Cloud App Security

Administration Guide
for Dropbox

SONICWALL®

Contents

Understanding Cloud App Security

SonicWall Cloud App Security (CAS) offers complete, defense-in-depth security for Dropbox. 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 Dropbox 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 Dropbox 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.

Configuring Cloud App Security

Topics:

Subscribing to Cloud App Security

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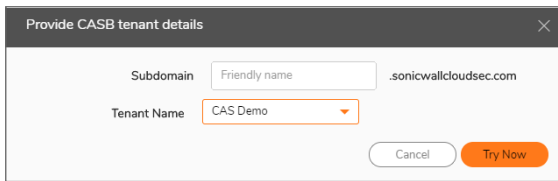
To subscribe to SonicWall Cloud App Security:

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

   ⓘ | **NOTE:** If you do not have a MySonicWall account, you will need to create one.
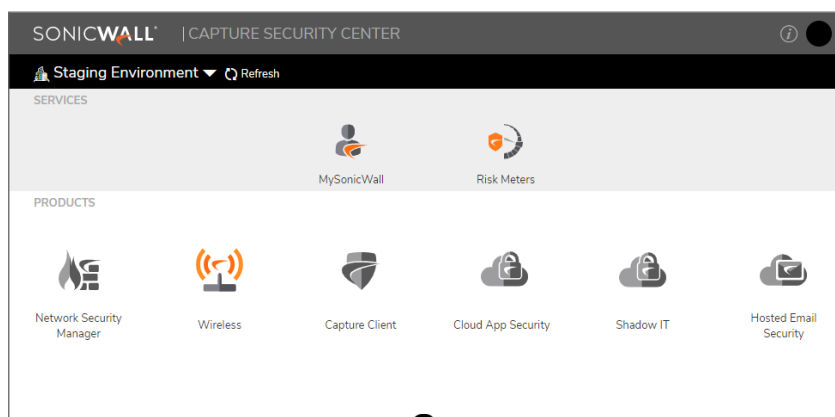
3. Click the **MySonicWall** tile. The MySonicWall dashboard displays.
4. Navigate to **Product Management > My Products**.
5. In the **Quick Register** field, enter your activation key.
6. Click **Register**.

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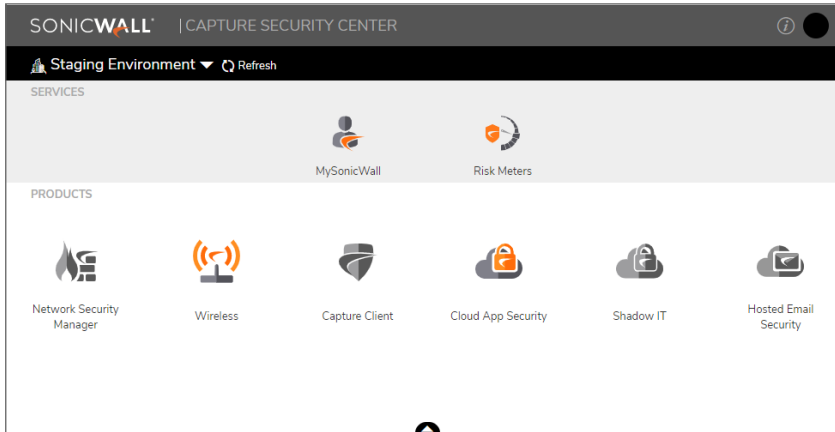
ⓘ | **NOTE:** It may require several minutes for the activation of SonicWall Cloud App Security to complete.

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 Dropbox with these subscription types:

- Dropbox Advanced
- Dropbox Enterprise

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

To activate Dropbox for Cloud App Security:

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

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

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

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

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

6. Click **Start** on the Dropbox tile.

For instructions for activating Dropbox cloud applications, see: Activating Dropbox for Cloud App Security.

Activating Dropbox for Cloud App Security

ⓘ **IMPORTANT:** Only Dropbox Advanced and Dropbox Business accounts are supported by SonicWall Cloud App Security.

To activate Dropbox 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 **Dropbox** tile.

3. Sign into your Dropbox business account to authorize SonicWall Cloud App Security.

4. On the **SaaS Selection** page, verify that a green checkbox appears on the tile for **Dropbox** indicating that the application has been activated for Cloud App Security.

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

6. On the **Dropbox** tile, click **Start** to start the protection of Dropbox using Cloud App Security.

   This begins the process of scanning existing files uploaded during the previous 7 days.

3

Managing Quarantine for Dropbox

Topics:

Setting Up a Quarantine Folder for Dropbox

Before you quarantine files stored in Dropbox, 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 Dropbox tile.
3. Select either:

   - **Create Quarantine folder in the root directory** to create a quarantine folder in the top-level directory of your Dropbox.
   - **Quarantine to existing directory** to quarantine files to an existing folder.

     ⓘ | **NOTE:** This folder must already exist as it cannot be created during this process.

4. In the **Select Quarantine Path** dropdown list, select the folder you want to designate as the quarantine folder.
5. Click **Ok**.

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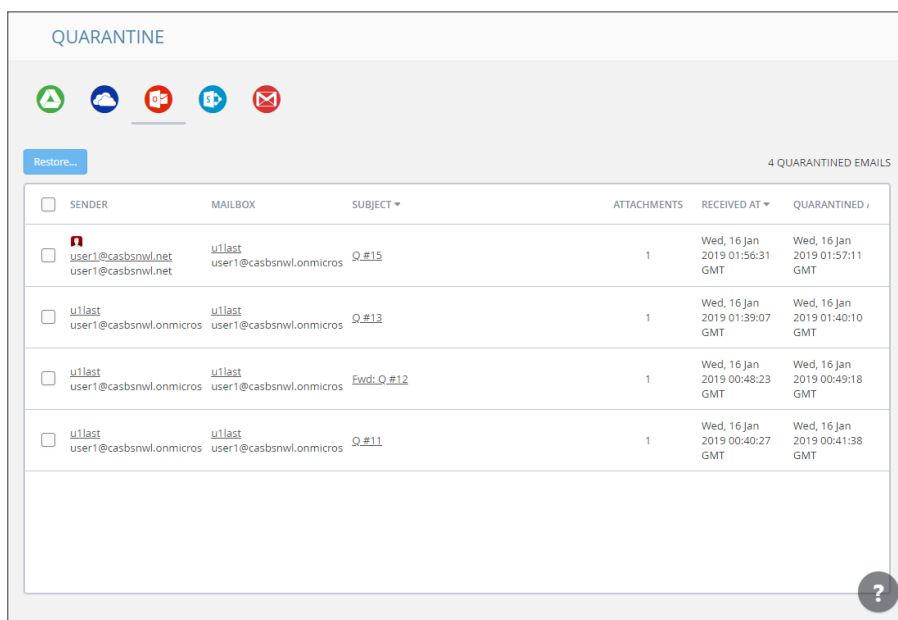
You can switch between the quarantined items for each cloud application by clicking on the icon for the application on the upper left of the page.
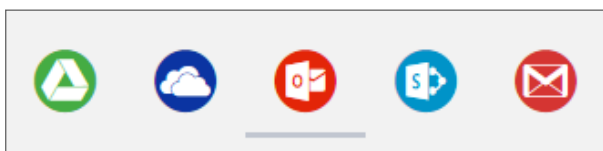
Topics:

- Managing Quarantine for Cloud Storage
- Using the Quarantined File Creator Dashboard
- Using the User Dashboard for Dropbox
- 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.

