Amazon Advertising IDs, Apple's identifierForAdvertising (IDFA), and Apple's identifierForVendor (IDFV).
Age of an individual	An age measured in months or years.
Credit card number	A credit card number is 12 to 19 digits long. They are used for payment transactions globally.
Credit Card Extended	Credit card numbers that match even if appearing as substrings. For example, AX123412345612345*1234
Credit card track number	A credit card track number is a variable length alphanumeric string. It is used to store key cardholder information.
Date of birth	A date of birth
Domain name	A domain name as defined by the DNS standard.
Email address	An email address identifies the mailbox that emails are sent to or from. The maximum length of the domain name is 255 characters, and the maximum length of the local-part is 64 characters.
Ethnic group	A person’s ethnic group.

Data Type Name	Description
Female name	A common female name.
First name	A first name is defined as the first part of a Person Name.
Gender	A person's gender identity.
Generic id	Alphanumeric and special character strings that may be personally identifying but do not belong to a well-defined category, such as user IDs or medical record numbers.
IBAN Americas	An International Bank Account Number (IBAN) is an internationally agreed-upon method for identifying bank accounts defined by the International Standard of Organization (ISO) 13616:2007 standard. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number. This rule detects American IBAN formats.
IBAN Asia	An International Bank Account Number (IBAN) is an internationally agreed-upon method for identifying bank accounts defined by the International Standard of Organization (ISO) 13616:2007 standard. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number. This rule detects Asian IBAN formats (see here: https://www.iban.com/structure,https://bfsfcu.org/pdf/IBAN.pdf).
IBAN Africa	An International Bank Account Number (IBAN) is an internationally agreed-upon method for identifying bank accounts defined by the International Standard of Organization (ISO) 13616:2007 standard. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number. This rule detects African IBAN formats (see here: https://www.iban.com/structure,https://bfsfcu.org/pdf/IBAN.pdf).
IBAN Europe	An International Bank Account Number (IBAN) is an internationally agreed-upon method for identifying bank accounts defined by the International Standard of Organization (ISO) 13616:2007 standard. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number. This rule detects European IBAN formats (see https://www.iban.com/structure,https://bfsfcu.org/pdf/IBAN.pdf).
HTTP cookie and set-cookie headers	An HTTP cookie is a standard way of storing data on a per website basis. This detector will find headers containing these cookies.

Data Type Name	Description
ICD9 code	The International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) lexicon is used to assign diagnostic and procedure codes associated with inpatient, outpatient, and physician office use in the United States. The US National Center for Health Statistics (NCHS) created the ICD-9-CM lexicon. It is based on the ICD-9 lexicon, but provides for more morbidity detail. The ICD-9-CM lexicon is updated annually on October 1.
ICD10 code	Like ICD-9-CM codes, the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) lexicon is a series of diagnostic codes. The World Health Organization (WHO) publishes the ICD-10-CM lexicon to describe causes of morbidity and mortality.
Patient Information	Detects leaked medical patient information. The detection is based on matching health codes and various personal information patterns.
Phone IMEI number	An International Mobile Equipment Identity (IMEI) hardware identifier, used to identify mobile phones.
IP address	An Internet Protocol (IP) address (either IPv4 or IPv6).
Last name	A last name is defined as the last part of a Person Name.
Street addresses and landmarks	A physical address or location.
MAC address	A media access control address (MAC address), which is an identifier for a network adapter.
Local MAC address	A local media access control address (MAC address), which is an identifier for a network adapter.
Male name	A common male name.
Medical term	Terms that commonly refer to a person's medical condition or health.
Local MAC address	A local media access control address (MAC address), which is an identifier for a network adapter.
Organization name	A name of a chain store, business or organization.

Data Type Name	Description
Passport Number	A passport number that matches passport numbers for the following countries: Australia, Canada, China, France, Germany, Japan, Korea, Mexico, Netherlands, Poland, Singapore, Spain, Sweden, Taiwan, United Kingdom, and the United States.
Person name	A full person name, which can include first names, middle names or initials, and last names.
Phone number	A telephone number.
Street address	A street address.
Bank SWIFT routing number	A SWIFT code is the same as a Bank Identifier Code (BIC). It's a unique identification code for a particular bank. These codes are used when transferring money between banks, particularly for international wire transfers. Banks also use the codes for exchanging other messages.
Date or Time	A date. This Rule name includes most date formats, including the names of common world holidays.
Human readable time	A timestamp of a specific time of day. For example, *09:54 pm*.
URL	A Uniform Resource Locator (URL).
Vehicle identification number	A vehicle identification number (VIN) is a unique 17-digit code assigned to every on-road motor vehicle.
Authentication token	An authentication token is a machine-readable way of determining whether a particular request has been authorized for a user. This detector currently identifies tokens that comply with OAuth or Bearer authentication.
Amazon Web Services credentials	Amazon Web Services account access keys.
Azure JSON web token	Microsoft Azure certificate credentials for application authentication.
HTTP Basic authentication header	A basic authentication header is an HTTP header used to identify a user to a server. It is part of the HTTP specification in RFC 1945, section 11.

Data Type Name	Description
Encryption key	An encryption key within configuration, code, or log text.
Google Cloud Platform API key	Google Cloud API key. An encrypted string that is used when calling Google Cloud APIs that don't need to access private user data.
Google Cloud Platform service account credentials	Google Cloud service account credentials. Credentials that can be used to authenticate with Google API client libraries and service accounts.
JSON web token	JSON Web Token. JSON Web Token in compact form. Represents a set of claims as a JSON object that is digitally signed using JSON Web Signature.
Password	Clear text passwords in configs, code, and other text.
Top 100,000 most common weakly hashed passwords	A weakly hashed password is a method of storing a password that is easy to reverse engineer. The presence of such hashes often indicate that a system's security can be improved.
Common headers containing XSRF tokens	An XSRF token is an HTTP header that is commonly used to prevent cross-site scripting attacks. Cross-site scripting is a type of security vulnerability that can be exploited by malicious sites.

Country Specific Data Types

Argentina

Data Type Name	Description
Argentina identity card number	An Argentine Documento Nacional de Identidad (DNI), or national identity card, is used as the main identity document for citizens.

Australia

Data TypeName	Description
Australia driver's license number	An Australian driver's license number.
Australia medicare number	A 9-digit Australian Medicare account number is issued to permanent residents of Australia (except for Norfolk island). The primary purpose of this number is to prove Medicare eligibility to receive subsidized care in Australia.
Australia passport number	An Australian passport number.
Australia tax file number	An Australian tax file number (TFN) is a number issued by the Australian Tax Office for taxpayer identification. Every taxpaying entity, such as an individual or an organization, is assigned a unique number.

