



# Cloud App Security

Administration Guide  
for G Suite

SONICWALL<sup>®</sup>

# Contents

<b>Understanding Cloud App Security</b> .....	<b>5</b>
Understanding Email Security .....	5
Understanding Post-Delivery Email Recheck .....	6
Using Data Leak Protection .....	7
Understanding Anomalies .....	7
Understanding Click-Time Protection .....	8
<b>Configuring Cloud App Security</b> .....	<b>9</b>
Subscribing to Cloud App Security .....	9
Activating Cloud Applications for Cloud App Security .....	10
Activating G Suite Cloud Applications .....	12
Using Cloud App Security with Google Cloud Directory Sync .....	17
<b>Managing Quarantine for G Suite</b> .....	<b>18</b>
Setting Up a Quarantine Mailbox for Gmail .....	18
Setting Up a Quarantine Folder for Google Drive .....	18
Using the Quarantine View for Gmail .....	19
Using the Quarantine Page .....	20
Using the Quarantined File Creator Dashboard .....	21
Using the User Dashboard for G Suite .....	22
Managing Restore Requests .....	23
<b>Using the SonicWall Cloud App Security Dashboard</b> .....	<b>24</b>
Using the Security Events Widgets .....	25
Changing a Security Event Widget to an Alert or Custom Query .....	26
Resetting a Security Event Widget .....	26
Hiding a Security Event Widget .....	27
Configuring Security Event Widget Custom Queries .....	27
Adjusting the Time Scale .....	28
Viewing the Summary of Security Events .....	28
Viewing Login Events .....	30
Viewing Secured Applications .....	32
Viewing the Scanned Files Summary .....	33
<b>Managing Security Events</b> .....	<b>34</b>
Using the Security Event Graphs .....	34
Viewing Security Events by Severity .....	35
Viewing Security Events by State .....	35
Viewing Security Events by Cloud Application .....	35

Viewing and Acting on Security Events .....	36
Removing Filters .....	37
Acting on Security Events .....	37
Managing Multiple Events .....	37
<b>Managing Policies .....</b>	<b>38</b>
Understanding Cloud App Security Policies .....	39
Before You Set Email Policies .....	39
Monitor only .....	39
Detect and Prevent .....	39
Protect (Inline) .....	40
Creating New Policy Rules .....	40
Creating Data Leak Protection Policy Rules .....	41
Creating Malware Policy Rules .....	43
Creating Threat Detection Policy Rules .....	44
Creating Policy Rules for Click-Time Protection .....	46
Creating Custom Query Policies .....	47
Stopping Policy Rules .....	47
Removing Policy Rules .....	48
<b>Using Data Leak Protection .....</b>	<b>49</b>
Configuring Data Leak Protection Detection Rules .....	49
Creating Data Leak Protection Policy Rules .....	50
Reactivating Data Leak Protection .....	52
Predefined Data Leak Protection Policy Rules .....	52
Global Rules .....	53
Credentials and Secrets .....	55
Predefined Data Leak Protection Rules for Specific Countries .....	56
<b>Managing Spam and Anti-Phishing .....</b>	<b>68</b>
Managing Spam .....	68
Customizing Warning Messages .....	69
Managing Nickname Impersonation .....	69
Managing the Anti-Phishing Exceptions .....	70
Managing Excluded Email Addresses .....	71
Managing Excluded IP Addresses .....	72
Managing Excluded Domains .....	72
Creating Block-List Rules from Email Messages .....	73
Managing the Anti-Phishing Allow-List .....	73
Managing the Anti-Phishing Block-List .....	75
<b>Configuring and Using Click-Time Protection .....</b>	<b>76</b>
Understanding Click-Time Protection .....	76
Activating Click-Time Protection .....	77
Configuring Click-Time Protection .....	78
Configuring the Click-Time Protection Workflow .....	78

Configuring Custom Click-Time Protection for Specific Domains .....	78
Using Click-Time Protection .....	79
Creating Policy Rules for Click-Time Protection .....	80
Viewing Security Events for Click-Time Protection .....	80
Managing Email Messages with Click-Time Protection .....	81
Creating Custom Queries for Click-Time Protection .....	81
<b>Using Cloud App Security Analytics .....</b>	<b>82</b>
Viewing the Summary Report .....	83
Viewing the Weekly Reports .....	84
Viewing Email Analytics .....	85
Viewing Google Drive Analytics .....	86
Viewing Shadow SaaS Analytics .....	87
Viewing and Creating Custom Queries .....	88
Creating Custom Queries .....	89
Adding Custom Queries to the Dashboard .....	90
<b>Configuring Cloud Applications in the Cloud App Store .....</b>	<b>91</b>
Activating Cloud Applications for Cloud App Security .....	92
Configuring G Suite for Cloud App Security .....	93
Re-Authorizing Cloud Applications .....	94
<b>Managing Security Applications in the Security App Store .....</b>	<b>95</b>
Starting Security Applications .....	96
Stopping Security Applications .....	96
<b>Managing Anomaly Exceptions .....</b>	<b>97</b>
Understanding Anomalies .....	97
Creating Exceptions Based on Anomaly Events .....	98
Sending Anomaly Event Notifications .....	98
<b>Managing Security Tool Exceptions .....</b>	<b>99</b>
<b>Using the System Log .....</b>	<b>100</b>
Viewing the System Log .....	100
Exporting the System Log .....	100
<b>Managing Cloud App Security Licenses .....</b>	<b>101</b>
Adding Administrator Users .....	102
Adding Read-Only Users .....	102
Managing Group Licensing .....	102
Unassigning Cloud App Security Licenses .....	103
<b>SonicWall Support .....</b>	<b>104</b>
About This Document .....	105

# Understanding Cloud App Security

SonicWall Cloud App Security (CAS) offers complete, defense-in-depth security for G Suite. 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 G Suite 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 G Suite 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 G Suite 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 G Suite 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 G Suite by connecting within the G Suite 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 G Suite, 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 G Suite.

By connecting to the cloud environment via the G Suite 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](#)
- [Managing Spam and Anti-Phishing](#)
- [Understanding Post-Delivery Email Recheck](#)

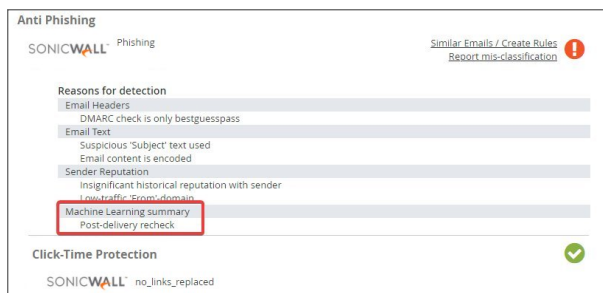
## Understanding Post-Delivery Email Recheck

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:

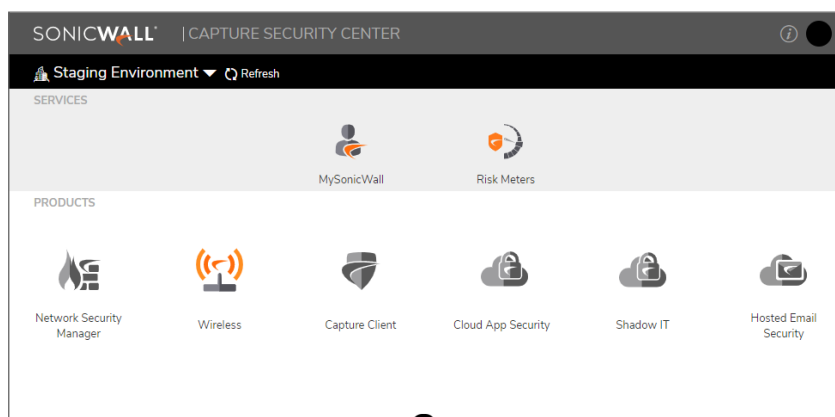
- [Subscribing to Cloud App Security](#)
- [Activating Cloud Applications for Cloud App Security](#)
- [Activating G Suite Cloud Applications](#)

## 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.

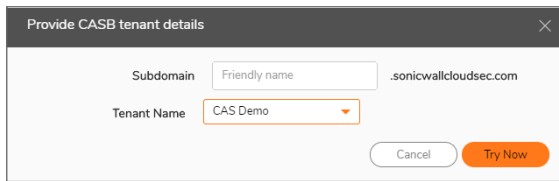
### To subscribe to SonicWall Cloud App Security:

1. Navigate to [cloud.sonicwall.com](https://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](#).



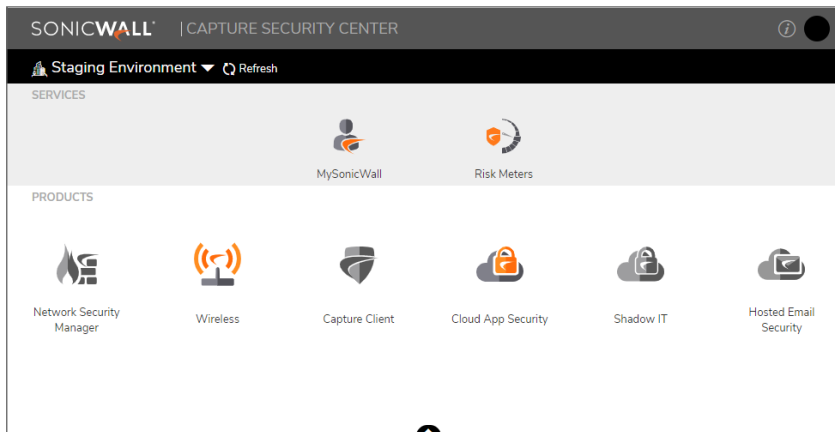
3. Click the **MySonicWall** tile. The MySonicWall dashboard displays.
4. Navigate to **Product Management > My Products**.
5. In the **Quick Register** field, enter your activation key.
6. Click **Register**.

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 G Suite applications with these subscription types:

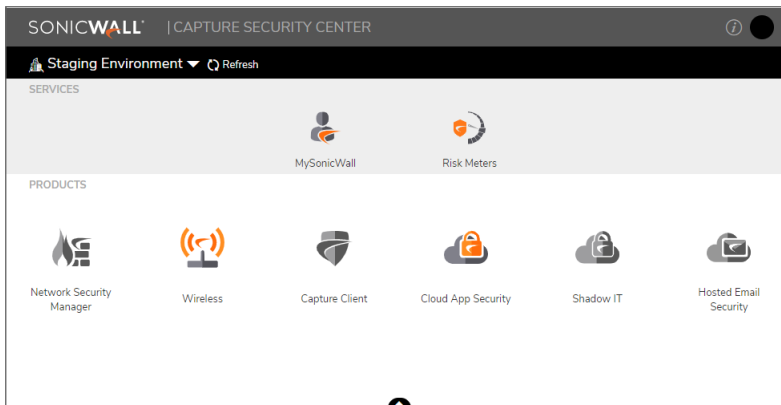
- G Suite Business
- G Suite Enterprise

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

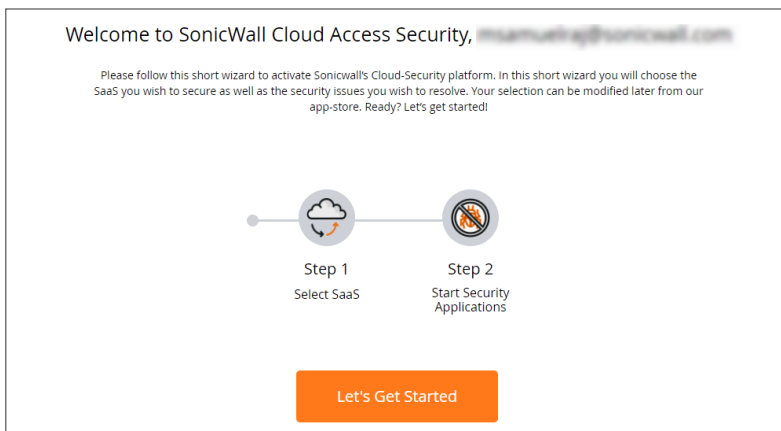
### **To activate G Suite applications for Cloud App Security:**

1. Navigate to [cloud.sonicwall.com](https://cloud.sonicwall.com).
2. Login with your **MySonicWall** credentials to get to the Capture Security Center.