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

Managing Quarantine for Dropbox

Topics:

- Setting Up a Quarantine Folder for Dropbox
- Using the Quarantined File Creator Dashboard
- Using the User Dashboard for Dropbox

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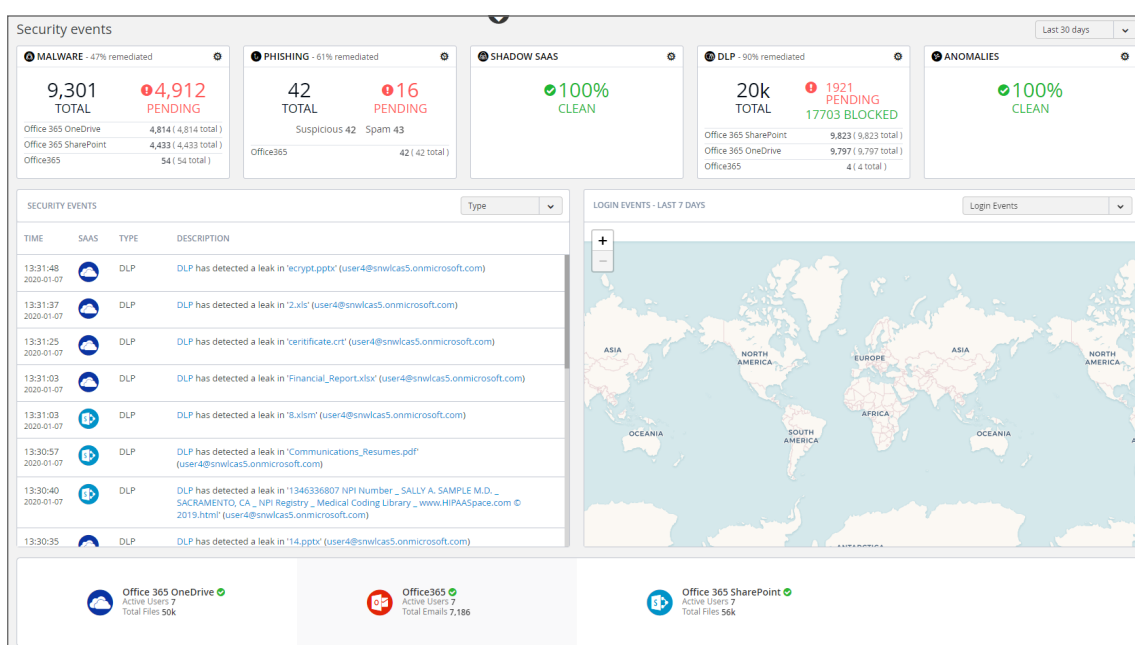
The Dashboard provides you with a summary of all of your secured cloud application with:

- 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.
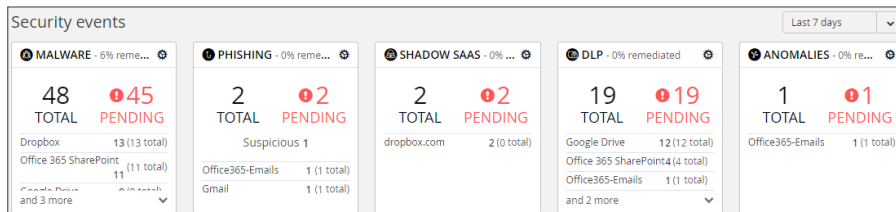
The numbers in each widget designate:

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.
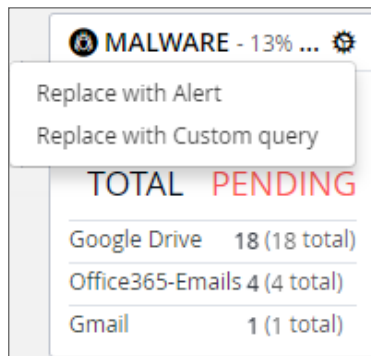
2. From the dropdown list, select:

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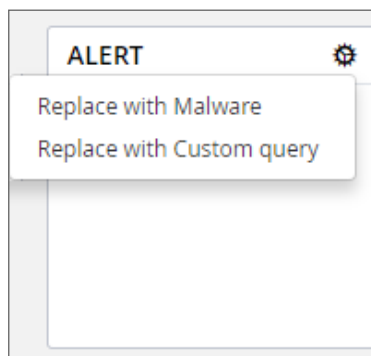
2. From the dropdown list, select the original name of the widget.

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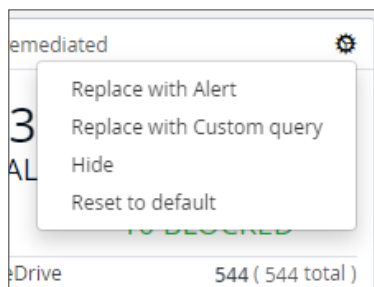
2. From the dropdown list, select **Hide**.

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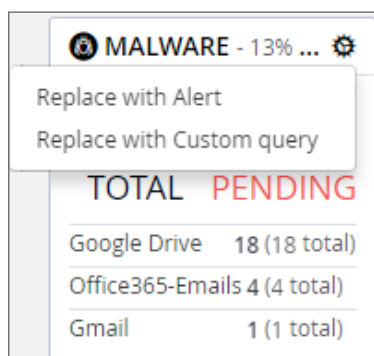
2. From the dropdown list, select **Replace with Custom query**.
3. Click the gear icon again.
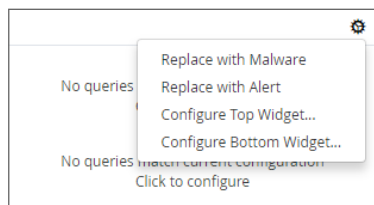
4. Select either:

   - **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.
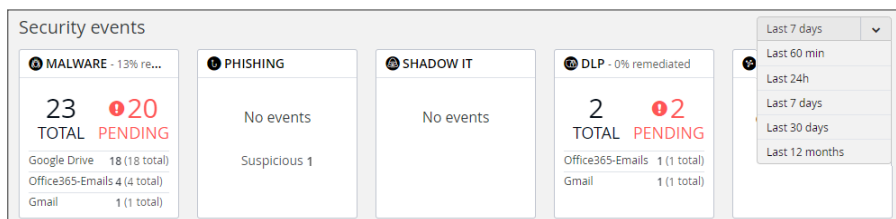
To adjust the time scale for the security events:

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.

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:
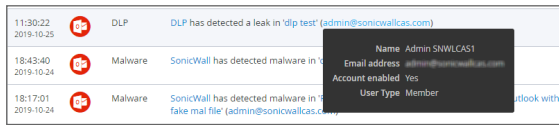
- For documents containing possible malware, see information about the file and the rules that detected it:
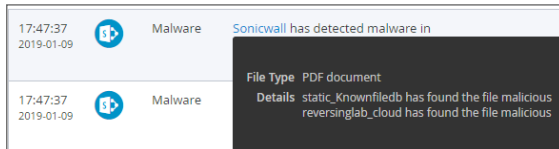
- For websites containing possible malware, see the information about the website and the action taken:
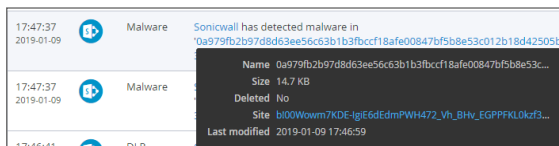
- For a data leak, see the information found and its possible type:
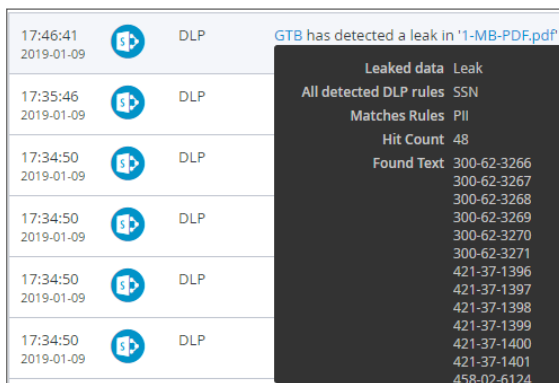
Clicking on the security event item itself will display it on the Events page, with the selected security event highlighted. (See Managing Security Events for more information.)

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.