Belgium

Data Type Name	Description
Belgium National Identity card number	A 12-digit Belgian national identity card number.

Brazil

Data Type Name	Description
Brazil individual taxpayer identification number	The Brazilian Cadastro de Pessoas Físicas (CPF) number, or Natural Persons Register number, is an 11-digit number used in Brazil for taxpayer identification.

Canada

Data Type Name	Description
Canada bank account number	A Canadian bank account number.
British Columbia public health network number	The British Columbia Personal Health Number (PHN) is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of British Columbia.
Canada driver’s license number	A driver's license number for each of the ten provinces in Canada (the three territories are currently not covered).
Ontario health insurance number	The Ontario Health Insurance Plan (OHIP) number is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of Ontario.
Canada passport number	A Canadian passport number.
Quebec health insurance number	The Québec Health Insurance Number (also known as the RAMQ number) is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of Québec.
Canada social insurance number	The Canadian Social Insurance Number (SIN) is the main identifier used in Canada for citizens, permanent residents, and people on work or study visas. With a Canadian SIN and mailing address, one can apply for health care coverage, driver's licenses, and other important services.

Chile

Data Type Name	Description
Chile identity card number	A Chilean Cédula de Identidad (CDI), or identity card, is used as the main identity document for citizens.

China

Data Type Name	Description
China resident number	A Chinese resident identification number.
China passport number	A Chinese passport number.

Colombia

Data Type Name	Description
Colombia identity card number	A Colombian Cédula de Ciudadanía (CDC), or citizenship card, is used as the main identity document for citizens.

Denmark

Data Type Name	Description
Denmark CPR Number	A Personal Identification Number (CPR, Det Centrale Personregister) is a national ID number in Denmark. It is used with public agencies such as health care and tax authorities. Banks and insurance companies also use it as a customer number. The CPR number is required for people who reside in Denmark, pay tax or own property there.

France

Data Type Name	Description
France national identity card number	The French Carte Nationale d'Identité Sécurisée (CNI or CNIS) is the French national identity card. It's an official identity document consisting of a 12-digit identification number. This number is commonly used when opening bank accounts and when paying by check. It can sometimes be used instead of a passport or visa within the European Union (EU) and in some other countries.
France national insurance number	The French Numéro d'Inscription au Répertoire (NIR) is a permanent personal identification number that's also known as the French social security number for services including healthcare and pensions.
France passport number	A French passport number.
France tax identification number	The French tax identification number is a government-issued ID for all individuals paying taxes in France.

Finland

Data Type Name	Description
Finland personal identity code	A Finnish personal identity code, a national government identification number for Finnish citizens used on identity cards, driver's licenses and passports.

Germany

Data Type Name	Description
Germany driver's license number	A German driver's license number.
German identity card number	The German Personalausweis, or identity card, is used as the main identity document for citizens of Germany.

Data Type Name	Description
Germany passport number	A German passport number. The format of a German passport number is 10 alphanumeric characters, chosen from numerals 0–9 and letters C, F, G, H, J, K, L, M, N, P, R, T, V, W, X, Y, Z.
Germany taxpayer identification number	An 11-digit German taxpayer identification number assigned to both natural-born and other legal residents of Germany for the purposes of recording tax payments.
Germany Schufa identification number	A German Schufa identification number. Schufa Holding AG is a German credit bureau whose aim is to protect clients from credit risk.

Hong Kong

Data Type Name	Description
Hong Kong identity card number	The 香港身份證, or Hong Kong identity card (HKIC), is used as the main identity document for citizens of Hong Kong.

India

Data Type Name	Description
India Aadhaar number	The Indian Aadhaar number is a 12-digit unique identity number obtained by residents of India, based on their biometric and demographic data.
India GST identification number	The Indian GST identification number (GSTIN) is a unique identifier required of every business in India for taxation.
India permanent account number	The Indian Personal Permanent Account Number (PAN) is a unique 10-digit alphanumeric identifier used for identification of individuals—particularly people who pay income tax. It's issued by the Indian Income Tax Department. The PAN is valid for the lifetime of the holder.

Indonesia

Data Type Name	Description
Indonesia identity number (Nomor Induk Kependudukan)	An Indonesian Single Identity Number (Nomor Induk Kependudukan, or NIK) is the national identification number of Indonesia. The NIK is used as the basis for issuing Indonesian resident identity cards (Kartu Tanda Penduduk, or KTP), passports, driver's licenses and other identity documents.

Ireland

Data Type Name	Description
Ireland driving license number	An Irish driving license number.
Ireland Eircode	Eircode is an Irish postal code that uniquely identifies an address.
Ireland passport number	An Irish (IE) passport number.
Ireland Personal Public Service Number (PPSN)	The Irish Personal Public Service Number (PPS number, or PPSN) is a unique number for accessing social welfare benefits, public services, and information in Ireland.

Israel

Data Type Name	Description
Israel identity card number	The Israel identity card number is issued to all Israeli citizens at birth by the Ministry of the Interior. Temporary residents are assigned a number when they receive temporary resident status.

Italy

Data Type Name	Description
Italy fiscal code number	An Italy fiscal code number is a unique 16-digit code assigned to Italian citizens as a form of identification.

Japan

Data Type Name	Description
Japan bank account number	A Japanese bank account number.
Japan driver's license number	A Japanese driver's license number.
Japan individual number or "My Number"	The Japanese national identification number—sometimes referred to as "My Number"—is a new national ID number as of January 2016.
Japan passport number	A Japanese passport number. The passport number consists of two alphabetic characters followed by seven digits.

Korea

Data Type Name	Description
Korea passport number	A Korean passport number.
Korea resident registration number	A South Korean Social Security number.

Mexico

Data Type Name	Description
Mexico population registry number	The Mexico Clave Única de Registro de Población (CURP) number, or Unique Population Registry Code or Personal Identification Code number. The CURP number is an 18-character state-issued identification number assigned by the Mexican government to citizens or residents of Mexico and used for taxpayer identification.
Mexico passport number	A Mexican passport number.

The Netherlands

Data Type Name	Description
Netherlands citizen service number	A Dutch Burgerservicenummer (BSN), or Citizen's Service Number, is a state-issued identification number that's on driver's licenses, passports, and international ID cards.
Netherlands passport number	A Dutch passport number.

