



Cloud App Security

Administration Guide

for Office 365 and Microsoft 365

SONICWALL[®]

Contents

Understanding Cloud App Security	6
Understanding Email Security	6
Understanding Post-Delivery Email Recheck	7
Using Data Leak Protection	8
Understanding Anomalies	8
Understanding Click-Time Protection	9
Configuring Cloud App Security	11
Subscribing to Cloud App Security	11
Activating Cloud Applications for Cloud App Security	12
Activating Office 365 and Microsoft 365 Cloud Applications	14
Manually Configuring Office 365 and Microsoft 365 Cloud Applications During Activation	18
Managing Quarantine for Office 365 and Microsoft 365	30
Setting Up a Quarantine Mailbox for Office 365 and Microsoft 365 Email (Exchange Online)	30
Setting Up a Quarantine Folder for Office 365 and Microsoft 365 OneDrive	31
Setting Up a Quarantine Folder for Office 365 and Microsoft 365 SharePoint	31
Using the Quarantine View for Office 365 and Microsoft 365 Email (Exchange Online)	32
Using the Quarantine Page	33
Using the Quarantined File Creator Dashboard	34
Using the User Dashboard for Office 365 and Microsoft 365	35
Managing Restore Requests	36
Using the SonicWall Cloud App Security Dashboard	37
Using the Security Events Widgets	38
Changing a Security Event Widget to an Alert or Custom Query	39
Resetting a Security Event Widget	39
Hiding a Security Event Widget	40
Configuring Security Event Widget Custom Queries	40
Adjusting the Time Scale	41
Viewing the Summary of Security Events	41
Viewing Login Events	43
Viewing Secured Applications	45
Viewing the Scanned Files Summary	46
Managing Security Events	47
Using the Security Event Graphs	47
Viewing Security Events by Severity	48
Viewing Security Events by State	48

Viewing Security Events by Cloud Application	48
Viewing and Acting on Security Events	49
Removing Filters	50
Acting on Security Events	50
Managing Multiple Events	50
Managing Policies	51
Understanding Cloud App Security Policies	52
Before You Set Email Policies	52
Monitor only	52
Detect and Prevent	52
Protect (Inline)	53
Creating New Policy Rules	53
Creating Data Leak Protection Policy Rules	54
Creating Malware Policy Rules	56
Creating Threat Detection Policy Rules	57
Creating Policy Rules for Click-Time Protection	59
Creating Office 365 and Microsoft 365 Email Encryption Policy Rules	60
Creating Custom Query Policies	61
Stopping Policy Rules	61
Removing Policy Rules	61
Managing Office 365 and Microsoft 365 (Exchange Online) Mail-Flow Rules	62
Using Data Leak Protection	63
Configuring Data Leak Protection Detection Rules	63
Creating Data Leak Protection Policy Rules	64
Reactivating Data Leak Protection	66
Predefined Data Leak Protection Policy Rules	66
Global Rules	67
Credentials and Secrets	69
Predefined Data Leak Protection Rules for Specific Countries	70
Managing Spam and Anti-Phishing	82
Managing Spam	82
Managing User-Reported Phishing	83
Customizing Warning Messages	83
Managing Nickname Impersonation	84
Managing the Anti-Phishing Exceptions	85
Managing Excluded Email Addresses	85
Managing Excluded IP Addresses	86
Managing Excluded Domains	87
Creating Block-List Rules from Email Messages	88
Managing the Anti-Phishing Allow-List	88
Managing the Anti-Phishing Block-List	90

Using the Mail Explorer	91
Using the Mail Explorer to Search Emails	92
Using the Mail Explorer to Quarantine Items	92
Using the Mail Explorer to Add Items to the Blocked List	93
Working with Office 365 and Microsoft 365 Email Encryption	94
Creating Office 365 and Microsoft 365 Email Encryption Policy Rules	95
Configuring and Using Click-Time Protection	96
Understanding Click-Time Protection	96
Activating Click-Time Protection	97
Configuring Click-Time Protection	98
Configuring the Click-Time Protection Workflow	98
Configuring Custom Click-Time Protection for Specific Domains	98
Using Click-Time Protection	99
Creating Policy Rules for Click-Time Protection	100
Viewing Security Events for Click-Time Protection	100
Managing Email Messages with Click-Time Protection	101
Creating Custom Queries for Click-Time Protection	101
Using Cloud App Security Analytics	102
Viewing the Summary Report	103
Viewing the Weekly Reports	104
Viewing Email Analytics	105
Viewing Office 365 and Microsoft 365 OneDrive Analytics	106
Viewing Office 365 and Microsoft 365 SharePoint Analytics	107
Viewing Shadow SaaS Analytics	108
Viewing and Creating Custom Queries	109
Creating Custom Queries	110
Adding Custom Queries to the Dashboard	111
Configuring Cloud Applications in the Cloud App Store	112
Activating Cloud Applications for Cloud App Security	113
Configuring Office 365 and Microsoft 365 for Cloud App Security	114
Re-Authorizing Cloud Applications	115
Managing Security Applications in the Security App Store	117
Starting Security Applications	118
Stopping Security Applications	118
Managing Anomaly Exceptions	119
Understanding Anomalies	119
Creating Exceptions Based on Anomaly Events	120
Sending Anomaly Event Notifications	120

Managing Security Tool Exceptions	121
Using the System Log	122
Viewing the System Log	122
Exporting the System Log	122
Managing Cloud App Security Licenses	123
Adding Administrator Users	124
Adding Read-Only Users	124
Managing Group Licensing	124
Unassigning Cloud App Security Licenses	125
SonicWall Support	126
About This Document	127

Understanding Cloud App Security

SonicWall Cloud App Security (CAS) offers complete, defense-in-depth security for Office 365 and Microsoft 365. If your organization is making the transition from on-premise applications to the cloud, Cloud App Security offers the best way to ensure seamless security.

Cloud App Security connects to your Office 365 and Microsoft 365 environment via API and scans for threats after your existing security but before the inbox. It is laser-focused on advanced attacks while also filtering out spam and greymail. It deploys instantly with the only one-click, cloud-enabled platform with no need for a proxy, appliance or endpoint agent protection, web content filtering for remote users, and securing the use of web and cloud-based applications.

As an integral component of the SonicWall Capture Cloud Platform, Cloud App Security extends the most complete defense-in-depth security stack for Office 365 and Microsoft 365 users. Cloud App Security helps stop targeted phishing and zero-day attacks that bypass Microsoft, Google and Secure Email Gateway security filters.

Its API-based, multi-layered inline threat prevention system is invisible to hackers and enable full-suite protection for cloud email and SaaS applications. The solution easily deploys within minutes and employs a combination of machine learning, artificial intelligence and big-data analyses to provide powerful anti-phishing, attachment sandboxing, click-time URL analysis, impersonation, file sandboxing, and data leakage protection.

Topics:

- [Understanding Email Security](#)
- [Using Data Leak Protection](#)
- [Understanding Anomalies](#)
- [Understanding Click-Time Protection](#)

Understanding Email Security

The widespread adoption of Office 365 and Microsoft 365 makes it an easy target for every hacker. Never have they given so many mailboxes with identical security. Hackers also leverage the fact these cloud accounts are sources of authentication to other enterprise SaaS apps. This is the real and present danger of the cloud security monoculture. What bypasses one, bypasses all. Unfortunately, native cloud security is not enough. Secure Email Gateways (SEGs) are not built for the cloud, only secure inbound and outbound email, and broadcast themselves to hackers.

Given the many limitations of securing cloud email with traditional SEGs and security shortfalls within Office 365 and Microsoft 365 filters, a best-practice solution must be cloud-native and designed to augment, not replace, existing security layers. This ensures that the basic filtering as well as new attack signatures are constantly updated, while advanced threat analyses address modern targeted phishing and evolving zero-day attacks.

A best practice solution must:

- Block harmful messages, URLs, and attachments from reaching the inbox
- Scan all emails preventing insider threats from compromised or trusted internal accounts
- Synchronous threat management via Capture Cloud Platform

Cloud App Security complements the default security of Office 365 and Microsoft 365 by connecting within the Office 365 and Microsoft 365 environment via API and scanning emails after the email provider's built-in security scan. This has several advantages over the proxy method utilized by SEGs.

By scanning after the default security of Office 365 and Microsoft 365, Cloud App Security utilizes the built-in security features as opposed to scanning before default security in the case of SEGs. This allows Cloud App Security to focus on more sophisticated phishing attacks that are designed to bypass the filters in place by Office 365 and Microsoft 365.

By connecting to the cloud environment via the Office 365 and Microsoft 365 API, Cloud App Security can extend their security beyond just inbound and outbound emails to scan internal emails as well for account compromised and data leakage.

Topics:

- [Before You Set Email Policies](#)
- [Using the Mail Explorer](#)
- [Managing Spam and Anti-Phishing](#)
- [Understanding Post-Delivery Email Recheck](#)
- [Working with Office 365 and Microsoft 365 Email Encryption](#)

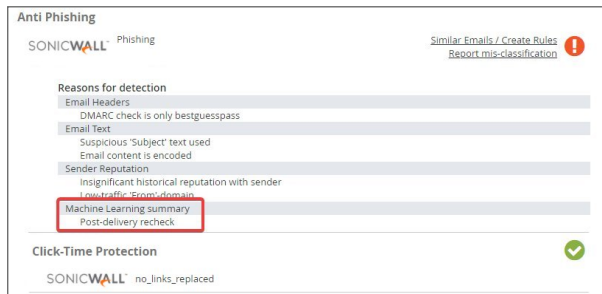
Understanding Post-Delivery Email Recheck

Post-Delivery Security extends the security to email messages already in the inbox. Email Recheck expands post-delivery protection, providing another layer of protection in addition to [Click-Time Protection](#).

Post-Delivery Email Recheck is a multi-phase process:

1. The Email Recheck process can be triggered by several sources, including end-users and administrators. For example: emails that were reported by the end-users as suspected phishing, clicks on malicious URLs in emails protected by Click-Time Protection, and email reclassification by the administrators.
2. The email messages are examined by Cloud App Security.
3. A global block action is issued, across all mailboxes protected by Cloud App Security. The block action includes all emails that match the relevant match criteria.
4. All marked emails are processed by the relevant customer policy workflows. The emails are removed from the inbox and placed in quarantine, while security events are generated, and notifications sent to the users and administrators.

The security event appears as **Post-delivery recheck** as a detection reason in the detailed information for the email message.



Using Data Leak Protection

① **NOTE:** Data Leak Protection (DLP) protection is only available with Advanced licenses for SonicWallCloud App Security.

Data Leak Protection (DLP) helps protect your organization's data from potential data breaches or data ex-filtration transmissions. Data Leak Protection can scan emails and text messages posted on cloud application email and storage platforms, and detect data patterns that should not be shared with unauthorized persons or targets.

SonicWall Cloud App Security uses the SmartDLP engine to implement Data Leak Protection. The benefits of SmartDLP include:

- Fast, modern DLP solution for scanning files and images
- Many built-in DLP detection rules for many verticals and countries
- Seamless setup
- Simple, cross-platform security policies
- Simple, yet powerful actions
- Integration with other SonicWall Cloud App Security security tools

Topics:

- [Reactivating Data Leak Protection](#)
- [Configuring Data Leak Protection Detection Rules](#)
- [Creating Data Leak Protection Policy Rules](#)
- [Predefined Data Leak Protection Policy Rules](#)

Understanding Anomalies

One threat individuals in your organization can face is the takeover of their account(s). SonicWall Cloud App Security can detect this by analyzing unusual behavior an account user, such:

- logins to an account from new browsers, devices, or locations
- suspicious email activity or configurations, such as deleting all incoming email messages or forwarding messages to an external account or domain
- email account configurations that are insecure or make extensive use of filters, forwarding, or secondary accounts
- accounts where two-factor authentication has been disabled
- suspicious internal emails, often with multiple recipients
- multiple account password resets within an unusually short period of time
- changes in the grouping of contacts in emails messages or mailing lists
- changes in the usual characteristics of user sessions (such as the time of day, length of login session, or applications used)

Topics:

- [Managing Anomaly Exceptions](#)

Understanding Click-Time Protection

Click-Time Protection (CTP) is based on URL “rewrites”. Every link within the subject and body of incoming email messages is replaced with an Cloud App Security-generated URL. When the user clicks on the link, Cloud App Security tests the site before redirecting the user to that website.

Click-Time Protection provides

- Another layer of post-delivery protection
- Enhanced protection for zero-day attacks, as URLs can later become malicious
- Forensics

Click-time Protection provides these options for how malicious websites can be handled :

- Do nothing and allow users to go through to the site
- Completely prevent users from visiting the site
- Display a warning to users with the option to continue to the site

Once enabled, all links contained in the subject or content of an incoming email message are replaced with an SonicWall link. When the user clicks on the link, it triggers an immediate scan of the target website.

- If the website is determined to be benign, the user continues without interruption.
- If the website is determined to be malicious, the user is forwarded to a warning page.



Each stage of the Click-time Protection process is recorded for forensic and auditing purposes: from the original URL substitution event to the result of the time-of-click scan. If configured in 'warning only' mode, user clicks of the continue link are recorded.

Topics:

- [Configuring and Using Click-Time Protection](#)

Configuring Cloud App Security

Topics:

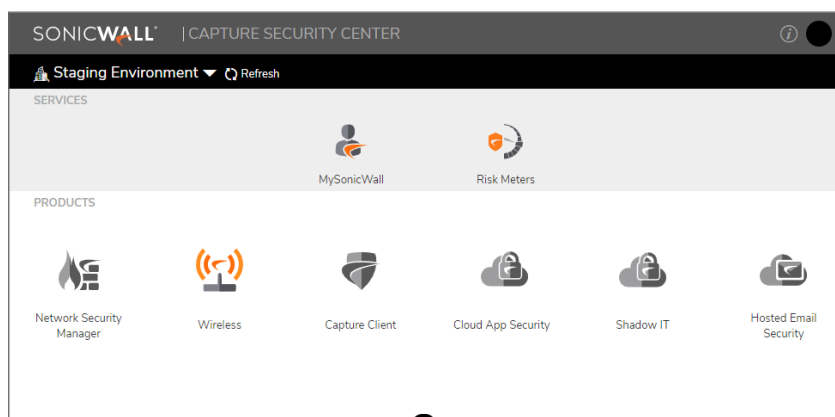
- [Subscribing to Cloud App Security](#)
- [Activating Cloud Applications for Cloud App Security](#)
- [Activating Office 365 and Microsoft 365 Cloud Applications](#)

Subscribing to Cloud App Security

Before you can use SonicWall Cloud App Security, you must set up an account and subscribe to the Cloud App Security service.

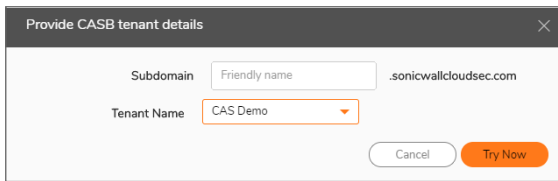
To subscribe to SonicWall Cloud App Security:

1. Navigate to cloud.sonicwall.com.
2. Login with your [MySonicWall](#) credentials to get to the Capture Security Center.
① | **NOTE:** If you do not have a MySonicWall account, you will need to [create one](#).



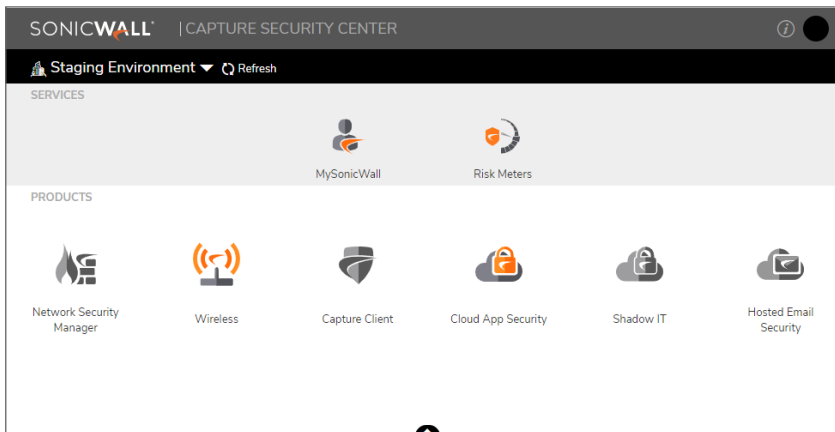
3. Click the **MySonicWall** tile. The MySonicWall dashboard displays.
4. Navigate to **Product Management > My Products**.
5. In the **Quick Register** field, enter your activation key.
6. Click **Register**.

7. When prompted, enter a unique subdomain name.



This subdomain name will be used to create your tenant in the SonicWall Cloud App Security service.

8. Click on the arrowhead at the top of the window to return to the Capture Security Center.
9. Verify that **Cloud App Security** has been activated.



① | **NOTE:** It may require several minutes for the activation of SonicWall Cloud App Security to complete.

Activating Cloud Applications for Cloud App Security

After you have subscribed to the Cloud App Security service, you can add the cloud applications that you want to monitor and control.

Cloud App Security can secure Office 365 and Microsoft 365 applications with these subscription types:

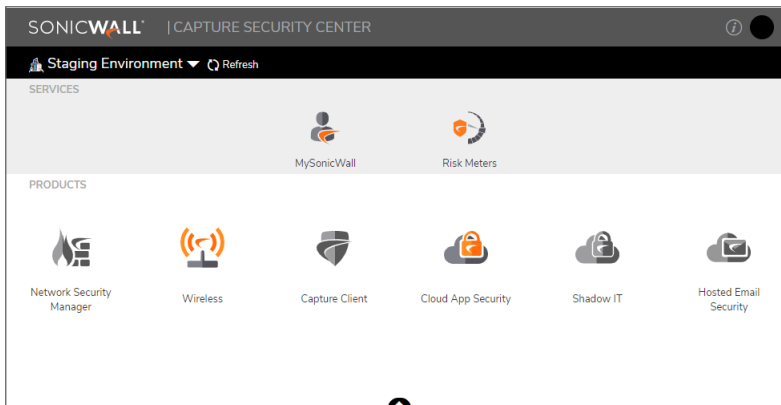
- Office 365 and Microsoft 365 Business
- Office 365 and Microsoft 365 Apps
- Office 365 and Microsoft 365 Education
- Office 365 and Microsoft 365 Enterprise

① | **NOTE:** Personal and Home subscription plans are not supported by SonicWall Cloud App Security.

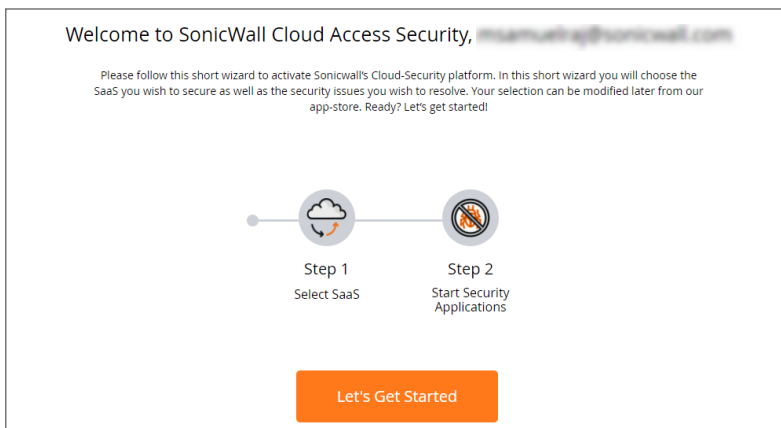
To activate Office 365 and Microsoft 365 applications for Cloud App Security:

1. Navigate to cloud.sonicwall.com.
2. Login with your **MySonicWall** credentials to get to the Capture Security Center.

3. Click the **Cloud App Security** tile.

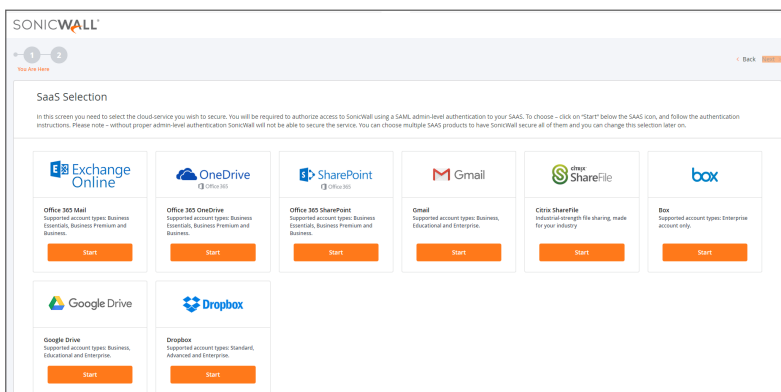


4. The **Welcome to SonicWall Cloud Access Security** page displays.



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

The **SaaS Selection** page displays. This page lists all of the cloud applications which can be monitored using SonicWall Cloud App Security.



6. Click **Start** on the tile for the Office 365 and Microsoft 365 application you want to activate.

For instructions for activating Office 365 and Microsoft 365 cloud applications, see: [Activating Office 365 and Microsoft 365 Cloud Applications](#).

Activating Office 365 and Microsoft 365 Cloud Applications

① **IMPORTANT:** Cloud App Security can secure cloud applications with these subscription types:

- Business
- Microsoft 365 Apps
- Education

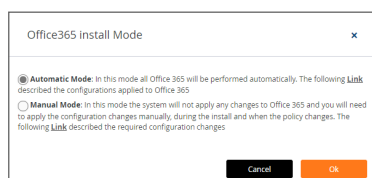
Office 365 and Microsoft 365 Personal and Home subscription plans are not supported by SonicWall Cloud App Security.

① **IMPORTANT:** If you plan to assign Cloud App Security licenses to only a specific set of Office 365 and Microsoft 365 users, create the Office 365 and Microsoft 365 user group before activating your Office 365 and Microsoft 365 cloud applications for Cloud App Security. After initial cloud application activation, the cloud application onboarding process may take up to 12 hours.

Adding new users to the Office 365 and Microsoft 365 group later may result in delay in synchronizing the licensed users with both systems. For more information, refer to [Managing Cloud App Security Licenses](#).

To activate Office 365 and Microsoft 365 cloud applications for Cloud App Security:

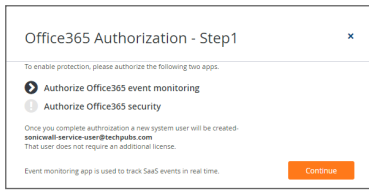
1. Navigate to either the:
 - **SaaS Selection** page (during initial setup and configuration).
 - **Cloud App Store** page.
2. Click **Start** on the tile for the Office 365 and Microsoft 365 cloud application you want activate.
3. Select the installation mode you want to use to activate the Office 365 and Microsoft 365 cloud application.



4. To automatically activate the Office 365 and Microsoft 365 cloud application, select **Automatic Mode** and click **Ok**.

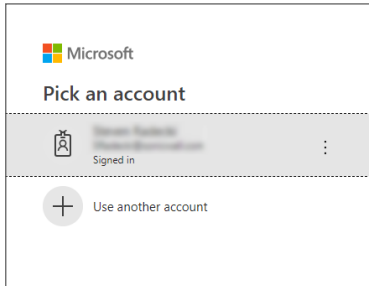
① **NOTE:** **Automatic Mode** is the recommended activation mode and will work for most organizations. **Manual Mode** is intended for use by experienced Office 365 and Microsoft 365 administrators. For information on how to manually activate Office 365 and Microsoft 365 cloud applications using **Manual Mode**, see [Manually Configuring Office 365 and Microsoft 365 Cloud Applications During Activation](#).)

5. Click **Continue** to authorize any supporting applications.

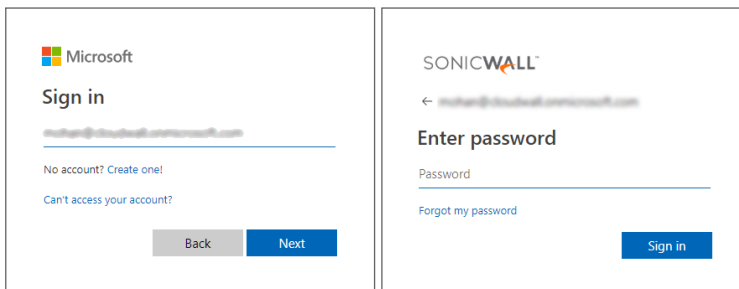


6. Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

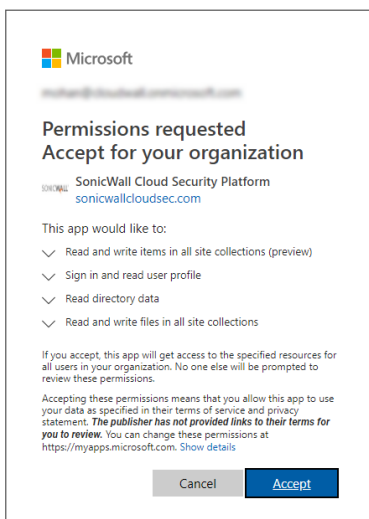
① | **NOTE:** This must be an administrator account associated with your Microsoft account.