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

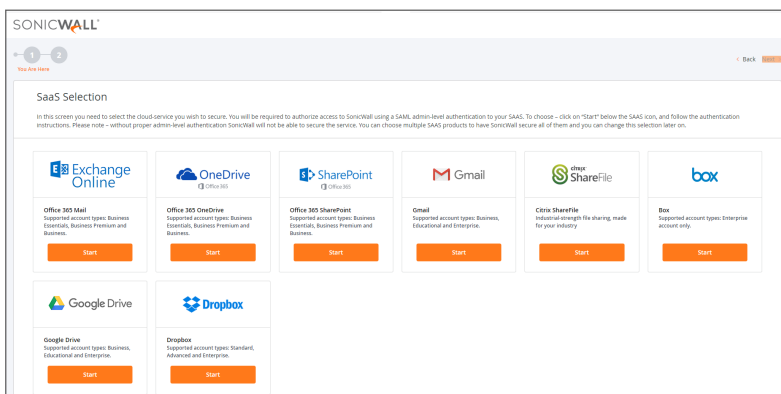


4. The **Welcome to SonicWall Cloud Access Security** page displays.



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 G Suite application you want to activate.

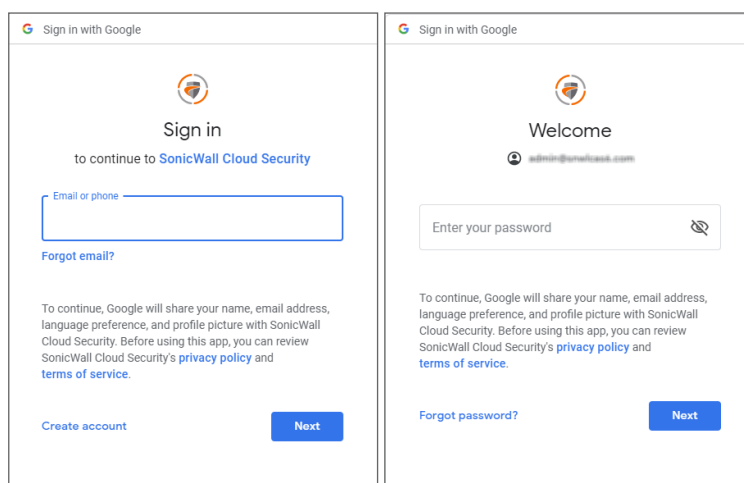
For instructions for activating G Suite cloud applications, see: [Activating G Suite Cloud Applications](#).

# Activating G Suite Cloud Applications

- ① **IMPORTANT:** SonicWall Cloud App Security only supports G Suite Business and G Suite Enterprise accounts. When you attempt to activate a non-business Google account for SonicWall Cloud App Security, the activation will fail with the error message, “This app isn't verified”.
- ① **IMPORTANT:** If you plan to assign Cloud App Security licenses to only a specific set of G Suite users, create the G Suite group before activating your G Suite 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 G Suite 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 G Suite cloud applications for Cloud App Security:

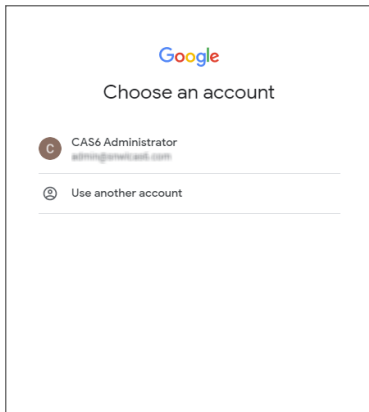
1. Navigate to either the:
  - **SaaS Selection** page (during initial setup and configuration).
  - **Cloud App Store** page.
2. Click **Start** on the tile for the **G Suite** cloud application you want activate.
3. When prompted, log into your Google business account.



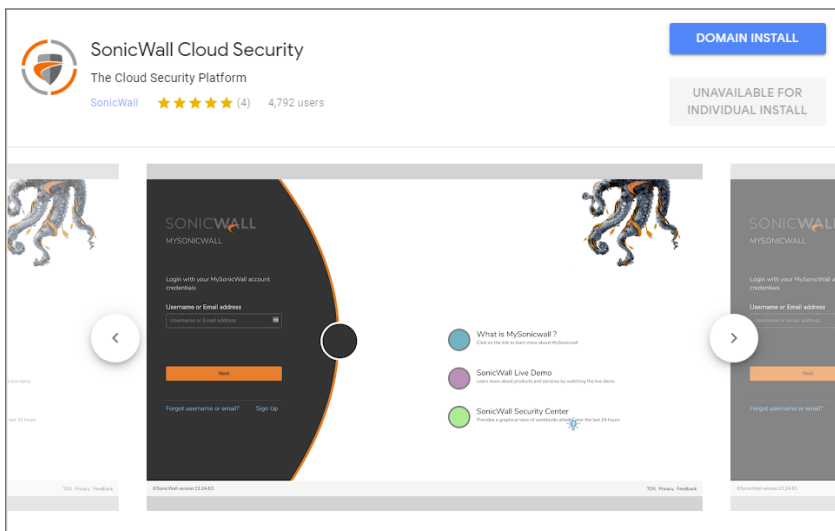
- ① **NOTE:** Only G Suite Business and G Suite Enterprise accounts are supported by SonicWall Cloud App Security.

4. Click Next.

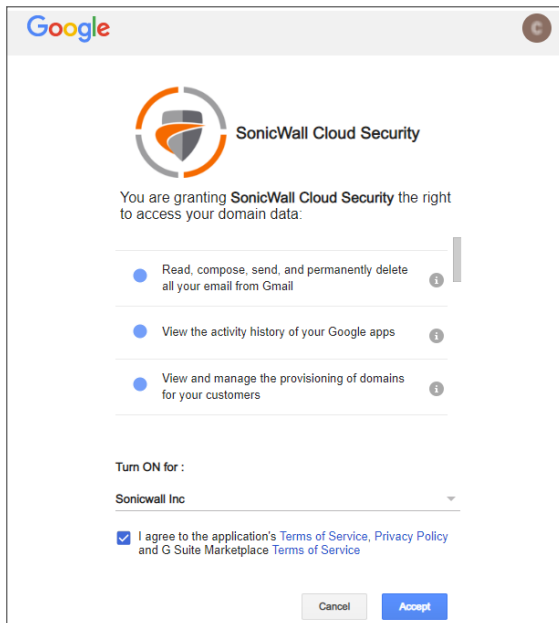
5. Select your Google account.



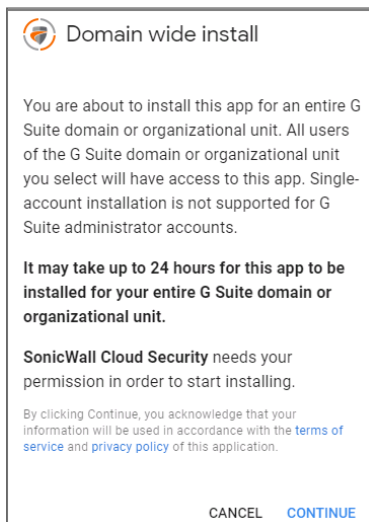
6. On the G Suite Marketplace, click the **Domain Install** button on the upper right of the page to install SonicWall Cloud App Security.



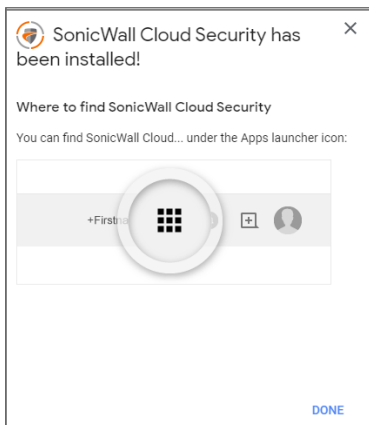
7. When prompted to grant access, click **Accept**.



8. When prompted for a **Domain wide install**, click **Continue**.

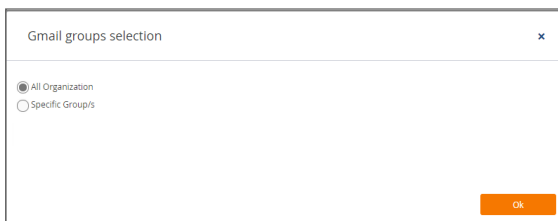


9. When the installation completes, a confirmation message displays.

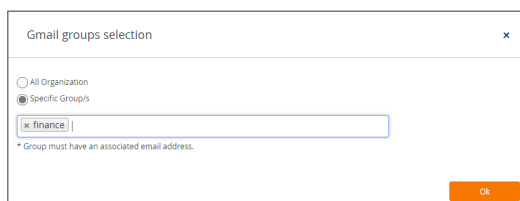


Click **Done** to continue.

10. Click **Start** on the tile for the G Suite cloud application you want to configure.
11. On the **Gmail groups selection** or Google Drive 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 G Suite group 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.



- 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.

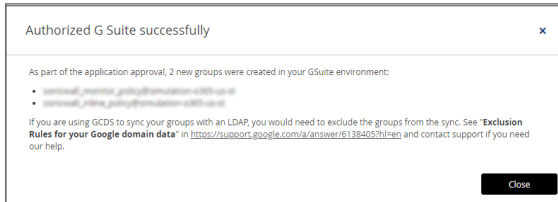
Enter the name of the G Suite group to which you want to assign the licenses.

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

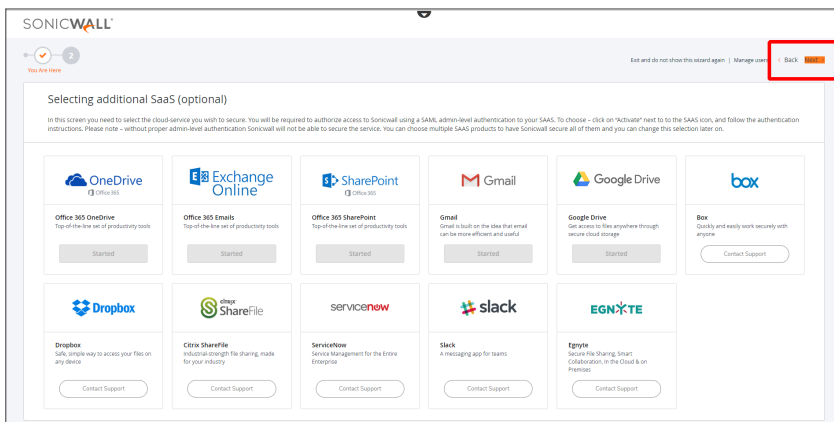
You can change this setting later, if you needed, on the **Configuration > Cloud App Store** page. Refer to [Managing Cloud App Security Licenses](#) for more information.

**NOTE:** If you add users to the G Suite 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](#).

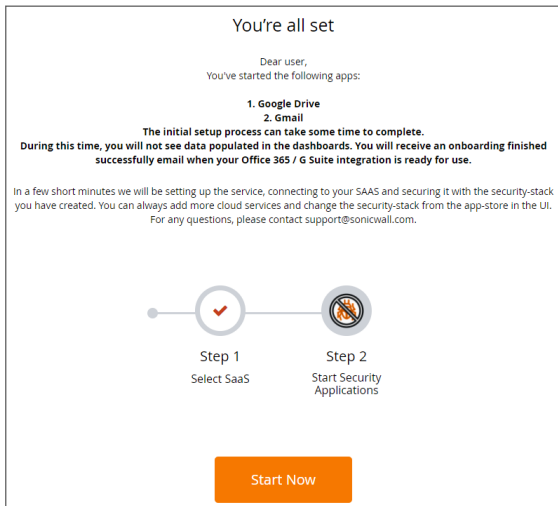
12. A confirmation message displays. Click **Close** to complete the activation process.