Norway

Data Type Name	Description
Norway national identity number	Norway‘s Fødselsnummer, National Identification Number, or Birth Number is assigned at birth, or on migration into the country. It is registered with the Norwegian Tax Office.

Paraguay

Data Type Name	Description
Paraguay identity card number	A Paraguayan Cédula de Identidad Civil (CIC), or civil identity card, is used as the main identity document for citizens.

Peru

Data Type Name	Description
Peru identity card number	A Peruvian Documento Nacional de Identidad (DNI), or national identity card, is used as the main identity document for citizens.

Poland

Data Type Name	Description
Poland PESEL number	The PESEL number is the national identification number used in Poland. It is mandatory for all permanent residents of Poland, and for temporary residents staying there longer than 2 months. It is assigned to just one person and cannot be changed.
Poland national id number	The Polish identity card number. is a government identification number for Polish citizens. Every citizen older than 18 years must have an identity card. The local Office of Civic Affairs issues the card, and each card has its own unique number.
Poland Passport	A Polish passport number. Polish passport is an international travel document for Polish citizens. It can also be used as a proof of Polish citizenship.

Portugal

Data Type Name	Description
Portugal identity card number	A Portuguese Cartão de cidadão (CDC), or Citizen Card, is used as the main identity, Social Security, health services, taxpayer, and voter document for citizens.

Singapore

Data Type Name	Description
Singapore national registration number	A unique set of nine alpha-numeric characters on the Singapore National Registration Identity Card.
Singapore passport number	A Singaporean passport number.

Spain

Data Type Name	Description
Spain CIF or Código de Identificación Fiscal	The Spanish Código de Identificación Fiscal (CIF) was the tax identification system used in Spain for legal entities until 2008. It was then replaced by the Número de Identificación Fiscal (NIF) for natural and juridical persons.
Spain DNI or Documento Nacional de Identidad	A Spain national identity number.
Spain driver's license number	A Spanish driver's license number.
Spain foreigner tax identification number	The Spanish Número de Identificación de Extranjeros (NIE) is an identification number for foreigners living or doing business in Spain. An NIE number is needed for key transactions such as opening a bank account, buying a car, or setting up a mobile phone contract.
Spain tax identification number	The Spanish Número de Identificación Fiscal (NIF) is a government identification number for Spanish citizens. An NIF number is needed for key transactions such as opening a bank account, buying a car, or setting up a mobile phone contract.
Spain passport number	A Spanish Ordinary Passport (Pasaporte Ordinario) number. There are 4 different types of passports in Spain. This detector is for the Ordinary Passport (Pasaporte Ordinario) type, which is issued for ordinary travel, such as vacations and business trips.
Spain social security number	The Spanish Social Security number (Número de Afiliación a la Seguridad Social) is a 10-digit sequence that identifies a person in Spain for all interactions with the country's Social Security system.

Sweden

Data Type Name	Description
Sweden personal identity number	A Swedish Personal Identity Number (personnummer), a national government identification number for Swedish citizens.
Sweden passport number	A Swedish passport number.

Taiwan

Data Type Name	Description
Taiwan passport number	A Taiwanese passport number.

Thailand

Data Type Name	Description
Thai national identification card number	The Thai บัตรประจำตัวประชาชนไทย, or identity card, is used as the main identity document for Thai nationals.

Turkey

Data Type Name	Description
Turkish identification number	A unique Turkish personal identification number, assigned to every citizen of Turkey.

United Kingdom

Data Type Name	Description
Scotland community health index number	The Scotland Community Health Index Number (CHI number) is a 10-digit sequence used to uniquely identify a patient within National Health Service Scotland (NHS Scotland).
United Kingdom drivers license number	A driver's license number for the United Kingdom of Great Britain and Northern Ireland (UK).
United Kingdom national health service number	A National Health Service (NHS) number is the unique number allocated to a registered user of the three public health services in England, Wales, and the Isle of Man.

Data Type Name	Description
United Kingdom national insurance number	The National Insurance number (NINO) is a number used in the United Kingdom (UK) in the administration of the National Insurance or social security system. It identifies people, and is also used for some purposes in the UK tax system. The number is sometimes referred to as NI No or NINO.
United Kingdom passport number	A United Kingdom (UK) passport number.
United Kingdom taxpayer reference number	A United Kingdom (UK) Unique Taxpayer Reference (UTR) number. This number, comprised of a string of 10 decimal digits, is an identifier used by the UK government to manage the taxation system. Unlike other identifiers, such as the passport number or social insurance number, the UTR is not listed on official identity cards.

United States

Data Type Name	Description
American Bankers CUSIP ID	An American Bankers' Committee on Uniform Security Identification Procedures (CUSIP) number is a 9-character alphanumeric code that identifies a North American financial security.
Medical drug names	The US National Drug Code (NDC) is a unique identifier for drug products, mandated in the United States by the Food and Drug Administration (FDA).
USA Adoption Taxpayer Identification Number	A United States Adoption Taxpayer Identification Number (ATIN) is a type of United States Tax Identification Number (TIN). An ATIN is issued by the Internal Revenue Service (IRS) to individuals who are in the process of legally adopting a US citizen or resident child.
USA bank routing number	The American Bankers Association (ABA) Routing Number (also called the transit number) is a nine-digit code. It's used to identify the financial institution that's responsible to credit or entitled to receive credit for a check or electronic transaction.
USA Current Procedural Terminology	Current Procedural Terminology (CPT) detects codes, descriptions, and guidelines intended to describe procedures and services performed by physicians and other health care providers. Matches five-digit CPT codes combined with medical key words detections (i.e. 'procedural').

Data Type Name	Description
US DEA number	A US Drug Enforcement Administration (DEA) number is assigned to a health care provider by the US DEA. It allows the health care provider to write prescriptions for controlled substances. The DEA number is often used as a general "prescriber number" that is a unique identifier for anyone who can prescribe medication.
USA drivers license number	A driver's license number for the United States. Format can vary depending on the issuing state.
Employer Identification Number	A United States Employer Identification Number (EIN) is also known as a Federal Tax Identification Number, and is used to identify a business entity.
USA healthcare national provider identifier	The US National Provider Identifier (NPI) is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS). The NPI has replaced the unique provider identification number (UPIN) as the required identifier for Medicare services. It's also used by other payers, including commercial healthcare insurers.
USA Individual Taxpayer Identification Number	A United States Individual Taxpayer Identification Number (ITIN) is a type of Tax Identification Number (TIN), issued by the Internal Revenue Service (IRS). An ITIN is a tax processing number only available for certain nonresident and resident aliens, their spouses, and dependents who cannot get a Social Security Number (SSN).
USA Medical Record Number	A Medical Record Number (MRN) matches the default format XXX-X-XXXXX, with or without dashes, in close proximity to medical terms (such as MRN, medical, record).
USA Medical Record Number - Open Format	Matches a Medical Record Number (MRN, see above) patterns in a less rigid formatting, in a close proximity to medical terms (such as MRN, medical, record). Note: this detection rule matches more patterns, thus presents increased probability for false detections. Recommended to be used combined with additional rules for detection.
USA passport number	A United States passport number.
USA Preparer Taxpayer Identification Number	A United States Preparer Taxpayer Identification Number (PTIN) is an identification number that all paid tax return preparers must use on US federal tax returns or claims for refund submitted to the US Internal Revenue Service (IRS).