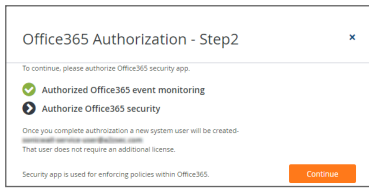
7. Sign into your Microsoft business account.



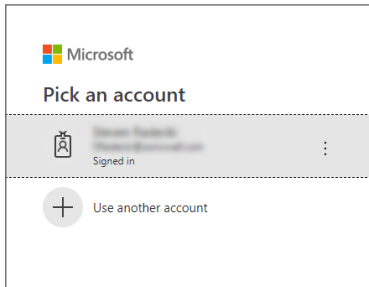
8. When prompted with a list of permissions to which to grant SonicWall Cloud App Security access, click **Accept**.



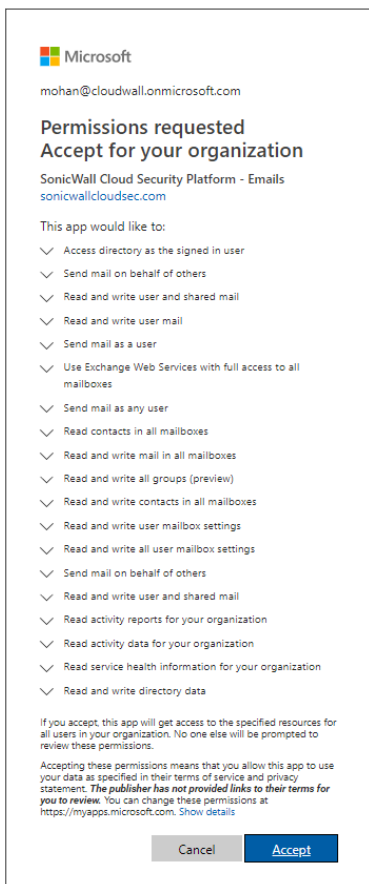
9. Click **Continue** to continue the activation process.



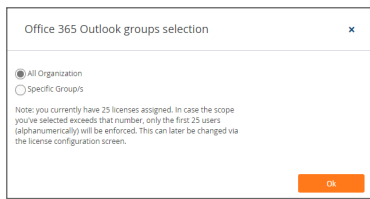
10. Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.
- ① | **NOTE:** Make certain that you select the same Microsoft account that you used in previous steps.



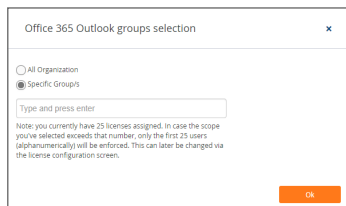
11. When prompted with a new list of permissions to which to grant Cloud App Security access, click **Accept**.



12. On the Office 365 and Microsoft 365 groups selection page:



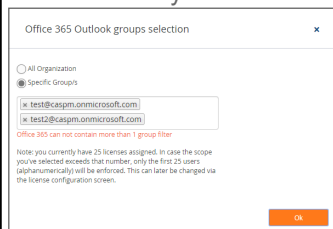
- Select **All Organization** if you want to assign Cloud App Security licenses to all of the users in your organization.
- Select **Specific Group/s** if you want to assign Cloud App Security licenses to only a specific Office 365 and Microsoft 365 group in your organization. Using Group Filters is the most effective way to manage you Cloud App Security licenses for a specific subset of users within your organization.



- NOTE:** Licenses are assigned in alphabetical order.
- If the number of users exceeds the number of available licenses, all user licenses will be assigned in alphabetical order by the system automatically. You can manually unassign users in order to free up licenses.
 - If the number of licenses exceeds the number of users, the remaining licenses will remain unassigned. Any new users added to the group will be assigned from the available license pool.
- Refer to [Managing Cloud App Security Licenses](#) for more information.

Enter the name of the Office 365 and Microsoft 365 group to which you want to assign the licenses.

- NOTE:** Only one group is supported for Office 365 and Microsoft 365 cloud applications at this time. If you enter more than one group, an error message is displayed.



You can change this setting later, if you needed, on the **Configuration > Cloud App Store** page. Refer to [Managing Cloud App Security Licenses](#) for more information.

- NOTE:** If you add users to the Office 365 and Microsoft 365 group later, it may take up to 12 hours for the user licenses to synchronize between the systems. For more information, refer to [Managing Cloud App Security Licenses](#).

13. Click **Ok**.

14. On the **SaaS Selection** page, verify that a green checkbox appears on the tile for the Office 365 and Microsoft 365 cloud application indicating that the application has been activated for SonicWall Cloud App Security.

15. Navigate to the **Configuration > Cloud App Store** page.
16. On the tile for the Office 365 and Microsoft 365 application(s) you want to run, click **Start** to start the protection of Office 365 and Microsoft 365 using Cloud App Security.

This begins the process of scanning existing email messages and files.

- For email messages: previous 5 days
- For cloud storage: previous 7 days

- ① **NOTE:** If you have only activated Office 365 and Microsoft 365 cloud application at this time, you will not need to reauthorize Cloud App Security again when you activate any additional Office 365 and Microsoft 365 cloud applications.
- ① **NOTE:** The Office 365 and Microsoft 365 cloud application activation process can take several hours, depending on the number of users in the Office 365 and Microsoft 365 account. An email will be sent to the email address associated with your MySonicWall account after the process has completed.

Manually Configuring Office 365 and Microsoft 365 Cloud Applications During Activation

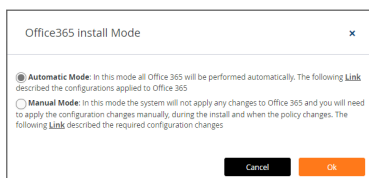
- ① **IMPORTANT:** Cloud App Security can secure cloud applications with these subscription types:

- Business
- Microsoft 365 Apps
- Education

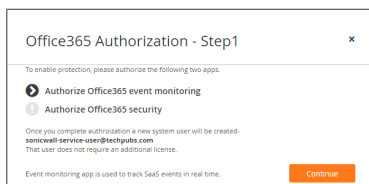
Office 365 and Microsoft 365 Personal and Home subscription plans are not supported by SonicWall Cloud App Security.

To manually configure Office 365 cloud applications during activation:

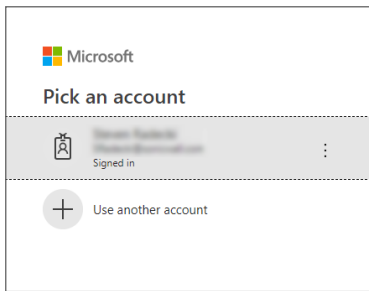
1. Select the installation mode you want to use to activate the Office 365 and Microsoft 365 cloud application.



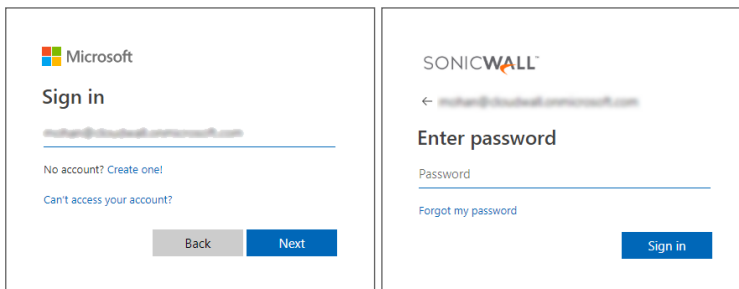
2. To manually activate the Office 365 and Microsoft 365 cloud application, select **Manual Mode** and click **Ok**. (For information on how to automatically activate the Office 365 and Microsoft 365 cloud application, see [Activating Office 365 and Microsoft 365 Cloud Applications](#).)
3. Click **Continue** to authorize any supporting applications.



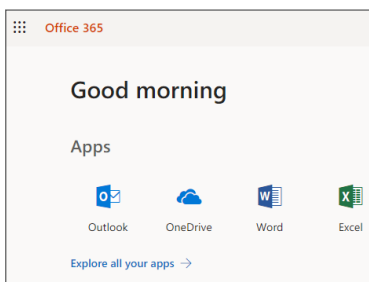
4. Select your Office 365 and Microsoft 365 account from the list and, if prompted, log in using your Office 365 and Microsoft 365 account username and password.



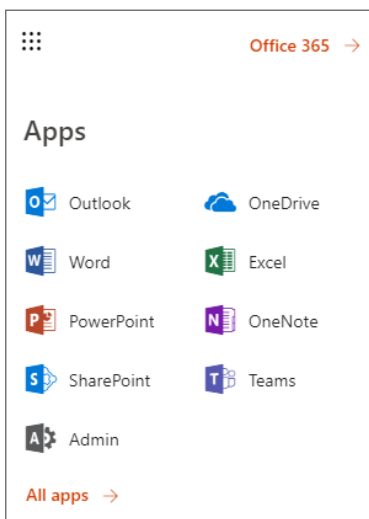
5. Sign into your Office 365 and Microsoft 365 business account.



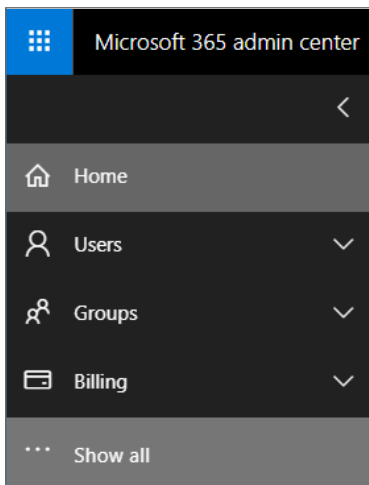
6. Click the  in the upper left area of the page.



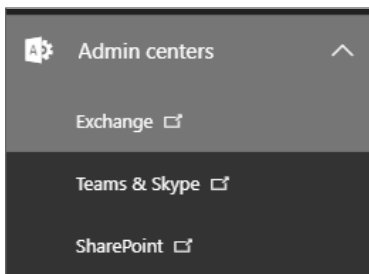
7. When the **Apps** area appears, select **Admin**.



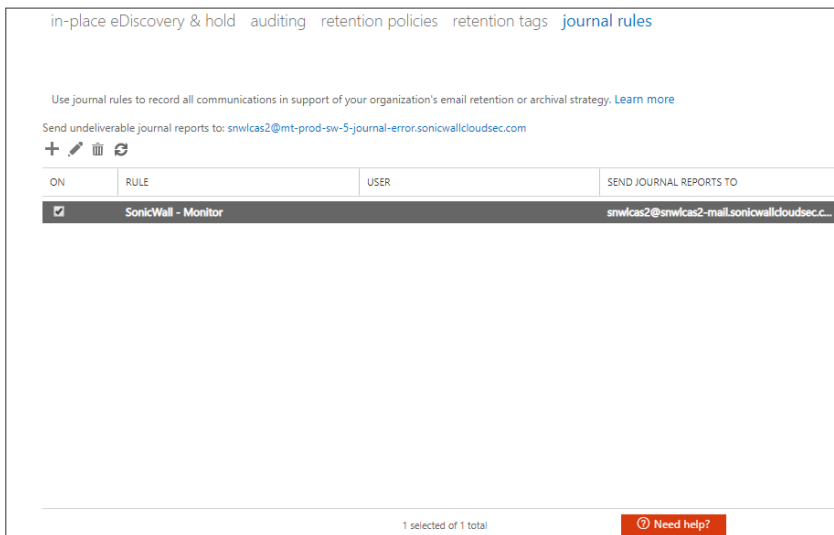
8. From the **Office 365 and Microsoft 365 admin center**, click **Show all**.



9. Scroll down to **Admin centers** and click **Exchange**.



10. On the **Exchange admin center** page, click **compliance management > journal rules**.



11. In the **Send journal reports to** field, enter the email address in your domain to which the journal reports should be sent.

SonicWall - Monitor

Apply this rule...

*Send journal reports to:

Name:

*If the message is sent to or received from...

*Journal the following messages...

The journal rule is used for the monitoring mode. The journal rule configures Office 365 and Microsoft 365 to send all emails to the system.

12. Click **Save**.
13. On the **Exchange admin center** page, click **mail flow > connectors**.

Exchange admin center

dashboard rules message trace accepted domains remote domains **connectors**

recipients permissions compliance management organization protection **mail flow** mobile public folders unified messaging hybrid

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first [check to see if you should create a connector](#).

Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS	NAME	FROM	TO
On	SonicWall Inbound	Partner organization	Office 365
On	SonicWall Journaling Ou...	Office 365	Partner organization

0 selected of 2 total

14. To configure the inbound connector, select it in the list and either double-click or click the **Edit** icon.

rules message trace accepted domains remote domains **connectors**

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first [check to see if you should create a connector](#).

Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

+ ✎ 🗑️ ↺

STATUS	NAME	FROM	TO	
On	SonicWall Inbound	Partner organization	Office 365	SonicWall Inbound
On	SonicWall Journaling Ou...	Office 365	Partner organization	Mail flow scenario From: Partner organization To: Office 365 Description SonicWall Inbound Connector Status On Turn it off

- a. Enter a **Name** and **Description** for the inbound connector.

Edit Connector

This connector enforces routing and security restrictions for email messages sent from your partner organization or service provider to Office 365.

*Name:
SonicWall Inbound

Description:
SonicWall Inbound Connector

What do you want to do after connector is saved?
 Turn it on

Next Cancel

- b. Select **Turn it on** if you want to connector enabled after you complete its configuration.
c. Click **Next**.

- d. Select **where to use the domain name** or the IP address of the sender.

The screenshot shows the 'Edit Connector' page. The title is 'Edit Connector'. Below the title is the question 'How do you want to identify the partner organization?'. Underneath, there is a sub-question: 'Specify whether you want to use a domain or IP address to identify the partner organization. [Learn more](#)'. There are two radio button options: 'Use the sender's domain' (which is unselected) and 'Use the sender's IP address' (which is selected). A callout box on the right points to the selected option and contains the text: 'Select this option to apply this connector to email messages that come from your partner's domains.' At the bottom of the page are three buttons: 'Back', 'Next', and 'Cancel'.

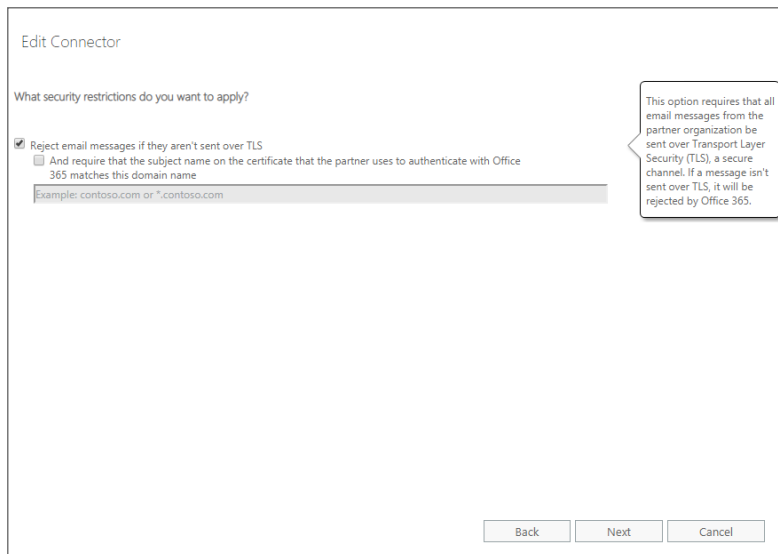
- e. Click **Next**.
- f. Select the IP addresses you want to use to identify your sender.

The screenshot shows the 'Edit Connector' page. The title is 'Edit Connector'. Below the title is the question 'What sender IP addresses do you want to use to identify your partner?'. Underneath, there is a sub-question: 'Specify the sender IP address range.' Below this, there are three icons: a plus sign, an eraser, and a minus sign. A list box contains one entry: '192.168.1.1/24'. A callout box on the right points to the list box and contains the text: 'Specify IP address ranges that this connector applies to.' At the bottom of the page are three buttons: 'Back', 'Next', and 'Cancel'.

You can also add, edit, or delete sender IP addresses on this page.

- g. Click **Next**.

- h. Select **Reject email messages if they aren't sent over TLS** to reject any email messages from the sender that are not sent using Transport Layer Security (TLS).

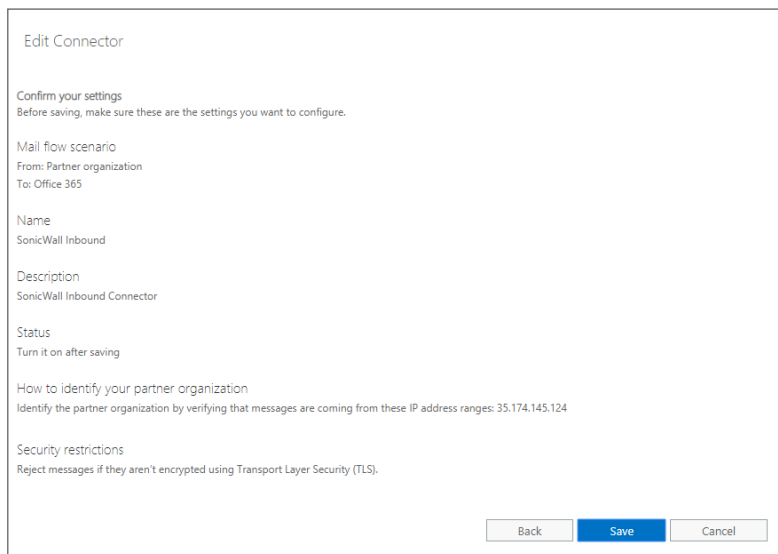


The screenshot shows the 'Edit Connector' dialog box with the following content:

- Title: Edit Connector
- Section: What security restrictions do you want to apply?
- Option 1: Reject email messages if they aren't sent over TLS
- Option 2: And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name
- Text input field: Example: contoso.com or *.contoso.com
- Callout box: This option requires that all email messages from the partner organization be sent over Transport Layer Security (TLS), a secure channel. If a message isn't sent over TLS, it will be rejected by Office 365.
- Buttons: Back, Next, Cancel

You can add an additional level of security by selecting **And require that the subject name on the certificate that the partner uses to authenticate with Office 365 and Microsoft 365 matches this domain name** and specifying a required domain name.

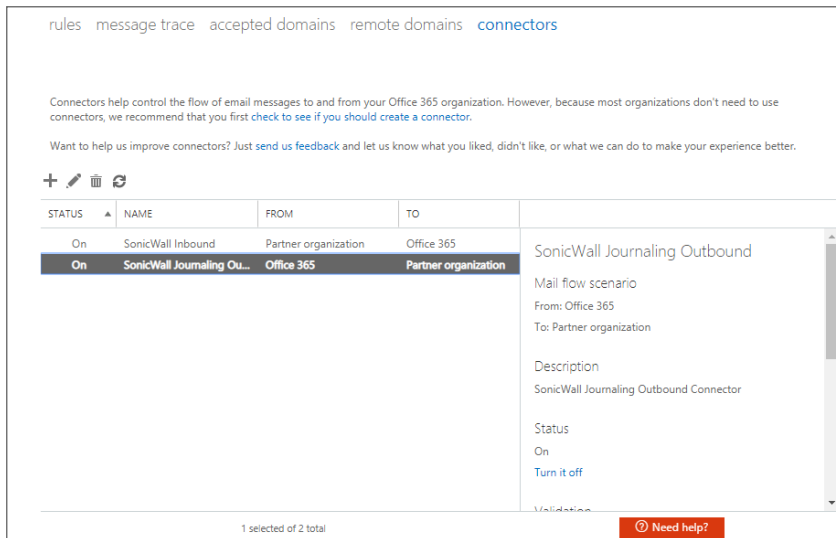
- i. Verify your settings for the inbound connector and click **Save**.



The screenshot shows the 'Edit Connector' dialog box with the following configuration summary:

- Title: Edit Connector
- Section: Confirm your settings
- Text: Before saving, make sure these are the settings you want to configure.
- Section: Mail flow scenario
- Text: From: Partner organization
- Text: To: Office 365
- Section: Name
- Text: SonicWall Inbound
- Section: Description
- Text: SonicWall Inbound Connector
- Section: Status
- Text: Turn it on after saving
- Section: How to identify your partner organization
- Text: Identify the partner organization by verifying that messages are coming from these IP address ranges: 35.174.145.124
- Section: Security restrictions
- Text: Reject messages if they aren't encrypted using Transport Layer Security (TLS).
- Buttons: Back, Save, Cancel

15. To configure the outbound connector, select it in the list and either double-click or click the **Edit** icon.



- a. Enter a **Name** and **Description** for the outbound connector.

Edit Connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

*Name:
SonicWall Journaling Outbound

Description:
SonicWall Journaling Outbound Connector

What do you want to do after connector is saved?
 Turn it on

Next Cancel

- b. Select **Turn it on** if you want to connector enabled after you complete its configuration.
- c. Click **Next**.

d. Set when you want the connector to be used.

Edit Connector

When do you want to use this connector?

Only when I have a transport rule set up that redirects messages to this connector

Only when email messages are sent to these domains

+ ✎ -

snw/cas2-mail.sonicwallcloudsec.com

Back Next Cancel

Select this option only if you created a rule that redirects email messages to this connector. [Learn more](#)

e. Set how you want the email messages routed.

Edit Connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

Use the MX record associated with the partner's domain

Route email through these smart hosts

+ ✎ -

snw/cas2-host.sonicwallcloudsec.com

Back Next Cancel

Select to send messages to the MX record destination for the targeted recipients.

- f. Select **Always use Transport Layer Security (TLS)** to secure the connection (recommended) to only connect to the email server of the email recipient is TLS is used to secure the connection. (This option is selected by default.)

The screenshot shows the 'Edit Connector' dialog box. The title is 'Edit Connector'. Below the title, it asks 'How should Office 365 connect to your partner organization's email server?'. There are three radio button options: 1. 'Always use Transport Layer Security (TLS) to secure the connection (recommended)' - This is selected. Below it, it says 'Connect only if the recipient's email server certificate matches this criteria'. 2. 'Any digital certificate, including self-signed certificates'. 3. 'Issued by a trusted certificate authority (CA)'. Below these is a checkbox 'And the subject name or subject alternative name (SAN) matches this domain name:' with a text input field containing 'Example: contoso.com or *.contoso.com'. To the right of the dialog is a callout box explaining TLS: 'TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.' At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'.

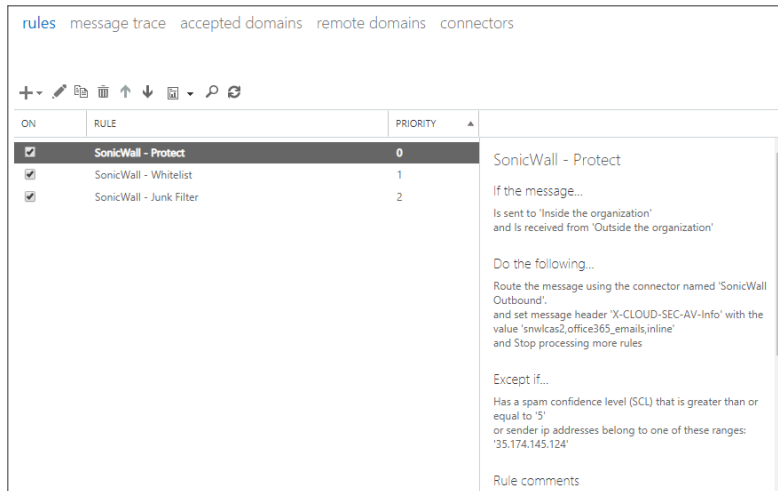
You can also increase the security of the connection by requiring the presence of an email server certificate, either self-signed or issued by a recognized certificate authority.

- g. Verify your settings for the outbound connector and click **Save**.