Viewing Login Events

With geo-location tracking, Login Events are globally mapped and identified using their IP address.
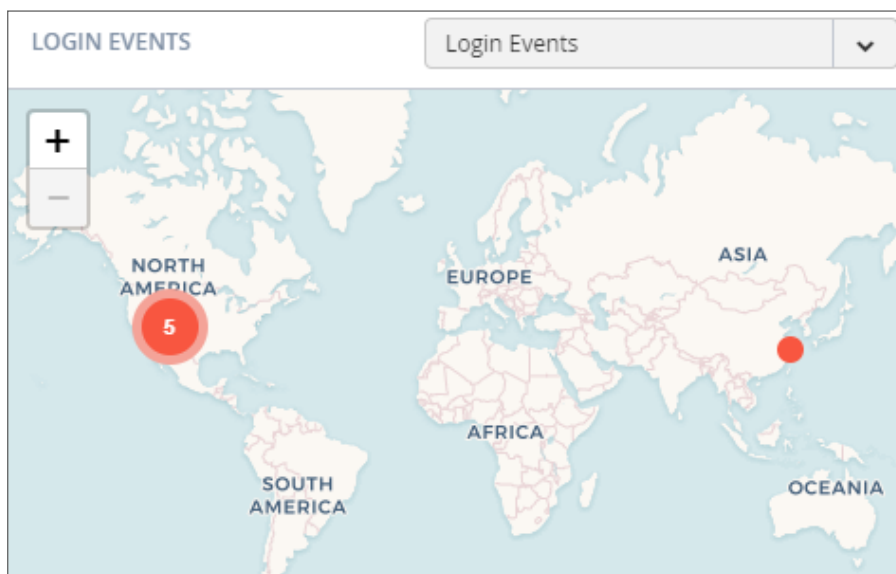
The color of the numerical indicator provides information about the number of occurrences from the same user logins from a specific IP address.

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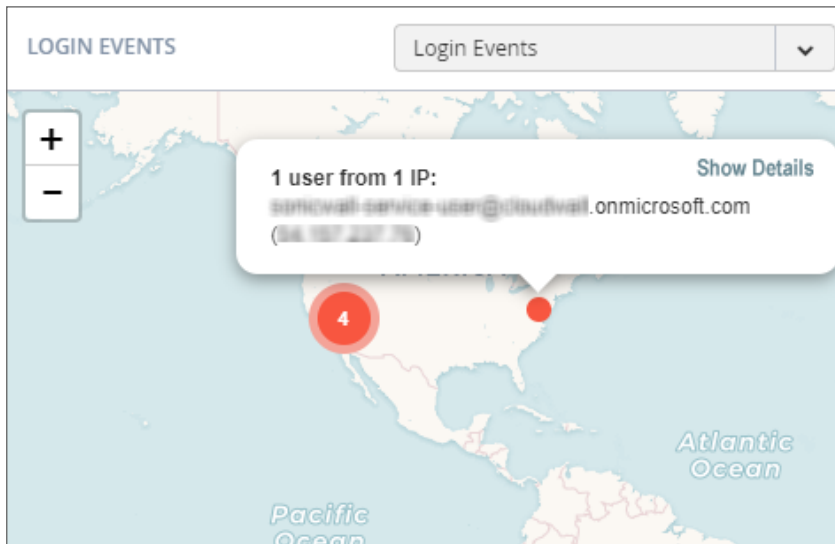
2. A popup displays that contains the email and IP address of the user at that location.
3. You can click **Show Details** to view more detailed information about the login event.

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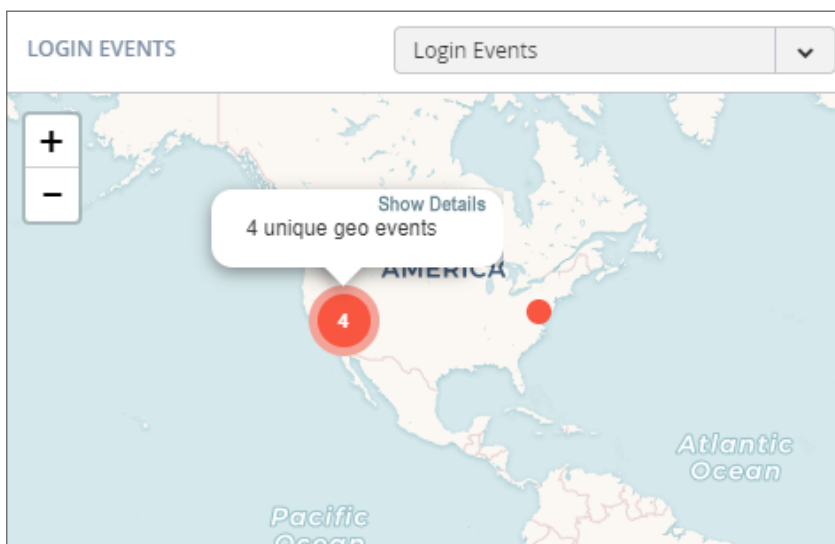
2. Click on the number until you see only single login events (shown without a number).

3. Hover the cursor over the specific login event for which you want to see more information.
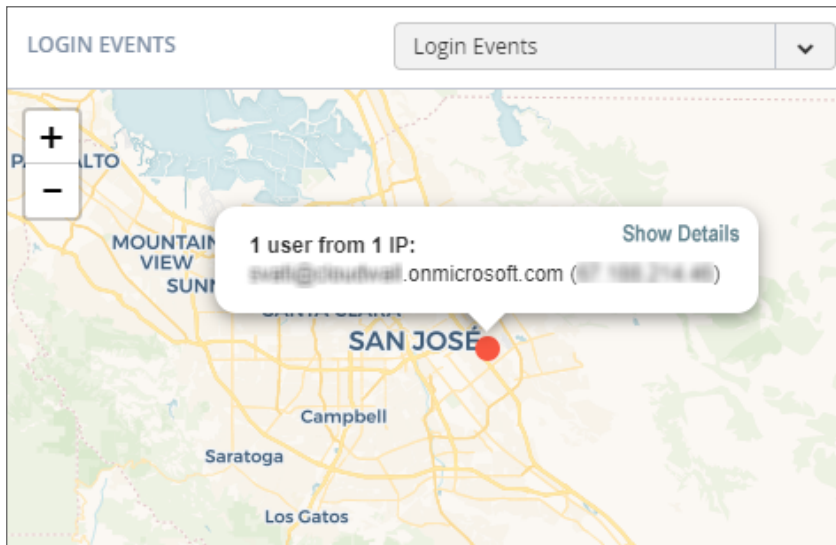
4. You can click **Show Details** to view more detailed information about the login event.

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.
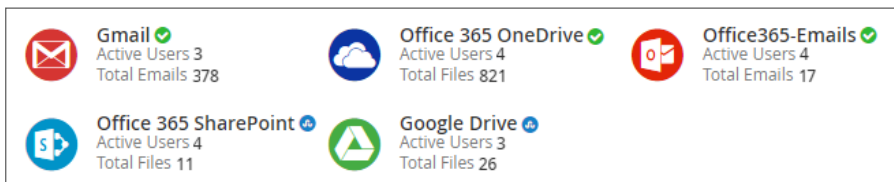
You can:

- click on the application icon or name to view the Analytics for that could 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 in 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.
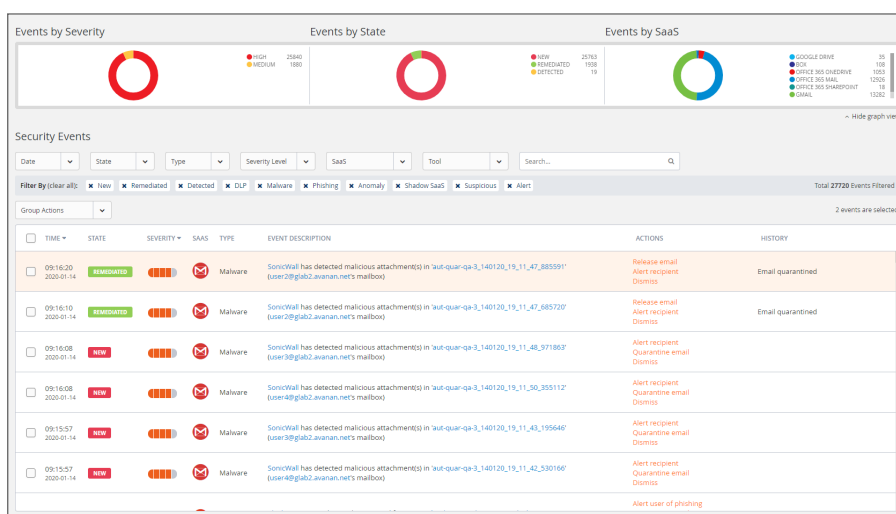
Topics:

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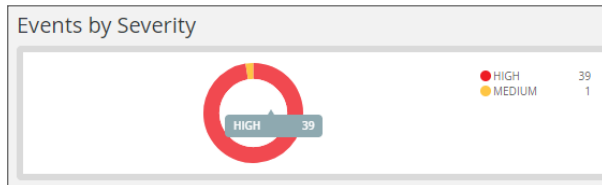
Hover over sections of the graphics to see the detailed information about that section, including the number of security events that occurred with that severity.