Data Type Name	Description
US Social Security Number	A United States Social Security number (SSN) is a 9-digit number issued to US citizens, permanent residents, and temporary residents. This detector will not match against numbers with all zeroes in any digit group (that is, 000-##-####, ###-00-####, or ###-##-0000), against numbers with 666 in the first digit group, or against numbers whose first digit is 9.
USA state name	A United States state name.
USA toll free phone number	A US toll-free telephone number.
USA vehicle identification number	A vehicle identification number (VIN) is a unique 17-digit code assigned to every on-road motor vehicle in North America.

Uruguay

Data Type Name	Description
Uruguay identity card number	A Uruguayan Cédula de Identidad (CDI), or identity card, is used as the main identity document for citizens.

Venezuela

Data Type Name	Description
Venezuela identity card number	A Venezuelan Cédula de Identidad (CDI), or national identity card, is used as the main identity document for citizens.

DLP Categories

The table below shows the default rules of each DLP category for Infinity Portal accounts residing in different regions.

Note - To configure the DLP Data Type of each of the DLP categories, see *"DLP Categories" on page 111*.

DLP Category	Default Data Type for Infinity Portal accounts residing in US/Canada region	Default Data Type for Infinity Portal accounts residing in other regions
PHI	ICD9 description match ICD10 description match USA healthcare national provider identifier	ICD9 description match ICD10 description match Australia medicare number British Columbia public health network number Ontario health insurance number Quebec health insurance number Ireland Personal Public Service Number (PPSN) Scotland community health index number United Kingdom national health service number USA healthcare national provider identifier

DLP Category	Default Data Type for Infinity Portal accounts residing in US/Canada region	Default Data Type for Infinity Portal accounts residing in other regions
PII	Passport number USA drivers license number USA passport number USA social security number USA vehicle identification number	Passport number Vehicle identification number Argentina identity card number Australia driver's license number Australia passport number Belgium National Identity card number Brazil individual taxpayer identification number Canada driver's license number Canada passport number Canada social insurance number Chile identity card number China resident number China passport number Colombia identity card number Denmark CPR number France national identity card number France national insurance number France passport number Finland personal identity code Germany driver's license number German identity card number German passport number Hong Kong identity card number India Aadhaar number India permanent account number Indonesia identity number (Nomor Induk Kependuduken) Ireland driver license number Ireland passport number Israel identity card number Italy fiscal code number Japan driver's license number Japan individual number or "My Number" Japan passport number Korea passport number Korea resident registration number Mexico population registry number

DLP Category	Default Data Type for Infinity Portal accounts residing in US/Canada region	Default Data Type for Infinity Portal accounts residing in other regions
		Mexico passport number Netherlands citizen service number Norway national identity number Paraguay identity card number Peru identity card number Poland PESEL number Poland national id number Poland passport Portugal identity card number Singapore national registration number Singapore passport number Spain DNI or Documento Nacional de Identidad Spain driver's license number Spain foreigner tax identification number Spain tax identification number Spain passport number Spain social security number Sweden personal identity number Sweden passport number Taiwan passport number Thai national identification card number Turkish identification number United Kingdom drivers license number United Kingdom national insurance number United Kingdom passport number USA drivers license number USA passport number USA social security number Uruguay identity card number Venezuela identity card number

DLP Category	Default Data Type for Infinity Portal accounts residing in US/Canada region	Default Data Type for Infinity Portal accounts residing in other regions
Financial	Bank SWIFT routing number IBAN Africa IBAN Americas IBAN Asia IBAN Europe American Bankers CUSIP identifier USA Adoption Taxpayer Identification number USA bank routing number USA Individual Taxpayer Identification Number USA Preparer Taxpayer Identification Number	Bank SWIFT routing number IBAN Africa IBAN Americas IBAN Asia IBAN Europe Australia tax file number Canada bank account number France tax identification number Germany taxpayer identification number Germany Schufa identification number India GST identification number Japan bank account number Spain CIF or Código de Identificación Fiscal United Kingdom taxpayer reference number American Bankers CUSIP identifier USA Adoption Taxpayer Identification number USA bank routing number USA Employer Identification Number USA Individual Taxpayer Identification Number USA Preparer Taxpayer Identification Number

DLP Category	Default Data Type for Infinity Portal accounts residing in US/Canada region	Default Data Type for Infinity Portal accounts residing in other regions
Access Control	Advertising Identifier Phone IMEI number MAC address Local MAC address Authentication token Amazon Web Services credentials Azure JSON Web Token HTTP basic authentication header Encryption key Google Cloud Platform API key Google Cloud Platform service account credentials JSON Web Token Top 100,000 most common weekly hashed passwords Common headers containing xsrf tokens	Advertising Identifier Phone IMEI number MAC address Local MAC address Authentication token Amazon Web Services credentials Azure JSON Web Token HTTP basic authentication header Encryption key Google Cloud Platform API key Google Cloud Platform service account credentials JSON Web Token Top 100,000 most common weekly hashed passwords Common headers containing xsrf tokens
PCI	Credit card number Credit card track number	Credit card number Credit card track number
HIPAA	ICD9 description match ICD10 description match USA DEA number USA healthcare national provider identifier USA Medical Record Number (MRN) USA Current Procedural Terminology (CPT)	ICD9 description match ICD10 description match USA DEA number USA healthcare national provider identifier

Appendix D: Supported Languages for Anti-Phishing

The Anti-Phishing engine analyzes different components of an email, such as attachments, links, language, sender reputation, domain analysis, OCR, and many more. As part of the inspection, it analyzes the language used in the email using the NLP engine.