13. On the **SaaS Selection** page, click **Next** in upper right area of the page.



14. Click **Start Now** to view the SonicWallCloud App Security Dashboard.



15. Navigate to the **Configuration > Cloud App Store** page.



16. On the tile for the G Suite application(s) you want to run, click **Start** to start the protection of G Suite 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 one G Suite cloud application at this time, you will not need to reauthorize SonicWall Cloud App Security again when you activate any additional G Suite cloud applications.

### Topics:

- [Using Cloud App Security with Google Cloud Directory Sync](#)

## Using Cloud App Security with Google Cloud Directory Sync

If your organization uses Google Cloud Directory Sync (GCDS), you will need to perform additional configuration of your Exclusion Rules to work properly with SonicWall Cloud App Security.

① **IMPORTANT:** You need to complete this configuration change before authorizing SonicWall for Gmail. Otherwise, the Google Groups will be deleted when Cloud App Security synchronizes with the Google Cloud after authorization.

Cloud App Security automatically creates and manages four Google Groups when you complete the authorization of the Gmail cloud application.

GCDS deletes the SonicWall groups when Cloud App Security synchronizes with the Google Cloud. By configuring the Exclusions Rules, the groups will not be deleted during synchronization.

### *To configure the Exclusion Rules for Cloud App Security:*

1. Log into your Google Cloud management account.
2. Navigate to **Google Domain Configuration**.
3. Click on **Exclusion Rules**.
4. Click **Add Exclusion Rule**.
5. Create four new Exclusion Rules. Each new rule should contain the specified values for these fields:
  - **Type:** Group Email Address
  - **Match Type:** Exact Match
6. Assign one of these email addresses to each new Exclusion Rule:
  - sonicwall\_inline\_policy@yourdomain.com
  - sonicwall\_inline\_rule@yourdomain.com
  - sonicwall\_monitor\_policy@yourdomain.com
  - sonicwall\_monitor\_rule@yourdomain.com
7. Click **OK**.
8. Click **Sync**.

You can now authorize Gmail for SonicWall without the Google Groups getting deleted.

# Managing Quarantine for G Suite

## Topics:

- [Setting Up a Quarantine Folder for Google Drive](#)
- [Using the Quarantine Page](#)
- [Using the Quarantined File Creator Dashboard](#)
- [Using the Quarantine View for Gmail](#)
- [Using the User Dashboard for G Suite](#)
- [Managing Restore Requests](#)

## Setting Up a Quarantine Mailbox for Gmail

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 **G Suite** 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.  
**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 Google Drive

Before you quarantine files stored in Google Drive, 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 **Google Drive** tile.
3. In the **Quarantine Email Address** field, select the email address to which all quarantined email should be routed. This email address will also receive all notifications for quarantined email messages.  
The email address will be displayed with a message that the email address needs to be verified.
4. Click **Verify Now**.
5. In the **Confirm e-mail address** dialog, enter the verification code sent to the email address specified.
6. Click **Verify**.
7. When the **Configure Google Drive Security** dialog displays again, Click **Ok**.

## Using the Quarantine View for Gmail

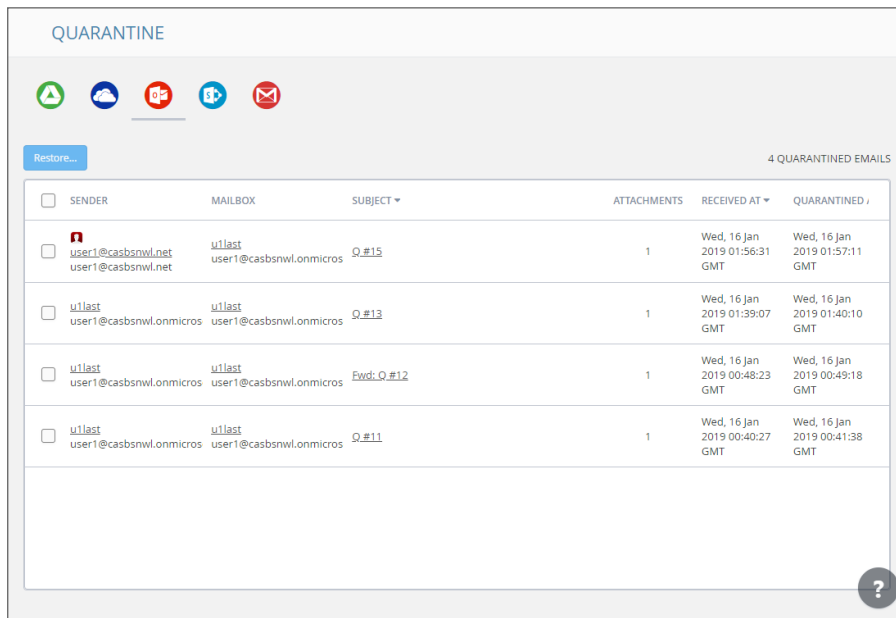
The **Quarantine** view for Gmail provides you with information about the:

- 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

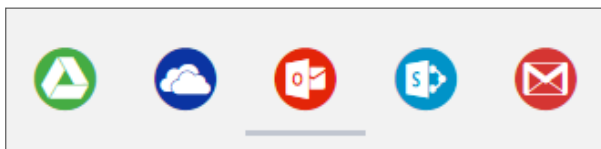
<input type="checkbox"/>	FROM ▾	MAILBOX	SUBJECT ▾	ATTACHMENTS	RECEIVED AT	QUARANTINE
<input type="checkbox"/>	admin@snwlcas1.com	Admin_SNWLCAS2 admin@snwlcas2.com	malware sample	1	Tue, 05 Feb 2019 07:59:16 GMT	Tue, 05 Feb 2019 07:59:45 GMT
<input type="checkbox"/>	admin@snwlcas1.com	Admin_SNWLCAS2 admin@snwlcas2.com	MALWARE (detect and prevent)	1	Tue, 05 Feb 2019 07:46:06 GMT	Tue, 05 Feb 2019 07:46:24 GMT

# 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 G Suite](#)
- [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 dashboard for a quarantined email message titled "Fwd: capture atp test gmail realtime testing". The interface 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 email's history with timestamps and subjects.
- Live event log:** A table detailing security events, such as "Email Body" and "high\_confidence1.xlsm" inspected by SonicWall Cloud Application Security.

Widget	Description
<b>Email Profile</b>	<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 <a href="#">Using the User Dashboard for G Suite</a> for more information.)</p> <p>You can click the <b>Restore from quarantine</b> or <b>Restore Email</b> 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 <b>Advanced options</b> that allow you to recheck the item, or access the raw header or body from the quarantined email message.</p>
<b>Security Stack</b>	<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> <p>Depending on the item and the security tool, you can report that the items has been misclassified as a threat.</p>

Widget	Description
<b>Email attachments</b>	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.
<b>Conversation</b>	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.
<b>Live event log</b>	Detailed list of the events associated with the quarantined email message or file.

## Using the User Dashboard for G Suite

The User Dashboard for G Suite shows you the:

- name and email address of the user for the email message
- application used to send the email message
- user groups to which the user is included
- files shared by the user
- user sharing activity during the past seven days
- the location(s) from where the events associated with this user has occurred
- the real-time list of events associated with this user

The screenshot displays the 'User' dashboard for 'Admin SNWLCAS2' (admin@snwlcas2.com). The dashboard is divided into several sections:

- User info:** Shows the user's profile picture and name/email.
- Application used:** A table with a 'NAME' header.
- User groups:** A table with a 'GROUP' header.
- Files shared:** An empty table.
- User sharing activity:** A line graph showing activity over time from 19-02-13 to 19-03-09. The y-axis ranges from 0 to 1.
- Event map:** A map showing the user's location history, with labels for 'EUROPE', 'AFRICA', and 'Atlantic ocean'.
- Live event log:** A table listing recent events.

DATE/TIME	USER	EVENT	IP	COUNTRY	CITY	DESCRIPTION
Wed, 27 Feb 2019 23:01:54 GMT	Admin SNWLCAS2	login_success	4.78.245.197	United States	San Jose	
Wed, 27 Feb 2019 23:01:54 GMT	Admin SNWLCAS2	login_success	4.78.245.197	United States	San Jose	

# 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:*

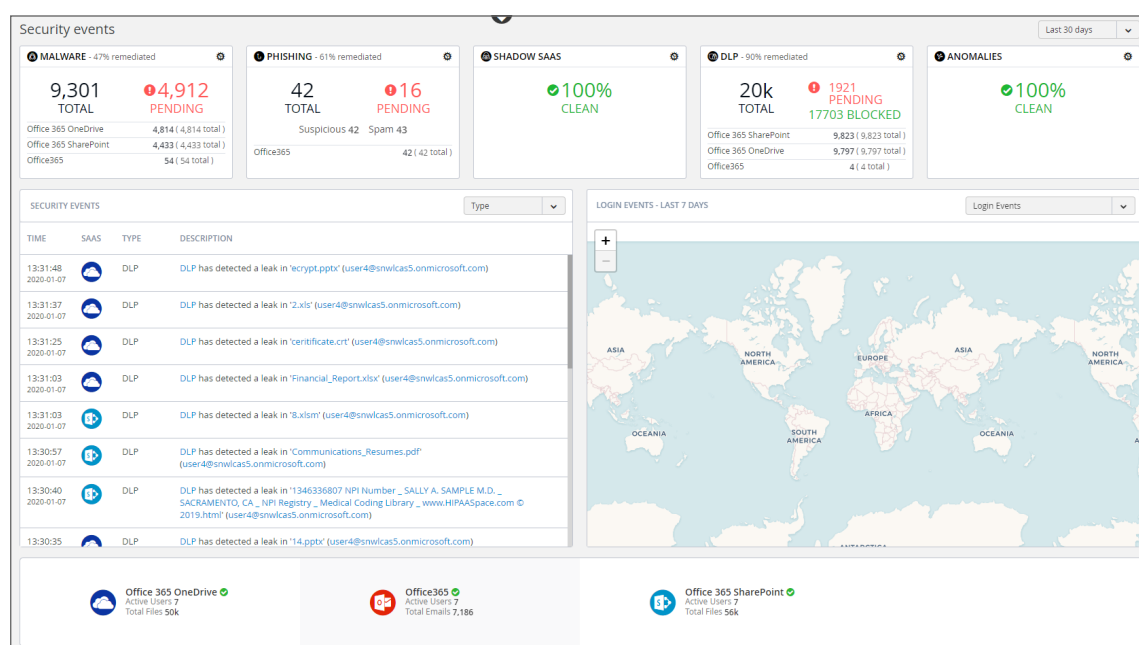
1. Navigate to the **Quarantine** page.
2. From the Quarantined File Creator Dashboard, select the items you want moved out of quarantine.
3. Click the **Restore...** button.
4. When prompted **Are you sure you want to continue?**, click **Ok**.

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



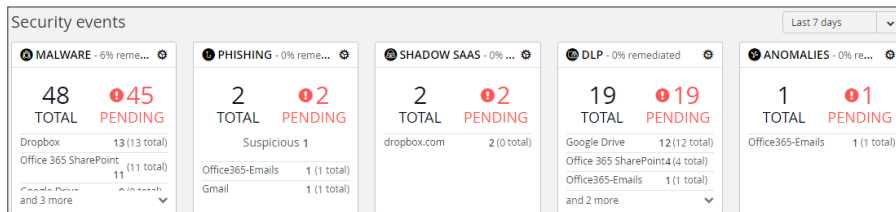
The menu located on the left side is displayed at all times and allows you to navigate between the other Cloud App Security views.

### 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.

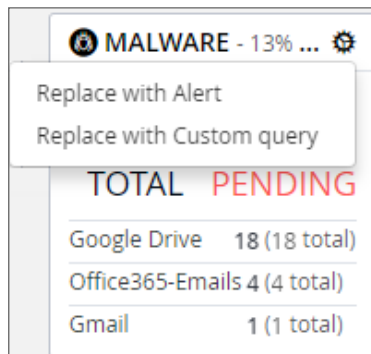
### Topics:

- [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.