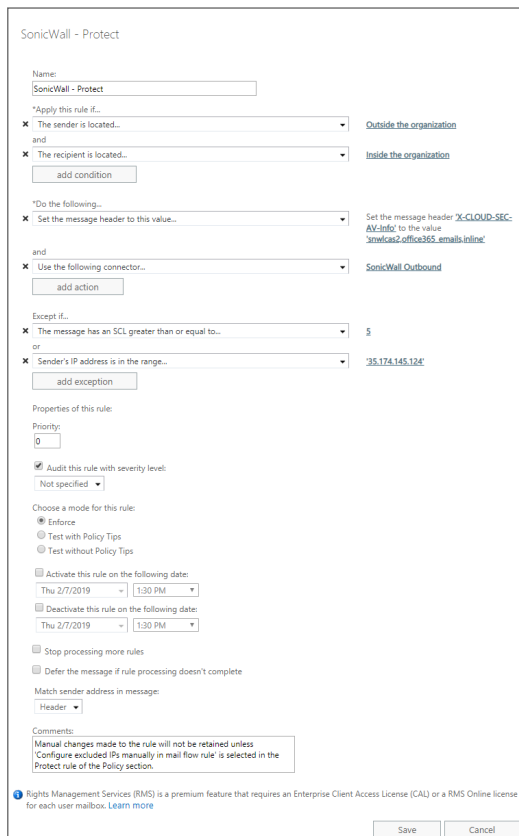
The screenshot shows the 'Edit Connector' dialog box in a confirmation stage. The title is 'Edit Connector'. Below the title, it says 'Confirm your settings' and 'Before we validate this connector for you, make sure these are the settings you want to configure.' The settings listed are: 'Mail flow scenario' (From: Office 365, To: Partner organization), 'Name' (SonicWall Journaling Outbound), 'Description' (SonicWall Journaling Outbound Connector), 'Status' (Turn it on after saving), 'When to use the connector' (Use only for email sent to these domains: snwlcas2-mail.sonicwallcloudsec.com), 'Routing method' (Route email messages through these smart hosts: snwlcas2-host.sonicwallcloudsec.com), and 'Security restrictions'. At the bottom right are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

16. Navigate to **mail flow > rules**.

- a. Select the rule that contains “Protect” and double-click on it or click the **Edit** icon.



- b. Set the values of the fields to use the connectors that you created.



- **Apply this rule if...:** Set the condition(s) under which the rule should be applied. In this example, the rule is only applied to emails that originate outside the organization/domain and the email address of the recipient is within the organization/domain.

- **Do the following...:** Specify the action(s) to be taken when the rule is applied.
In this example, the header of the email message is assigned a specific value so that processed email messages can be more easily detected and then forwarded to the outbound connector that you created.
- **Except if...:** Specify any exceptions for when the rule's actions should not be taken.
 - ① **IMPORTANT:** One of your exceptions should include **Sender's IP address is in the range...** that includes the IP address(es) specified in your inbound connectors to prevent the email messages from being processed in an endless loop.
In this example, the actions are not taken if the email message has already been classified by Microsoft as spam (an Spam Confidence Level [SCL] greater than 5) or is a message that is identified as having been processed.
- Select **Stop processing more rules** to end the processing if the email message was processed by this rule.
 - ① **NOTE:** Every time you change the scope of the inline policy (such as when you add or remove users or groups), you will need to edit the **Apply this rule if... The recipient is ...** section.

17. Click **Save**.

Managing Quarantine for Office 365 and Microsoft 365

Topics:

- [Setting Up a Quarantine Mailbox for Office 365 and Microsoft 365 Email \(Exchange Online\)](#)
- [Setting Up a Quarantine Folder for Office 365 and Microsoft 365 OneDrive](#)
- [Setting Up a Quarantine Folder for Office 365 and Microsoft 365 SharePoint](#)
- [Using the Quarantine Page](#)
- [Using the Quarantined File Creator Dashboard](#)
- [Using the Quarantine View for Office 365 and Microsoft 365 Email \(Exchange Online\)](#)
- [Using the User Dashboard for Office 365 and Microsoft 365](#)
- [Managing Restore Requests](#)

Setting Up a Quarantine Mailbox for Office 365 and Microsoft 365 Email (Exchange Online)

Before you quarantine email messages and attachments, you need to designate and configure a quarantine mailbox.

To set up a quarantine mailbox:

1. Navigate to **Configuration > Cloud App Store**.
2. On the **Office 365 and Microsoft 365** tile, click **Configure**.
3. In the **Quarantine Email Address** field, enter the email address to which all quarantined email should be routed. This email address will also receive all notifications for quarantined email messages.
 - ① **NOTE:** The email address used for quarantined email messages must be a valid email address account within your organization.
4. In the **Restore requests approver** field, enter the email address(es) of the users who can approve restore requests for quarantined email messages.

5. Click the **Advanced** heading if you want to customize the email messages that are sent for quarantined email messages.
6. Click **Ok**.

Setting Up a Quarantine Folder for Office 365 and Microsoft 365 OneDrive

Before you quarantine files stored in OneDrive, you need to designate and configure a quarantine folder.

To set up a quarantine mailbox:

1. Navigate to **Configuration > Cloud App Store**.
2. Click **Configure** on the **OneDrive** tile.
3. Select either:
 - **Create Quarantine folder in the root directory** to create a quarantine folder in the top-level directory of your OneDrive.
 - **Quarantine to existing directory** to quarantine files to an existing folder.
 - ① | **NOTE:** This folder must already exist as it cannot be created during this process.
 - In the **Select Quarantine Path** dropdown list, select the folder you want to designate as the quarantine folder.
4. Click **Enable Remove Action** to allow remove actions to be used. (This option is selected by default.)
5. Click **Ok**.

Setting Up a Quarantine Folder for Office 365 and Microsoft 365 SharePoint

Before you quarantine files stored in SharePoint, you need to designate and configure a quarantine folder.

To set up a quarantine mailbox:

1. Navigate to **Configuration > Cloud App Store**.
2. Click **Configure** on the SharePoint tile.
3. Select either:
 - **Create Quarantine folder in the root directory** to create a quarantine folder in the top-level directory of your SharePoint.
 - **Quarantine to existing directory** to quarantine files to an existing folder.
 - ① | **NOTE:** This folder must already exist as it cannot be created during this process.
 - In the **Select Quarantine Path** dropdown list, select the folder you want to designate as the quarantine folder.
4. Click **Force Site Admin** to require actions by the site administrators.


5. Click **Advanced** to view the **Authorization Scope** options:
 - Select **Authorize for all sites** to enforce the quarantine settings for all SharePoint sites.
 - Select **Authorize for specific sites only** to enforce the quarantine settings for only specified SharePoint sites.

In the **Restrict to these sites only** field, enter the sites for which the quarantine settings will be used.
6. Click **Ok**.

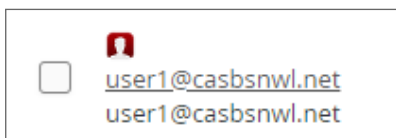
Using the Quarantine View for Office 365 and Microsoft 365 Email (Exchange Online)

The **Quarantine** view for Office 365 and Microsoft 365 Email (Exchange Online) provides you with information about the:

- sender of the email message
- mailbox in which the message is stored
- Subject line of the email message
- number of attachments
- date and time when it was received
- date and time when it was quarantined

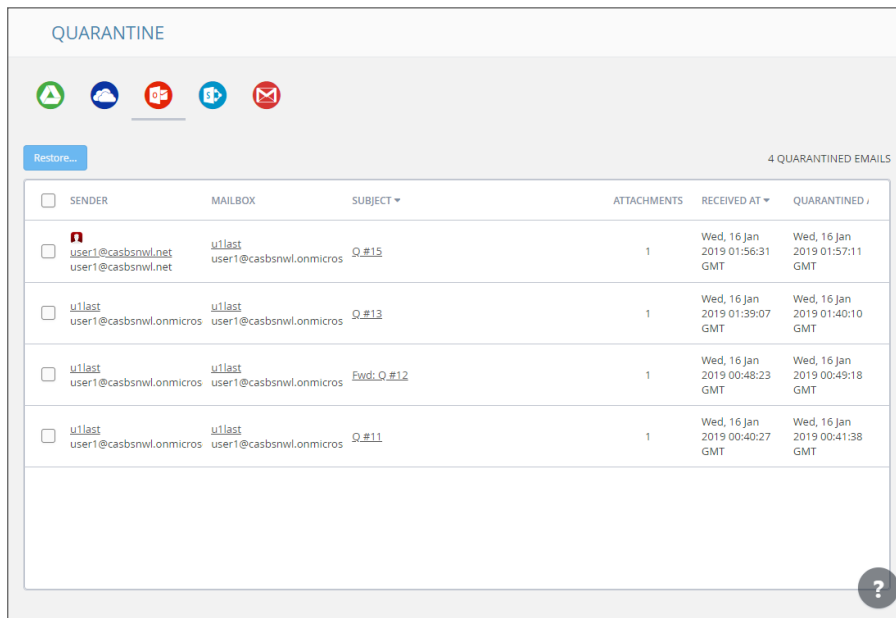
SENDER	MAILBOX	SUBJECT	ATTACHMENTS	RECEIVED AT	QUARANTINED
 user1@casbsnwl.net user1@casbsnwl.net	u1last user1@casbsnwl.onmicrosoft	Q_#15	1	Wed, 16 Jan 2019 01:56:31 GMT	Wed, 16 Jan 2019 01:57:11 GMT
u1last user1@casbsnwl.onmicrosoft	u1last user1@casbsnwl.onmicrosoft	Q_#13	1	Wed, 16 Jan 2019 01:39:07 GMT	Wed, 16 Jan 2019 01:40:10 GMT
u1last user1@casbsnwl.onmicrosoft	u1last user1@casbsnwl.onmicrosoft	Fwd: Q_#12	1	Wed, 16 Jan 2019 00:48:23 GMT	Wed, 16 Jan 2019 00:49:18 GMT
u1last user1@casbsnwl.onmicrosoft	u1last user1@casbsnwl.onmicrosoft	Q_#11	1	Wed, 16 Jan 2019 00:40:27 GMT	Wed, 16 Jan 2019 00:41:38 GMT

Users external to your organization are designated with a red icon.

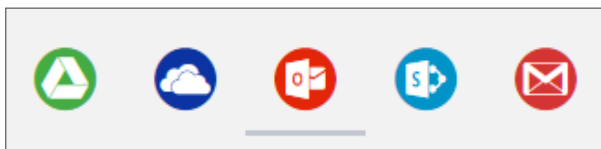


Using the Quarantine Page

The **Quarantine** page lists all of the items quarantined through the policy rules that you have set. (Refer to [Managing Policies](#) for information on setting policy rules.)



You can switch between the quarantined items for each cloud application by clicking on the icon for the application on the upper left of the page.



Topics:

- [Managing Quarantine for Email](#)
- [Managing Quarantine for Cloud Storage](#)
- [Using the Quarantined File Creator Dashboard](#)
- [Using the User Dashboard for Office 365 and Microsoft 365](#)
- [Managing Restore Requests](#)

Using the Quarantined File Creator Dashboard

The Quarantined File Creator Dashboard provides you with information about email messages and files that have been quarantined.

The screenshot displays the Quarantined File Creator Dashboard for a message titled "Fwd: capture atp test gmail realtime testing". The dashboard is divided into several sections:

- Email Profile:** Shows sender (Mohan Samuelraj), recipient (Admin SNWL CAS2), subject, content type (HTML), and a "Restore from quarantine" button.
- Security Stack:** Includes "Anti Phishing" (SONICWALL) with a "Mark as phishing" option and "Insecure attachments found" (high_confidence1.xlsm) with a "Submit file for analysis" option.
- Email attachments:** A table listing the attachment "high_confidence1.xlsm" (15.2 Kilobytes).
- Conversation:** A table showing the message history with timestamps and subjects.
- Live event log:** A table showing inspection events for the email body and the attachment.

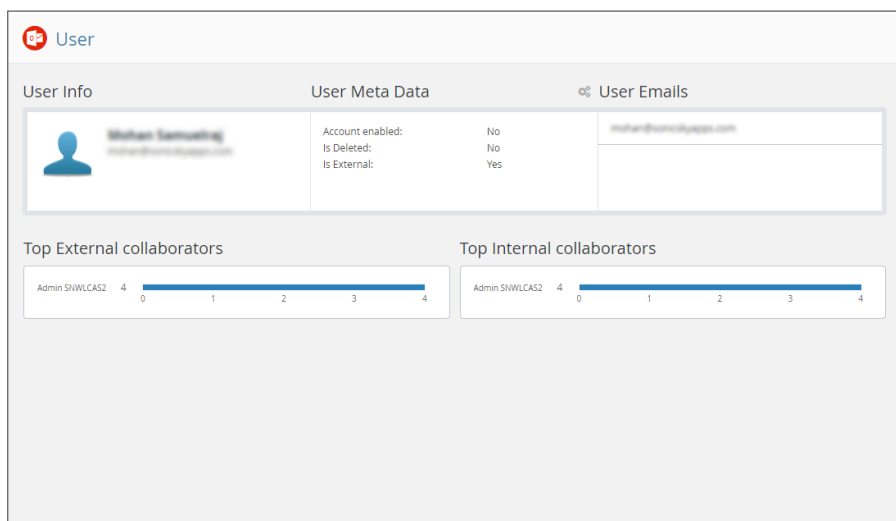
Widget	Description
Email Profile	<p>summary information about the email message, including its Subject line, sender, recipient(s), date and time sent, and current status. You can click on the user email address to view more detailed information about the user. (See Using the User Dashboard for Office 365 and Microsoft 365 for more information.)</p> <p>You can click the Restore from quarantine or Restore Email button to remove the email message or file from quarantine.</p> <p>You can click the gear icon in the upper right above the widget to access Advanced options that allow you to recheck the item, or access the raw header or body from the quarantined email message.</p>
Security Stack	<p>information reported by the installed security tools for the quarantined email message or file. You can click the gear icon in the upper right above the widget to download a copy of the quarantined item.</p>

Widget	Description
	Depending on the item and the security tool, you can report that the items has been misclassified as a threat.
Email attachments	lists the attachments associated with the quarantined email message. You can click on the link of the Name of the attachment to view more information about it.
Conversation	lists all of the email messages in the thread associated with the quarantined email message. You can click the link of the Subject line to view the details of those messages.
Live event log	Detailed list of the events associated with the quarantined email message or file.

Using the User Dashboard for Office 365 and Microsoft 365

The User Dashboard for Office 365 and Microsoft 365 shows you the:

- name and email address of the user for the email message
- information about the status and location (internal or external) of the email account
- email accounts associated with the user



Managing Restore Requests

Users can request that email messages and files in cloud storage applications can be moved out of quarantine.

To restore a quarantined email message or file:

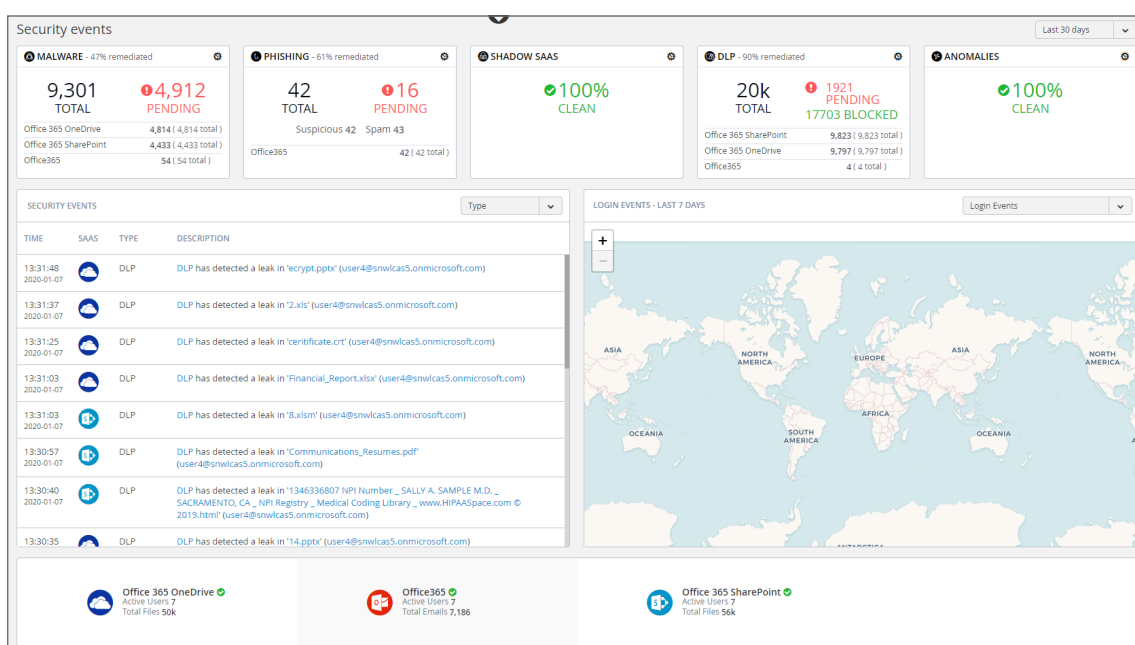
1. Navigate to the **Quarantine** page.
2. From the Quarantined File Creator Dashboard, select the items you want moved out of quarantine.
3. Click the **Restore...** button.
4. When prompted **Are you sure you want to continue?**, click **Ok**.

or

1. Navigate to the **Quarantine > Restore requests** page.
2. Select the items you want to manage:
 - Click the **Restore...** button to remove the selected items from quarantine.
 - Click the **Decline...** button to decline the restore request for the selected items.

Using the SonicWall Cloud App Security Dashboard

The SonicWall Cloud App Security Dashboard provides you with an overview of the state of all your currently monitored cloud applications.



The Dashboard provides you with a summary of all of your secured cloud application with:

- detailed analytics, including the number of emails or files detected and remediated
- a timeline of security incidents affecting your secured cloud applications in real-time
- geo-location tracking for complete user awareness

Through the Cloud App Security Dashboard, you can:

- view discovered and remediated security events
- create and edit policies
- understand your security with analytics
- examine quarantined files and emails
- configure settings to match the requirements of your organization

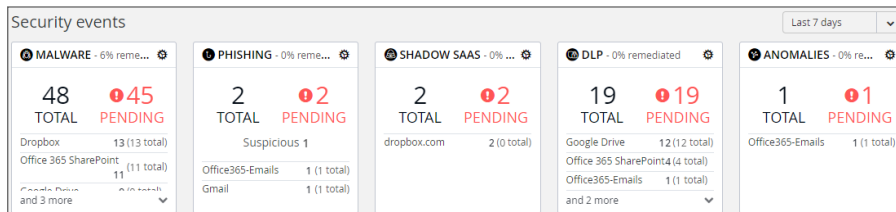
The menu located on the left side is displayed at all times and allows you to navigate between the other Cloud App Security views.

Topics:

- [Using the Security Events Widgets](#)
- [Viewing the Summary of Security Events](#)
- [Viewing Login Events](#)
- [Viewing Secured Applications](#)
- [Viewing the Scanned Files Summary](#)

Using the Security Events Widgets

The widgets at the top of the Cloud App Security Dashboard provide you with a summary of the security events for your organization over a period of time that you can specify.



The numbers in each widget designate:

Total the total number of events reported

Pending the number of events that need to be managed by the administrator

Each widget can be customized to display the information in which you are most interested. Customization of Security Event widgets are saved in your user preferences and are applied every time you log on.

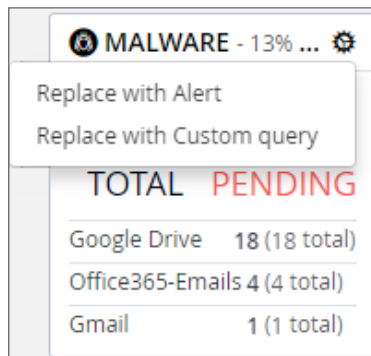
Topics:

- [Changing a Security Event Widget to an Alert or Custom Query](#)
- [Resetting a Security Event Widget](#)
- [Hiding a Security Event Widget](#)
- [Configuring Security Event Widget Custom Queries](#)
- [Adjusting the Time Scale](#)

Changing a Security Event Widget to an Alert or Custom Query

To change a Security Event widget to an Alert or Custom Query:

1. Click on the gear icon in the upper right corner of the Security Event widget.

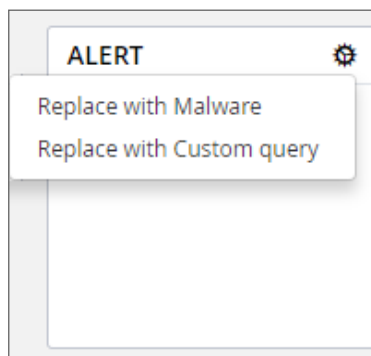


2. From the dropdown list, select:
 - **Replace with Alert**
 - **Replace with Custom query** (Refer to [Creating Custom Query Policies](#) for information on creating custom queries.)

Resetting a Security Event Widget

To change a Security Event widget to its original state:

1. Click on the gear icon in the upper right corner of the Security Event widget.



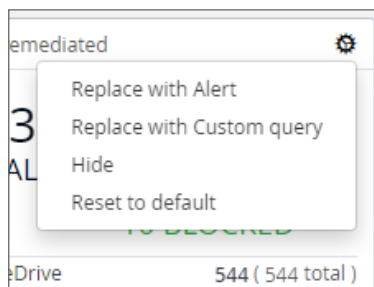
2. From the dropdown list, select the original name of the widget.

Hiding a Security Event Widget

You can hide Security Events widgets from your Dashboard.

To hide a Security Event widget:

1. Click on the gear icon in the upper right corner of the Security Event widget.

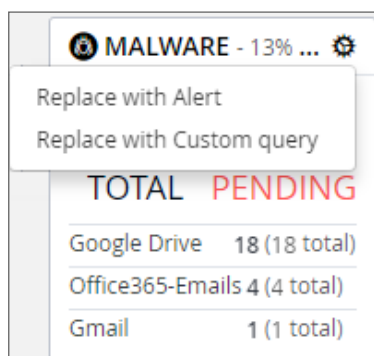


2. From the dropdown list, select **Hide**.

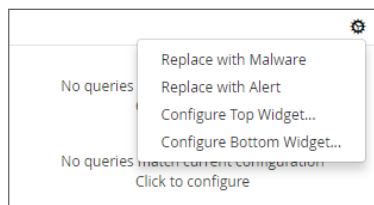
Configuring Security Event Widget Custom Queries

To configure a Security Event widget custom query:

1. Click on the gear icon in the upper right corner of the Security Event widget.



2. From the dropdown list, select **Replace with Custom query**.
3. Click the gear icon again.

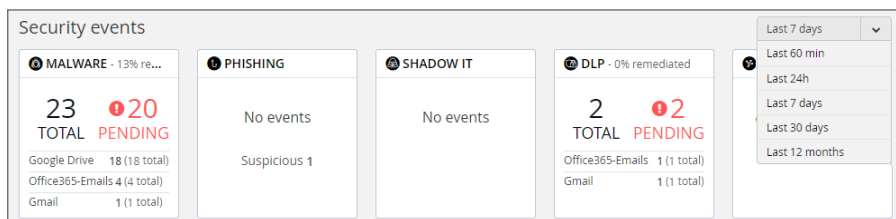


4. Select either:
 - **Configure Top Widget...**
 - **Configure Bottom Widget...**

5. Configure the top or bottom section of the widget or to replace the current widget with Shadow IT events.
6. Enter the title, followed by the value description.
7. Select whether you would like the query to fetch by tag or by queries.
8. Choose from these values:
 - **none**
 - **History**
 - **Another value**

Adjusting the Time Scale

You can adjust the time scale during which the information about the security events is displayed.



To adjust the time scale for the security events:

1. Click on the dropdown list to the far right of the security event widgets.
2. Select on the time period for which you want the security event data displayed on the Dashboard.

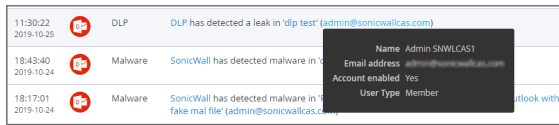
Viewing the Summary of Security Events

The Cloud App Security Dashboard provides a summary of the security events associated with your secured cloud applications during the specified time scale.

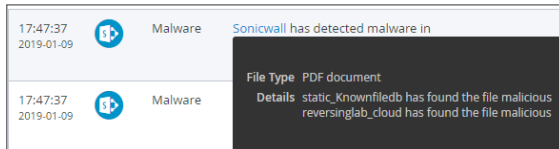
TIME	SAAS	TYPE	DESCRIPTION
05:07:35 2019-01-09		Malware	Sonicwall has detected malware in 'a8c57b6b159dae911e72e34555f0e0f8' (malware@sonicwall.com)
05:07:34 2019-01-09		Malware	Sonicwall has detected malware in '527b2d1dfe167d33ab4e3ccbadebf3bd' (malware@sonicwall.com)
05:07:25 2019-01-09		Malware	Sonicwall has detected malware in 'ffb96a704106fe8c9fad45bc7cc48898' (malware@sonicwall.com)
05:07:16		Malware	Sonicwall has detected malware in

You can hover over elements of each security event to get more information:

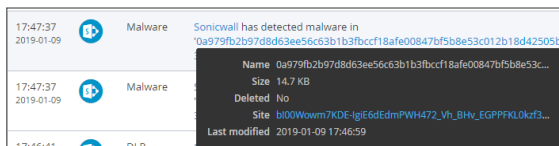
- For files with possible malware or data leaks, see the information about the file, its site of origin, and the action taken:



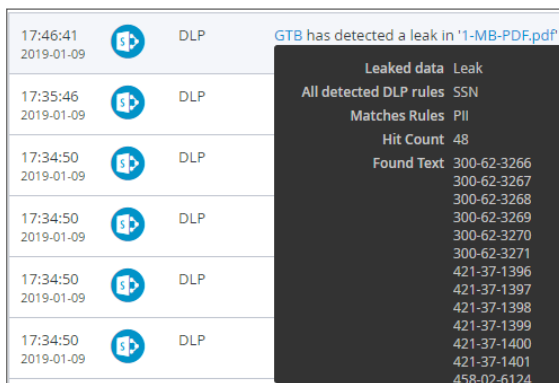
- For documents containing possible malware, see information about the file and the rules that detected it:



- For websites containing possible malware, see the information about the website and the action taken:



- For a data leak, see the information found and its possible type:



Clicking on the security event item itself will display it on the Events page, with the selected security event highlighted. (See Managing Security Events for more information.)