NLP engine supports these languages:

- Afrikaans
- Albanian
- Arabic
- Aragonese
- Armenian
- Asturian
- Azerbaijani
- Bashkir
- Basque
- Bavarian
- Belarusian
- Bengali
- Bishnupriya Manipuri
- Bosnian
- Breton
- Bulgarian
- Burmese
- Catalan
- Cebuano
- Chechen
- Chinese (Simplified)
- Chinese (Traditional)
- Chuvash

- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- Galician
- Georgian
- German
- Greek
- Gujarati
- Haitian
- Hebrew
- Hindi
- Hungarian
- Icelandic
- Ido
- Indonesian
- Irish
- Italian
- Japanese
- Javanese
- Kannada
- Kazakh
- Kirghiz
- Korean
- Latin

- Latvian
- Lithuanian
- Lombard
- Low Saxon
- Luxembourgish
- Macedonian
- Malagasy
- Malay
- Malayalam
- Marathi
- Minangkabau
- Mongolian
- Nepali
- Newar
- Norwegian (Bokmal)
- Norwegian (Nynorsk)
- Occitan
- Persian (Farsi)
- Piedmontese
- Polish
- Portuguese
- Punjabi
- Romanian
- Russian
- Scots
- Serbian
- Serbo-Croatian
- Sicilian
- Slovak

- Slovenian
- South Azerbaijani
- Spanish
- Sundanese
- Swahili
- Swedish
- Tagalog
- Tajik
- Tamil
- Tatar
- Telugu
- Thai
- Turkish
- Ukrainian
- Urdu
- Uzbek
- Vietnamese
- Volapük
- Waray-Waray
- Welsh
- West Frisian
- Western Punjabi
- Yoruba

Appendix E: Data Retention Policy

Introduction

The Data Retention Policy describes how long Avanan stores emails from Microsoft 365 or Gmail in its database. You can search and view emails stored in the database using *"Mail Explorer" on page 371* and *"Custom Queries" on page 379*.

Default Retention Period of Emails

By default, Avanan retains the emails as follows:

Verdict and Enforcement	Raw Email (Original email with attachments)	Email Meta Data (Attributes and data detected from the security scan)
Clean emails (Includes emails with re-written links in the email body)	14 days	14 days
Emails with modified attachments and emails that have cleaned (sanitized) attachments, removed as password-protected attachments, and re-written links	14 days	180 days
Emails containing threats but not quarantined (includes emails with phishing /spam / malware / DLP detection that are not quarantined)	14 days	180 days
Quarantined emails (includes manually quarantined emails)	180 days	180 days
Emails quarantined by Microsoft	180 days	180 days

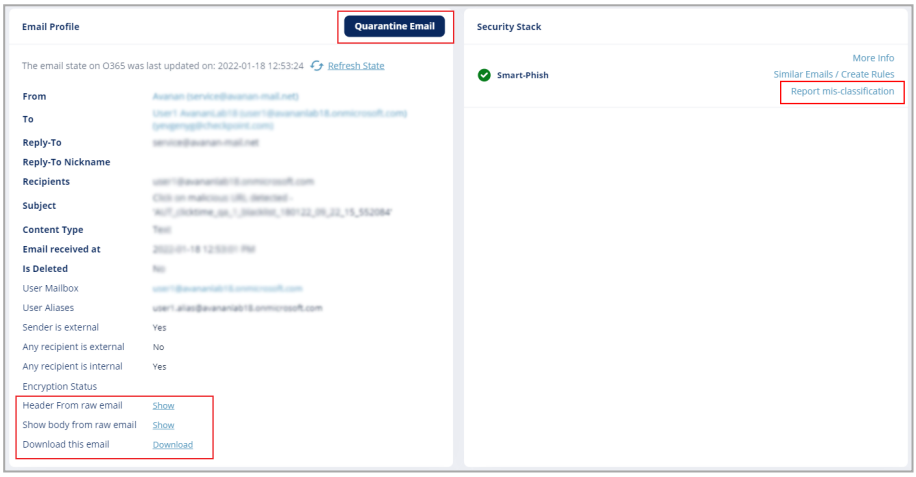
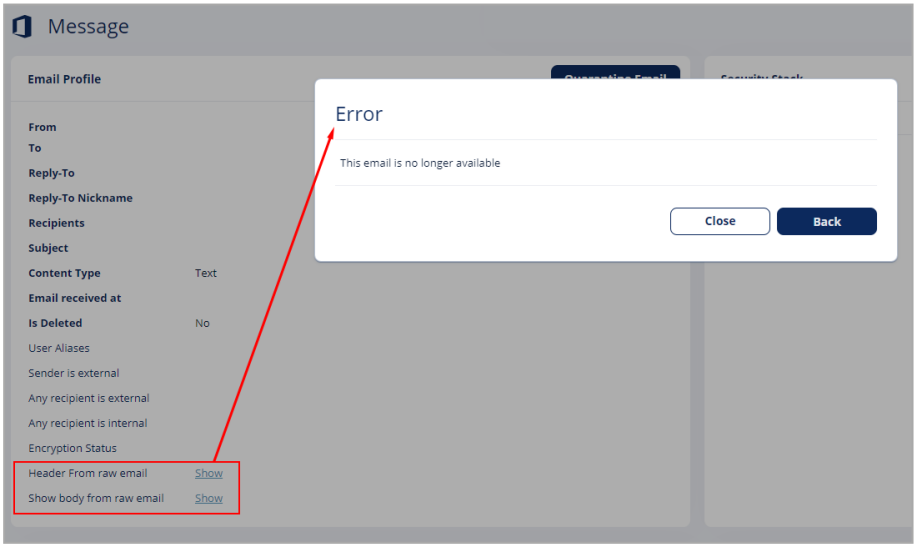
Avanan retains security events for 12 months. For more information, see *"Retention of Security Events" on page 371*.

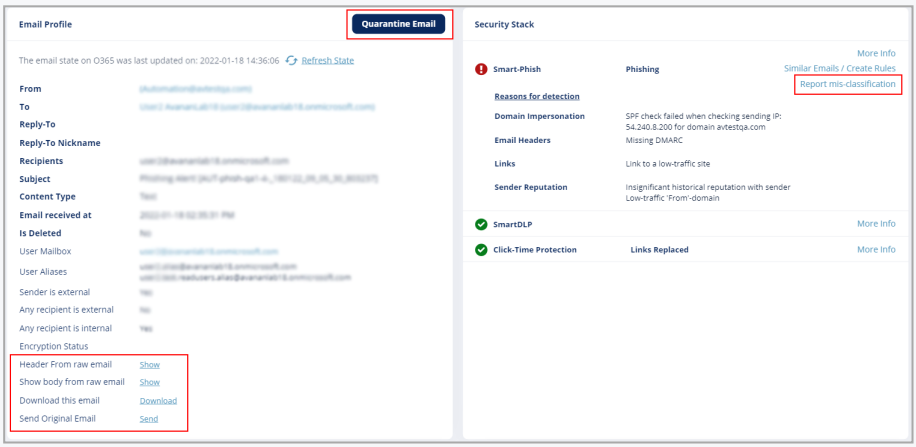
For information about the procedure to customize the retention period, see *"Customizing Retention Period of Emails" on page 452*.

