

Integration Guide: Cloud App Security (SaaS Security) and Office 365

February 2020

This document describes how SonicWall® Cloud App Security (SaaS Security) is integrated with Office 365.

Topics:

- [About Cloud App Security \(SaaS Security\)](#)
- [System Requirements](#)
- [Activating Office 365 for Cloud App Security](#)
- [Configuring Office 365 for Cloud App Security](#)
- [Testing Your Integration](#)
- [For More Information](#)

About Cloud App Security (SaaS Security)

Cloud App Security (SaaS Security) solution delivers out-of-band scanning of traffic to sanctioned and unsanctioned SaaS applications using APIs and traffic log analysis. The solution seamlessly integrates with the sanctioned SaaS applications using native APIs delivering next-gen email security for cloud email and providing data protection capabilities: visibility, advanced threat protection, data loss prevention (DLP) and compliance. When deployed with SonicWall next-generation firewall (NGFW), Cloud App Security (SaaS Security) offers shadow IT visibility and control for cloud usage on the network.

System Requirements

- SonicWall Cloud App Security (SaaS Security)
- Cloud App Security can secure Office 365 cloud applications with these subscription levels:
 - Business
 - Business Essentials
 - Business Premium
 - ProPlus
 - Enterprise (E)

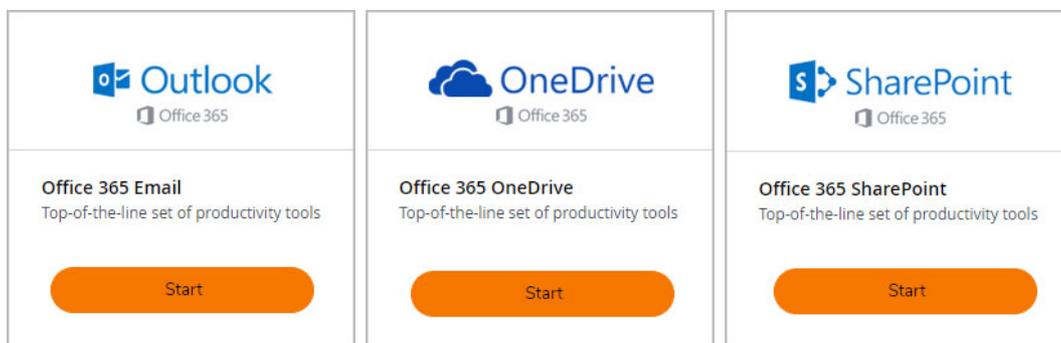
NOTE: Personal and Home subscription plans are not supported by Cloud App Security.

i **IMPORTANT:** If you plan to assign Cloud App Security licenses to only a specific set of Office 365 users, create the Office 365 before activating your Office 365 cloud applications for Cloud App Security. After initial cloud application activation, the cloud application onboarding process may take up to 12 hours. Adding new users to the Office 365 group later may result in delay in synchronizing the licensed users with both systems. For more information, refer to “Managing Cloud App Security (SaaS Security) Licenses” in the *Cloud App Security (SaaS Security) Administration Guide for Office 365*.

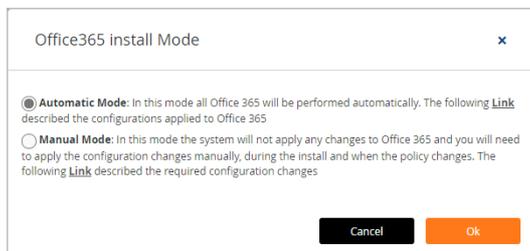
Activating Office 365 for Cloud App Security

To activate Office 365 for Cloud App Security:

- 1 In Cloud App Security, navigate to either the:
 - **SaaS Selection** page (during initial setup and configuration).
 - **Cloud App Store** page.
- 2 Click **Start** on the **Outlook**, **OneDrive**, or **SharePoint** tile.