Viewing Security Events by State

The **Events by State** graph displays all of the security events represented by their state.
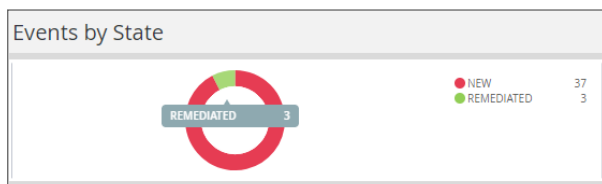
Hover over sections of the graphics to see the detailed information about that section, including the number of security events with that state.

Viewing Security Events by Cloud Application

The **Events by SaaS** graph displays all of the security events represented each active cloud application.
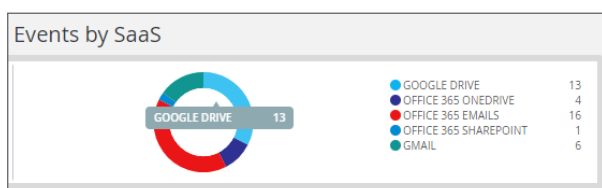
Hover over sections of the graphics to see the detailed information about that section, including the number of security events that occurred for that cloud application.

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.

SECURITY EVENTS FILTERS AND DESCRIPTIONS

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

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

Topics:

- Removing Filters
- Acting on Security Events

Removing Filters

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

Filter By (clear all): x New x Remediated x DLP x Malware x Phishing x Anomaly x Shadow IT x Suspicious x Alert — Total **39** Events Filtered
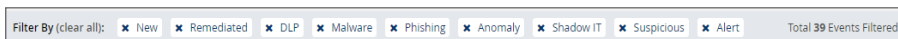
Acting on Security Events

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.

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

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.

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 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)

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.

      ⓘ **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 that 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. 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.

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

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 > 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 **Ok**.

5. In the **Advanced > Alerts** section:

   a. 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.

   b. 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.

   c. 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.

6. Click **Save and Apply**.

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

ⓘ **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-it 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 exfiltration 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)

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.

ⓘ **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 that 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. 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.

7. 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.

   ⓘ | **NOTE:** If two vertical white bars are visible in the green circle on the top left of the SmartDLP tile, then the SmartDLP security application is already currently running and does not need to be restarted.

Predefined Data Leak Protection Policy Rules

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

- Global Rules
- Credentials and Secrets

SmartDLP also provides many predefined Data Leak Protection policy rules for many specific countries and regions.

Global Rules

Rule	Description
Advertising identifier	Identifiers used by developers to track users for advertising purposes. These include Google Play Advertising IDs, Amazon Advertising IDs, Apple's identifierForAdvertising (IDFA), and Apple's identifierForVendor (IDFV).
Age of an individual	An age measured in months or years.
Credit card number	A credit card number is 12 to 19 digits long. They are used for payment transactions globally.
Credit card track number	A credit card track number is a variable length alphanumeric string. It is used to store key cardholder information.
Date of birth	A date of birth.
Domain name	A domain name as defined by the DNS standard.

Rule	Description
Email address	An email address identifies the mailbox that emails are sent to or from. The maximum length of the domain name is 255 characters, and the maximum length of the local-part is 64 characters.
Ethnic group	A person's ethnic group.
Female name	A common female name.
First name	A first name is defined as the first part of a Person Name.
Gender	A person's gender identity.
Generic id	Alphanumeric and special character strings that may be personally identifying but do not belong to a well-defined category, such as user IDs or medical record numbers.
IBAN Americas **IBAN Asia** **IBAN Africa** **IBAN Europe**	An International Bank Account Number (IBAN) is an internationally agreed-upon method for identifying bank accounts defined by the International Standard of Organization (ISO) 13616:2007 standard. The European Committee for Banking Standards (ECBS) created ISO 13616:2007. An IBAN consists of up to 34 alphanumeric characters, including elements such as a country code or account number.
HTTP cookie and set- cookie headers	An HTTP cookie is a standard way of storing data on a per website basis. This detector will find headers containing these cookies.
ICD9 code	The International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) lexicon is used to assign diagnostic and procedure codes associated with inpatient, outpatient, and physician office use in the United States. The US National Center for Health Statistics (NCHS) created the ICD-9-CM lexicon. It is based on the ICD-9 lexicon, but provides for more morbidity detail. The ICD-9-CM lexicon is updated annually on October 1.
ICD10 code	Like ICD-9-CM codes, the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) lexicon is a series of diagnostic codes. The World Health Organization (WHO) publishes the ICD-10-CM lexicon to describe causes of morbidity and mortality.
Phone IMEI number	An International Mobile Equipment Identity (IMEI) hardware identifier, used to identify mobile phones.

Rule	Description
IP address	An Internet Protocol (IP) address (either IPv4 or IPv6).
Last name	A last name is defined as the last part of a Person Name.
Street addresses and landmarks	A physical address or location.
MAC address	A media access control address (MAC address), which is an identifier for a network adapter.
Local MAC address	A local media access control address (MAC address), which is an identifier for a network adapter.
Male name	A common male name.
Medical term	Terms that commonly refer to a person's medical condition or health.
Organization name	A name of a chain store, business or organization.
Passport Number	A passport number that matches passport numbers for the following countries: Australia, Canada, China, France, Germany, Japan, Korea, Mexico, The Netherlands, Poland, Singapore, Spain, Sweden, Taiwan, United Kingdom, and the United States.
Patient information	Detects leaked medical patient information, based on matching health codes and other personal information patterns.
Person name	A full person name, which can include first names, middle names or initials, and last names.
Phone number	A telephone number.
Street address	A street address.
Bank SWIFT routing number	A SWIFT code is the same as a Bank Identifier Code (BIC). It's a unique identification code for a particular bank. These codes are used when transferring money between banks, particularly for international wire transfers. Banks also use the codes for exchanging other messages.
Date or Time	A date. This rule name includes most date formats, including the names of common world holidays.
Human readable time	A timestamp of a specific time of day, e.g. 9:54 pm.
URL	A Uniform Resource Locator (URL).
Vehicle identification number	A vehicle identification number (VIN) is a unique 17-digit code assigned to every on-road motor vehicle.

Credentials and Secrets

Rule name	Description
Authentication token	An authentication token is a machine-readable way of determining whether a particular request has been authorized for a user. This detector currently identifies tokens that comply with OAuth or Bearer authentication.
Amazon Web Services credentials	Amazon Web Services account access keys.
Azure JSON web token	Microsoft Azure certificate credentials for application authentication.
HTTP Basic authentication header	A basic authentication header is an HTTP header used to identify a user to a server. It is part of the HTTP specification in RFC 1945, section 11.
Encryption key	An encryption key within configuration, code, or log text.
Google Cloud Platform API key	Google Cloud API key. An encrypted string that is used when calling Google Cloud APIs that don't need to access private user data.

Predefined Data Leak Protection Rules for Specific Countries

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

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

Argentina

Rule name	Description
Argentina identity card number	An Argentine Documento Nacional de Identidad (DNI), or national identity card, is used as the main identity document for citizens.

Australia

Rule name	Description
Australia driver's license number	An Australian driver's license number.
Australia medicare number	A 9-digit Australian Medicare account number is issued to permanent residents of Australia (except for Norfolk island). The primary purpose of this number is to prove Medicare eligibility to receive subsidized care in Australia.
Australia passport number	An Australian passport number.
Australia tax file number	An Australian tax file number (TFN) is a number issued by the Australian Tax Office for taxpayer identification. Every taxpaying entity, such as an individual or an organization, is assigned a unique number.