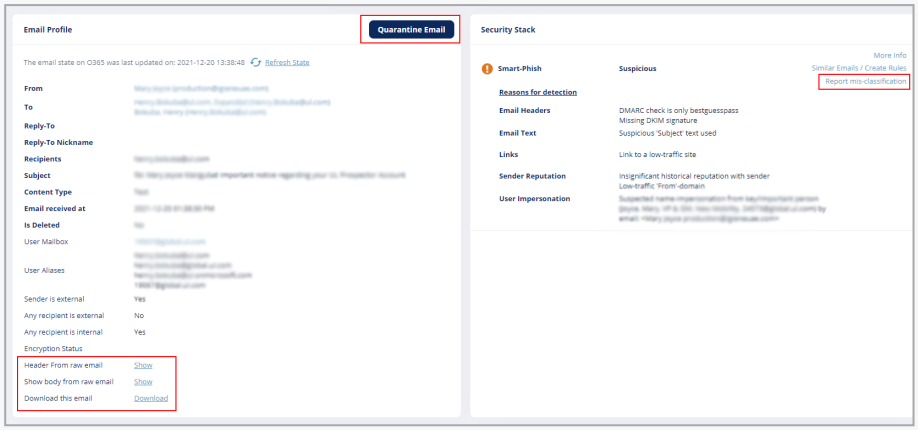
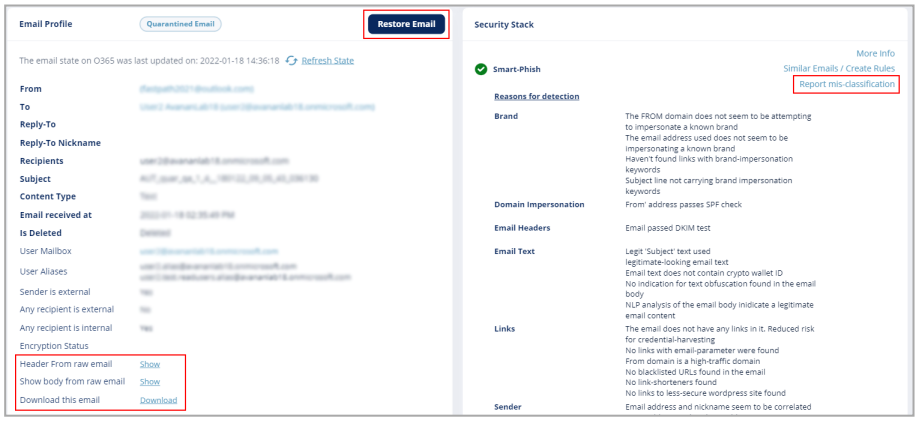
Note - Avanan keeps backend logs on emails for seven days after the email is delivered.

Available Actions on Emails During and After the Retention Period

Actions you can perform after you open an email:

<table>
<tr><th>Email Type</th><th>Period</th><th>Actions</th></tr>
<tr><td rowspan="4">Clean Email</td><td>During the retention period</td><td>Quarantine Email
Show header from raw email
Show body from raw email
Download this email
Report mis-classification</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>After the retention period</td><td>Email is not available.</td></tr>
<tr><td colspan="2"> 
</td></tr>
</table>

Email Type	Period	Actions
Detected but non-quarantined email	During the retention period	■ Quarantine Email ■ Show header from raw email ■ Show body from raw email ■ Download this email ■ Send original email ■ Report mis-classification
		
	After the retention period (Configured retention period - 180 days)	■ Quarantine Email ■ Show header from raw email ■ Show body from raw email ■ Report mis-classification

Email Type	Period	Actions
		
	After 180 days	Email is not available.
Quarantined email	During the retention period	■ Restore Email ■ Show header from raw email ■ Show body from raw email ■ Download this email ■ Report mis-classification
		
	After the retention period	Email is not available.

Data Retention Policy for Non-email Applications

The data retention policy for non-email applications is applicable for:

- Office 365 Sharepoint
- Office 365 OneDrive
- Microsoft Teams
- Google Drive
- Slack
- Dropbox
- Box

Notes:

- Metadata for both clean and malicious items (messages, shared files) is saved for 6 months.
- The data (files / messages) is stored for 24 hours.
- Quarantined items are saved for 6 months.

Appendix F: Activating Office 365 Mail in Hybrid Environments

A hybrid environment is a setup in which some mailboxes are in Microsoft 365, and some mailboxes are on your organization's email servers (on-premises Exchange server).

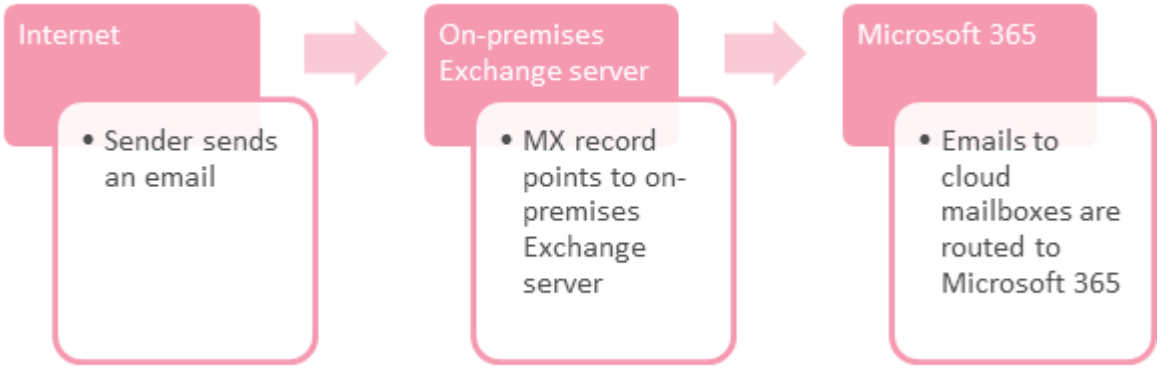
The most common use case for hybrid environments is with organizations migrating the mailboxes group by group to Microsoft 365.