You can also select which security events are displayed by selecting a value from the list in the top right of the Security Events list.

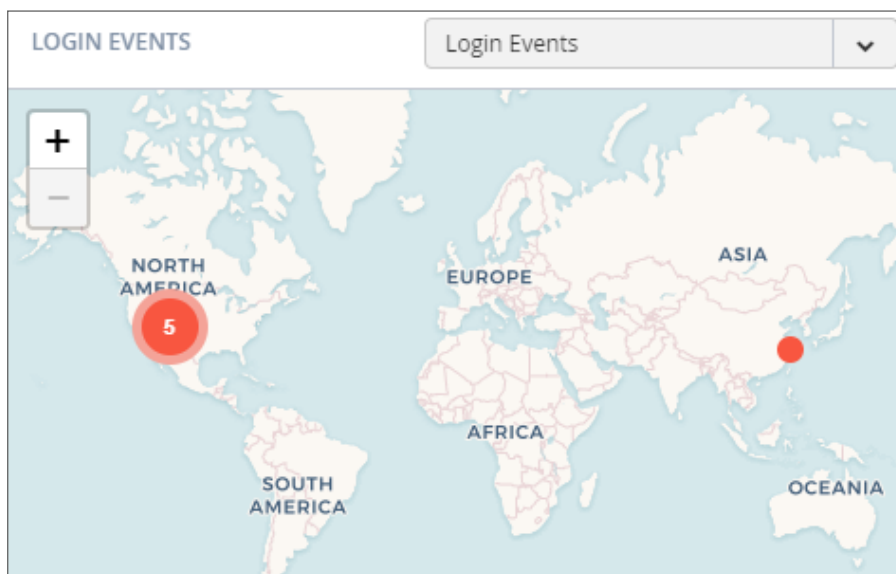
TIME	SAAS	TYPE	DESCRIPTION
09:20:19 2021-02-11		DLP	SmartDLP has detected a leak in 'ENCRYPT: This is a test message for Subject Regex' (mohan@cloudwall.onmicrosoft.com)
10:40:12 2021-02-09		DLP	SmartDLP has detected a leak in 'ENCRYPT: this message dlp test of r (mohan@cloudwall.onmicrosoft.com)
10:39:46 2021-02-09		DLP	SmartDLP has detected a leak in 'ENCRYPT: this message dlp test of r (mohan@cloudwall.onmicrosoft.com)
01:45:00 2020-11-30		DLP	SmartDLP has detected a leak in 'smartDLP SIN' (mohan@cloudwall.onmicrosoft.com)
01:37:33 2020-11-30		DLP	SmartDLP has detected a leak in 'smart DLP test' (mohan@cloudwall.onmicrosoft.com)

Type ▼

- DLP
- Malware
- Phishing
- Anomaly
- Suspicious Mal...
- Suspicious Phis...
- Shadow SaaS
- Alert
- Spam

Viewing Login Events

With geo-location tracking, Login Events are globally mapped and identified using their IP address.



The color of the numerical indicator provides information about the number of occurrences from the same user logins from a specific IP address.

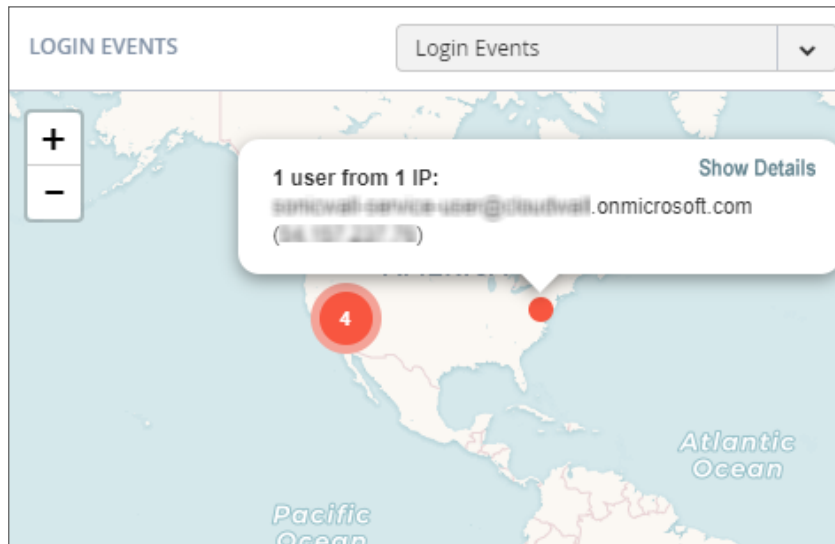
Color	Description
Blue	Many logins from a user from the same IP address
Yellow	Some logins from a user from the same IP address
Red	Few logins from a user from the same IP address

To view specific login events:

1. Click on the dropdown menu on the top right.
2. Choose the option for the login events you want to view on the map.

To view detailed information about a single login event:

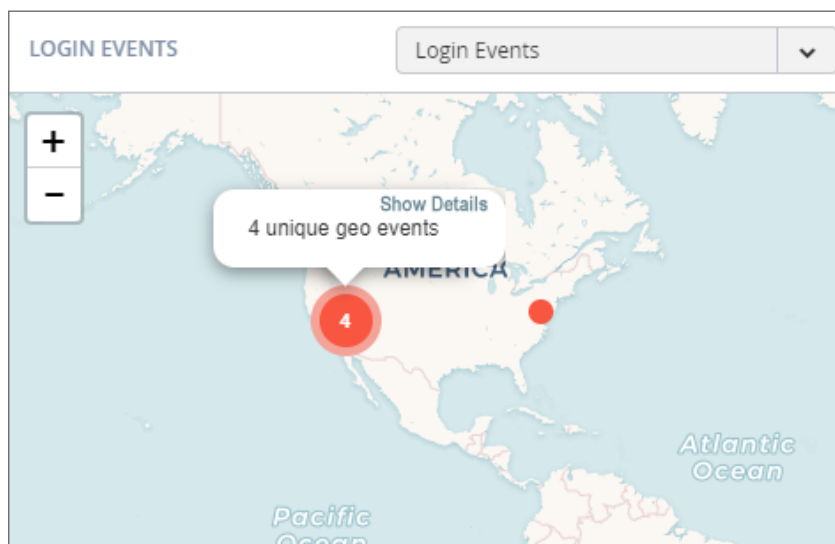
1. Hover the cursor over the login event for which you want to see more information.



2. A popup displays that contains the email and IP address of the user at that location.
3. You can click **Show Details** to view more detailed information about the login event.

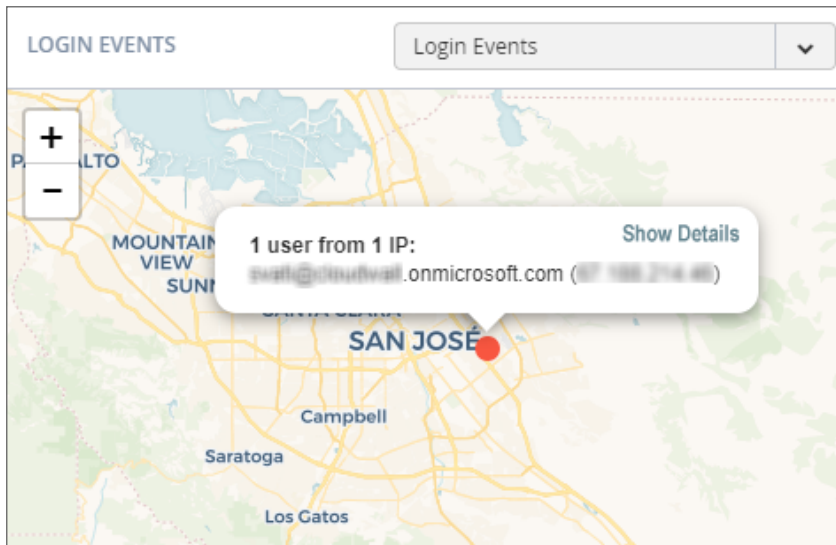
To view detailed information about multiple login events:

1. Hover the cursor over the login events for which you want to see more information (designated as a number reflecting the number of login events at that location).



2. Click on the number until you see only single login events (shown without a number).

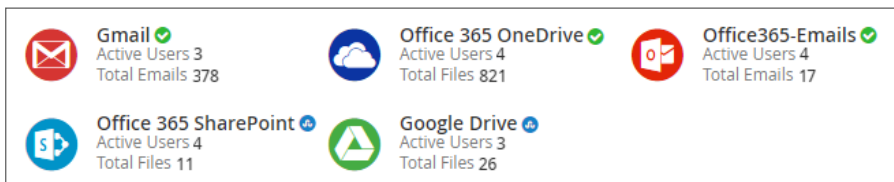
3. Hover the cursor over the specific login event for which you want to see more information.



4. You can click **Show Details** to view more detailed information about the login event.

Viewing Secured Applications

The bottom left section of the Cloud App Security Dashboard shows you the cloud applications you have currently secured with SonicWall Cloud App Security.



You can:

- click on the application icon or name to view the Analytics for that cloud application.
- click on the Active Users link to view the current users of that cloud application.
- click on the Total Files or Total Emails link to view a detailed list of files or emails processed by SonicWall Cloud App Security.

An icon indicating the current protection status of each SaaS application monitored by Cloud App Security is displayed next to the application in the bottom section of the Cloud App Security Dashboard.

Icon	Protection Status
Green	Protection on
Blue	Starting
Red	Error
Orange	Warning

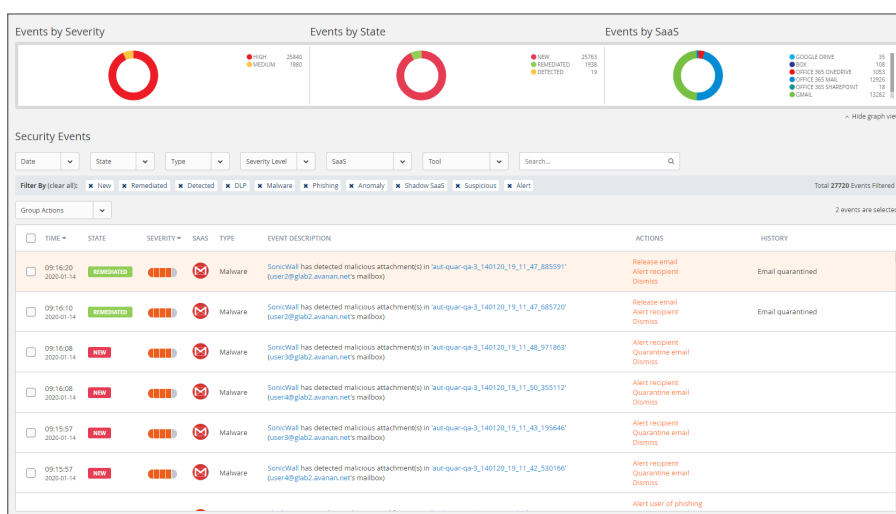
Viewing the Scanned Files Summary

The pane at the bottom right of the Cloud App Security (SaaS Security) Dashboard displays a summary of the number of files and emails scanned by SonicWall Cloud App Security. The number of threats detected is displayed in red.

✓ Anti-phishing	Scanned: 17 (no detections)
✓ DLP	Scanned: 889 (2 detected)
✓ Advanced Threat Pr...	Scanned: 882 (23 detected)

Managing Security Events

The Events page provides you with graphs showing the different classifications of the recorded security events, as well as more detailed information about each event.



Topics:

- [Using the Security Event Graphs](#)
- [Viewing and Acting on Security Events](#)
- [Managing Multiple Events](#)

Using the Security Event Graphs

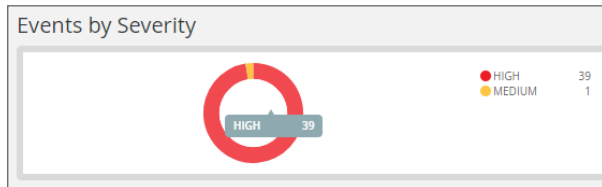
The Security Event Graphs show the security events grouped in different ways.

- [Viewing Security Events by Severity](#)
- [Viewing Security Events by State](#)
- [Viewing Security Events by Cloud Application](#)

You can hide the graphs by clicking **Hide graph view** in the lower right area under the graphs.

Viewing Security Events by Severity

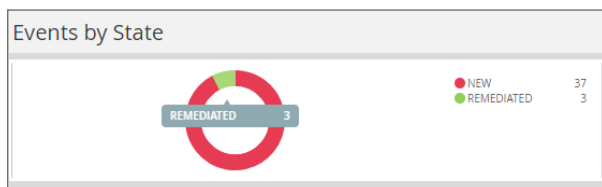
The **Events by Severity** graph displays all of the security events represented by severity.



Hover over sections of the graphics to see the detailed information about that section, including the number of security events that occurred with that severity.

Viewing Security Events by State

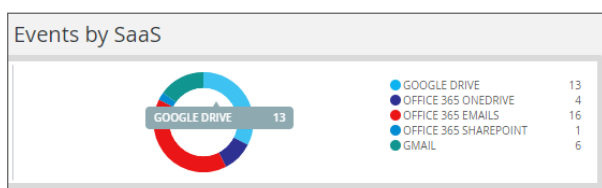
The **Events by State** graph displays all of the security events represented by their state.



Hover over sections of the graphics to see the detailed information about that section, including the number of security events with that state.

Viewing Security Events by Cloud Application

The **Events by SaaS** graph displays all of the security events represented each active cloud application.



Hover over sections of the graphics to see the detailed information about that section, including the number of security events that occurred for that cloud application.

Viewing and Acting on Security Events

The **Security Events** table lists all of the security events for your secured cloud applications. You can be filter what is displayed in this in several ways.

The screenshot shows the 'Security Events' interface. At the top, there are filter menus for Date, State, Type, Severity Level, SaaS, and Tool, along with a search bar. Below these is a 'Filter By' bar with checkboxes for various event categories: New, Remediated, Detected, DLP, Malware, Phishing, Anomaly, Shadow SaaS, Suspicious, and Alert. The total number of filtered events is 27720. A 'Group Actions' dropdown is also visible. The main table has columns for Time, State, Severity, SaaS, Type, Event Description, Actions, and History. The table contains several rows of security events, each with a checkbox, a timestamp, a state (e.g., REMEDIATED, NEW), a severity level (represented by a bar chart), a SaaS icon, a type (Malware), an event description, and a list of actions (e.g., Release email, Alert recipient, Dismiss, Quarantine email).

SECURITY EVENTS FILTERS AND DESCRIPTIONS

Security Events Filters	Description
Date	Timeframe during the security events occurred: previous 60 minutes, 24 hours, 7 days, 30 days, or 12 months.
State	State of the security events: these can be new events, remediated events, exceptions, or dismissed events.
Type	Security types: DLP, Malware, Malicious, Phishing, Anomaly, Suspicious, Shadow IT, Alert, or Spam.
Severity Level	Severity level of the security events: Critical, High, Medium, Low, or Lowest.
SaaS	All active cloud applications (Office 365 Emails, Gmail, etc.)
Tool	Tool that identified the threat (Anti-phishing, DLP, Advanced Threat Protection)
Search	Search for specific events based on the information available for the events.
Group Actions	Take action on a selection group of security events.

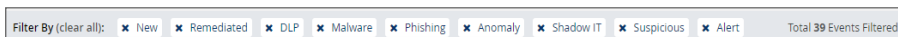
The active filters are displayed above the data listed in the table. Displayed on the far right is the total number of security events that match the filtering criteria.

Topics:

- [Removing Filters](#)
- [Acting on Security Events](#)

Removing Filters

You can remove a filter by clicking on the **x** next to it.



Acting on Security Events

Listed in the **Actions** column for an event are the actions that you can take for that event. (The available actions may vary depending on the type of event or cloud application.) These actions might include:

- Alerting the user or recipient
- Quarantining the email message or file
- Dismissing the alert
- Creating a new rule based on the event(s) for that item (refer to [Creating New Policy Rules](#) for more information)

Managing Multiple Events

If more than one Security Event is raised when processing an email message, they are listed as a single collapsed event. You can expand the item to view all of the events reported for the affected email message and perform actions (such as Quarantine) or on all of the events listed in the grouped events.

For example, if malware, DLP, and phishing alerts have all been assigned to the same email message, the email message will only be listed once, but all three of these events will be listed. You can then act on all of the events reported for the email message or only specific ones.

Managing Policies

The **Policy** page displays the policy rules that assigned to each secured cloud application.

POLICY

Policy Rules + Add a New Policy Rule

- Google Drive** + TOTAL 2 RULES / 2 RUNNING ▼
- Office 365 OneDrive** + TOTAL 2 RULES / 2 RUNNING ▼
- Office 365 Emails** + TOTAL 2 RULES / 2 RUNNING ▲

STATUS	MODE	RULE NAME	SCOPE	REMIEDIATION WORKFLOW	ORDER
RUNNING	Monitor only	Office365 Emails Threat Protection (Default)	All Users and groups		
RUNNING	Monitor only	Office365 Emails DLP (Default)	All Users and groups		
- Office 365 SharePoint** + TOTAL 2 RULES / 2 RUNNING ▼
- Gmail** + TOTAL 2 RULES / 2 RUNNING ▼

Topics:

- [Understanding Cloud App Security Policies](#)
- [Creating New Policy Rules](#)
- [Stopping Policy Rules](#)
- [Removing Policy Rules](#)
- [Managing Office 365 and Microsoft 365 \(Exchange Online\) Mail-Flow Rules](#)

Understanding Cloud App Security Policies

Cloud App Security provides these modes of protection for your organization:

- [Monitor only](#)
- [Detect and Prevent](#)
- [Protect \(Inline\)](#)

Topics:

- [Before You Set Email Policies](#)

Before You Set Email Policies

Before you can configure any group-based policies, you must specify:

- a dedicated quarantine mailbox that will be used to store any emails or attachments that are quarantined during the scanning process. For instructions on doing this, refer to [Managing Quarantine for Email](#).
- a restore request approver email account. This must be a current administrator in the Cloud App Security platform. This account will be used to notify administrators when a user has requested that an email to be released from quarantine.

Monitor only

Monitor only mode provides visibility into the cloud-hosted email and files leveraging publicly-available APIs and a journal entry from the SaaS email provider. This is the default policy mode for Cloud App Security. Monitor only mode will only report detected issues, but will take no action on them. This mode is non-intrusive.

Incoming email passes through the spam filter managed by email provider. Emails are then sorted into these categories:

- Rejected
- Accepted, Moved to Junk
- Accepted, Moved to Inbox

Manual and automated query-based quarantine policies are available after delivery of the email messages or files to the user's mailbox or cloud-based storage.

Detect and Prevent

Detect and Prevent mode provides an increased level of protection that scans email using journaling leveraging the SaaS email and storage provider APIs. Automated policy actions quarantine email messages and files that might contain such threats as malware, data leaks, and phishing attacks. User notifications and release workflows are available in this mode.

1. Incoming email or file arrives in the respective mailbox or storage folder.
2. Cloud App Security detects new that new email or file has arrived and scans it.
3. If an email message or file is classified as malicious, Cloud App Security takes action based on the policies that have been defined. Otherwise, the email or file is passed or stored unchanged to the intended recipient.
4. Optionally, the email user maybe notified of the actions taken on email messages or files sent to them.

Protect (Inline)

Protect (inline) mode provides the highest level of protection, scanning email and files prior to delivery to the user. Leveraging the SaaS email and storage provider APIs, and implementing mail flow rules, Cloud App Security can scan email and files to protect end users from such threats as malware, data leaks, and phishing attacks. Scanning and quarantining happens before email messages and files are delivered to the user, ensuring that threats are detected and remediated before the user has access to the email messages or files:

1. Incoming email and files heads to the processing flow.
2. Cloud App Security redirects the email or file to the Cloud App Security platform for scanning.
3. If an email or file is classified as malicious, Cloud App Security takes action based on the policies that have been defined. Otherwise, the email or file is returned to the proocessing flow.
4. User notifications and release workflows are performed based on defined policies.

Creating New Policy Rules

You can create policies that can be applied to all or only selected users or user groups. You can also designate that specific users or user groups be excluded from individual policies.

To create a new policy rule:

1. Click on either the:
 - **Add a New Policy Rule** button in the upper right area of the page.
 - plus sign (+) button next to the name of the cloud application.The **New Policy Rule** page displays.
2. From the **Choose SaaS** list, select the cloud application for which to apply the new rule.
3. From the **Choose Security** list, select the security service or custom query you want to use for the selected cloud application.
4. Click **Next**.
5. If you selected:
 - a. a security service:
 1. Set the options you want to use for the cloud application.
 - [Creating Data Leak Protection Policy Rules](#)
 - [Creating Malware Policy Rules](#)
 - [Creating Threat Detection Policy Rules](#)

- [Creating Policy Rules for Click-Time Protection](#)
 - [Creating Office 365 and Microsoft 365 Email Encryption Policy Rules](#)
 - [Creating Custom Query Policies](#)
2. Click **Save and Apply**.
- b. **Custom Query**, select from your custom queries or any of the available query templates. (Refer to [Creating Custom Query Policies](#) for information on how to create new policy rules based on custom queries.)

Creating Data Leak Protection Policy Rules

Data Leak Protection (DLP) helps protect your organization's data from potential data breaches or data ex-filtration transmissions. Data Leak Protection can scan emails and text messages posted on cloud application email and storage platforms, and detect data patterns that should not be shared with unauthorized persons or targets. For more information, see [Using Data Leak Protection](#).

To create a DLP policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select the mode in which you want the DLP policy rule to operate:
 - **Monitor only**
 - **Detect and Prevent** (cloud application storage only)
 - **Protect (Inline)** (email only)
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **DLP Criteria** section:
 - a. From the **DLP Rules** list, select the detection rules you want applied:
 - **PII**
 - **PHI**
 - **Financial**
 - **Encrypted Content**
 - **Access Control**
 - **Intellectual Property**
 - **PCI**
 - **Resume**
 - **SOX**
 - **HIPAA**

For more information about the predefined DLP policy rules, refer to [Predefined Data Leak Protection Policy Rules](#).

- b. From the **Sensitivity** list, select the sensitivity (based on the hit count) to be used to apply the rules.
- c. Select **Skip internal items** to have the rules not applied to items not shared with external users.

Depending on the type of cloud application and the **Mode**, you may see a different set of options in the **Advanced** section.

5. In the **Advanced > Actions** section:
 - a. Select **Send files with sensitive data to vault** to send the affected files to a secure vault location.
 - ① **NOTE:** A vault is a secure location accessible only to users with specific access privileges (such as a data privacy team). It is a different location than the quarantine area defined in your Cloud App Security cloud application configuration.
 - b. Select **Alert admin(s)** to notify administrators when a possible leak is detected.
 - Click the gears icon to modify the email message sent to administrators.
 - Click the users icon to select which administrators should receive the message.
 - c. Select **Alert file owner** to notify the user sharing the file when a possible leak is detected.
 - Click the gears icon to modify the email message sent to the file owner.
 - d. Select **Quarantine drive files** to quarantine detected files to the quarantine folder defined in your Cloud App Security configuration.
6. From the **DLP Workflow** list, select which action should be taken when a possible leak is detected:
 - **Email is blocked. User is alerted and allowed to request a restore (admin must approve)**
 - **Email is blocked. User is alerted and allowed to restore the email**
 - **Email is allowed. Header is added to the email**
 - **Email is allowed. Encrypted by Microsoft**
 - ① **NOTE:** This action is only visible and available if you subscribe to Microsoft encryption services and have encryption enabled.
 - ① **NOTE:** Encrypted Office 365 and Microsoft 365 Email support requires that you have the necessary Office 365 and Microsoft 365 or Exchange Online subscription level from Microsoft and a Cloud App Security Advanced license from SonicWall.
 - Do nothing
7. In the **Advanced > Alerts** section:
 - a. Select **Send email alert** to notify specific users when a possible leak is detected.
 - Click the gears icon to modify the email message sent to the file owner.
8. Click **Save and Apply**.

Using Regular Expressions in DLP Policies for Email

Using regular expressions, you can configure specific DLP policies to be triggered based on the content of the subject line of an email message.

Regular expression support for Data Leak Protection (DLP) requires an Advanced license for Cloud App Security.