Belgium

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

Brazil

Rule name	Description
Brazil individual taxpayer identification number	The Brazilian Cadastro de Pessoas Físicas (CPF) number, or Natural Persons Register number, is an 11-digit number used in Brazil for taxpayer identification.

Canada

Rule name	Description
Canada bank account number	A Canadian bank account number.

Rule name	Description
British Columbia public health network number	The British Columbia Personal Health Number (PHN) is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of British Columbia.
Canada driver's license number	A driver's license number for each of the ten provinces in Canada (the three territories are currently not covered).
Ontario health insurance number	The Ontario Health Insurance Plan (OHIP) number is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of Ontario.
Canada passport number	A Canadian passport number.
Quebec health insurance number	The Québec Health Insurance Number (also known as the RAMQ number) is issued to citizens, permanent residents, temporary workers, students, and other individuals who are entitled to health care coverage in the Province of Québec.
Canada social insurance number	The Canadian Social Insurance Number (SIN) is the main identifier used in Canada for citizens, permanent residents, and people on work or study visas. With a Canadian SIN and mailing address, one can apply for health care coverage, driver's licenses, and other important services.

Chile

Rule name	Description
Chile identity card number	A Chilean Cédula de Identidad (CDI), or identity card, is used as the main identity document for citizens.

China

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

Columbia

Rule name	Description
Colombia identity card number	A Colombian Cédula de Ciudadanía (CDC), or citizenship card, is used as the main identity document for citizens.

Denmark

Rule name	Description
Denmark CPR Number	A Personal Identification Number (CPR, Det Centrale Personregister) is a national ID number in Denmark. It is used with public agencies such as health care and tax authorities. Banks and insurance companies also use it as a customer number. The CPR number is required for people who reside in Denmark, pay tax or own property there.

Finland

Rule name	Description
Finland personal identity code	A Finnish personal identity code, a national government identification number for Finnish citizens used on identity cards, driver's licenses and passports.

France

Rule name	Description
France national identity card number	The French Carte Nationale d'Identité Sécurisée (CNI or CNIS) is the French national identity card. It's an official identity document consisting of a 12-digit identification number. This number is commonly used when opening bank accounts and when paying by check. It can sometimes be used instead of a passport or visa within the European Union (EU) and in some other countries.
France national insurance number	The French Numéro d'Inscription au Répertoire (NIR) is a permanent personal identification number that's also known as the French social security number for services including healthcare and pensions.

Rule name	Description
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.

Rule name	Description
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.
Ireland Personal Public Service Number (PPSN)	The Irish Personal Public Service Number (PPS number, or PPSN) is a unique number for accessing social welfare benefits, public services, and information in Ireland.

Israel

Rule name	Description
Israel identity card number	The Israel identity card number is issued to all Israeli citizens at birth by the Ministry of the Interior. Temporary residents are assigned a number when they receive temporary resident status.

Italy

Rule name	Description
Italy fiscal code number	An Italy fiscal code number is a unique 16-digit code assigned to Italian citizens as a form of identification.

Japan

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

Korea

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

Mexico

Rule name	Description
Mexico population registry number	The Mexico Clave Única de Registro de Población (CURP) number, or Unique Population Registry Code or Personal Identification Code number. The CURP number is an 18-character state-issued identification number assigned by the Mexican government to citizens or residents of Mexico and used for taxpayer identification.
Mexico passport number	A Mexican passport number.

The Netherlands

Rule name	Description
Netherlands citizen service number	A Dutch Burgerservicenummer (BSN), or Citizen's Service Number, is a state-issued identification number that's on driver's licenses, passports, and international ID cards.
Netherlands passport number	A Dutch passport number.

Norway

Rule name	Description
Norway national identity number	Norway's Fødselsnummer, National Identification Number, or Birth Number is assigned at birth, or on migration into the country. It is registered with the Norwegian Tax Office.

Paraguay

Rule name	Description
Paraguay identity card number	A Paraguayan Cédula de Identidad Civil (CIC), or civil identity card, is used as the main identity document for citizens.

Peru

Rule name	Description
Peru identity card number	A Peruvian Documento Nacional de Identidad (DNI), or national identity card, is used as the main identity document for citizens.

Poland

Rule name	Description
Poland PESEL number	The PESEL number is the national identification number used in Poland. It is mandatory for all permanent residents of Poland, and for temporary residents staying there longer than 2 months. It is assigned to just one person and cannot be changed.

Rule name	Description
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.
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.

Rule name	Description
Spain tax identification number	The Spanish Número de Identificación Fiscal (NIF) is a government identification number for Spanish citizens. An NIF number is needed for key transactions such as opening a bank account, buying a car, or setting up a mobile phone contract.
Spain passport number	A Spanish Ordinary Passport (Pasaporte Ordinario) number. There are 4 different types of passports in Spain. This detector is for the Ordinary Passport (Pasaporte Ordinario) type, which is issued for ordinary travel, such as vacations and business trips.
Spain social security number	The Spanish Social Security number (Número de Afiliación a la Seguridad Social) is a 10-digit sequence that identifies a person in Spain for all interactions with the country's Social Security system.

Sweden

Rule name	Description
Sweden personal identity number	A Swedish Personal Identity Number (personnummer), a national government identification number for Swedish citizens.
Sweden passport number	A Swedish passport number.

Taiwan

Rule name	Description
Taiwan passport number	A Taiwanese passport number.

Thailand

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

Turkey

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

United Kingdom

Rule name	Description
Scotland community health index number	The Scotland Community Health Index Number (CHI number) is a 10-digit sequence used to uniquely identify a patient within National Health Service Scotland (NHS Scotland).
United Kingdom drivers license number	A driver's license number for the United Kingdom of Great Britain and Northern Ireland (UK).
United Kingdom national health service number	A National Health Service (NHS) number is the unique number allocated to a registered user of the three public health services in England, Wales, and the Isle of Man.
United Kingdom national insurance number	The National Insurance number (NINO) is a number used in the United Kingdom (UK) in the administration of the National Insurance or social security system. It identifies people, and is also used for some purposes in the UK tax system. The number is sometimes referred to as NI No or NINO.
United Kingdom passport number	A United Kingdom (UK) passport number.
United Kingdom taxpayer reference number	A United Kingdom (UK) Unique Taxpayer Reference (UTR) number. This number, comprised of a string of 10 decimal digits, is an identifier used by the UK government to manage the taxation system. Unlike other identifiers, such as the passport number or social insurance number, the UTR is not listed on official identity cards.

United States

Rule name	Description
American Bankers CUSIP Id	An American Bankers' Committee on Uniform Security Identification Procedures (CUSIP) number is a 9-character alphanumeric code that identifies a North American financial security.

Rule name	Description
Medical drug names	The US National Drug Code (NDC) is a unique identifier for drug products, mandated in the United States by the Food and Drug Administration (FDA).
USA Adoption Taxpayer Identification Number	A United States Adoption Taxpayer Identification Number (ATIN) is a type of United States Tax Identification Number (TIN). An ATIN is issued by the Internal Revenue Service (IRS) to individuals who are in the process of legally adopting a US citizen or resident child.
USA bank routing number	The American Bankers Association (ABA) Routing Number (also called the transit number) is a nine-digit code. It's used to identify the financial institution that's responsible to credit or entitled to receive credit for a check or electronic transaction.
US DEA number	A US Drug Enforcement Administration (DEA) number is assigned to a health care provider by the US DEA. It allows the health care provider to write prescriptions for controlled substances. The DEA number is often used as a general "prescriber number" that is a unique identifier for anyone who can prescribe medication.
USA drivers license number	A driver's license number for the United States. Format can vary depending on the issuing state.
Employer Identification Number	A United States Employer Identification Number (EIN) is also known as a Federal Tax Identification Number, and is used to identify a business entity.
USA healthcare national provider identifier	The US National Provider Identifier (NPI) is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS). The NPI has replaced the unique provider identification number (UPIN) as the required identifier for Medicare services. It's also used by other payers, including commercial healthcare insurers.
USA Individual Taxpayer Identification Number	A United States Individual Taxpayer Identification Number (ITIN) is a type of Tax Identification Number (TIN), issued by the Internal Revenue Service (IRS). An ITIN is a tax processing number only available for certain nonresident and resident aliens, their spouses, and dependents who cannot get a Social Security Number (SSN).
USA passport number	A United States passport number.