Mail Flow in Hybrid Environments

Legacy Hybrid Architecture – MX Points to On-Premises Exchange Server

While migrating from an on-premises environment to the cloud (Exchange Online), organizations usually start with a basic architecture where the MX record points to the on-premises Exchange server or to the legacy Secure Email Gateway (SEG) that protects the on-premises Exchange server.

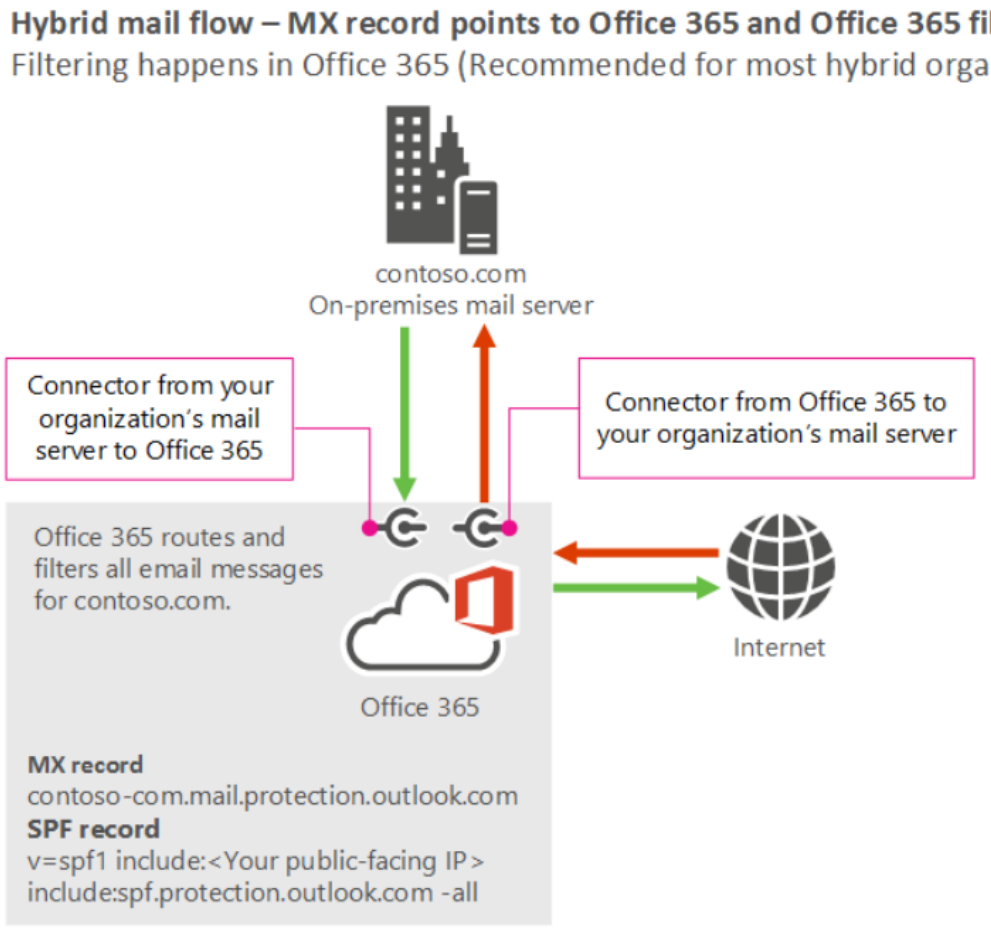
So the mail flows from the sender to the on-premises Exchange server and then gets routed to Microsoft 365.



Modern Hybrid Architecture – MX Points to Microsoft 365

To reduce the load on the organization's network and to ensure all emails are secured, organizations often change the mail flow so that the MX record points to Microsoft 365.

Microsoft 365 performs all the filtering and routes the emails sent to on-premises mailboxes to the on-premises Exchange server. For this scenario, your organization's mail flow setup looks like the following diagram.



Note - To protect mailboxes in hybrid environments, Avanan need the modern hybrid architecture, where MX points to Microsoft 365. See *"Modern Hybrid Architecture – MX Points to Microsoft 365" above*.

Best Practice - Microsoft recommended this architecture for hybrid environments. For more information, see Microsoft documentation.

Modern Hybrid Architecture – Licensing Considerations

Before migrating to the modern hybrid architecture, make sure you have the required licenses:

- For incoming emails, Microsoft usually does not require additional cloud mailbox licenses. The licenses you have for your on-premises mailboxes should be enough.
- For outgoing emails, Microsoft might require additional licenses to route outgoing emails from on-premises mailboxes through Microsoft 365.

Note - Before migrating, consult your Microsoft representative to ensure you have the required licenses.

Avanan Support for Hybrid Environments

Avanan can protect mailboxes in multiple locations (Exchange Online and on-premises Exchange Server) with modern hybrid architecture mail flow, where the MX record points to Microsoft 365. See *"Modern Hybrid Architecture - MX Points to Microsoft 365" on the previous page*.

Hybrid Environments – Protection Scope

When integrated with a modern hybrid environment, where the MX points to Microsoft 365, Avanan can protect these:

- Microsoft OneDrive, Microsoft SharePoint and Microsoft Teams (The protection to these SaaS applications is not affected by the environment being hybrid)
- All incoming and outgoing emails, whether they are sent to or sent from mailboxes in on-premises Exchange Server or Exchange Online (cloud mailboxes)
- Internal emails, only when the mailbox of either the sender or one of the recipients is in the Exchange Online (cloud mailboxes)

Limitations for On-premises Mailboxes

Avanan does not have API access to the mailboxes in on-premises Exchange Server. So, these are the limitations.

- Avanan cannot pull the emails from on-premise mailboxes to quarantine.

  Important - To secure hybrid environments, you must keep the Avanan policies in **Prevent (Inline)** mode. Otherwise, phishing emails sent to on-premises mailboxes will not be quarantined.

- Avanan cannot present the status of the emails (deleted, forwarded, replied to etc.).

Enabling Office 365 Mail Protection in Hybrid Environments

Prerequisites

Before you connect Avanan to your environment, perform these steps:

- Ensure that the mail flow is configured correctly, where the MX points to Microsoft 365. For more details, contact your Microsoft technical representative.
- Ensure you have the required licenses from Microsoft. See *"Modern Hybrid Architecture - Licensing Considerations" on the previous page*.