For example:

- If the policy of your organization is to include the word "Confidential" in the subject line whenever an email with confidential data is sent outside of your organization, your DLP policy rule can instruct the sender of the email message to include the keyword "Confidential" when it was added automatically by Cloud App Security to the subject line of the email message.
- Including the keyword "ENCRYPT" in the subject line of the email message will cause it be encrypted before it is sent to the intended recipient.

① | **NOTE:** Regular expression support is only available for the subject line of email messages. It is not supported within the content of the email messages.

To configure regular expression support:

1. Navigate to **Policy**.
2. Select an existing DLP policy or create a new one.
 - ① | **NOTE:** Regular expression support for email notifications is only available for DLP policies.
3. In the **DLP Criteria** section, select **Detect Phrases in Email Subject**.
4. In the **Phrase to detect (Regular Expression)** field, enter the text or regular expression to be evaluated.
5. From the **DLP workflow** list, select **Email is allowed. Encrypted by Microsoft**.
6. In the **Alerts** section, you select:
 - **Send email alert to sender when Subject Regex is used** to have an email message sent to the sender when
 - Click the gears icon to modify the email message sent to the sender.
 - **Send email alert to sender when Subject Regex is not used** to have an email message sent to the sender when
 - Click the gears icon to modify the email message sent to the sender.
7. Click **Save and Apply**.

Creating Malware Policy Rules

To create a malware policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select the mode in which you want the DLP policy rule to operate:
 - **Monitor only**
 - **Detect and Prevent**
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **Advanced > Security Tools** section, select **All running threat detection tools** to use all of the activated **Security Tools**. (This is on by default.) If you unselect this option, you can then select which specific **Security Tools** are used.

5. In the **Advanced > Actions** section:
 - a. Select **Quarantine drive files** to quarantine detected files to the quarantine folder defined in your Cloud App Security configuration.
 - b. Select **Alert file owner of malware** to notify the user sharing the file when possible malware is detected.
 - Click the gears icon to modify the email message sent to the file owner.
 - c. Select **Alert admin(s)** to notify administrators when possible malware is detected.
 - Click the gears icon to modify the email message sent to administrators.
 - Click the users icon to select which administrators should receive the message.
6. Click **Save and Apply**.

Creating Threat Detection Policy Rules

To create a Threat Detection policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select the mode in which you want the DLP policy rule to operate:
 - **Monitor only**
 - **Detect and Prevent**
 - **Protect (Inline)**
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **Advanced** section, the workflow options you see will depend on the **Mode** set for the policy.
 - For the **Malicious attachment workflow**, you can specify that:
 - messages or files be quarantined, and the recipient is alerted and allowed to restore the email messages or files.
 - messages or files be quarantined, and the recipient is alerted and allowed to request that the email or files be restored by an administrator.
 - messages or files be quarantined, but the recipient is not alerted. However, an administrator can restore the message.
 - no action be taken on the message. The event will still be logged.
 - For the **Phishing workflow**, you can specify that:
 - messages or files be sent to the intended recipient with a warning.
 - messages or files be quarantined, and the recipient is alerted and allowed to restore the messages or files.
 - messages or files be quarantined, and the recipient is alerted and allowed to request that the messages or files be restored by an administrator.
 - messages or files be quarantined, but the recipient is not alerted. However, an

- administrator can restore the messages or files.
 - no action be taken on the messages or files. The event will still be logged.
- For the **Suspicious phishing workflow**, you can specify that:
 - messages or files be sent to the intended recipient with a warning.
The content and formatting of the warning can be customized by clicking the gear icon to the right of the list.
 - messages or files be quarantined, and the recipient is alerted and allowed to request that the messages or files be restored by an administrator.
 - messages or files be quarantined, but the recipient is not alerted. However, an administrator can restore the message.
 - no action be taken on the messages or files. The event will still be logged.
- For the **Spam workflow**, you can specify that:
 - email messages be sent to the intended recipient with “[Spam]” added to the Subject line.
 - email messages be sent to the intended recipient with “[Spam]” added to the Subject line and delivered to the Junk folder.
 - email messages be quarantined, the recipient is alerted, and the recipient can restore the email message.
 - email messages be quarantined, but the recipient is not alerted. However, an administrator can restore the email message.
 - no action be taken on the email message. The event will still be logged.
- From the **Severity** list, specify severity level with which the event will be recorded:
 - Auto
 - Critical
 - High
 - Medium
 - Low
 - Lowest

5. In the **Advanced > Security Tools** section:

- a. Select **All running threat detection tools** to use all of the activated **Security Tools**. (This is on by default.) If you unselect this option, you can then select which specific **Security Tools** are used.
- b. Click **Configure Anti-Impersonation and Phishing Confidence-Level** to configure additional anti-phishing options.
 - Select a value for the **Confidence** level field to set a default confidence level. By setting a higher confidence level, you should see fewer detections and fewer false-positive results.
 - Enable **Warn users of suspected impersonations** to warn users of suspected impersonated messages and accounts. You can set the detection level to all internal users or only senior-level users within your organization.
 - Select **Allow end users to Allowed list senders they trust via in-mail link** to allow your end users to add senders they trust to the Allowed list using a link provided in the email message.
 - Select **Allow list emails with MSFT SCL = -1** to automatically allow emails that Microsoft marks as allowed by placing `SCL=-1` in the header of the email message.

For more information about configuring the anti-impersonation options, refer to [Managing Nickname Impersonation](#).

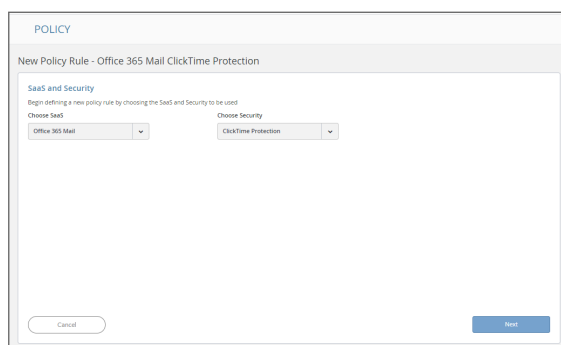
- c. Click **Ok**.
6. In the **Advanced > Alerts** section:
 - a. Select **Send email alert to admin(s) about phishing** to notify administrators when a possible leak is detected.
 - Click the gears icon to modify the email message sent to administrators.
 - Click the users icon to select which administrators should receive the message.
 - b. Select **Send Email alert to...** to notify specific users sharing the file when a possible threat is detected.
 - Click the gears icon to modify the email message sent to the users.
 - c. Select **Send email alert to admin(s) about malware** to notify administrators when a possible threat is detected.
 - Click the gears icon to modify the email message sent to administrators.
 - Click the users icon to select which administrators should receive the message.
 - d. Select **Alert recipient** to inform the recipient of the message when a possible threat is detected.
 - Click the gears icon to modify the email message sent to the recipient.
7. Click **Save and Apply**.

Creating Policy Rules for Click-Time Protection

After you have activated and configured Click-Time Protection (refer to [Activating Click-Time Protection](#) and [Configuring Click-Time Protection](#) for more information), you will need to create new policy rules that use this feature.

To create a policy rule for Click-Time Protection:

1. Navigate to **Policy**.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** list, select the email application for which you want to create the new policy rule.



4. From the **Choose Security** list, select **Click-Time Protection**.
5. Click **Next**.

6. The **Mode** will automatically be set to **Protect (inline)**. **NOTE:** This value cannot be changed.
7. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
8. Click **Save and Apply**.

Refer to [Managing Policies](#) for more information about managing policies for Cloud App Security.

Creating Office 365 and Microsoft 365 Email Encryption Policy Rules

To create an Office 365 email encryption policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select **Protect (inline)**.
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **DLP Criteria** section:
 - a. From the **DLP Rules** list, select the rules you want applied.
 - b. From the **Sensitivity** list, select the sensitivity (based on the hit count) to be used to apply the rules.
- ① **NOTE:** Depending on the type of cloud application and the **Mode**, you may see a different set of options in the **Advanced** sections.
5. From the **DLP Workflow** list, select which action should be taken when a possible leak is detected:
 - **Email is blocked. User is alerted and allowed to request a restore (admin must approve)**
 - **Email is blocked. User is alerted and allowed to restore the email**
 - **Email is blocked and user can request to resend as encrypted (admin must approve)**
 - **Email is blocked and user can request to resend as encrypted**
 - **Email is allowed. Header is added to the email**
 - **Email is allowed. Encrypted by Microsoft**
 - **Do nothing**
- ① **NOTE:** Action requiring encryption are only visible and available if you subscribe to Microsoft encryption services and have encryption enabled. Encrypted Office 365 and Microsoft 365 Email support requires that you have the necessary Office 365 and Microsoft 365 or Exchange Online subscription level from Microsoft and a Cloud App Security Advanced license from SonicWall.
6. In the **Advanced > Alerts** section:
 - a. Select **Send email alert** to notify specific users when a possible leak is detected.
 - b. Click the gears icon if you want to modify the email message sent to the file owner.

7. Click **Save and Apply**.

For more information about creating policy rules, refer to [Creating New Policy Rules](#).

Creating Custom Query Policies

To create a Custom Query policy:

1. Click on either:
 - **Add a New Policy Rule** button in the upper right area of the page.
 - plus sign (+) button next to the name of the cloud application.The **New Policy Rule** page displays.
2. From the **Choose SaaS** list, select the cloud application for which to apply the new rule.
3. From the **Choose Security** list, select **Custom Query**.
4. Click **Next**. The **Query Create** page displays.
5. Select from the **Query Templates** or **My Queries** list the query on which you want to base your new custom query.
6. From **Query** menu, select **Save As**. The **Save as query** dialog displays.
 - a. In the **Query Name** field, enter the name for your new custom query.
 - b. In the **Query description** field, enter a description for your new custom query.
 - c. From the **Query severity** list, select the severity to be assigned to your new custom query.
 - d. In the **Query tags** field, enter any tags you want associated with your new custom query.
7. Click **Ok**.

Stopping Policy Rules

To stop a policy rule from operating:

1. Click the down arrow on the far right of the area for the cloud application for which you want to stop the policy rule from operating.
2. Click on the **Running** status. This will stop the rule. The status label will change to **Stopped**.

Removing Policy Rules

To remove a policy rule:

1. Click the down arrow on the far right of the area for the cloud application for which you want to delete the policy rule.
2. Hover over the blank area to the left of the policy status until an **X** appears.
3. Click the **X** to delete the policy rule.

Managing Office 365 and Microsoft 365 (Exchange Online) Mail-Flow Rules

The SonicWall Cloud App Security Office 365 and Microsoft 365 Mail-Flow Rules automate actions for emails-in-traffic based on custom policies. In most enterprise environments, every mail-flow rule falls under one of these categories:

- **Delivery Rule:** A mail-flow rule that modifies the delivery of the email. For example, a Delivery Rule might:
 - quarantine emails from a specified domain.
 - add emails to the Allowed list that come from a specific IP address.
 - mark emails with a specified nickname as Spam (SCL).
 - send emails to a specified connector.
 - forward emails sent to a specific email address to a different specified email address.
- **Modification Rule:** A mail-flow rule that modifies the content of the email. For example, a Modification Rule rule might:
 - add [EXTERNAL] to the subject line of an email message, if the sender of the email is from outside your organization.
 - add a disclaimer to the email body footer.

The SonicWall Cloud App Security Protect policy for Office 365 and Microsoft 365 for Exchange Online automatically creates a mail-flow rule with the name of “SonicWall - 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 SonicWall Protect Rule between the Delivery Rules and the Modification Rules.

Using Data Leak Protection

① **NOTE:** Data Leak Protection (DLP) protection is only available with Advanced licenses for SonicWallCloud App Security.

Data Leak Protection (DLP) helps protect your organization's data from potential data breaches or data ex-filtration transmissions. Data Leak Protection can scan emails and text messages posted on cloud application email and storage platforms, and detect data patterns that should not be shared with unauthorized persons or targets.

SonicWall Cloud App Security uses the SmartDLP engine to implement Data Leak Protection. The benefits of SmartDLP include:

- Fast, modern DLP solution for scanning files and images
- Many built-in DLP detection rules for many verticals and countries
- Seamless setup
- Simple, cross-platform security policies
- Simple, yet powerful actions
- Integration with other SonicWall Cloud App Security security tools

Topics:

- [Reactivating Data Leak Protection](#)
- [Configuring Data Leak Protection Detection Rules](#)
- [Creating Data Leak Protection Policy Rules](#)
- [Predefined Data Leak Protection Policy Rules](#)

Configuring Data Leak Protection Detection Rules

To configure Data Leak Protection:

1. Navigate to **Configuration > Security App Store**.
2. In the **Data Leakage Prevention** section, locate the **SmartDLP** tile.
3. If the SmartDLP security application is not currently running (as indicated by two vertical white bars in the green circle on the top left of the tile), [activate the SmartDLP security application](#).
4. Click **Configure**. The **Configure SmartDLP** dialog displays.

5. From the **Detected Text Storage Mode** list, select what scanned data will be saved and how:
 - **Store detected text strings:** Detected data is saved and can be displayed on the security events for the forensic process.
 - **Obfuscate detected text prior to storage:** Detected data is saved and displayed in obfuscated format on the security events. The original data is discarded and cannot be accessed.
 - **Do not store detected text:** No detected data is saved or displayed on the security events.
6. From the **Minimal Likelihood** list, select one of the options:
 - **Very Unlikely:** It is very unlikely that the data matches the given information type.
 - **Unlikely:** It is unlikely that the data matches the given information type.
 - **Possible:** It is possible that the data matches the given information type.
 - **Likely:** It is likely that the data matches the given information type. It may also depend on the context of the information.
 - **Very Likely:** It is very likely that the data matches the given information type. It may also depend on the context of the information.

The **Minimal Likelihood** is determined by the number of matching elements a result contains. SmartDLP uses a bucketized representation of likelihood intended to indicate how likely it is that the data matches the specified DLP detection rules.

7. In the **Detection Types** section, select which predefined DLP rules are you want included for each of the DLP detection categories:
 - **PII**
 - **PHI**
 - **Financial**
 - **Encrypted Content**
 - **Access Control**
 - **Intellectual Property**
 - **PCI**
 - **Resume**
 - **SOX**
 - **HIPAA**

8. Click **Ok** to save your SmartDLP configuration settings.

Creating Data Leak Protection Policy Rules

Data Leak Protection (DLP) helps protect your organization's data from potential data breaches or data ex-filtration transmissions. Data Leak Protection can scan emails and text messages posted on cloud application email and storage platforms, and detect data patterns that should not be shared with unauthorized persons or targets. For more information, see [Using Data Leak Protection](#).

To create a DLP policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select the mode in which you want the DLP policy rule to operate:
 - **Monitor only**
 - **Detect and Prevent** (cloud application storage only)
 - **Protect (Inline)** (email only)
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **DLP Criteria** section:
 - a. From the **DLP Rules** list, select the detection rules you want applied:
 - **PII**
 - **PHI**
 - **Financial**
 - **Encrypted Content**
 - **Access Control**
 - **Intellectual Property**
 - **PCI**
 - **Resume**
 - **SOX**
 - **HIPAA**

For more information about the predefined DLP policy rules, refer to [Predefined Data Leak Protection Policy Rules](#).

- b. From the **Sensitivity** list, select the sensitivity (based on the hit count) to be used to apply the rules.
- c. Select **Skip internal items** to have the rules not applied to items not shared with external users.

Depending on the type of cloud application and the **Mode**, you may see a different set of options in the **Advanced** section.

5. In the **Advanced > Actions** section:
 - a. Select **Send files with sensitive data to vault** to send the affected files to a secure vault location.
 - ① **NOTE:** A vault is a secure location accessible only to users with specific access privileges (such as a data privacy team). It is a different location than the quarantine area defined in your Cloud App Security cloud application configuration.
 - b. Select **Alert admin(s)** to notify administrators when a possible leak is detected.
 - Click the gears icon to modify the email message sent to administrators.
 - Click the users icon to select which administrators should receive the message.
 - c. Select **Alert file owner** to notify the user sharing the file when a possible leak is detected.
 - Click the gears icon to modify the email message sent to the file owner.
 - d. Select **Quarantine drive files** to quarantine detected files to the quarantine folder defined in your Cloud App Security configuration.

6. From the **DLP Workflow** list, select which action should be taken when a possible leak is detected:
 - **Email is blocked. User is alerted and allowed to request a restore (admin must approve)**
 - **Email is blocked. User is alerted and allowed to restore the email**
 - **Email is allowed. Header is added to the email**
 - **Email is allowed. Encrypted by Microsoft**
 - ① **NOTE:** This action is only visible and available if you subscribe to Microsoft encryption services and have encryption enabled.
 - ① **NOTE:** Encrypted Office 365 and Microsoft 365 Email support requires that you have the necessary Office 365 and Microsoft 365 or Exchange Online subscription level from Microsoft and a Cloud App Security Advanced license from SonicWall.

For more information about using Encrypted Office 365 and Microsoft 365 Email support with Cloud App Security, refer to [Working with Office 365 and Microsoft 365 Email Encryption](#).

- Do nothing
7. In the **Advanced > Alerts** section:
 - a. Select **Send email alert** to notify specific users when a possible leak is detected.
 - Click the gears icon to modify the email message sent to the file owner.
8. Click **Save and Apply**.

Reactivating Data Leak Protection

Data Leak Protection is enabled by default when you activate Cloud App Security. If the Data Leak Protection security application has been paused or disabled, it can be restarted again.

To reactivate Data Leak Protection:

1. Navigate to **Configuration > Security App Store**.
2. In the **Data Leakage Prevention** section, locate the **SmartDLP** tile.
3. Start the SmartDLP security application by clicking the white arrow in green circle on the top left of the tile.
 - ① **NOTE:** If two vertical white bars are visible in the green circle on the top left of the SmartDLP tile, then the SmartDLP security application is already currently running and does not need to be restarted.

Predefined Data Leak Protection Policy Rules

SmartDLP provides many predefined policy rules for processing email messages and files for Data Leak Protection, including:

- [Global Rules](#)
- [Credentials and Secrets](#)

SmartDLP also provides many predefined Data Leak Protection policy rules for many [specific countries and regions](#).

Global Rules

Rule	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 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.
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 IBAN Asia IBAN Africa 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. The European Committee for Banking Standards (ECBS) created ISO 13616:2007. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number.
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.

Rule	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.
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.
Organization name	A name of a chain store, business or organization.
Passport Number	A passport number that matches passport numbers for the following countries: Australia, Canada, China, France, Germany, Japan, Korea, Mexico, The Netherlands, Poland, Singapore, Spain, Sweden, Taiwan, United Kingdom, and the United States.
Patient information	Detects leaked medical patient information, based on matching health codes and other personal information patterns.

Rule	Description
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, e.g. 9:54 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.

Credentials and Secrets

Rule name	Description
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.
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.

Predefined Data Leak Protection Rules for Specific Countries

SmartDLP also provides many predefined Data Leak Protection policy rules for many specific countries and regions, including:

- Argentina
- Australia
- Belgium
- Brazil
- Canada
- Chile
- China
- Columbia
- Denmark
- Finland
- France
- Germany
- Hong Kong
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Korea
- Mexico
- The Netherlands
- Norway
- Paraguay
- Peru
- Poland
- Portugal
- Singapore
- Spain
- Sweden
- Taiwan
- Thailand
- Turkey
- United Kingdom
- United States
- Uruguay
- Venezuela

Argentina

Rule 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

Rule name	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

Rule name	Description
Belgium National Identity card number	A 12-digit Belgian national identity card number.

Brazil

Rule 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

Rule 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

Rule 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

Rule name	Description
China resident number	A Chinese resident identification number.
China passport number	A Chinese passport number.

Columbia

Rule 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

Rule 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.

Finland

Rule 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.

France

Rule 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.

Germany

Rule 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.
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

Rule 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

Rule 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

Rule 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

Rule 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.

Rule name	Description
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

Rule 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

Rule 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

Rule 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

Rule name	Description
Korea passport number	A Korean passport number.
Korea resident registration number	A South Korean Social Security number.

Mexico

Rule 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

Rule 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

Rule 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

Rule 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

Rule 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

Rule 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

Rule 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

Rule 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

Rule 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.

Rule name	Description
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

Rule 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

Rule name	Description
Taiwan passport number	A Taiwanese passport number.

Thailand

Rule name	Description
Thai national identification card number	The Thai บัตรประจำตัวประชาชนไทย, or identity card, is used as the main identity document for Thai nationals.

Turkey

Rule name	Description
Turkish identification number	A unique Turkish personal identification number, assigned to every citizen of Turkey.

United Kingdom

Rule 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.
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

Rule 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.
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.

Rule name	Description
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 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).
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

Rule 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

Rule 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.

Managing Spam and Anti-Phishing

Cloud App Security offers protection that can:

- block spam and junk email messages
- detect and prevent phishing attempts

Topics:

- [Managing Spam](#)
- [Managing User-Reported Phishing](#)
- [Customizing Warning Messages](#)
- [Managing Nickname Impersonation](#)
- [Managing the Anti-Phishing Exceptions](#)

Managing Spam

Cloud App Security offers protection that can block spam and junk email messages, preventing them from filling up the inboxes of your users.

Options to manage spam are available when you create threat detection policies. (Refer to [Creating Threat Detection Policy Rules](#) for detailed information about all of the available policy rule options.)

To configure spam management of email messages:

1. From the **Mode** dropdown list, select the mode in which you want the DLP policy rule to operate:
 - [Detect and Prevent](#)
 - [Protect \(Inline\)](#)
2. In the policy rule, navigate to the **Advanced** section.
3. From the **Spam workflow** list, select one of these options:
 - **Do Nothing:** no action be taken on the email message. The event will still be logged
 - **Add [Spam] to subject:** email messages be sent to the intended recipient with “[Spam]” added to the Subject line.
 - **Quarantine. User is alerted and allowed to restore the email:** email messages be quarantined, the recipient is alerted, and the recipient can restore the email message.
 - **Quarantine. User is not alerted (admin can restore):** email messages be quarantined, but the recipient is not alerted. However, an administrator can restore the email message.

4. Set any other options that you want to apply for the policy. (Refer to [Creating Threat Detection Policy Rules](#) for detailed information about all of the available policy rule options.)
5. Click **Save and Apply**.

Managing User-Reported Phishing

Email users in your organization are an important element in detecting and combating phishing attempts. Users can help identify undetected phishing attempts, allowing your administrators to block the those attacks as well as be prepared for future similar phishing attempts.

Users using Outlook can identify email messages as phishing attempts from within the application by choosing **Mark as Phishing**. Doing this notifies Microsoft of the suspected phishing attempt and Cloud App Security can capture those email messages and report them as suspected phishing attempts. Administrators can then quarantine the message, create a block list rule based on the email message, or disregard the report.

To enable user-reported phishing:

1. Make certain that **Anti-phishing** is running and enabled. (Refer to [Starting Security Applications](#) for more information.)
2. Options to manage user-reported phishing are available when you create threat detection policies. (Refer to [Creating Threat Detection Policy Rules](#) for detailed information about all of the available policy rule options.)

In the **Advanced** section, under **Security Tools**, click **Configure Anti-Impersonation and Phishing Confidence-Level**.

3. For **Import Office365 emails reported by users**, select one of these options:
 - **Create an "Alert" event**
 - **Create a "Phishing" event**
4. Click **Ok**.

Customizing Warning Messages

You can custom the warning message displayed for users when potential threats are detected for these workflows:

- Malicious attachment workflow
- Phishing workflow
- Suspicious phishing workflow

To customize the content and formatting of a warning message:

1. Create or edit a **Threat Detection** policy rule. (Refer to [Creating Threat Detection Policy Rules](#) for more information.)
2. Click the **Advanced** section to expand and view it.

3. Click the gear icon to the right of the workflow for which you want to customize the message.
 - For the **Phishing workflow** and **Suspicious phishing workflow**: In the **Phishing alert body prefix format** field, you can edit and add HTML tags and content for the message.
 - **Malicious attachment workflow**: Edit the content in the **Quarantine notification subject** and **Quarantine notification body fields**.
4. Click **Ok**.

Managing Nickname Impersonation

Nickname impersonation (also known as "executive spoofing") can occur when the names or email addresses of company executives are spoofed in an effort to get internal employees to disclose sensitive professional or personal information. By default, Cloud App Security automatically detects nickname impersonations for any internal user, disabled and deleted accounts, and self-impersonation. Settings can be customized based on the needs of your organization with administrator-configured actions.

To configure Cloud App Security to detect and manage nickname impersonation attempts:

1. Make certain that **Anti-phishing** is running and enabled. (Refer to [Starting Security Applications](#) for more information.)
2. Options to manage nickname impersonation are available when you create threat detection policies. (Refer to [Creating Threat Detection Policy Rules](#) for detailed information about all of the available policy rule options.)