Rule name	Description
USA Preparer Taxpayer Identification Number	A United States Preparer Taxpayer Identification Number (PTIN) is an identification number that all paid tax return preparers must use on US federal tax returns or claims for refund submitted to the US Internal Revenue Service (IRS).
US Social Security Number	A United States Social Security number (SSN) is a 9-digit number issued to US citizens, permanent residents, and temporary residents. This detector will not match against numbers with all zeroes in any digit group (that is, 000-##- ####, ###-00-####, or ###-##-0000), against numbers with 666 in the first digit group, or against numbers whose first digit is 9.
USA state name	A United States state name.
USA toll free phone number	A US toll-free telephone number.
USA vehicle identification number	A vehicle identification number (VIN) is a unique 17-digit code assigned to every on-road motor vehicle in North America.

Uruguay

Rule name	Description
Uruguay identity card number	A Uruguayan Cédula de Identidad (CDI), or identity card, is used as the main identity document for citizens.

Venezuela

Rule name	Description
Venezuela identity card number	A Venezuelan Cédula de Identidad (CDI), or national identity card, is used as the main identity document for citizens.

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 messsages, attachments, and users
- quantity of files, folders, applications, and security in cloud storage and Shadow SaaS applications

Topics:

- Viewing the Summary ReportViewing the Summary Report
- Viewing the Weekly Reports
- Viewing Dropbox 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.

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.

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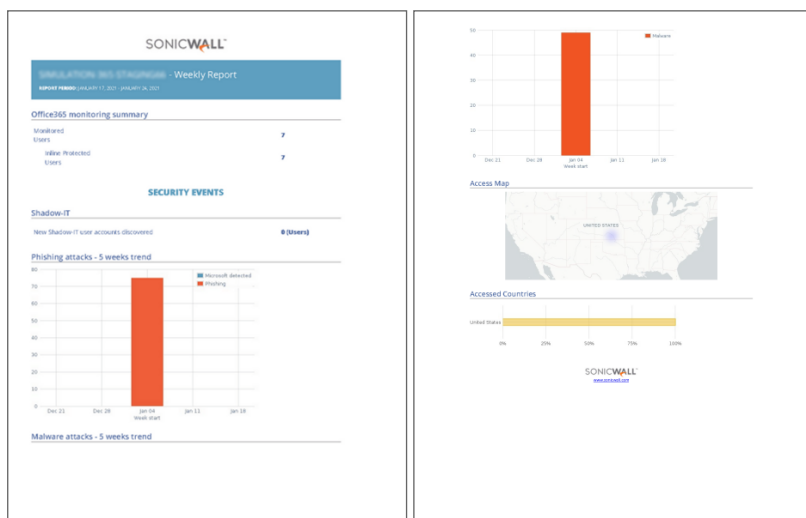
(i) **NOTE:** The weekly reports are only available to administrators both via email and in the Cloud App Security web management interface. Read-only users do not have access to these reports.

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.

(i) **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 Dropbox Analytics

The Analytics for Dropbox provides information about the quantity of files, folders, applications, and security events.
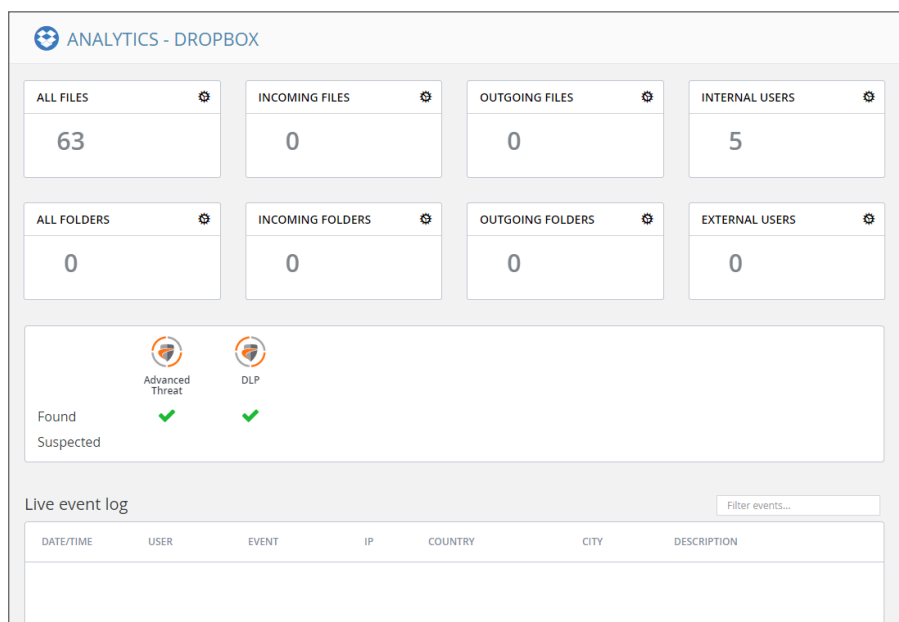
Widget	Description
All Files	The total number of files in your Dropbox.
Incoming Files	The number of files received.
Outgoing Files	The number of files shared with people outside the company
Internal Users	The number of internal users who have access to your Dropbox
All Folders	The total number of folders in your Dropbox
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.
External Users	The number of external users who have access to your Dropbox
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.
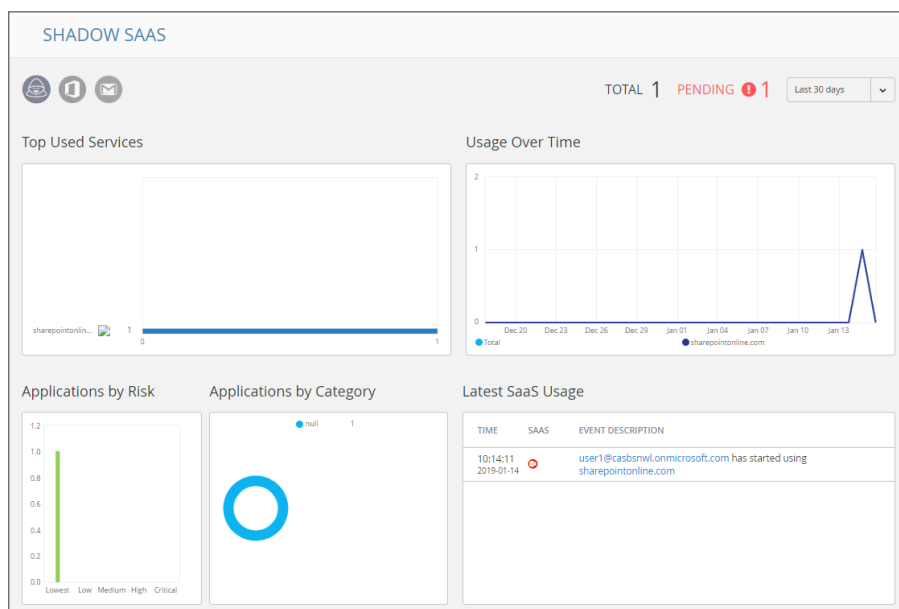
Panel	Description
Top Used Services	The most commonly used cloud applications discovered within your organization
Usage Over Time	The usage pattern of the discovered cloud applications over time
Applications by Risk	The number of discovered cloud applications and their associated risk level
Applications by Category	The number of discovered cloud applications arranged by application category
Latest Cloud Usage	The most recent events associated with the usage of the discovered cloud applications