Connecting Avanan to Microsoft 365

After all the prerequisites are met, you can connect and protect your hybrid environments with Avanan.

To connect with Avanan, see *"Activating Office 365 Mail" on page 47*.

Important - To secure hybrid environments, you must keep the Avanan policies in **Prevent (Inline)** mode. Otherwise, phishing emails sent to on-premises mailboxes will not be quarantined.

If you need help in connecting your SaaS application with Avanan, contact *Avanan Support*.

.

Appendix G: Permitted IP Addresses to access the Avanan Azure Application

When activating protection for Office 365, Avanan installs the **Avanan Cloud Security Platform–Emails V2** Azure application in your Microsoft 365 environment.

Avanan uses API calls directed to the **Avanan Cloud Security Platform–Emails V2** application to quarantine or restore emails, block users, and perform other actions.

Avanan sends API calls to this application from a specific set of IP networks.

Note - The administrator must treat access attempts from any other IP addresses as unauthorized and potentially originating from threat actors.

Data Region	Public IP address
US	■ 18.205.98.112/32 ■ 18.209.206.31/32 ■ 18.210.117.69/32 ■ 18.213.153.231/32 ■ 18.233.42.246/32 ■ 18.233.230.110/32 ■ 52.203.130.172/32 ■ 184.73.16.161/32
Australia	■ 3.105.233.198/32 ■ 13.55.67.239/32 ■ 13.236.139.38/32 ■ 13.236.230.143/32 ■ 13.238.33.116/32 ■ 13.238.203.5/32 ■ 3.24.247.108/32 ■ 54.206.57.198/32
Canada	■ 3.98.134.58/32 ■ 3.99.86.89/32 ■ 15.156.252.195/32 ■ 35.182.41.230/32 ■ 35.182.206.225/32 ■ 52.60.99.220/32 ■ 52.60.244.192/32 ■ 99.79.92.175/32
Europe	■ 3.252.50.22/32 ■ 3.252.50.23/32 ■ 3.252.50.24/32 ■ 3.252.50.25/32 ■ 3.252.50.26/32 ■ 3.252.50.27/32 ■ 3.252.50.28/32 ■ 34.240.80.65/32

Data Region	Public IP address
India	■ 3.6.250.10/32 ■ 3.109.29.21/32 ■ 13.126.227.64/32 ■ 13.200.211.62/32 ■ 13.202.15.143/32 ■ 13.202.52.212/32 ■ 13.235.12.63/32 ■ 43.204.80.178/32
UAE	■ 3.28.79.88/32 ■ 3.28.167.79/32 ■ 3.29.197.188/32 ■ 3.29.205.82/32 ■ 40.172.29.94/32 ■ 40.172.67.2/32 ■ 40.172.71.158/32 ■ 51.112.36.44/32
UK	■ 3.10.25.136/32 ■ 3.10.90.25/32 ■ 3.11.98.163/32 ■ 3.11.212.17/32 ■ 13.41.113.229/32 ■ 13.42.125.75/32 ■ 18.170.128.61/32 ■ 52.56.244.250/32

Notes:

- A limitation in Microsoft prevents the application from restricting access to these IP addresses. Avanan recommends using available tools to monitor and alert users of unauthorized access.
- Avanan may change the list with sufficient notice provided in advance through the product updates blog.

Appendix H: Supported File Types for DLP

Avanan detects DLP violations in a large list of file types, including EML, HTML, PDF, Microsoft Office files, images, and many more.

For the complete list of supported file types, see the Apache Tika article.

However, for the file types mentioned in the article, these file types are not supported.

- DAT
- INK
- PLIST
- RPMSG
- Mime types
    - application/font-sfnt
    - application/javascript
    - application/postscript
    - application/vnd.google-earth.kmz
    - application/vnd.ms-cab-compressed
    - application/vnd.ms-msi
    - application/vnd.ms-opentype
    - application/x-dosexec
    - application/x-empty
    - application/x-java-applet
    - application/x-msi
    - application/x-qgis
    - application/x-rdp
    - application/x-shockwave-flash
    - application/x-sql
    - application/x-trash
    - application/x-wine-extension-ini
    - application/x-eps
    - text/x-java
    - video/mp4
    - video/MP2T
    - video/quicktime
    - video/x-ms-asf

- application/x-midi
- audio/vnd.wave
- audio/x-wav
- audio/basic
- audio/x-aiff
- audio/midi
- audio/mpeg
- audio/mp4
- audio/x-oggflac
- audio/x-flac
- audio/ogg
- audio/x-oggpcm
- audio/opus
- audio/speex
- audio/vorbis
- video/daala
- video/x-ogguvs
- video/x-ogm
- application/kate
- application/ogg
- video/ogg
- video/x-dirac
- video/x-oggrgb
- video/x-oggyuv
- video/theora
- video/x-flv
- video/x-m4v
- application/mp4
- video/3gpp

- video/3gpp2

Appendix I: Troubleshooting

Common user issues and solutions:

Issue	Solution
Errors for protected SaaS service below the Overview page	To view the error details, hover over the protected SaaS health status icon. For more information, see *"Application Protection Health" on page 334*.
Security events are not created in the portal	■ Verify that Avanan was properly authorized with the SaaS application without errors. After successful authorization, you should see updated statistics of active users and total files/emails at the bottom of the **Overview** page ■ The scanned files/email may contain no malicious/phishing activity and are therefore not presented as security events. Create custom query for files/emails and inspect the relevant item for malicious findings. **Recent Emails query:** **Analytics** > **Add new query** > **Show recent emails** **Recent files query:** **Analytics** > **Add new query** > **Show recent files** ■ Contact your Avanan representative to report any missed detections.
Security event is created with a "NEW" state in the portal but the user receives phishing/malicious emails	■ Verify the specific user is covered by the relevant scope of the configured Inline Prevent rule. ■ Verify that the rule's **Suspected Phishing workflow** is not configured to **Do nothing**. ■ For the **Monitor only** operation mode, it is expected to get only notifications for any events that happened. ■ For the **Protect (Inline)** operation mode, security events for users covered by the rule's scope should be created in **REMEDIATED** state. ■ The user is alerted based on the workflow of the configured rule.

Issue	Solution
Security events are created for legitimate emails or files	■ After initial configuration, the system is "learning" the user's behavior and may produce false detections (called false positives) during this period. For such cases, manually add an email exception ■ If a security event is created for a legitimate file(s), contact your Avanan representative or *Avanan Support* support to report the false detection.

Check Point Copyright Notice