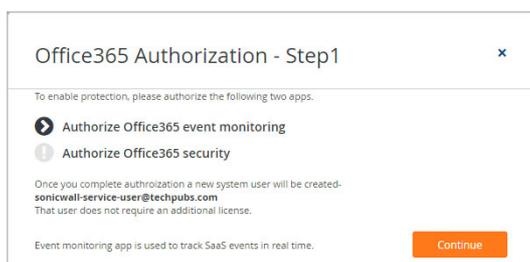
- 3 Select the installation mode you want to use to activate the Office365 cloud application.



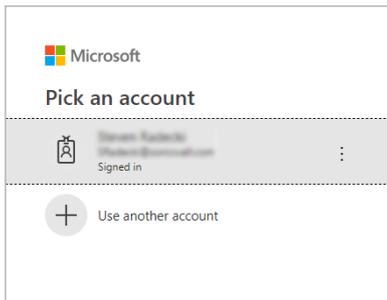
- 4 To automatically activate the Office365 cloud application, select **Automatic Mode** and click **Ok**.

i **NOTE:** **Automatic Mode** is the recommended activation mode and will work for most organizations. **Manual Mode** is intended for use by experienced Office 365 administrators. For information on how to manually activate Office365 cloud applications using **Manual Mode**, see [Manually Configuring Office 365 Cloud Applications During Activation.](#))

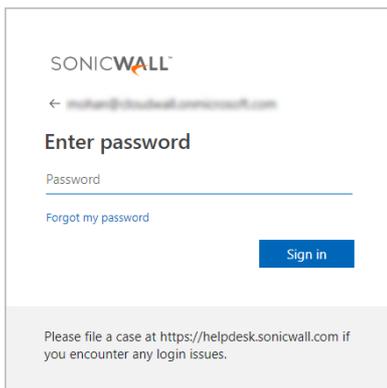
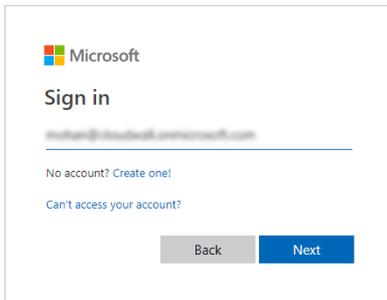
- 5 Click **Continue** to authorize any supporting applications.



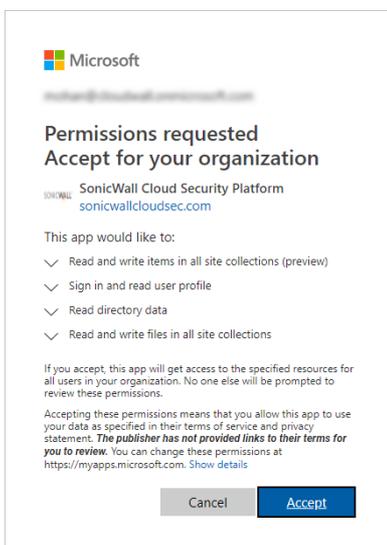
- 6 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.



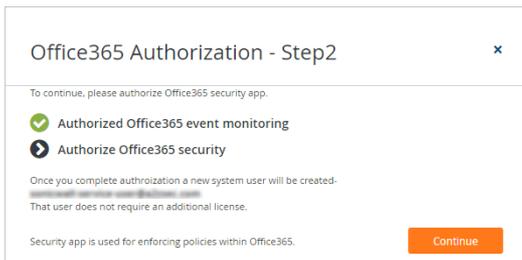
- 7 Sign into your Microsoft business account.