Viewing and Creating Custom Queries

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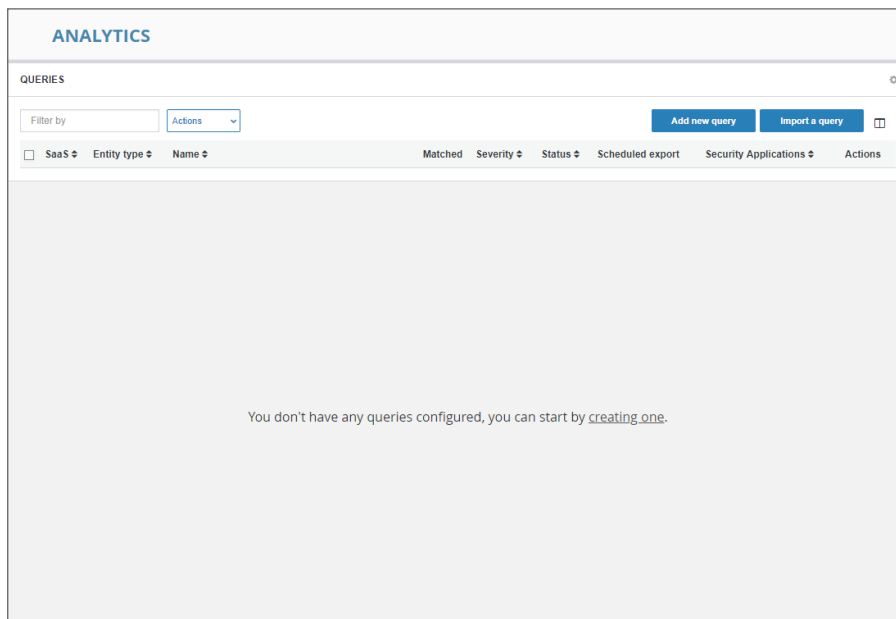
Topics:

- Creating Custom Queries
- Adding Custom Queries to the Dashboard

Creating Custom Queries

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

To create a custom query:

1. Navigate to the **ANALYTICS > Custom queries** page.
2. Click **Add new query** in the upper left side of the page. The **Query Create** page displays.
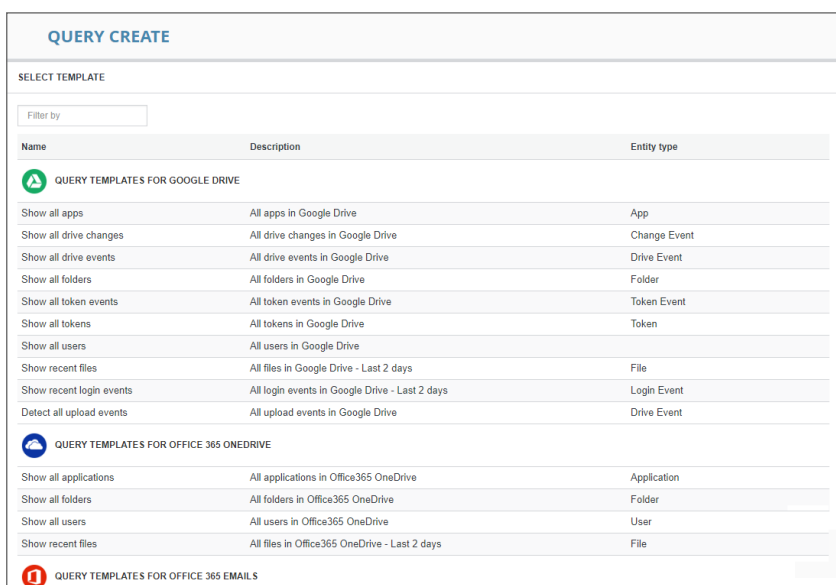
3. Click the query template under the cloud application for which you want to create a query. The results for that query are displayed.
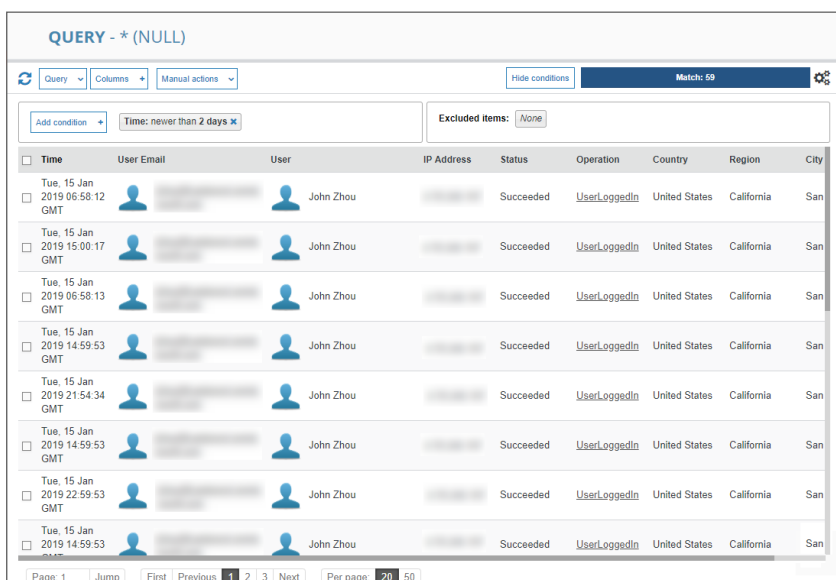
4. Modify the query by adding conditions using the **Add condition** button.

5. Save your query by selecting **Save as…** from the **Query** dropdown in the upper left area of the page.
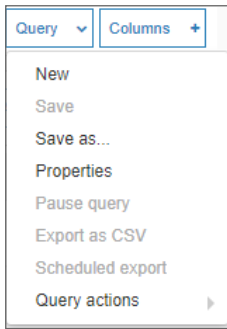
Adding Custom Queries to the Dashboard

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

Configuring Cloud Applications in the Cloud App Store

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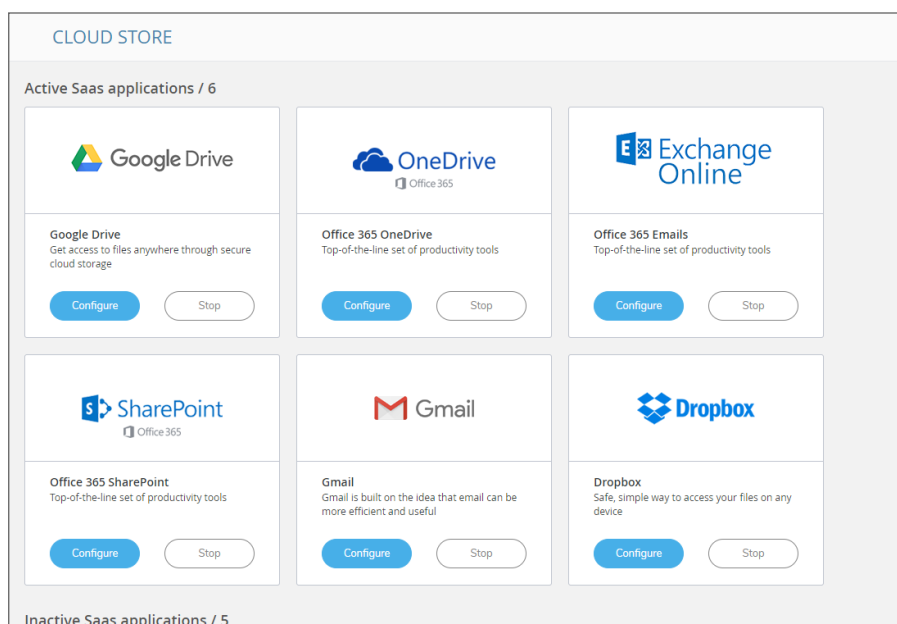
Topics:

Activating Cloud Applications for Cloud App Security

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 Dropbox with these subscription types:

- Dropbox Advanced
- Dropbox Enterprise

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

To activate Dropbox for Cloud App Security:

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

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

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

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

6. Click **Start** on the Dropbox tile.

For instructions for activating Dropbox cloud applications, see: Activating Dropbox for Cloud App Security.