In the **Advanced** section, under **Security Tools**, click **Configure Anti-Impersonation and Phishing Confidence-Level**.
3. From the **Detect nickname impersonation attempts** from list, select one of these options:
 - **Important/key-people only**
 - **Any internal user**
4. In the **Except when coming from domains** field, enter any domains that you want to exempt from impersonation detections.
 - Domain names are not case-sensitive.
 - You can enter more than one domain name by separating them with a comma.
5. By default, the system determines who qualifies as important or key people by referencing the job titles as they are stored in the organization's Office 365 and Microsoft 365 directories.

Administrators can also select specific people to protect from nickname impersonation by adding them to a security group. In the **Important/key-people group** field, enter the security group name of people to be specifically checked for nickname impersonation.

① **IMPORTANT:** Enter the security group name, not the email address. The group name is case-sensitive.
6. For **When a nickname impersonation is detected**, select one of these options:
 - **Trigger "Phishing" workflow**
 - **Trigger "Suspicious" workflow**
7. Select **Detect impersonation attempts only from new/first-time sender** to limit nickname impersonation detection only to never-seen-before email addresses.

- ① | **NOTE:** While limiting nickname impersonation protection, selecting this option greatly reduces false positive results.
8. Select **Detect impersonation to disabled accounts** to activate nickname impersonation detection for email accounts that are disabled.
 9. Select **Detect impersonation to deleted accounts** to activate nickname impersonation detection for email accounts that are deleted.
 10. By default impersonation detection algorithm ignores email messages that are sent from the same name as the receiver, as these email message are very unlikely to be real nickname impersonation. Select **Include suspected self-impersonation in impersonation-detection algorithm** to detect as nickname impersonation email messages that have the same email address for both the sender and the recipient.

① | **NOTE:** Enabling this option often results in increased false positives.
 11. Click **Ok**.
- ① | **TIP:** To avoid false positive detections, it is recommended that you begin with a small group of senior-level people (**Important/key-people only**). If you want to configure nickname impersonation detection for all internal users (**Any internal user**), it is best to select **Trigger "Suspicious" workflow**.
- ① | **TIP:** Protected users should be advised to not use their personal email addresses, as these will be detected as impersonations.

Managing the Anti-Phishing Exceptions

You can use the **Anti-Phishing Allow-List** and **Anti-Phishing Block-List** pages to add and remove exceptions to your anti-phishing rules.

Topics:

- [Managing Excluded Email Addresses](#)
- [Managing Excluded IP Addresses](#)
- [Managing Excluded Domains](#)
- [Creating Block-List Rules from Email Messages](#)
- [Managing the Anti-Phishing Allow-List](#)
- [Managing the Anti-Phishing Block-List](#)

Managing Excluded Email Addresses

You can prevent specific email addresses from being classified as phishing.

- ① | **NOTE:** Under some configurations, email messages that contain your Junk Summary reports may be identified as phishing. If that occurs, you can create a rule that prevents the email messages that contain those reports from being classified as phishing.

Click the icon to the right of the **Add emails** button to view additional columns in the **Excluded Emails** list.

Topics:

- [Adding Email Addresses to the Anti-Phishing Block-List](#)
- [Removing Email Addresses from the Anti-Phishing Block-List](#)

Adding Email Addresses to the Anti-Phishing Block-List

To add an email address to the Anti-Phishing Blocked List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Click the **Add OutlookBlock-List Rule** button. The **Add exception** dialog displays.
3. In the **Email** field, enter the email addresses you want to add to the **Anti-Phishing Block-List**.
4. Optionally, you can enter additional information in the **Comment (optional)** field.
5. Select **Ignore SPF check** to skip Sender Policy Framework verifications for the email addresses entered.
6. Click **Ok**.

Removing Email Addresses from the Anti-Phishing Block-List

To remove an email address from the Anti-Phishing Blocked List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Select the email addresses you want to remove from the **Anti-Phishing Block-List**.
3. Click the **Remove** button.
4. When prompted, click **Ok**.

Managing Excluded IP Addresses

You can prevent specific IP addresses from being classified as phishing.

Click the icon to the right of the **Add IPs** button to view additional columns in the **Excluded IPs** list.

Topics:

- [Adding IP Addresses to the Anti-Phishing Block-List](#)
- [Removing IP Addresses from the Anti-Phishing Block-List](#)

Adding IP Addresses to the Anti-Phishing Block-List

To add an IP address to the Anti-Phishing Block-List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Click the **Add OutlookBlock-List Rule** button. The **Add exception** dialog displays.
3. In the **IP** field, enter the IP addresses you want to add to the **Anti-Phishing Block-List**.
4. Optionally, you can enter additional information in the **Comment (optional)** field.
5. Click **Ok**.

Removing IP Addresses from the Anti-Phishing Block-List

To remove an IP address from the Anti-Phishing Block-List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Select the IP addresses you want to remove from the **Anti-Phishing Block-List**.
3. Click the **Remove** button.
4. When prompted, click **Ok**.

Managing Excluded Domains

You can prevent specific domains from being classified as phishing.

Click the icon to the right of the **Add Domains** button to view additional columns in the **Excluded Domains** list.

Topics:

- [Adding Domains to the Anti-Phishing Block-List](#)
- [Removing Domains from the Anti-Phishing Block-List](#)

Adding Domains to the Anti-Phishing Block-List

To add a domain to the Anti-Phishing Block-List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Click the **Add OutlookBlock-List Rule** button. The **Add exception** dialog displays.
3. In the **Domain** field, enter the domains you want to add to the **Anti-Phishing Block-List**.
4. Optionally, you can enter additional information in the **Comment (optional)** field.
5. Select **Ignore SPF check** to skip Sender Policy Framework verifications for the domains entered.
6. Click **Ok**.

Removing Domains from the Anti-Phishing Block-List

To remove a domain from the Anti-Phishing Block-List:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Select the domains you want to remove from the **Anti-Phishing Block-List**.
3. Click the **Remove** button.
4. When prompted, click **Ok**.

Creating Block-List Rules from Email Messages

You can create blocked list rules directly from the description of an email messages captured as a security event.

To create a blocked list rule from an email message:

1. Navigate to either the **Dashboard** or **Events** page.
2. Click on the link for the email message from which you want to create a blocked list rule.
3. Under the **Security Stack** section, in the **Anti Phishing** block, click **Create Blocked-List rule**. The **Mark emails as clean** dialog displays.
4. Select the fields and associated values you want assigned to the new blocked list rule. The list at the bottom of the dialog will dynamically update to display all of the messages that would be affected by the settings in your new blocked list rule.
5. Click **Create blocked list rule**.

Managing the Anti-Phishing Allow-List

The **Anti-Phishing Allow-List** displays the information about email addresses that have been identified as safe senders (based on email address, IP address, or domain) to your organization.

Topics:

- [Creating Anti-Phishing Allow-List Rules from the Security Events Page](#)
- [Creating Anti-Phishing Allow-List Rules from the Anti-Phishing Allow-List Page](#)

Creating Anti-Phishing Allow-List Rules from the Security Events Page

To create an Anti-Phishing Allow-List rule from the Security Events page:

1. Navigate to **Events > Security Events**.
2. In the **Actions** column for the item from which you want to create an allowed list rule, click **Create Allow-List Rule**. The **Mark emails as clean** dialog displays.

Mark emails as clean ✕

The selected emails as well as any future emails that meet all of the criteria below will be handled as clean-emails

Sender IP (SMTP)
 Sender Email

Sender Name
 Sender Domain

757 matching emails detected

RECEIVED	RECIPIENTS	SENDER IP (SMTP)	SENDER EMAIL	SENDER NAME
Tue, 14 Jan 2020 22:15:59 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:15:49 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:12:05 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:54 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:54 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:53 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:53 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:51 GMT	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020	user@ghs2.avtest...	196.2.135.21	automation@avtest...	automation@avtest...

3. Select the options in the four checkboxes on which you want to base the new allowed list rule.
4. Click **Create exception**.

Creating Anti-Phishing Allow-List Rules from the Anti-Phishing Allow-List Page

To create an Anti-Phishing Allow-List rule from the Anti-Phishing Allow-List page:

1. Navigate to **Configuration > Anti-Phishing Allow-List**.
2. Click **Create Allow-List Rule** in the upper right. The **Create Allow-List Rule** dialog displays.

Create Allow-list Rule ✕

Emails:

IPs:

Domains:

Nicknames:

Comment (optional):

Ignore SPF check
 Dismiss all relevant security events

3. In the **Emails** field, enter the email addresses you want to add to the **Anti-Phishing Allow-List**.

4. In the **IPs** field, enter the IP addresses you want to add to the **Anti-Phishing Allow-List**.
5. In the **Domains** field, enter the domains you want to add to the **Anti-Phishing Allow-List**.
6. In the **Nickname** field, enter the email nickname(s) you want to add to the **Anti-Phishing Allow-List**.
7. Optionally, you can enter additional information in the **Comment (optional)** field.
8. Select **Ignore SPF check** to skip Sender Policy Framework verifications for the domains entered.
9. Click **Dismiss all relevant security events** to clear all of the security events previously detected based on the criteria specified here.
10. Click **Ok**.

Managing the Anti-Phishing Block-List

The **Anti-Phishing Block-List** displays the information about email addresses that have been identified as phishing threats and blocked from your organization.

To remove an email address from the Excluded Emails Per Owner list:

1. Navigate to **Configuration > Anti-Phishing Block-List**.
2. Select the email address you want to remove from the **Anti-Phishing Block-List**.
3. Click the **Remove** button.
4. When prompted, click **Ok**.

You can also add items to the **Anti-Phishing Block-List** from the email message description using the [Using the Mail Explorer](#).

Using the Mail Explorer

The screenshot shows the Mail Explorer interface with the following search criteria:

- From (exact): 2020-01-01 13:38:42
- To: 2020-01-13 13:38:42
- Subject: (empty)
- Sender Name: (empty)
- Sender IP (SMTP) (exact): (empty)
- Sender IP (Client) (exact): (empty)
- Sender Email: (empty)
- Sender Domain (exact): (empty)

Buttons: Search, Quarantine, Blacklist

0 emails selected | 6748 matching emails detected

<input type="checkbox"/>	SUBJECT	SENDER NAME	SENDER IP (SMTP) (EXACT)	SENDER IP (CLIENT) (EXACT)	SENDER EMAIL	RECIPIENTS	RECEIVED
<input type="checkbox"/>	aut-clean-pdf-ga-3_130120_23_17_11_041760		198.2.154.21	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:17:14 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-clean-ga-3_130120_23_16_47_408714		198.2.187.11	0.0.0.0	web_blacklist@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:16:49 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-quer-ga-3_130120_23_11_34_569106		198.2.187.11	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:59 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-quer-ga-3_130120_23_11_36_227603		198.2.187.11	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:39 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-spam-ga-3_130120_23_11_36_833148		198.2.128.3	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:39 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-quer-ga-3_130120_23_11_33_343149		198.2.154.21	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:38 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-phish-ga-3_130120_23_11_35_797116		198.2.187.11	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:38 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-susp-ga-3_130120_23_11_36_437018		198.2.154.21	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:37 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-susp-ga-3_130120_23_11_34_101577		198.2.187.11	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:37 GMT-0800 (Pacific Standard Time)
<input type="checkbox"/>	aut-spam-ga-3_130120_23_11_35_380478		198.2.154.21	0.0.0.0	Automation@bentigo.com	user@bentigo.com	Mon Jan 13 2020 13:11:37 GMT-0800 (Pacific Standard Time)

Per page: 20 | 50 | First | Previous | 1 | 2 | 3 | 4 | 5 | ... | 175 | Next | Page: 1 | jump

Use the Mail Explorer to display email messages based on these search criteria:

- Date range (From through To)
- Subject
- Sender Name
- Sender IP address (SMTP)
- Sender IP address (Client)
- Sender email address
- Sender domain

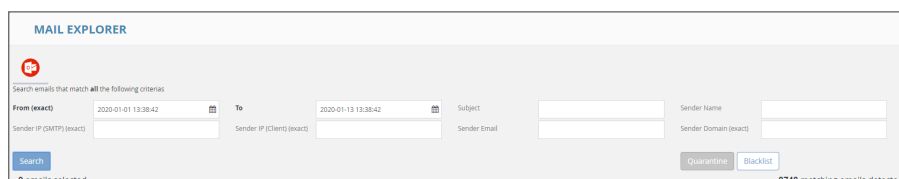
Administrators may quarantine or add affected email messages to the Blocked list.

Topics:

- [Using the Mail Explorer to Search Emails](#)
- [Using the Mail Explorer to Quarantine Items](#)
- [Using the Mail Explorer to Add Items to the Blocked List](#)

Using the Mail Explorer to Search Emails

Use the search capabilities of the Mail Explorer to locate and manage email messages that fit a specified criteria.



MAIL EXPLORER

Search emails that match all the following criterias

From (exact) 2020-01-01 13:38:42 To 2020-01-13 13:38:42 Subject

Sender IP (SMTP) (exact) Sender IP (Client) (exact) Sender Email Sender Name Sender Domain (exact)

Search Quarantine Blacklist

0 emails selected 8748 matching emails detected

You can search for email messages based on these criteria:

- Date range (From through To)
- Subject
- Sender Name
- Sender IP address (SMTP)
- Sender IP address (Client)
- Sender email address
- Sender domain

To search for email messages based on specific criteria:

1. Navigate to **Mail Explorer**.
2. Enter the values in the fields provided to set the criteria.
3. Click **Search**.

After the results are displayed, you can select either specific or all email messages and then either quarantine them or add them to the **Antiphishing Block-List**.

Using the Mail Explorer to Quarantine Items

You can quarantine email messages using the Mail Explorer.

To quarantine email messages:

1. Navigate to **Mail Explorer**.
2. Enter the values in the fields provided to set the criteria.
3. Click **Search**.
4. Select either the email messages that you want to quarantine.
5. Click **Quarantine**.
6. When prompted, click **Quarantine**.

Using the Mail Explorer to Add Items to the Blocked List

You can use the Mail Explorer to add items directly to the Blocked List.

To add email messages to the Antiphishing Blocked List:

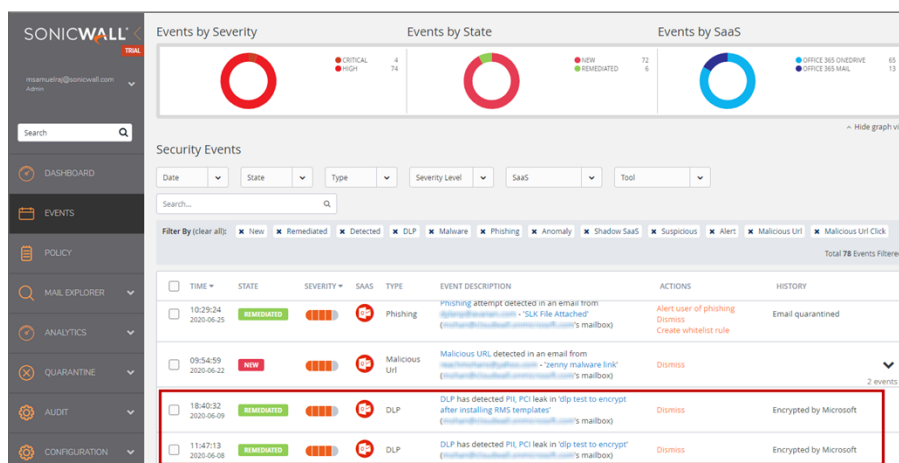
1. Navigate to **Mail Explorer**.
2. Enter the values in the fields provided to set the criteria.
3. Click **Search**.
4. Select either the email messages on which you want to create a new blocked list rule.
5. Click **Blocked list**.
6. Select **Do not include existing emails** if you do not want the new blocked list rule to be applied to existing email messages.
7. When prompted, click **Create Blocked List Rule**.

Working with Office 365 and Microsoft 365 Email Encryption

- ① **IMPORTANT:** Encrypted Office 365 and Microsoft 365 Email support requires that you have the necessary Office 365 and Microsoft 365 or Exchange Online subscription level from Microsoft and a Cloud App Security Advanced license from SonicWall. Verify that your Microsoft subscription type and any Microsoft add-on packages you have purchased include Microsoft encryption services.

Office 365 and Microsoft 365 Email Encryption encrypts email messages regardless of their destination email addresses (Gmail, Yahoo Mail, Outlook.com, etc.) using Right Management templates. Instead of an email message, a link to the email message is sent to the recipient. The encrypted email messages can be viewed after the recipient provides proper authentication.

Cloud App Security Data Leak Protection (DLP) policies for Office 365 and Microsoft 365 Email (Exchange Online) include an automated workflow that allows email messages that violate an enabled Cloud App Security DLP policy to be encrypted before being sent using the existing Office 365 and Microsoft 365 Encryption services.



Cloud App Security integrated with Office 365 and Microsoft 365 Email Encryption by:

- allowing you to create workflow rules when you create DLP email message policies to automatically encrypt Office 365 and Microsoft 365 email messages (refer to [Creating Data Leak Protection Policy Rules](#) for more information about creating DLP policies)
- intercepting email messages in **Protect (inline)** mode and evaluating them against your DLP policy rules

- encrypting email messages that match the DLP policy rules using the “Email is allowed. Encrypted by Microsoft” workflow

Topics:

- [Creating Office 365 and Microsoft 365 Email Encryption Policy Rules](#)

Creating Office 365 and Microsoft 365 Email Encryption Policy Rules

To create an Office 365 email encryption policy rule:

1. In the **Rule Name** field, enter the name you want to use to identify the rule.
2. From the **Mode** dropdown list, select **Protect (inline)**.
3. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
4. In the **DLP Criteria** section:
 - a. From the **DLP Rules** list, select the rules you want applied.
 - b. From the **Sensitivity** list, select the sensitivity (based on the hit count) to be used to apply the rules.

① **NOTE:** Depending on the type of cloud application and the **Mode**, you may see a different set of options in the **Advanced** sections.
5. From the **DLP Workflow** list, select which action should be taken when a possible leak is detected:
 - **Email is blocked. User is alerted and allowed to request a restore (admin must approve)**
 - **Email is blocked. User is alerted and allowed to restore the email**
 - **Email is blocked and user can request to resend as encrypted (admin must approve)**
 - **Email is blocked and user can request to resend as encrypted**
 - **Email is allowed. Header is added to the email**
 - **Email is allowed. Encrypted by Microsoft**
 - **Do nothing**

① **NOTE:** Action requiring encryption are only visible and available if you subscribe to Microsoft encryption services and have encryption enabled. Encrypted Office 365 and Microsoft 365 Email support requires that you have the necessary Office 365 and Microsoft 365 or Exchange Online subscription level from Microsoft and a Cloud App Security Advanced license from SonicWall.
6. In the **Advanced > Alerts** section:
 - a. Select **Send email alert** to notify specific users when a possible leak is detected.
 - b. Click the gears icon if you want to modify the email message sent to the file owner.
7. Click **Save and Apply**.

For more information about creating policy rules, refer to [Creating New Policy Rules](#).

Configuring and Using Click-Time Protection

Cloud App Security offers anti-phishing protection for email after it has been scanned by the cloud application email servers, but before it reaches the user's inbox. In most cases, a malicious URL will be blocked before it is even seen by the user.

New attacks, however, use compromised servers that appear benign until after the message has been delivered. Click-time Protection checks a URL each time the user clicks on a link, blocking access to the website should it be identified as malicious.

Topics:

- [Understanding Click-Time Protection](#)
- [Activating Click-Time Protection](#)
- [Configuring Click-Time Protection](#)
- [Using Click-Time Protection](#)

Understanding Click-Time Protection

Click-Time Protection (CTP) is based on URL "rewrites". Every link within the subject and body of incoming email messages is replaced with an Cloud App Security-generated URL. When the user clicks on the link, Cloud App Security tests the site before redirecting the user to that website.

Click-Time Protection provides

- Another layer of post-delivery protection
- Enhanced protection for zero-day attacks, as URLs can later become malicious
- Forensics

Click-time Protection provides these options for how malicious websites can be handled :

- Do nothing and allow users to go through to the site
- Completely prevent users from visiting the site
- Display a warning to users with the option to continue to the site

Once enabled, all links contained in the subject or content of an incoming email message are replaced with an SonicWall link. When the user clicks on the link, it triggers an immediate scan of the target website.

- If the website is determined to be benign, the user continues without interruption.
- If the website is determined to be malicious, the user is forwarded to a warning page.



Each stage of the Click-time Protection process is recorded for forensic and auditing purposes: from the original URL substitution event to the result of the time-of-click scan. If configured in 'warning only' mode, user clicks of the continue link are recorded.

Topics:

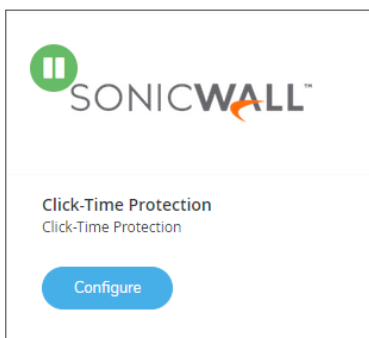
- [Configuring and Using Click-Time Protection](#)

Activating Click-Time Protection

To use Cloud App Security Click-Time Protection, you need to activate it in the **Security App Store**.

To activate *Click-Time Protection*:

1. Navigate to **Configuration > Security App Store**.
2. Scroll down to **Click-Time Protection**.



3. If Click-Time Protection is not already running (indicated by a green button with a white arrow on the upper left of the tile), click on the green button to start it.
4. When prompted, click **Start**.

For more information about using applications from the **Security App Store**, refer to [Managing Security Applications in the Security App Store](#).

Configuring Click-Time Protection

You can configure how Click-Time Protection manages links contained in incoming email messages, as well as customize for its behavior for specific domains.

Topics:

- [Configuring the Click-Time Protection Workflow](#)
- [Configuring Custom Click-Time Protection for Specific Domains](#)

Configuring the Click-Time Protection Workflow

You can configure how Click-Time Protection managed links contained in incoming email messages.

To configure the Click-Time Protection workflow:

1. Navigate to **Configuration > Security App Store**.
2. Locate the **Click-Time Protection** tile.
3. Click **Configure**.
4. From the **Click-Time Protection Workflow** list, select how you want links contained within email messages managed:
 - **Do nothing and allow the user to go through to the site**
 - **Completely prevent the user from visiting the site**
 - **Display a warning to the user with the option for them to continue to the site**Refer to [Configuring and Using Click-Time Protection](#) for more information about each of these options.
5. Click **Ok**.

Configuring Custom Click-Time Protection for Specific Domains

You can customize Click-Time Protection to handle email messages from specific domains in different ways.

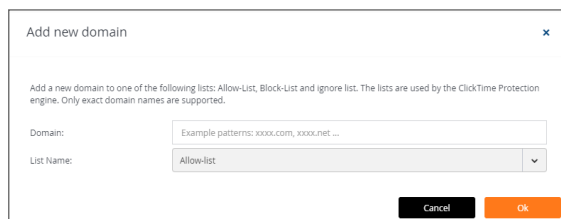
Topics:

- [Adding Custom Click-Time Protection for Specific Domains](#)
- [Deleting Custom Click-Time Protection for Specific Domains](#)

Adding Custom Click-Time Protection for Specific Domains

To add custom Click-Time Protection for specific domains:

1. Make certain that Click-Time Protection is activated. (Refer to [Activating Click-Time Protection](#) for more information.)
2. Navigate to **Configuration > Click-Time Protection Exceptions**.
3. Click **New**.
4. In the **Domain** field, enter the name of the domain from which you want to specifically manage the incoming email messages.



5. In the **List Name** field, select the list to which to assign the domain:
 - **Allow-list:** allows the user to click through to URLs in the specified domain
 - **Block-list:** always blocks URLs in the specified domain (regardless of being recognized as malicious or not)
 - **Ignore-list:** does not rewrite URLs in email messages for the specified domain
6. Click **Ok**.

Deleting Custom Click-Time Protection for Specific Domains

To delete custom Click-Time Protection for specific domains:

1. Make certain that Click-Time Protection is activated. (Refer to [Activating Click-Time Protection](#) for more information.)
2. Navigate to **Configuration > Click-Time Protection Exceptions**.
3. Select the domain for which you want to remove the custom Click-Time Protection configuration.
4. Click **Delete**.
5. When prompted for confirmation, click **Delete**.

Using Click-Time Protection

After you have [activated Click-Time Protection](#), you can create Click-Time Protection policy rules for email messages, view Click-Time Protection-related security events, and manage email messages that have been processed using Click-Time Protection.

Topics:

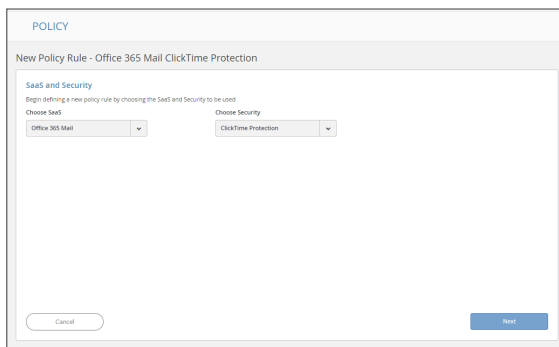
- [Creating Policy Rules for Click-Time Protection](#)
- [Viewing Security Events for Click-Time Protection](#)
- [Managing Email Messages with Click-Time Protection](#)
- [Creating Custom Queries for Click-Time Protection](#)

Creating Policy Rules for Click-Time Protection

After you have activated and configured Click-Time Protection (refer to [Activating Click-Time Protection](#) and [Configuring Click-Time Protection](#) for more information), you will need to create new policy rules that use this feature.