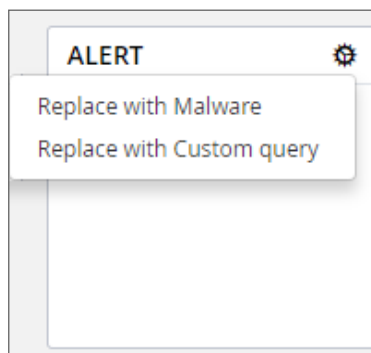


2. From the dropdown list, select:
  - **Replace with Alert**
  - **Replace with Custom query** (Refer to [Creating Custom Query Policies](#) for information on creating custom queries.)

# 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.



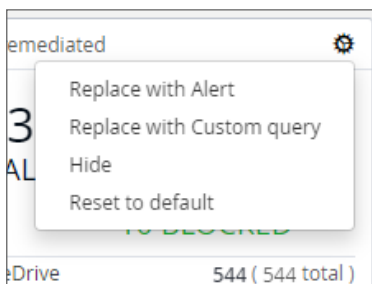
2. From the dropdown list, select the original name of the widget.

# 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.

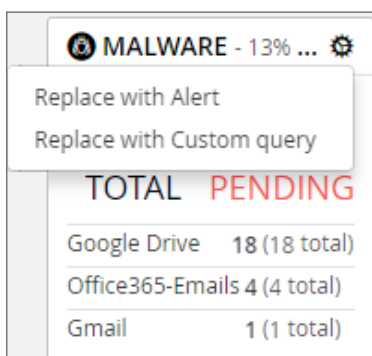


2. From the dropdown list, select **Hide**.

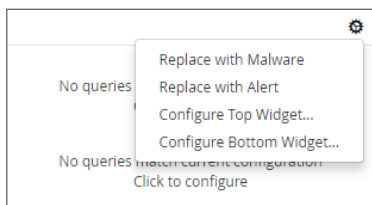
# Configuring Security Event Widget Custom Queries

## 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.

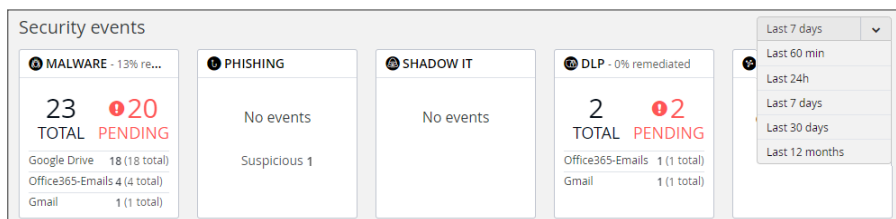


4. Select either:
  - **Configure Top Widget...**
  - **Configure Bottom Widget...**

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.

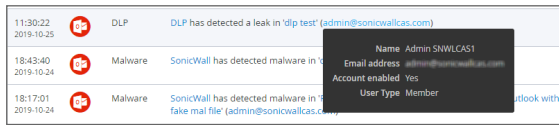
## Viewing the Summary of Security Events

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

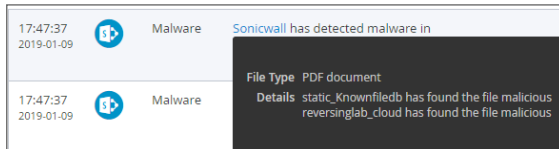
TIME	SAAS	TYPE	DESCRIPTION
05:07:35 2019-01-09		Malware	Sonicwall has detected malware in 'a8c57b6b159dae911e72e34555f0e0f8' ( <a href="#">malware@sonicwall.com</a> )
05:07:34 2019-01-09		Malware	Sonicwall has detected malware in '527b2d1dfe167d33ab4e3ccbade3bd' ( <a href="#">malware@sonicwall.com</a> )
05:07:25 2019-01-09		Malware	Sonicwall has detected malware in 'ffb96a704106fe8c9fad45bc7cc48898' ( <a href="#">malware@sonicwall.com</a> )
05:07:16		Malware	Sonicwall has detected malware in

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

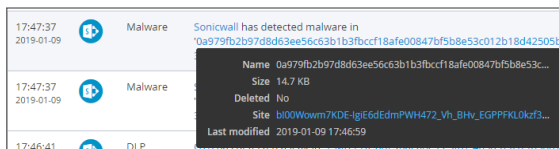
- For files with possible malware or data leaks, see the information about the file, its site of origin, and the action taken:



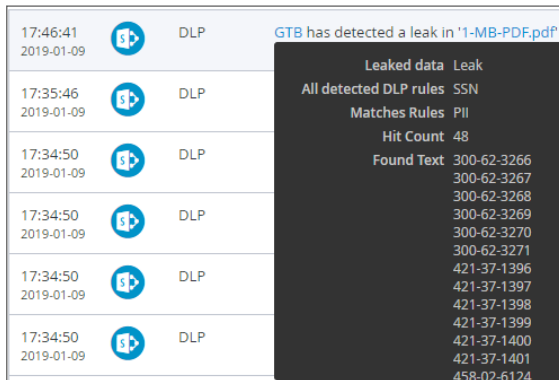
- For documents containing possible malware, see information about the file and the rules that detected it:



- 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.

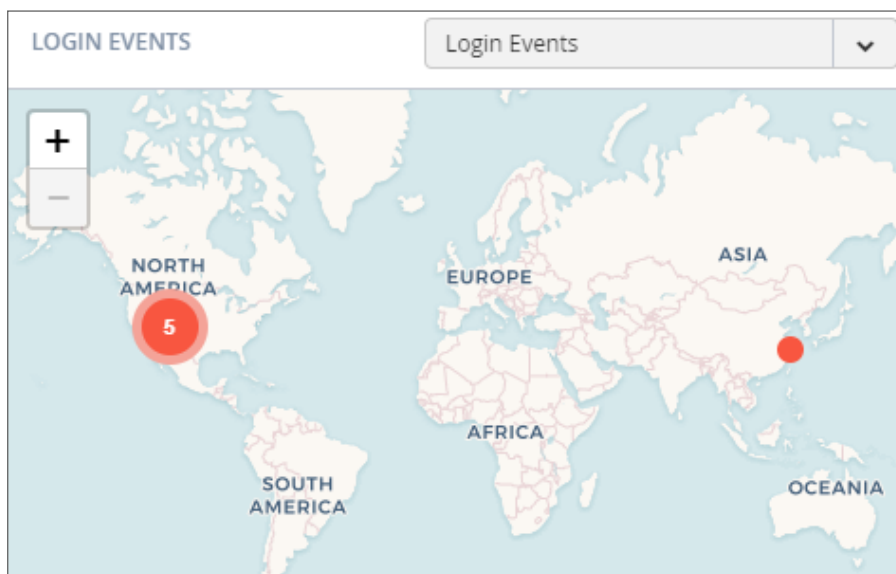
TIME	SAAS	TYPE	DESCRIPTION
09:20:19 2021-02-11		DLP	SmartDLP has detected a leak in 'ENCRYPT: This is a test message for Subject Regex' (mohan@cloudwall.onmicrosoft.com)
10:40:12 2021-02-09		DLP	SmartDLP has detected a leak in 'ENCRYPT: this message dlp test of r (mohan@cloudwall.onmicrosoft.com)
10:39:46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

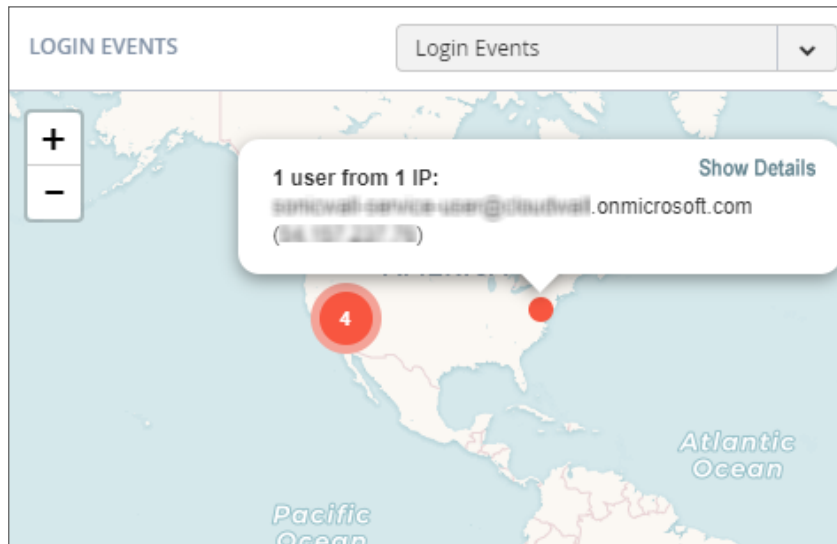
Color	Description
Blue	Many logins from a user from the same IP address
Yellow	Some logins from a user from the same IP address
Red	Few logins from a user from the same IP address

**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:**

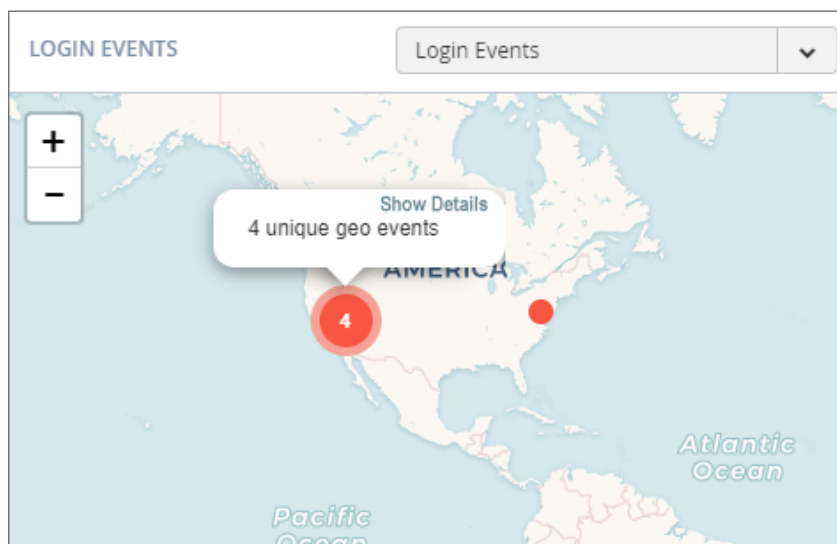
1. Hover the cursor over the login event for which you want to see more information.



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.

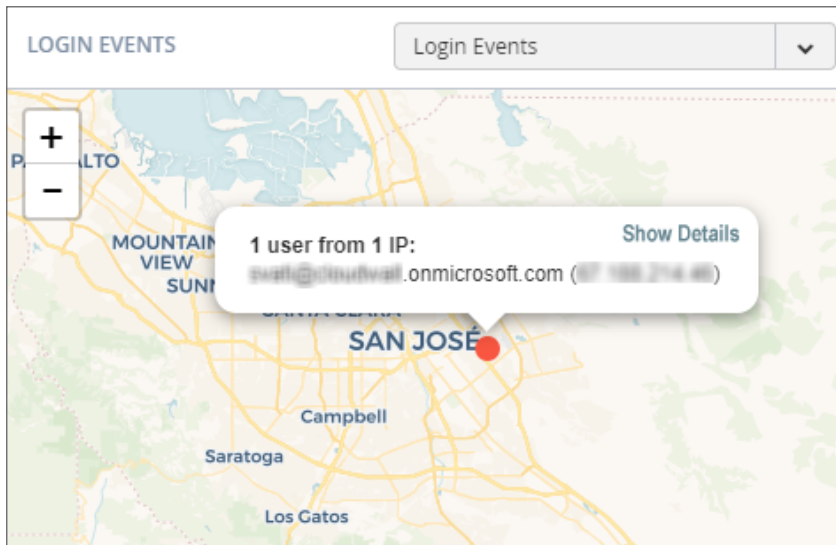
**To view detailed information about multiple login events:**

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).