Configuring Dropbox for Cloud App Security

To configure Dropbox for Cloud App Security:

1. Navigate to the **Configuration > Cloud App Store** page.
2. Click **Configure** on the **Dropbox** tile.
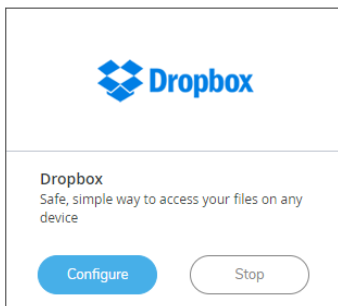
3. Set the options you want for the cloud application.
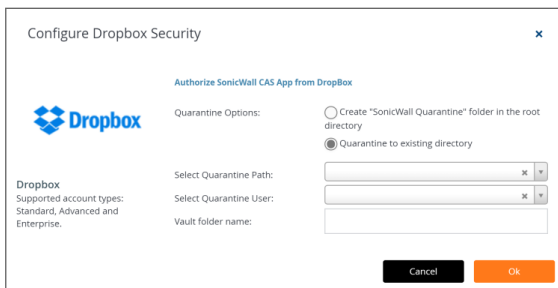
Most of the settings are related to specifying a quarantine email address and authorized administrators. See Managing Quarantine for Dropbox for more information on configuring these options.

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 Dropbox** link. The first step in the authorization for the cloud application displays.

For instructions for authorizing specific cloud applications, see Activating Dropbox for Cloud App SecurityActivating Box for Cloud App Security.

ⓘ | **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.
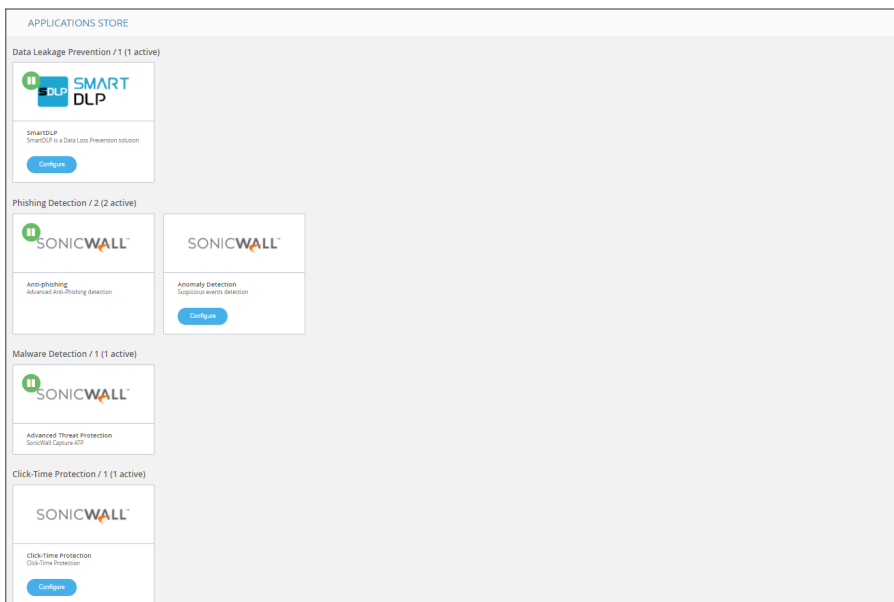
Topics:

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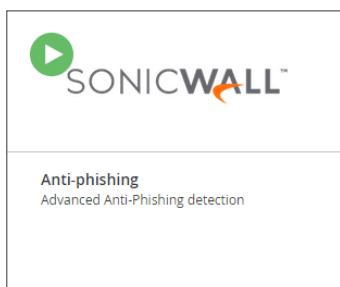
3. When prompted, click **Start** to start the security application.

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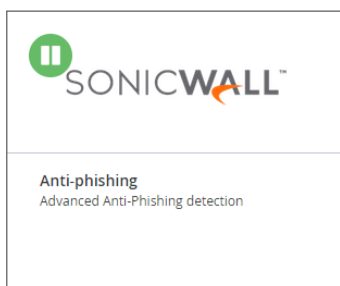
3. When prompted, click **Stop** to stop the security application.

Managing Security Tool Exceptions

You can manage which email addresses and files are exempt from being processed by the installed Security Tools.
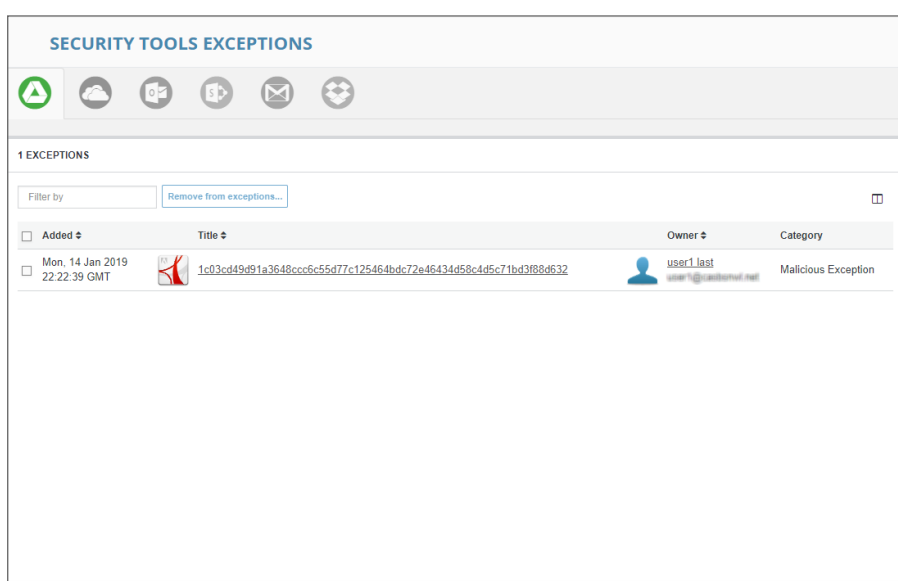
To switch between the security tool exceptions for each secured cloud application, click its icon at the upper left of the **Security Tools Exceptions** page.
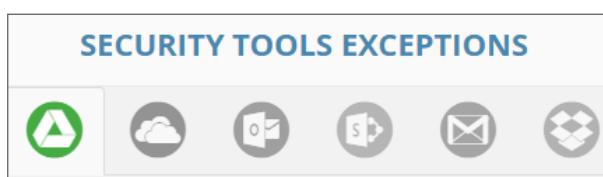
Lists for email cloud applications provide views both email messages and attachments.

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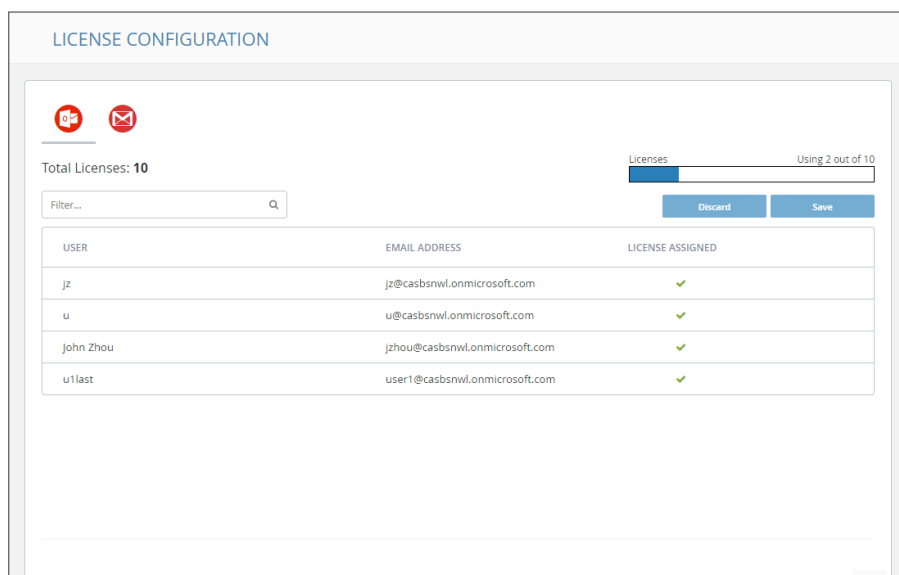
1. Navigate to the **Configuration > System Log** page.
2. Click the **Export as CSV** button on the upper right of the page. The file will be downloaded to your system. Depending on which browser you use, you may be prompted for a location where to save it.

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.

ⓘ | **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.

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**.

Unassigning Cloud App Security Licenses

To unassign a SonicWall Cloud App Security license:

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

3. Repeat this step for each user for you want to remove their license.

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

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

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

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

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

ⓘ | **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.**

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