To create a policy rule for Click-Time Protection:

1. Navigate to **Policy**.
2. Click **Add a New Policy Rule**.
3. From the **Choose SaaS** list, select the email application for which you want to create the new policy rule.



4. From the **Choose Security** list, select **Click-Time Protection**.
5. Click **Next**.
6. The **Mode** will automatically be set to **Protect (inline)**. **NOTE:** This value cannot be changed.
7. In the **Scope** section, either:
 - Select **All users and groups (all licensed users)** to have the policy rule either apply to all users.
 - In the **Specific users and groups** list, select the specific users or user groups to which the policy should apply or be excluded from being applied.
8. Click **Save and Apply**.

Refer to [Managing Policies](#) for more information about managing policies for Cloud App Security.

Viewing Security Events for Click-Time Protection

After you have [activated Click-Time Protection](#), Click-Time Protection-related security events are reported along with other security events.

To view Click-Time Protection-related security events:

1. Navigate to **Events**.
2. In the **Security Events** list, look for security events designated with a **Type** of either **Malicious URL** or **Malicious URL Click**.
3. Once you identified Click-Time Protection-related security events, you can:
 - take action or create rules based on those events (refer to [Acting on Security Events](#) to for more information)
 - manage several of these events at the same time (refer to [Managing Multiple Events](#) for more information)

For more information about managing security events, refer to [Viewing and Acting on Security Events](#).

Managing Email Messages with Click-Time Protection

After you have [activated Click-Time Protection](#), you can manage email messages that have been processed using Click-Time Protection.

To manage a email message processed by Click-Time Protection:

1. Navigate to **Events**.
2. Click the link for the subject of the email message event designated with a **Type** of either **Malicious URL** or **Malicious URL Click**. The email detail page displays.
3. Select either:
 - **Quarantine**: Quarantine the email message from the user.
 - **Send Original Email**: Release the original email message to the user.

For more information about managing quarantine for email messages, refer to [Managing Quarantine for Email](#).

Creating Custom Queries for Click-Time Protection

You can create custom queries to view a list of malicious URLs that have been clicked in user email messages.

To create a custom query for malicious URLs:

1. Navigate to **ANALYTICS > Custom queries** to [create a new custom query](#).
2. Click **Add condition**.
3. Select **Security Stack > Click-Time Protection > Detection**.
4. Set the values and conditions for the custom query.
5. Click **Add**.

Refer to [Viewing and Creating Custom Queries](#) for more information about creating and viewing custom queries.

Using Cloud App Security Analytics

Cloud App Security Analytics provide you with information about:

- secured cloud applications, with summary totals of information for each application
- quantity of email messages, attachments, and users
- quantity of files, folders, applications, and security in cloud storage and Shadow SaaS applications

Topics:

- [Viewing the Summary Report](#)[Viewing the Summary Report](#)
- [Viewing the Weekly Reports](#)
- [Viewing Email Analytics](#)
- [Viewing Office 365 and Microsoft 365 OneDrive Analytics](#)
- [Viewing Office 365 and Microsoft 365 SharePoint Analytics](#)
- [Viewing Shadow SaaS Analytics](#)
- [Viewing and Creating Custom Queries](#)

Viewing the Summary Report

The **Summary Report** provides a list of your secured cloud applications with summary totals of information for each application.

Office 365 Emails Summary

INCOMING ATTACHMENTS	68
OUTGOING ATTACHMENTS	44
INTERNAL USERS	4
EXTERNAL USERS	18

Office 365 Emails Risk Summary

Security Events

	TOTAL	WEEK	MONTH
MALWARE	22	22	22
PHISHING	6	6	6
SUSPICIOUS PHISHING	5	5	5
SHADOW IT	1	1	1

Scanned Objects

	TOTAL	WEEK	MONTH
ANTI-PHISHING	1	1	1
ADVANCED THREAT PROTECTION	74	74	74
DLP	1	1	1

Depending on the type and usage of a specific cloud application, different summary information will be displayed.

You can click on the numerical value to view the details for that item.

Events by Severity

Events by State

Events by SaaS

~ Hide graph view

Security Events

Date ▾
State ▾
Type ▾
Severity Level ▾
SaaS ▾
Group Actions ▾

Tool ▾

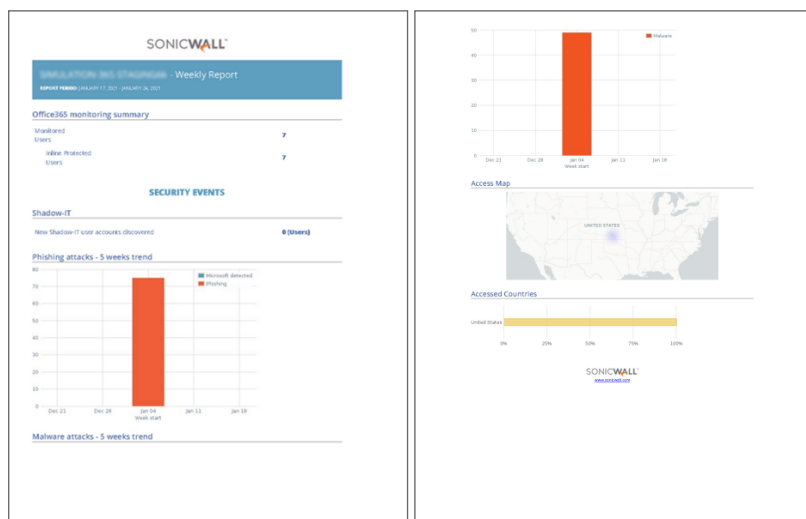
Filter By (clear all): Last 30 days Malware Google Drive New Remediated Total 14 Events Filtered

TIME	STATE	SEVERITY	SAAS	TYPE	EVENT DESCRIPTION	ACTIONS	HISTORY
04:52:58 2019-01-16	NEW	■ ■ ■		Malware	Sonicwall has detected malware in '1b45676144debc8e0bd2180fa0175251aa9' (Created by user1@casbsnwl.net)	Alert owner of malware Quarantine Dismiss	
04:52:42 2019-01-16	NEW	■ ■ ■		Malware	Sonicwall has detected malware in '1b47baf8d193bace2f3d4e30817c0db4da0c' (Created by user1@casbsnwl.net)	Alert owner of malware Quarantine Dismiss	
04:49:55 2019-01-16	NEW	■ ■ ■		Malware	Sonicwall has detected malware in '1b47baf8d193bace2f3d4e30817c0db4da0c' (Created by user1@casbsnwl.net)	Alert owner of malware Quarantine Dismiss	
23:35:16 2019-01-13	REMEDIED	■ ■ ■		Malware	Sonicwall has detected malware in '1b45676144debc8e0bd2180fa0175251aa9' (Created by user1@casbsnwl.net)	File quarantined Release Dismiss	File quarantined Owner alerted

See [Using the Security Event Graphs](#) for information on viewing and customizing these event reports.

Viewing the Weekly Reports

Weekly reports include breakdowns and trends that help you to gain better visibility into the attacks on your organization. The weekly reports provide a weekly summary of the events for each tenant, including user requests for quarantine releases and suspected phishing reports, and are sent on Sunday containing data from the previous week.



① **NOTE:** The weekly reports are only available to administrators both via email and in the Cloud App Security web management interface. Read-only users do not have access to these reports.

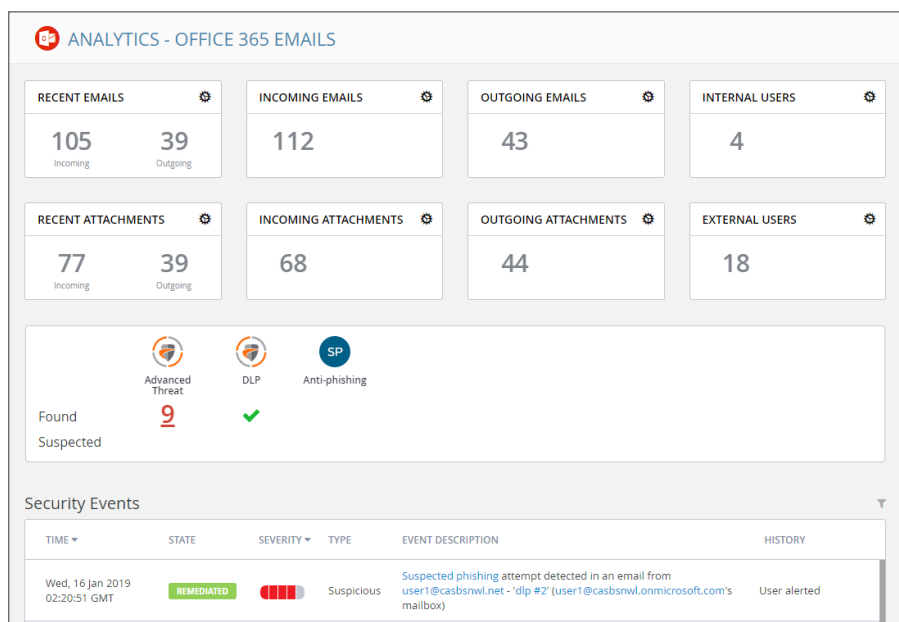
To access the weekly reports from the Cloud App Security management interface:

1. Navigate to **Analytics > Periodic Reports**.
2. Click on the icon on the far right for the report you want to view.

① **NOTE:** Weekly reports are generated and delivered via email automatically. To deactivate automatic delivery, please contact SonicWall support: <https://www.sonicwall.com/support/contact-support>.

Viewing Email Analytics

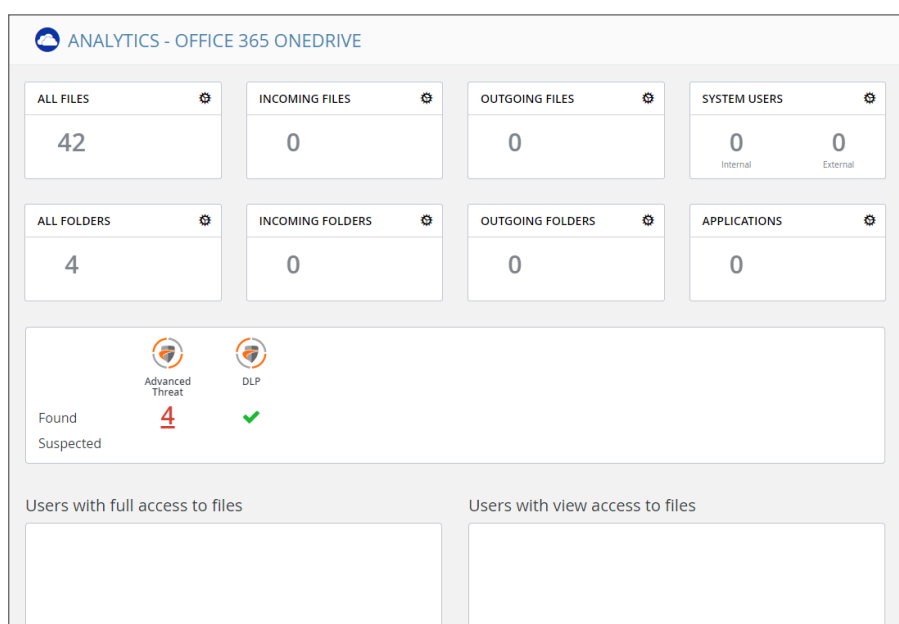
The Analytics for cloud-based email applications provide information about the quantity of emails, attachments, and users.



Widget	Description
Recent Emails	Number of emails recently sent and received.
Incoming Emails	Total number of received emails.
Outgoing Emails	Total number of sent emails.
Internal Users	Number of users actively accessing your cloud application.
Recent Attachments	Number of email attachments recently received and sent.
Incoming Attachments	Number of incoming emails with file attachments.
Outgoing Attachments	Number of outgoing emails with file attachments.
External Users	Number of external users that have contacted.
Security Scan Panel	Number of files that have been found to be malicious.
Security Events	Real-time events with detailed snapshots of time, state, severity level, security type, description, and history of attack.

Viewing Office 365 and Microsoft 365 OneDrive Analytics

The Analytics for Office 365 and Microsoft 365 OneDrive provides information about the quantity of files, folders, and applications.

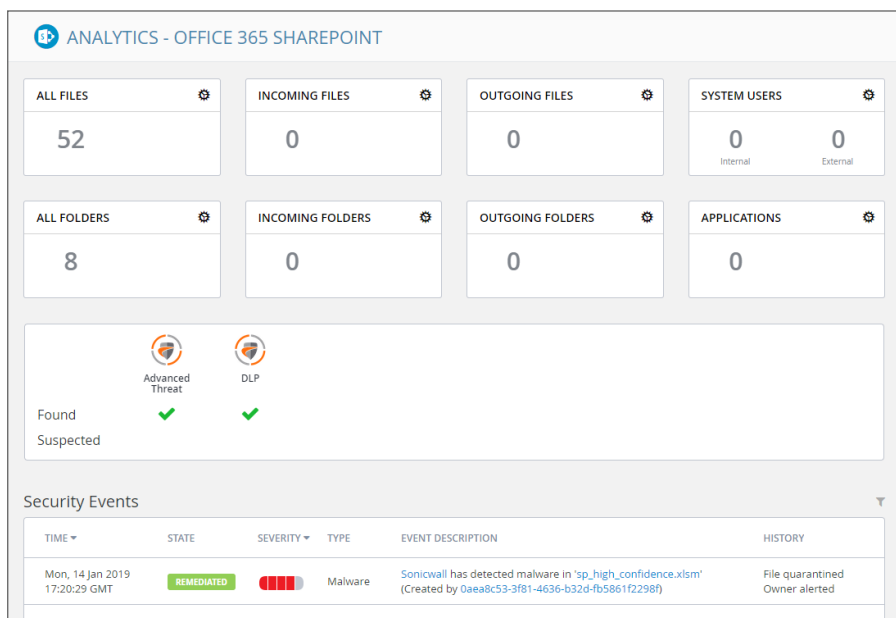


Widget	Description
All Files	The total number of files in your Office 365 and Microsoft 365 OneDrive.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with people outside the company
System Users	The number of active users that can access your Office 365 and Microsoft 365 OneDrive. (This does not include suspended or deleted users).
All Folders	The total number of folders in your Office 365 and Microsoft 365 OneDrive.
Incoming Folders	The number of folders created by external users and shared with internal users.
Outgoing Folders	The number of folders created internally and shared with external users.
Applications	Number of applications detected that have access to your Office 365 and Microsoft 365 OneDrive.
Security Scan	The number of files that have been flagged as malicious or potentially harmful. You can click the number to view a more detailed report.

Widget	Description
Users with full access to files	All users who have full access to the files in your Office 365 and Microsoft 365 OneDrive.
Users with view access to files	All users who have access to view the files in your Office 365 and Microsoft 365 OneDrive.

Viewing Office 365 and Microsoft 365 SharePoint Analytics

The Analytics for Office 365 and Microsoft 365 SharePoint provides information about the quantity of files, folders, applications, and security events.

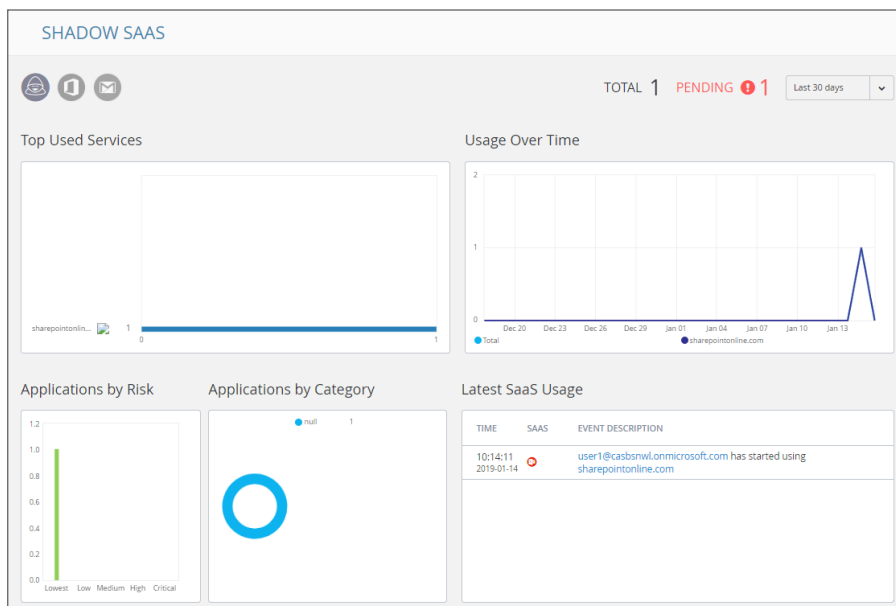


Widget	Description
All Files	The total number of files in your Office 365 and Microsoft 365 SharePoint.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with people outside the company
System Users	The number of active users that can access your Office 365 and Microsoft 365 SharePoint. (This does not include suspended or deleted users).
All Folders	The total number of folders in your Office 365 and Microsoft 365 SharePoint.
Incoming Folders	The number of folders created by external users and shared with internal users.

Widget	Description
Outgoing Folders	The number of folders created internally and shared with external users.
Applications	Number of applications detected that have access to your Office 365 and Microsoft 365 SharePoint.
Security Scan	The number of files that have been flagged as malicious or potentially harmful. You can click the number to view a more detailed report.
Security Events	Detailed list of events in real time.

Viewing Shadow SaaS Analytics

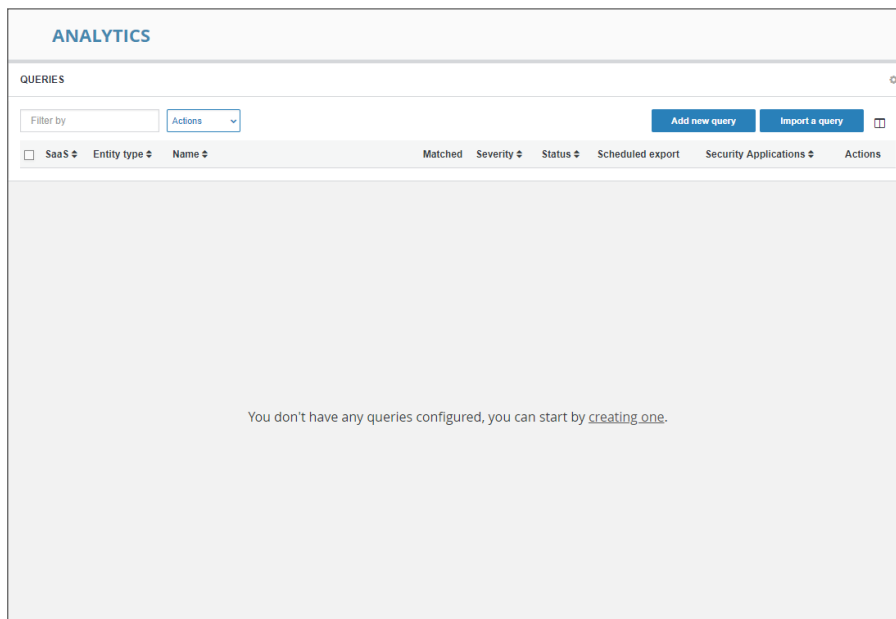
The Analytics for Shadow SaaS provides information about the quantity of files, folders, applications, and security events.



Panel	Description
Top Used Services	The most commonly used cloud applications discovered within your organization
Usage Over Time	The usage pattern of the discovered cloud applications over time
Applications by Risk	The number of discovered cloud applications and their associated risk level
Applications by Category	The number of discovered cloud applications arranged by application category
Latest Cloud Usage	The most recent events associated with the usage of the discovered cloud applications

Viewing and Creating Custom Queries

You can create your own custom queries to assist with your cloud application security reporting. These custom queries can also be added to the widgets on the SonicWall Cloud App Security Dashboard. (See [Changing a Security Event Widget to an Alert or Custom Query](#) for more information on adding custom queries to the Cloud App Security Dashboard.)



Topics:

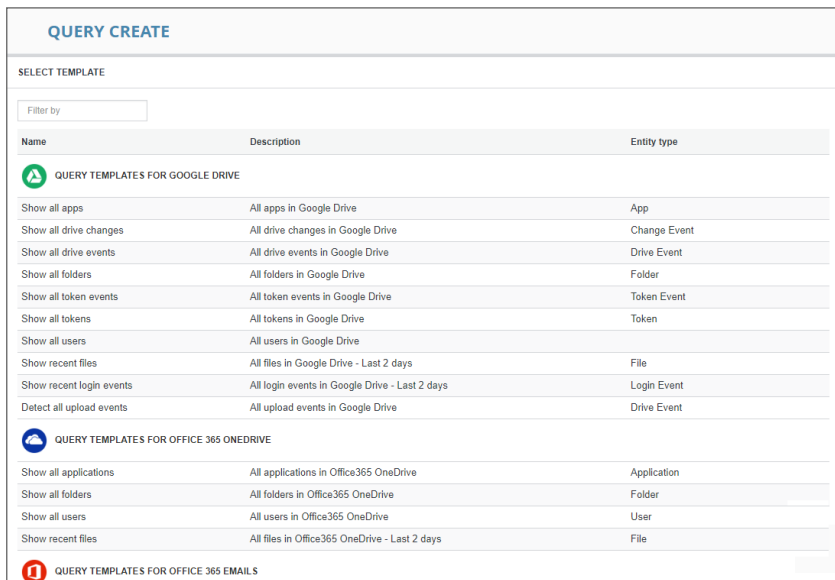
- [Creating Custom Queries](#)
- [Adding Custom Queries to the Dashboard](#)

Creating Custom Queries

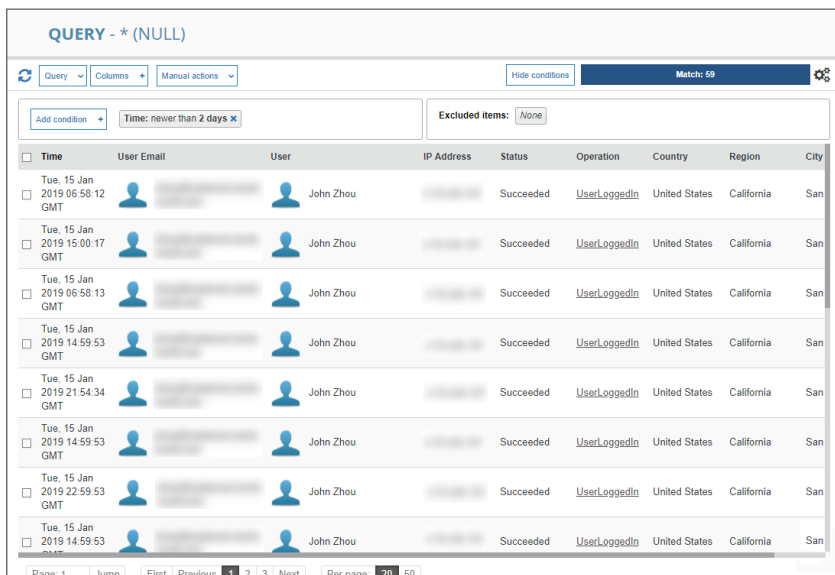
The easiest way to create new custom queries is by basing them on existing templates.

To create a custom query:

1. Navigate to the **ANALYTICS > Custom queries** page.
2. Click **Add new query** in the upper left side of the page. The **Query Create** page displays.

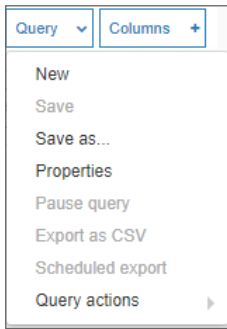


3. Click the query template under the cloud application for which you want to create a query. The results for that query are displayed.