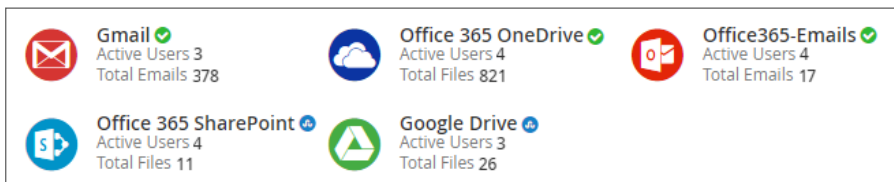
3. Hover the cursor over the specific login event for which you want to see more information.



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



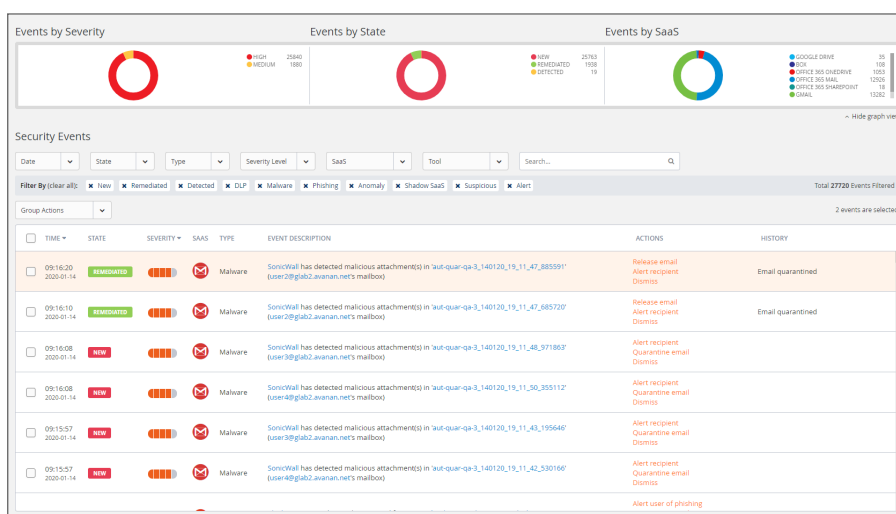
# Viewing the Scanned Files Summary

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

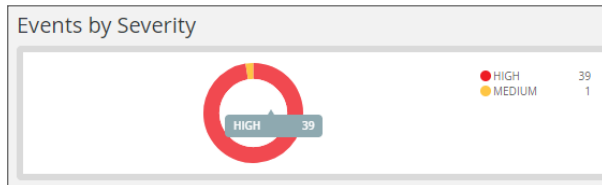
The Security Event Graphs show the security events grouped in different ways.

- [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

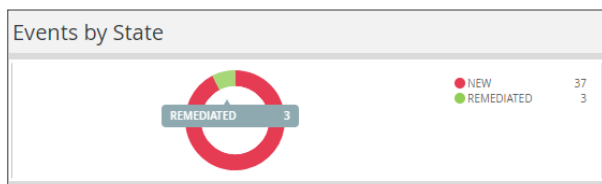
The **Events by Severity** graph displays all of the security events represented by severity.



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

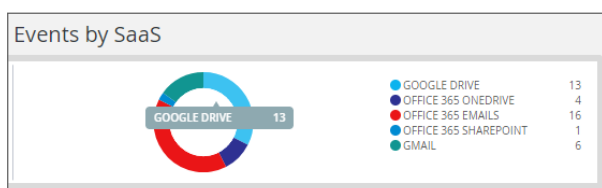
The **Events by State** graph displays all of the security events represented by their state.



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 several filter dropdowns: Date, State, Type, Severity Level, SaaS, and Tool, along with a search bar. Below these, a 'Filter By (clear all):' section shows active filters for New, Remediated, Detected, DLP, Malware, Phishing, Anomaly, Shadow SaaS, Suspicious, and Alert. A 'Total 27720 Events Filtered' indicator is on the right. A 'Group Actions' dropdown is also present, with a note '2 events are selected.' The main table has columns for TIME, STATE, SEVERITY, SaaS, TYPE, EVENT DESCRIPTION, ACTIONS, and HISTORY. It lists several Malware events with their respective states (REMEDIATED, NEW) and actions like 'Release email', 'Alert recipient', 'Quarantine email', and 'Dismiss'.

## SECURITY EVENTS FILTERS AND DESCRIPTIONS

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

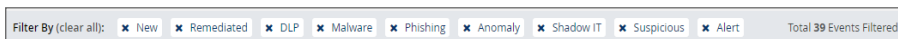
The active filters are displayed above the data listed in the table. Displayed on the far right is the total number of security events that match the filtering criteria.

### 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](#)

# 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 proccessing 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 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.

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**.

## 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 Spamfolder.
  - 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](#).

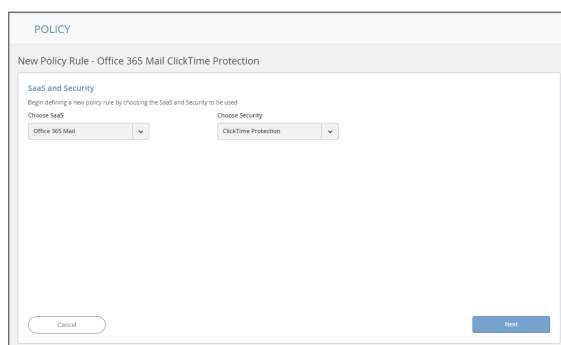
- c. Click **Ok**.
6. In the **Advanced > Alerts** section:
  - a. Select **Send email alert to admin(s) about phishing** to notify administrators when a possible leak is detected.
    - Click the gears icon to modify the email message sent to administrators.
    - Click the users icon to select which 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 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.



# 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
<b>Advertising identifier</b>	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).
<b>Age of an individual</b>	An age measured in months or years.
<b>Credit card number</b>	A credit card number is 12 to 19 digits long. They are used for payment transactions globally.
<b>Credit card track number</b>	A credit card track number is a variable length alphanumeric string. It is used to store key cardholder information.
<b>Date of birth</b>	A date of birth.
<b>Domain name</b>	A domain name as defined by the DNS standard.
<b>Email address</b>	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.
<b>Ethnic group</b>	A person's ethnic group.
<b>Female name</b>	A common female name.
<b>First name</b>	A first name is defined as the first part of a Person Name.
<b>Gender</b>	A person's gender identity.
<b>Generic id</b>	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.
<b>IBAN Americas IBAN Asia IBAN Africa IBAN Europe</b>	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.
<b>HTTP cookie and set-cookie headers</b>	An HTTP cookie is a standard way of storing data on a per website basis. This detector will find headers containing these cookies.

<b>Rule</b>	<b>Description</b>
<b>ICD9 code</b>	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.
<b>ICD10 code</b>	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.
<b>Phone IMEI number</b>	An International Mobile Equipment Identity (IMEI) hardware identifier, used to identify mobile phones.
<b>IP address</b>	An Internet Protocol (IP) address (either IPv4 or IPv6).
<b>Last name</b>	A last name is defined as the last part of a Person Name.
<b>Street addresses and landmarks</b>	A physical address or location.
<b>MAC address</b>	A media access control address (MAC address), which is an identifier for a network adapter.
<b>Local MAC address</b>	A local media access control address (MAC address), which is an identifier for a network adapter.
<b>Male name</b>	A common male name.
<b>Medical term</b>	Terms that commonly refer to a person's medical condition or health.
<b>Organization name</b>	A name of a chain store, business or organization.
<b>Passport Number</b>	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.
<b>Patient information</b>	Detects leaked medical patient information, based on matching health codes and other personal information patterns.

Rule	Description
<b>Person name</b>	A full person name, which can include first names, middle names or initials, and last names.
<b>Phone number</b>	A telephone number.
<b>Street address</b>	A street address.
<b>Bank SWIFT routing number</b>	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.
<b>Date or Time</b>	A date. This rule name includes most date formats, including the names of common world holidays.
<b>Human readable time</b>	A timestamp of a specific time of day, e.g. 9:54 pm.
<b>URL</b>	A Uniform Resource Locator (URL).
<b>Vehicle identification number</b>	A vehicle identification number (VIN) is a unique 17-digit code assigned to every on-road motor vehicle.

## Credentials and Secrets

Rule name	Description
<b>Authentication token</b>	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.
<b>Amazon Web Services credentials</b>	Amazon Web Services account access keys.
<b>Azure JSON web token</b>	Microsoft Azure certificate credentials for application authentication.
<b>HTTP Basic authentication header</b>	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.
<b>Encryption key</b>	An encryption key within configuration, code, or log text.
<b>Google Cloud Platform API key</b>	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
<b>Argentina identity card number</b>	An Argentine Documento Nacional de Identidad (DNI), or national identity card, is used as the main identity document for citizens.

## Australia

Rule name	Description
<b>Australia driver's license number</b>	An Australian driver's license number.
<b>Australia medicare number</b>	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.
<b>Australia passport number</b>	An Australian passport number.
<b>Australia tax file number</b>	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
<b>Belgium National Identity card number</b>	A 12-digit Belgian national identity card number.

## Brazil

Rule name	Description
<b>Brazil individual taxpayer identification number</b>	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
<b>Canada bank account number</b>	A Canadian bank account number.
<b>British Columbia public health network number</b>	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.
<b>Canada driver's license number</b>	A driver's license number for each of the ten provinces in Canada (the three territories are currently not covered).
<b>Ontario health insurance number</b>	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.
<b>Canada passport number</b>	A Canadian passport number.
<b>Quebec health insurance number</b>	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.
<b>Canada social insurance number</b>	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
<b>Ireland Personal Public Service Number (PPSN)</b>	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
<b>Israel identity card number</b>	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
<b>Italy fiscal code number</b>	An Italy fiscal code number is a unique 16-digit code assigned to Italian citizens as a form of identification.

## Japan

Rule name	Description
<b>Japan bank account number</b>	A Japanese bank account number.
<b>Japan driver's license number</b>	A Japanese driver's license number.
<b>Japan individual number or "My Number"</b>	The Japanese national identification number—sometimes referred to as "My Number"—is a new national ID number as of January 2016.
<b>Japan passport number</b>	A Japanese passport number. The passport number consists of two alphabetic characters followed by seven digits.

## Korea

Rule name	Description
<b>Korea passport number</b>	A Korean passport number.
<b>Korea resident registration number</b>	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
<b>Thai national identification card number</b>	The Thai บัตรประจำตัวประชาชนไทย, or identity card, is used as the main identity document for Thai nationals.

## Turkey

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

## United Kingdom

Rule name	Description
<b>Scotland community health index number</b>	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).
<b>United Kingdom drivers license number</b>	A driver's license number for the United Kingdom of Great Britain and Northern Ireland (UK).
<b>United Kingdom national health service number</b>	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.
<b>United Kingdom national insurance number</b>	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.
<b>United Kingdom passport number</b>	A United Kingdom (UK) passport number.
<b>United Kingdom taxpayer reference number</b>	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
<b>American Bankers CUSIP Id</b>	An American Bankers' Committee on Uniform Security Identification Procedures (CUSIP) number is a 9-character alphanumeric code that identifies a North American financial security.
<b>Medical drug names</b>	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).
<b>USA Adoption Taxpayer Identification Number</b>	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.
<b>USA bank routing number</b>	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.
<b>US DEA number</b>	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.
<b>USA drivers license number</b>	A driver's license number for the United States. Format can vary depending on the issuing state.
<b>Employer Identification Number</b>	A United States Employer Identification Number (EIN) is also known as a Federal Tax Identification Number, and is used to identify a business entity.
<b>USA healthcare national provider identifier</b>	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
<b>USA Individual Taxpayer Identification Number</b>	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).
<b>USA passport number</b>	A United States passport number.
<b>USA Preparer Taxpayer Identification Number</b>	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).
<b>US Social Security Number</b>	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.
<b>USA state name</b>	A United States state name.
<b>USA toll free phone number</b>	A US toll-free telephone number.
<b>USA vehicle identification number</b>	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
<b>Uruguay identity card number</b>	A Uruguayan Cédula de Identidad (CDI), or identity card, is used as the main identity document for citizens.

## Venezuela

Rule name	Description
<b>Venezuela identity card number</b>	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](#)
- [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**.

## 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 G Suite 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 Gmail Block-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 Gmail Block-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 Gmail Block-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.

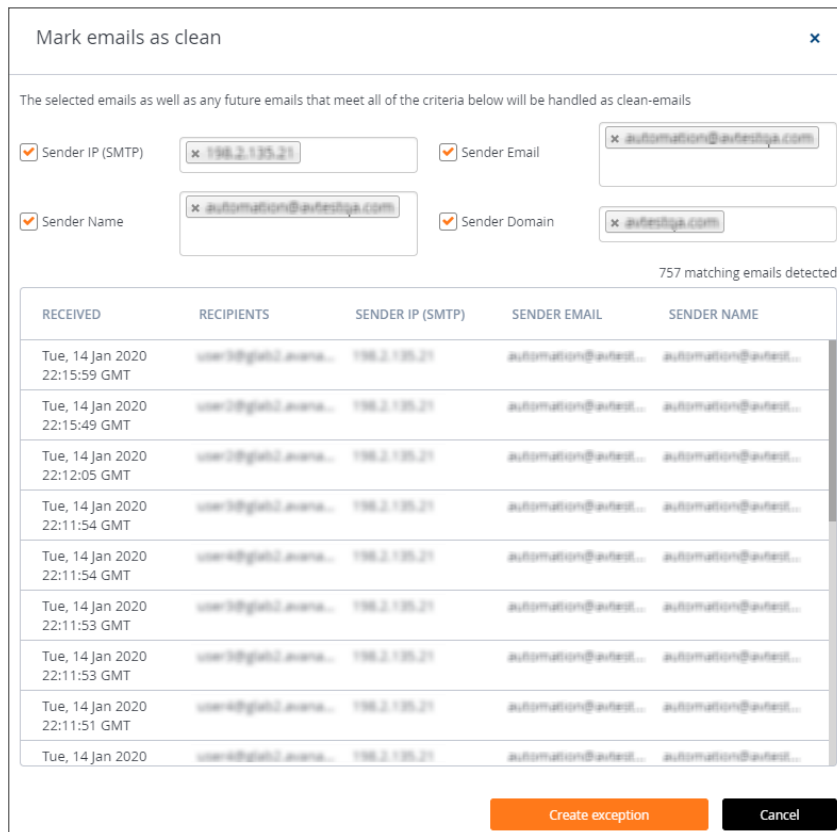
### **Topics:**

- [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...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:15:49 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:12:05 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:54 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:54 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:53 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:53 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020 22:11:51 GMT	user@ghs2.avtest...	198.2.135.21	automation@avtest...	automation@avtest...
Tue, 14 Jan 2020	user@ghs2.avtest...	198.2.135.21	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.

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**.

# 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:

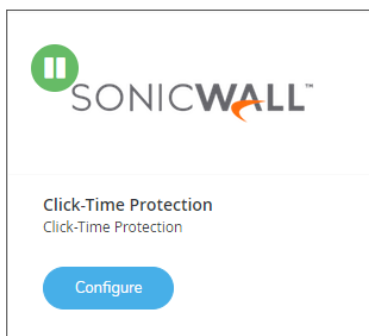
- [Configuring and Using Click-Time Protection](#)

## 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.

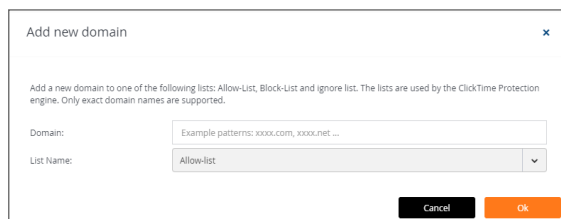
## Topics:

- [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:

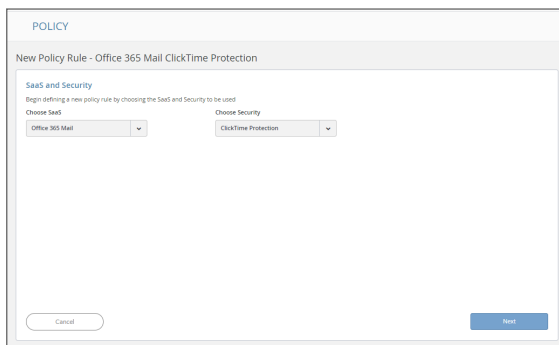
- [Creating Policy Rules for Click-Time Protection](#)
- [Viewing Security Events for Click-Time Protection](#)
- [Managing Email Messages with Click-Time Protection](#)
- [Creating Custom Queries for Click-Time Protection](#)

# 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 Google Drive 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	<b>68</b>
OUTGOING ATTACHMENTS	<b>44</b>
INTERNAL USERS	<b>4</b>
EXTERNAL USERS	<b>18</b>

Office 365 Emails Risk Summary

Security Events

	TOTAL	WEEK	MONTH
MALWARE	<b>22</b>	22	22
PHISHING	<b>6</b>	6	6
SUSPICIOUS PHISHING	<b>5</b>	5	5
SHADOW IT	<b>1</b>	1	1

Scanned Objects

	TOTAL	WEEK	MONTH
ANTI-PHISHING	<b>1</b>	1	1
ADVANCED THREAT PROTECTION	<b>74</b>	74	74
DLP	<b>1</b>	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 ▾

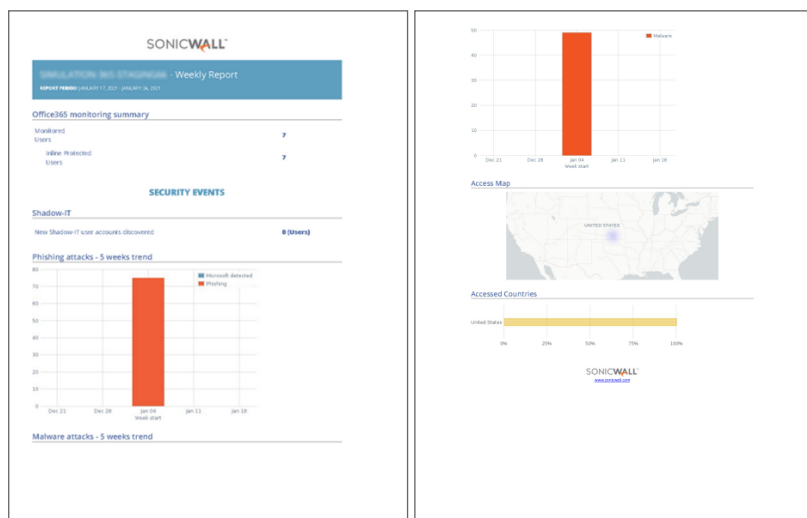
Filter By (clear all):  Last 30 days  Malware  Google Drive  New  Remediated Total 14 Events Filtered

TIME	STATE	SEVERITY	SAAS	TYPE	EVENT DESCRIPTION	ACTIONS	HISTORY
04:52:58 2019-01-16	NEW	HIGH	Malware	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	HIGH	Malware	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	HIGH	Malware	Malware	Sonicwall has detected malware in '1b47baf8d193bace2f3d4e30817c0db4da0c' (Created by user1@casbsnwl.net)	Alert owner of malware Quarantine Dismiss	
23:35:16 2019-01-13	REMEDIATED	HIGH	Malware	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, 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.

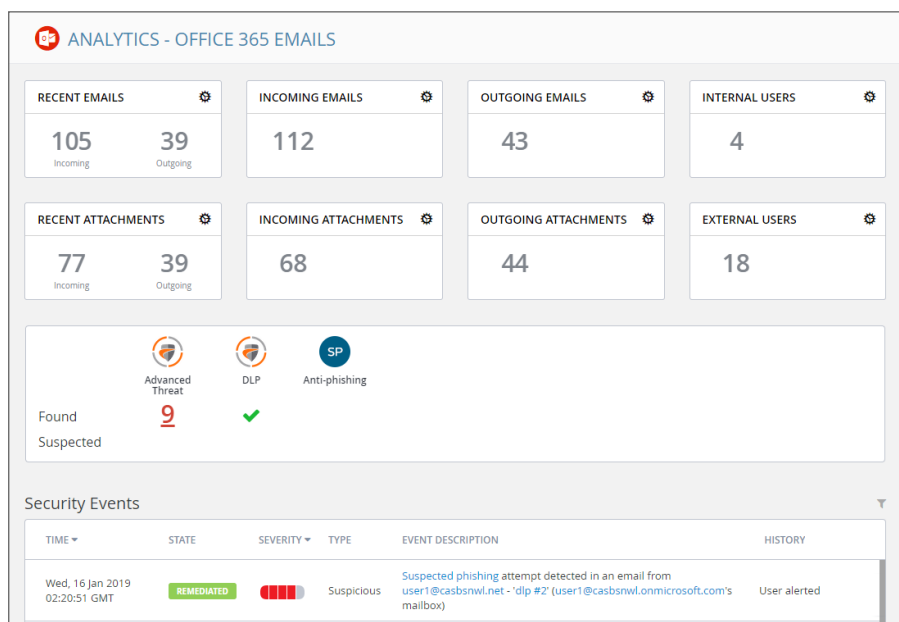
**To access the weekly reports from the Cloud App Security management interface:**

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

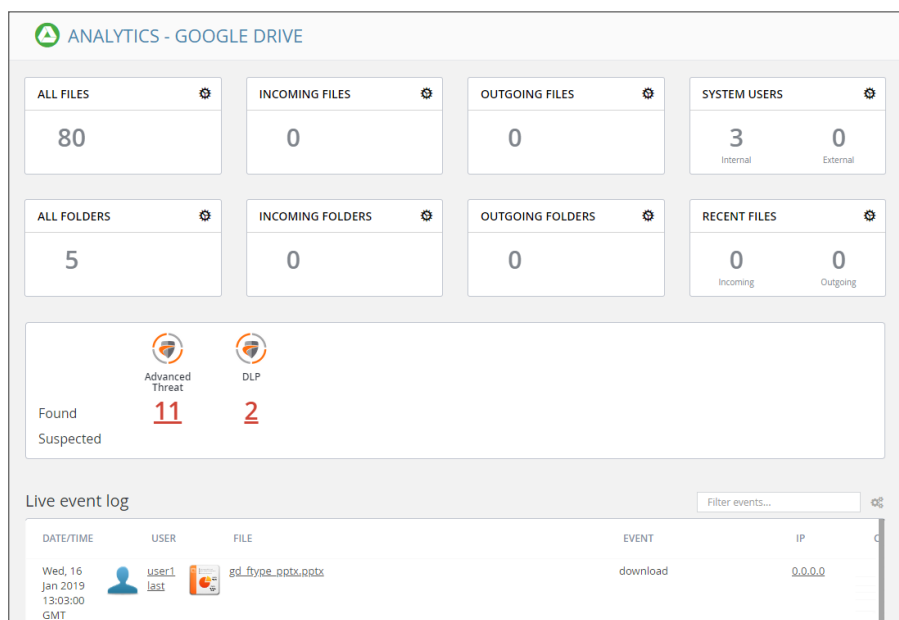
The Analytics for cloud-based email applications provide information about the quantity of emails, attachments, and users.