4. Modify the query by adding conditions using the **Add condition** button.

5. Save your query by selecting **Save as...** from the **Query** dropdown in the upper left area of the page.

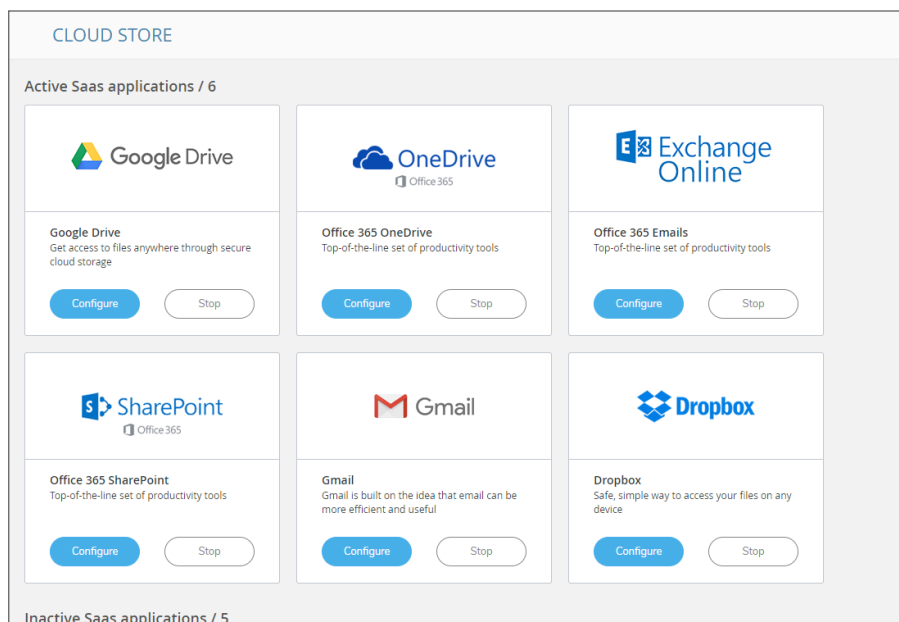


Adding Custom Queries to the Dashboard

See [Changing a Security Event Widget to an Alert or Custom Query](#) for information on adding custom queries to the Cloud App Security Dashboard.)

Configuring Cloud Applications in the Cloud App Store

The Cloud Store allows you to configure activated cloud applications and activate new cloud applications.



Topics:

- [Activating Cloud Applications for Cloud App Security](#)
- [Configuring Office 365 and Microsoft 365 for Cloud App Security](#)
- [Re-Authorizing Cloud Applications](#)

Activating Cloud Applications for Cloud App Security

After you have subscribed to the Cloud App Security service, you can add the cloud applications that you want to monitor and control.

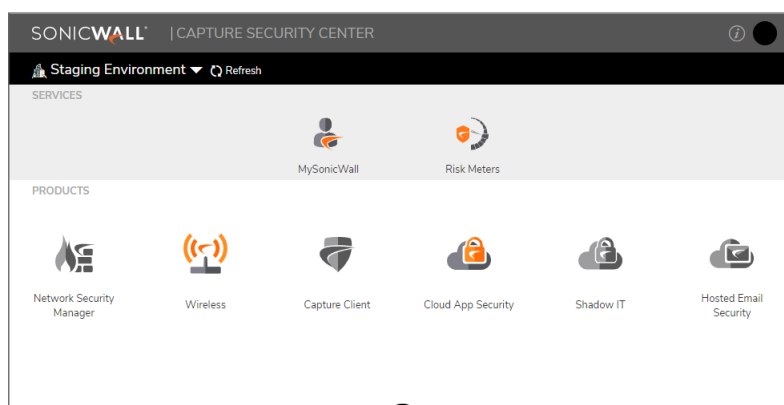
Cloud App Security can secure Office 365 and Microsoft 365 applications with these subscription types:

- Office 365 and Microsoft 365 Business
- Office 365 and Microsoft 365 Apps
- Office 365 and Microsoft 365 Education
- Office 365 and Microsoft 365 Enterprise

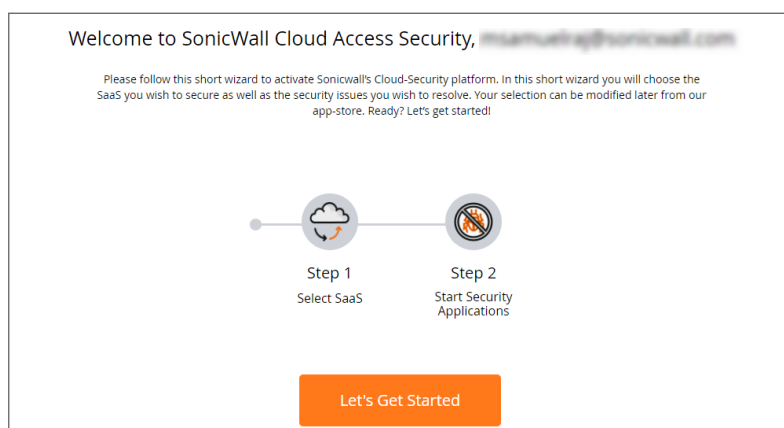
① | **NOTE:** Personal and Home subscription plans are not supported by SonicWall Cloud App Security.

To activate Office 365 and Microsoft 365 applications for Cloud App Security:

1. Navigate to cloud.sonicwall.com.
2. Login with your **MySonicWall** credentials to get to the Capture Security Center.
3. Click the **Cloud App Security** tile.

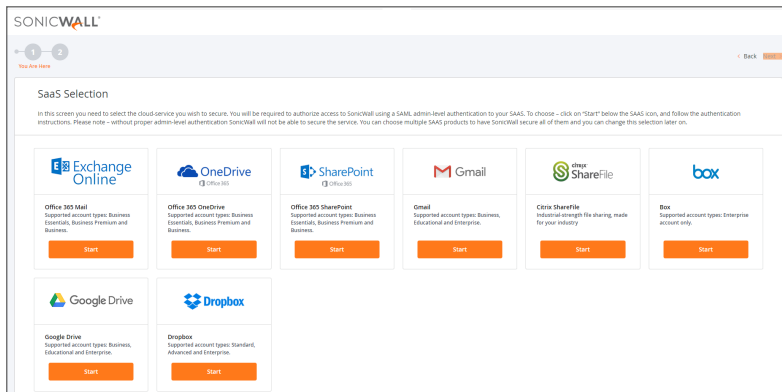


4. The **Welcome to SonicWall Cloud Access Security** page displays.



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

The **SaaS Selection** page displays. This page lists all of the cloud applications which can be monitored using SonicWallCloud App Security.



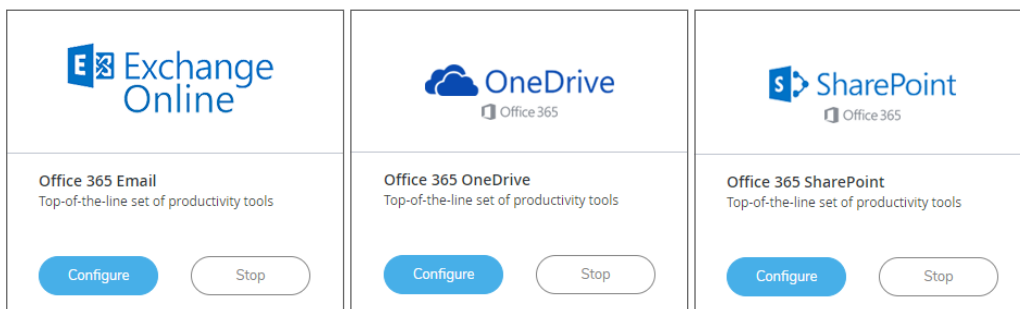
6. Click **Start** on the tile for the Office 365 and Microsoft 365 application you want to activate.

For instructions for activating Office 365 and Microsoft 365 cloud applications, see: [Activating Office 365 and Microsoft 365 Cloud Applications](#).

Configuring Office 365 and Microsoft 365 for Cloud App Security

To configure Office 365 and Microsoft 365 for Cloud App Security:

1. Navigate to the **Configuration > Cloud App Store** page.
2. Click **Configure** on the **Office 365 and Microsoft 365** tile.



3. Set the options you want for the cloud application.

Configure Office 365 Email Security

Exchange Online

Office 365 Mail
Supported account types:
Business Essentials, Business
Premium and Business.

Re-Authorize SonicWall CAS Office365 Emails App

Quarantine and workflow:

Dedicated quarantine mailbox:

Restore requests approver:

Advanced

Cancel Ok

Configure Office 365 OneDrive Security

OneDrive

Office 365 OneDrive
Top-of-the-line set of productivity
tools

Authorize SonicWall CAS Office365 OneDrive App

Quarantine Options:

Create Quarantine folder in the root directory

Quarantine to existing directory

Enable Remove Action:

Cancel Ok

Configure Office 365 SharePoint Security

SharePoint

Office 365 SharePoint
Top-of-the-line set of productivity
tools

Authorize

Quarantine Options:

Create a folder in the quarantine user's root
directory

Quarantine to existing directory

Force Site Admin:

Advanced

Authorization Scope:

Authorize for all sites

Authorize for specific sites only

Cancel Ok

Most of the settings are related to specifying a quarantine email address and authorized administrators. See [Managing Quarantine for Office 365 and Microsoft 365](#) for more information on configuring these options.

You can also:

- Re-authorize Cloud App Security for the cloud application. (See [Re-Authorizing Cloud Applications](#) for more information.)
- Configure the Group filter for licensing Cloud App Security. (See [Managing Cloud App Security Licenses](#) for more information.)

4. Click **Ok**.

Re-Authorizing Cloud Applications

If the access of Cloud App Security has been revoked to a cloud application for some reason, you can renew Cloud App Security authorization for access to the application.

To re-authorize a cloud application for Cloud App Security:

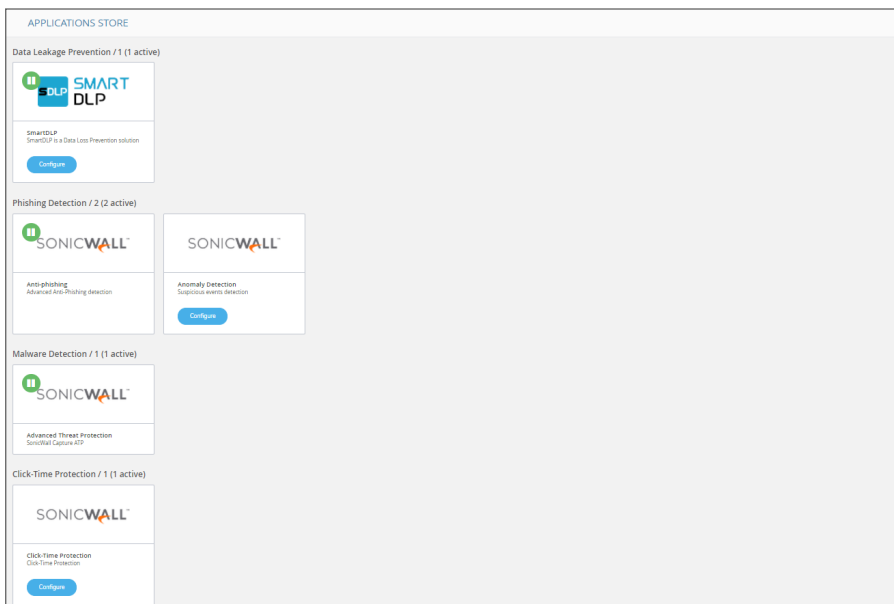
1. Navigate to **Configuration > Cloud App Store**.
2. Click **Configure** on the tile for the cloud application you need to re-authorize.
3. Click the **Re-Authorize SonicWall CAS Office 365 and Microsoft 365** link. The first step in the authorization for the cloud application displays.

For instructions for authorizing specific cloud applications, see [Activating Office 365 and Microsoft 365 Cloud Applications](#) Activating Box for Cloud App Security.

① **NOTE:** Cloud App Security can be re-authorized using a different account than the one from which Cloud App Security was originally authorized, but the account must be a global administrator account within the same domain.

Managing Security Applications in the Security App Store

Use the **Applications Store** to get new security applications, or to start or stop installed security applications.



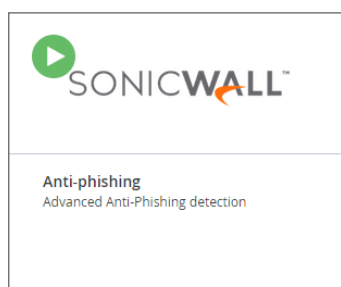
Topics:

- [Starting Security Applications](#)
- [Stopping Security Applications](#)
- [Managing Security Tool Exceptions](#)

Starting Security Applications

To start a security application:

1. Navigate to the **Configuration > Security App Store** page.
2. Click on the green button on the upper left of the tile for the security application you want to start.

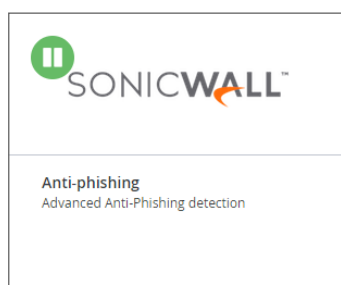


3. When prompted, click **Start** to start the security application.

Stopping Security Applications

To stop a security application:

1. Navigate to the **Configuration > Security App Store** page.
2. Click on the green button on the upper left of the tile for the security application you want to stop.



3. When prompted, click **Stop** to stop the security application.

Managing Anomaly Exceptions

Topics:

- [Understanding Anomalies](#)
- [Creating Exceptions Based on Anomaly Events](#)
- [Sending Anomaly Event Notifications](#)

Understanding Anomalies

One threat individuals in your organization can face is the takeover of their account(s). SonicWall Cloud App Security can detect this by analyzing unusual behavior an account user, such:

- logins to an account from new browsers, devices, or locations
- suspicious email activity or configurations, such as deleting all incoming email messages or forwarding messages to an external account or domain
- email account configurations that are insecure or make extensive use of filters, forwarding, or secondary accounts
- accounts where two-factor authentication has been disabled
- suspicious internal emails, often with multiple recipients
- multiple account password resets within an unusually short period of time
- changes in the grouping of contacts in emails messages or mailing lists
- changes in the usual characteristics of user sessions (such as the time of day, length of login session, or applications used)

Topics:

- [Managing Anomaly Exceptions](#)

Creating Exceptions Based on Anomaly Events

You add anomalous events to the Allow-List.

To add an anomalous event as an exception:

1. Navigate to **Events**.
2. In the **Security Events** table, in the **Actions** column for the anomaly from which you want to create a new exception, click **Add Exception**.
3. From the **Choose Allowed** list option list, select the option you want based on the information provided in the anomaly report.
4. From the **Apply** on all past events list, select:
 - **Yes**, if you want the new exception to be applied to all previously reported anomalies that match the criteria
 - **No**, if you want the new exception to be applied to only to future report anomaly events
5. From the **Apply for** list, select the duration for which you want the exception to apply.
6. Click **Ok**.

Sending Anomaly Event Notifications

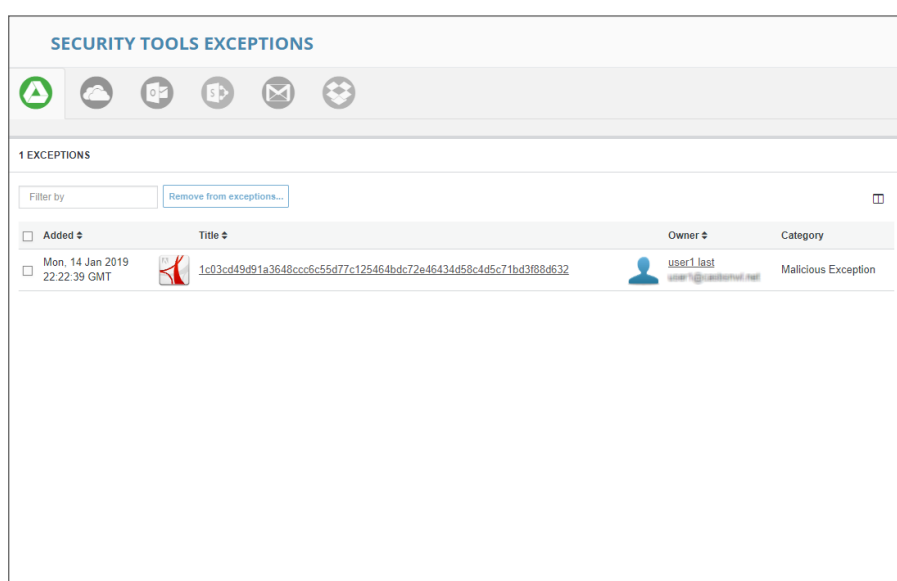
You can send alerts to administrators when anomalies are detected.

To configure anomaly notifications:

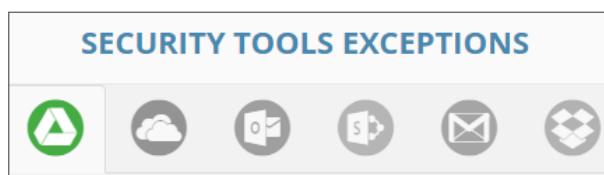
1. Navigate to **Configuration > Security App Store**.
 2. For the security application for which you want to configure anomaly reporting, click **Configure**.
 3. Select **Email anomaly alerts to admins**. This will send email alerts to Cloud App Security administrators.
 4. Click **Ok**.
- ① **NOTE:** Anomaly alert notifications are off by default. You must explicitly enable it for notifications to occur.

Managing Security Tool Exceptions

You can manage which email addresses and files are exempt from being processed by the installed Security Tools.



To switch between the security tool exceptions for each secured cloud application, click its icon at the upper left of the **Security Tools Exceptions** page.



Lists for email cloud applications provide views both email messages and attachments.

To remove an item from the Security Tools Exceptions list:

1. Navigate to **Configuration > Security Tools Exceptions**.
2. Select the items you want to remove from the **Security Tools Exceptions** list.
3. Click **Remove from exceptions....**
4. When prompted, click **Ok**.

Using the System Log

Topics:

- [Viewing the System Log](#)
- [Exporting the System Log](#)

Viewing the System Log

The **System Log** displays all of the system-level actions taken administrators for SonicWall Cloud App Security.

You can sort the items listed in the log by:

- Type
- User
- Description
- Time

Exporting the System Log

You can export the contents of the system log as a comma-separated values (CSV) file.

To export the system log:

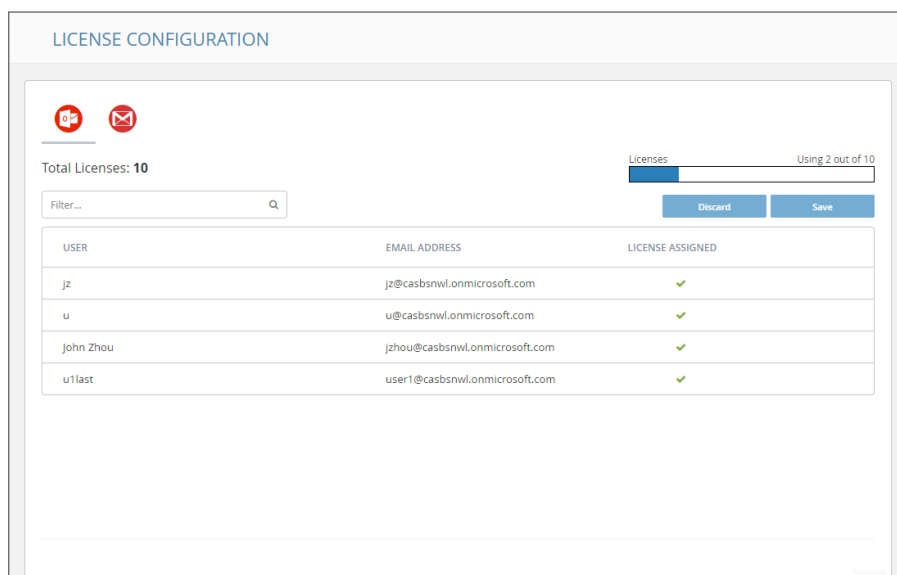
1. Navigate to the **Configuration > System Log** page.
2. Click the **Export as CSV** button on the upper right of the page. The file will be downloaded to your system. Depending on which browser you use, you may be prompted for a location where to save it.

Managing Cloud App Security Licenses

The **License Configuration** page displays the number of SonicWall Cloud App Security licenses assigned and allows you to manage those licenses.

① **NOTE:** The **License Configuration** page will not be available if your Cloud App Security license has expired. You will need to apply an active license through **MySonicWall** in order to access this page.

If you have licenses assigned to only a specific Group within your organization, you can also use this page to manage which users within the Group are granted a license for Cloud App Security.



The screenshot shows the 'LICENSE CONFIGURATION' page. At the top, there are two red icons (a person and an envelope). Below them, it says 'Total Licenses: 10' and 'Licenses Using 2 out of 10'. There is a search filter box and 'Discard' and 'Save' buttons. A table lists users with their email addresses and license status.

USER	EMAIL ADDRESS	LICENSE ASSIGNED
jz	jz@casbsnwl.onmicrosoft.com	✓
u	u@casbsnwl.onmicrosoft.com	✓
John Zhou	jzhou@casbsnwl.onmicrosoft.com	✓
u1last	user1@casbsnwl.onmicrosoft.com	✓

Licenses are assigned in alphabetical order.

- If the number of users exceeds the number of available licenses, then only the number of users, in alphabetical order, up to the number of available licenses are automatically assigned a license. You can manually unassign licenses in order to free up licenses.
- If the number of licenses exceeds the number of users, the remaining licenses will remain unassigned. You can manually assign these later when new users are added.

Refer to [Unassigning Cloud App Security Licenses](#) for information on unassigning licenses.

Topics:

- [Adding Administrator Users](#)
- [Adding Read-Only Users](#)
- [Managing Group Licensing](#)
- [Unassigning Cloud App Security Licenses](#)

Adding Administrator Users

You can designate users as administrators when you create their accounts in [MySonicWall](#). After they have completed their account validation, they should have access to administrator functions within Cloud App Security.

Adding Read-Only Users

You can create user accounts with read-only access to Cloud App Security when you create their accounts in [MySonicWall](#).

Users with read-only access have restricted access to Cloud App Security and cannot:

- stop, restart, or edit policies
- create custom queries
- act on quarantined items
- act on restore requests
- configure the anti-phishing blocked list, allowed list, or exceptions
- start or stop cloud applications
- enable or disable security applications

Read-only access for users is configured via [MySonicWall](#) through **My Workspace**.

Managing Group Licensing

If you originally assigned licenses to everyone in your organization, you can change the licensing to only a specific group within in your organization. Using Group Filters is the most effective way to manage your Cloud App Security licenses for a specific subset of users within your organization.

① **NOTE:** After changing to group licensing, or adding or removing users in a Office 365 and Microsoft 365 group, synchronization of the licensed users between the cloud application and Cloud App Security may require up to 24 hours.

To change to group licensing:

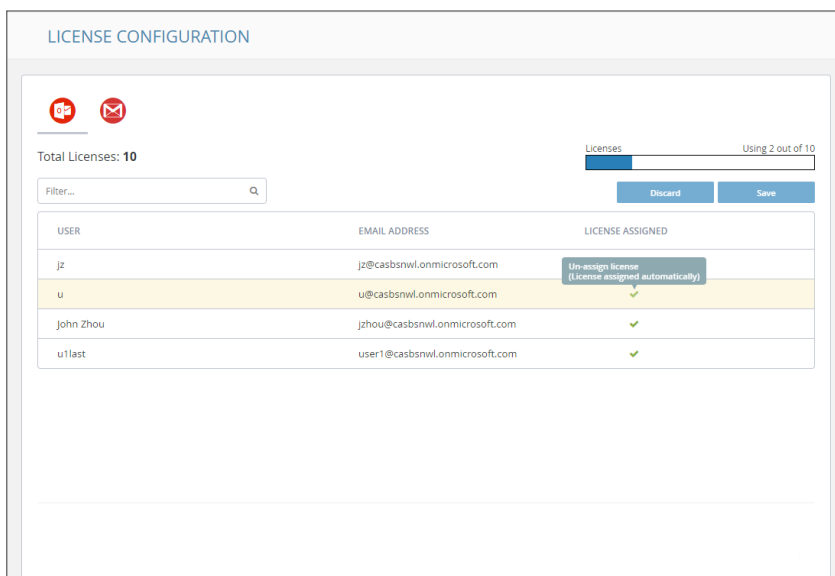
1. Navigate to **Configuration > Cloud App Store**.
2. Click **Configure** on the tile for the cloud application for which you want to change the licensing.
3. Click **Configure groups filter**.

4. Select **Specific Group/s**.
5. Enter the name of the group to which you want to assign the licenses.
Only one group is supported for Office 365 and Microsoft 365 cloud applications at this time. If you enter the name of more than one group, an error message is displayed.
6. Click **Ok**.

Unassigning Cloud App Security Licenses

To unassign a SonicWall Cloud App Security license:

1. Navigate to **Configuration > Licenses**.
2. Click the green checkmark in the **License Assigned** column in the row for the user for which want to remove their license. The checkmark will change to a link labeled **Assign**.
3. Repeat this step for each user for you want to remove their license.



4. In the upper right, under the bar graph showing the number of licenses used, click **Save**.

If you are assigning licenses to your entire organization, and not using Group Filters, Cloud App Security will attempt to use all of your available licenses. For example, if you have 100 licenses and 200 users, and unassign licenses for 5 users, the next five users alphabetically who did not previously have licenses will be automatically assigned one.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Cloud App Security Administration Guide for Office 365 and Microsoft 365
Updated - May 2021
232-005369-00 Rev B

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035