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

# Viewing Google Drive Analytics

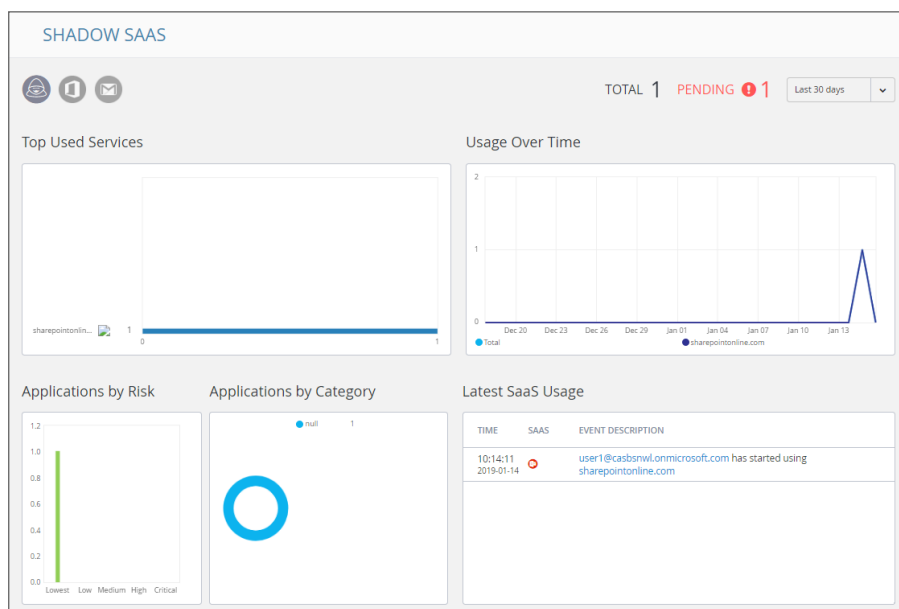
The Analytics for Google Drive provides information about the quantity of files, folders, applications, and security events.



Widget	Description
All Files	The total number of files in your Google Drive.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with people outside the company.
System Users	The number of active users that can access your Google Drive. (This does not include suspended or deleted users).
All Folders	The total number of folders in your Google Drive.
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 Google Drive.
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.
Live Event Log	Detailed list of events in real time.

# Viewing Shadow SaaS Analytics

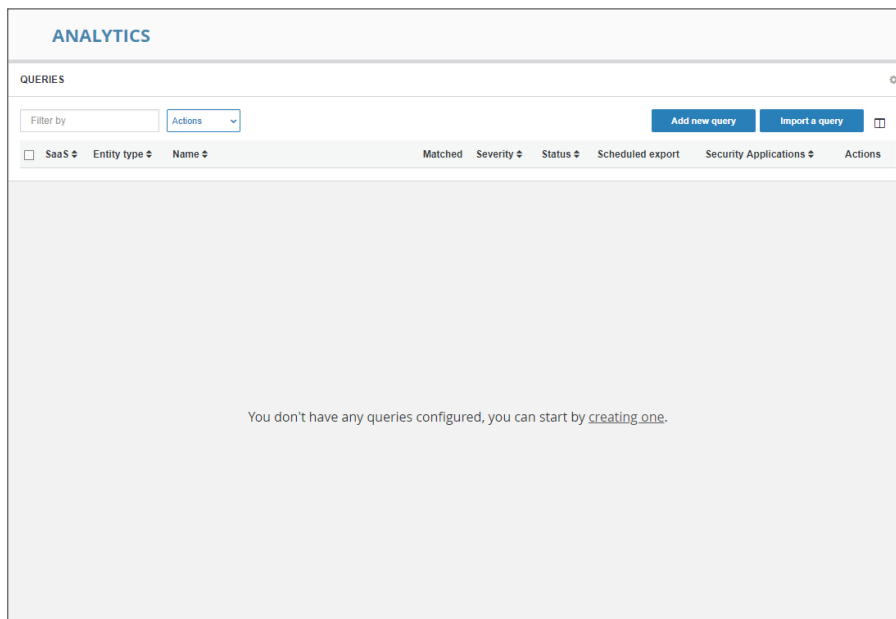
The Analytics for Shadow SaaS provides information about the quantity of files, folders, applications, and security events.



Panel	Description
<b>Top Used Services</b>	The most commonly used cloud applications discovered within your organization
<b>Usage Over Time</b>	The usage pattern of the discovered cloud applications over time
<b>Applications by Risk</b>	The number of discovered cloud applications and their associated risk level
<b>Applications by Category</b>	The number of discovered cloud applications arranged by application category
<b>Latest Cloud Usage</b>	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](#)

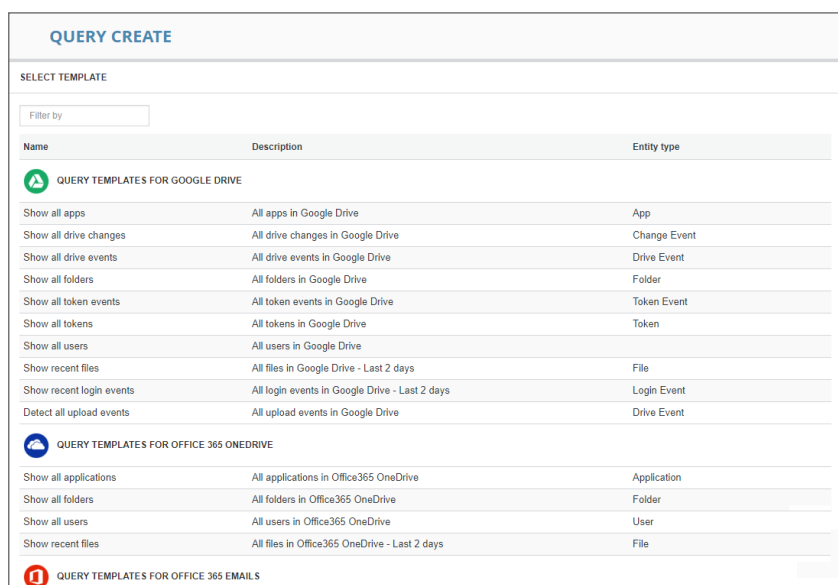


# Creating Custom Queries

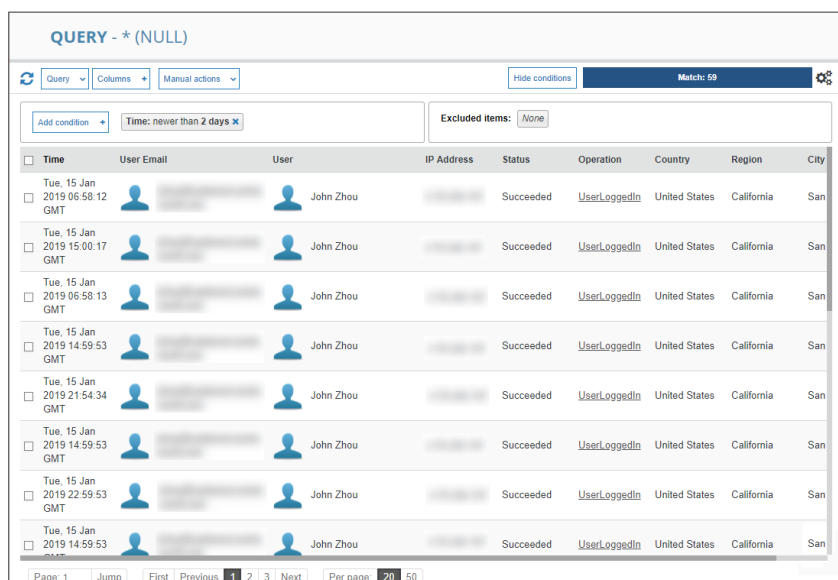
The easiest way to create new custom queries is by basing them on existing templates.

**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.

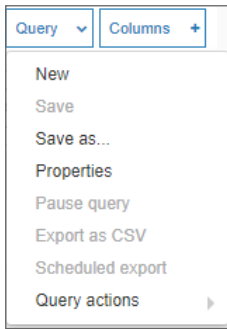


3. Click the query template under the cloud application for which you want to create a query. The results for that query are displayed.



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.

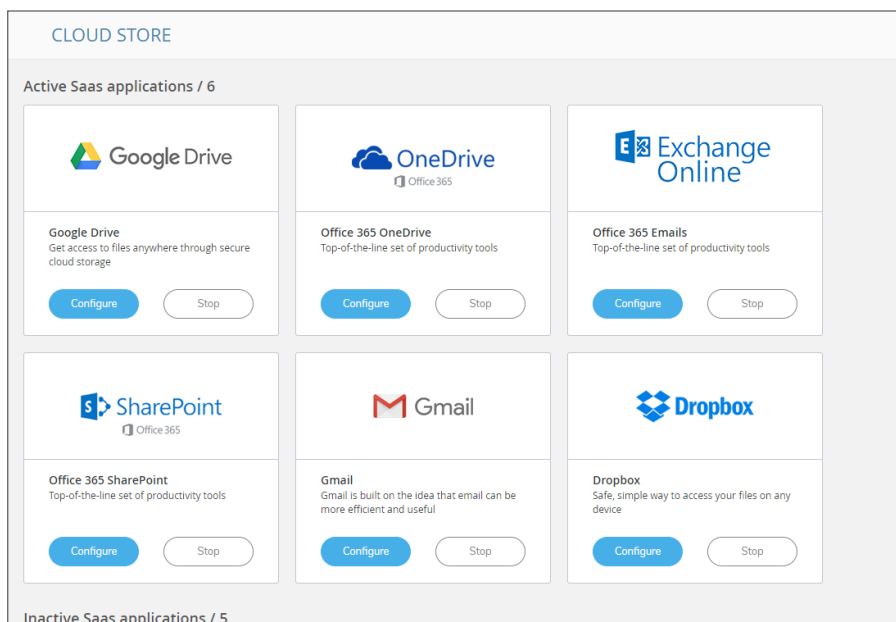


## Adding Custom Queries to the Dashboard

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 G Suite for Cloud App Security](#)
- [Re-Authenticating 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.

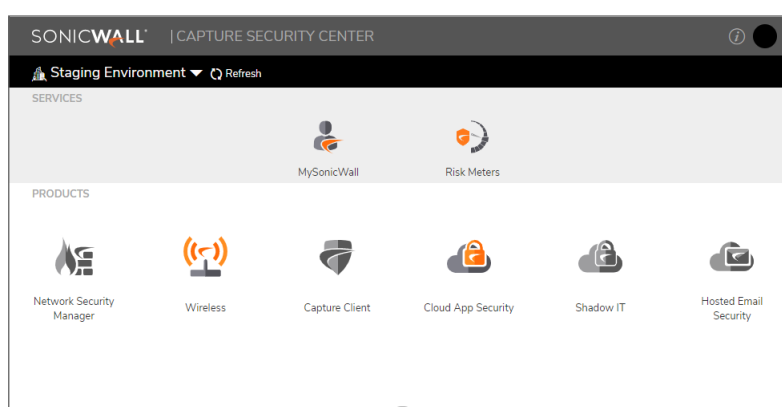
Cloud App Security can secure G Suite applications with these subscription types:

- G Suite Business
- G Suite Enterprise

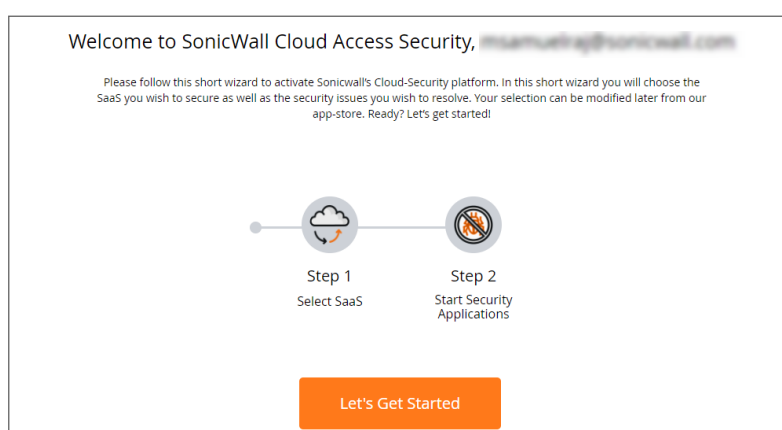
① | **NOTE:** Personal and Home subscription plans are not supported by SonicWall Cloud App Security.

**To activate G Suite applications for Cloud App Security:**

1. Navigate to [cloud.sonicwall.com](https://cloud.sonicwall.com).
2. Login with your **MySonicWall** credentials to get to the Capture Security Center.
3. Click the **Cloud App Security** tile.

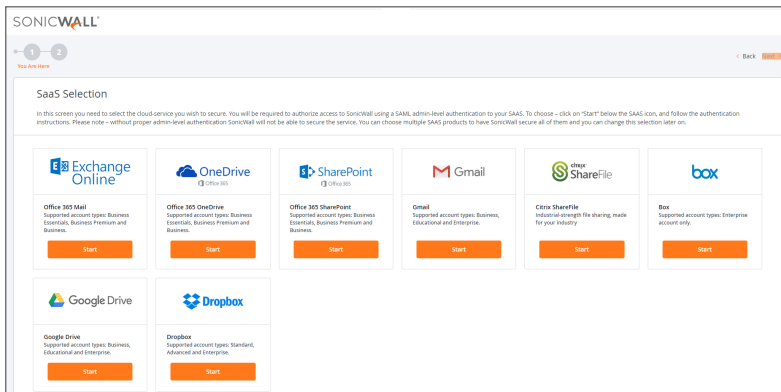


4. The **Welcome to SonicWall Cloud Access Security** page displays.



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.



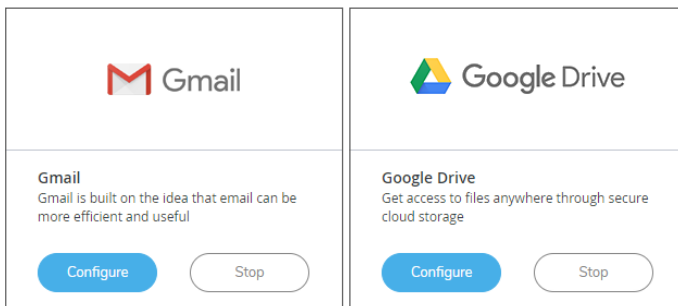
6. Click **Start** on the tile for the G Suite application you want to activate.

For instructions for activating G Suite cloud applications, see: [Activating G Suite Cloud Applications](#).

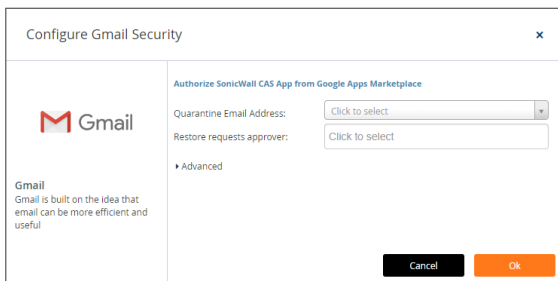
## Configuring G Suite for Cloud App Security

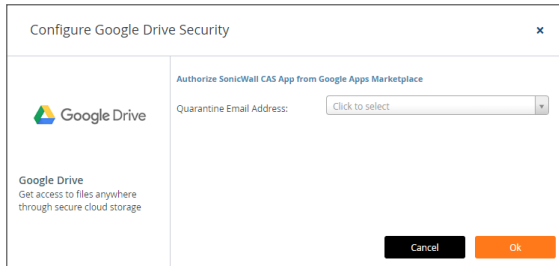
*To configure G Suite for Cloud App Security:*

1. Navigate to the **Configuration > Cloud App Store** page.
2. Click **Configure** on the **G Suite** tile.



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





Most of the settings are related to specifying a quarantine email address and authorized administrators. See [Managing Quarantine for G Suite](#) 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:*

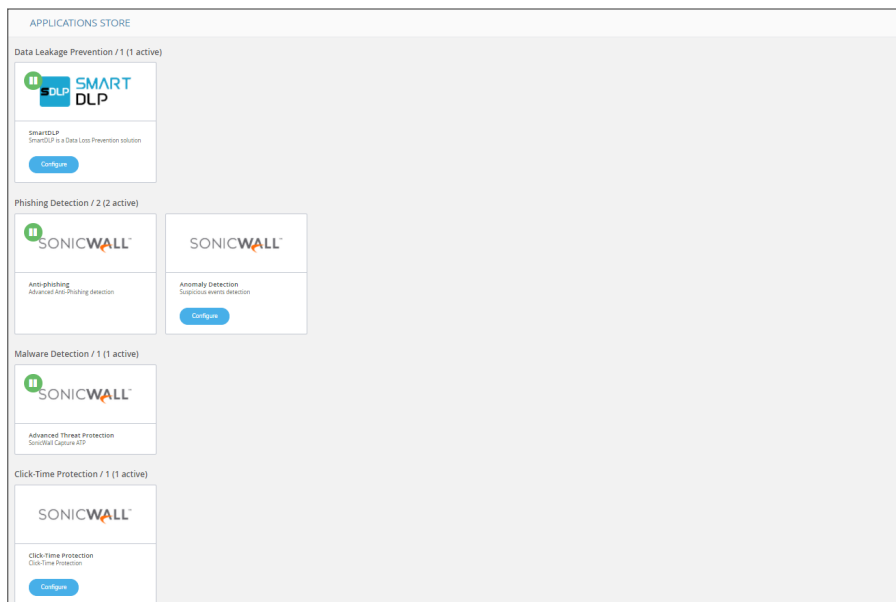
1. Navigate to **Configuration > Cloud App Store**.
2. Click **Configure** on the tile for the cloud application you need to re-authorize.
3. Click the **Re-Authorize SonicWall CAS G Suite** link. The first step in the authorization for the cloud application displays.

For instructions for authorizing specific cloud applications, see [Activating G Suite 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.



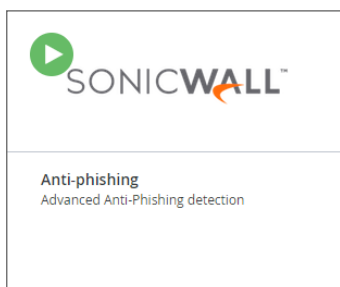
## Topics:

- [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.

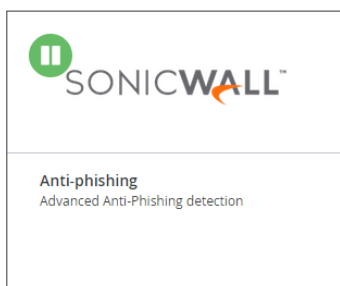


3. When prompted, click **Start** to start the security application.

# 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

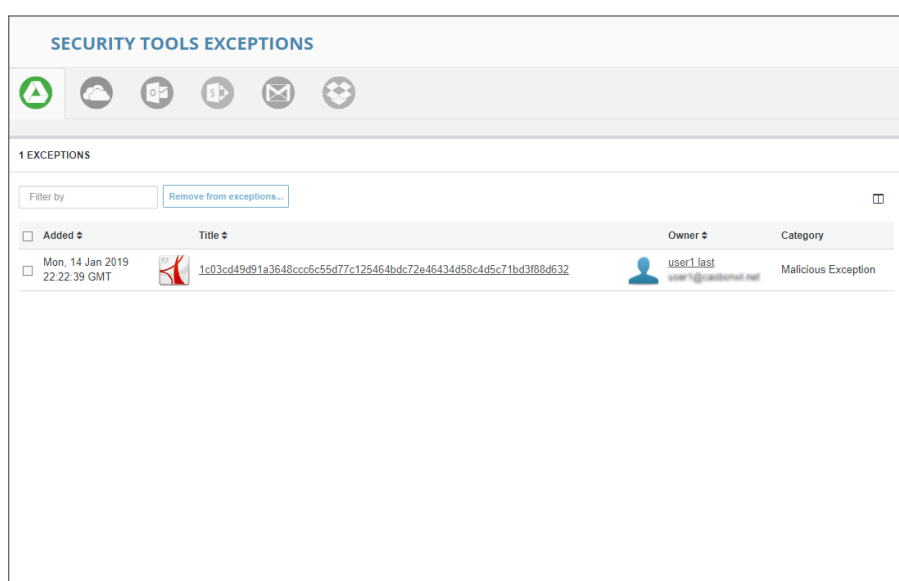
You can send alerts to administrators when anomalies are detected.

## *To configure anomaly notifications:*

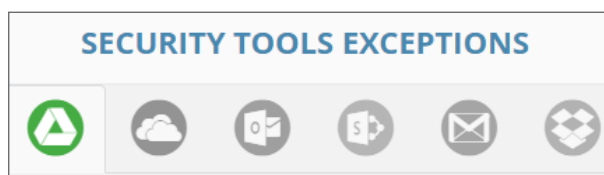
1. Navigate to **Configuration > Security App Store**.
  2. For the security application for which you want to configure anomaly reporting, click **Configure**.
  3. Select **Email anomaly alerts to admins**. This will send email alerts to Cloud App Security administrators.
  4. Click **Ok**.
- ① **NOTE:** 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:*

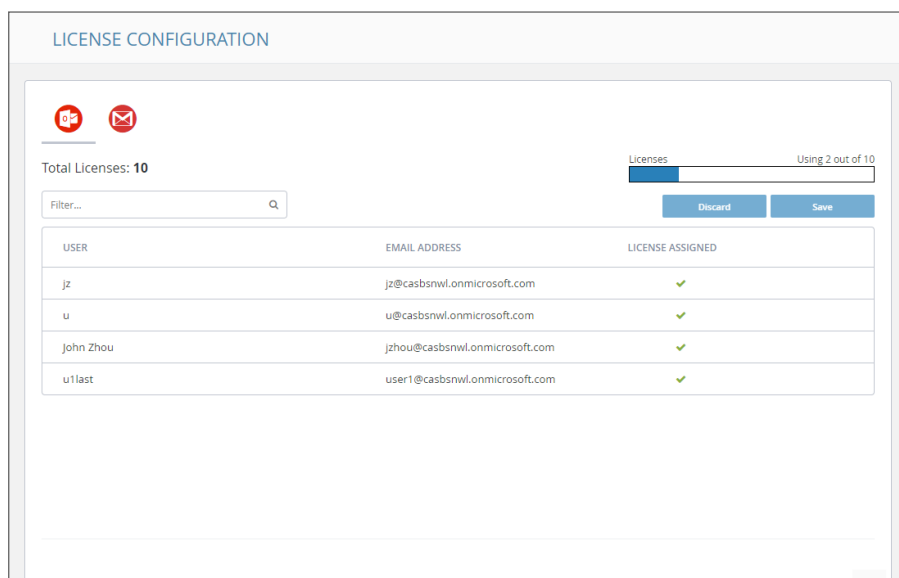
1. Navigate to the **Configuration > System Log** page.
2. Click the **Export as CSV** button on the upper right of the page. The file will be downloaded to your system. Depending on which browser you use, you may be prompted for a location where to save it.

# 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 assignment 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 G Suite 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.
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.

The screenshot shows the 'LICENSE CONFIGURATION' interface. At the top, there are two red circular icons. Below them, it says 'Total Licenses: 10' and 'Using 2 out of 10' with a bar graph. There is a 'Filter...' search box and 'Discard' and 'Save' buttons. The main part of the interface is a table with three columns: 'USER', 'EMAIL ADDRESS', and 'LICENSE ASSIGNED'. The table contains five rows of user data. The row for user 'u' is highlighted in yellow and has a tooltip that says 'Un-assign license (License assigned automatically)'. The other rows have green checkmarks in the 'LICENSE ASSIGNED' column.

USER	EMAIL ADDRESS	LICENSE ASSIGNED
jz	jz@casbsnwl.onmicrosoft.com	Un-assign license (License assigned automatically)
u	u@casbsnwl.onmicrosoft.com	Un-assign license (License assigned automatically)
John Zhou	jzhou@casbsnwl.onmicrosoft.com	✓
u1last	user1@casbsnwl.onmicrosoft.com	✓

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 G Suite  
Updated - May 2021  
232-005369-01 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