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

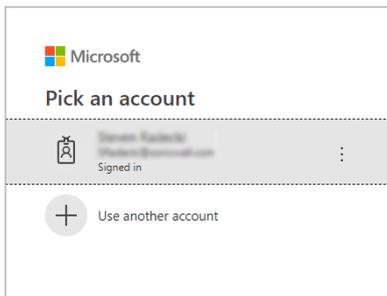


9 Click **Continue** to continue the activation process.



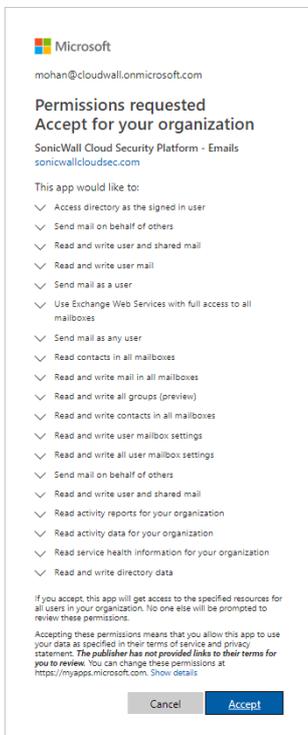
10 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

i **NOTE:** Make certain that you select the same Microsoft account that you used in previous steps.

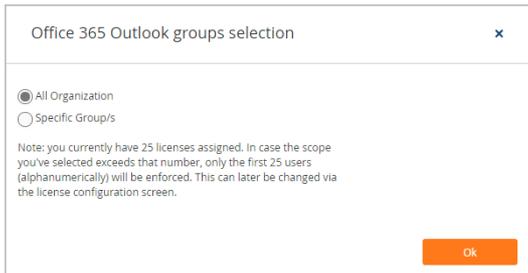


i **NOTE:** Make certain that you select the same Microsoft account that you used in previous steps.

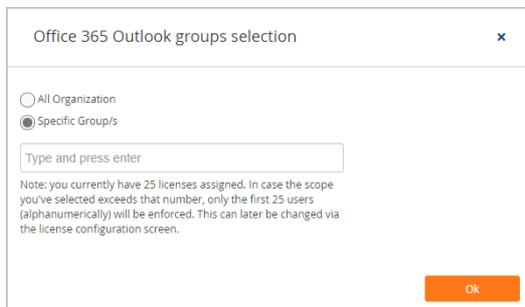
11 When prompted with a new list of permissions to which to grant Cloud App Security access, click **Accept**.



12 On the Office 365 groups selection page:



- Select **All Organization** if you want to assign Cloud App Security licenses to all of the users in your organization.
- Select **Specific Group/s** if you want to assign Cloud App Security licenses to only a specific Office 365 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.

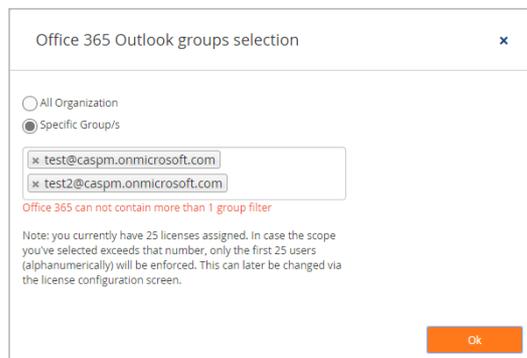
- If the number of users exceeds the number of available licenses, all user licenses will be assigned in alphabetical order by the system automatically. You can manually unassign users in order to free up licenses.
- If the number of licenses exceeds the number of users, the remaining licenses will remain unassigned. Any new users added to the group will be assigned from the available license pool.

Refer to “Managing Cloud App Security (SaaS Security) Licenses” in the *Cloud App Security (SaaS Security) Administration Guide* for more information.

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



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



You can change this setting later, if you needed, on the **Configuration > Cloud App Store** page. Refer to “Managing Cloud App Security (SaaS Security) Licenses” in the *Cloud App Security (SaaS Security) Administration Guide* for more information.

NOTE: If you add users to the Office 365 group later, it may take up to 12 hours for the user licenses to synchronize between the systems. For more information, refer to “Managing Cloud App Security (SaaS Security) Licenses” in the *Cloud App Security (SaaS Security) Administration Guide*.

13 Click **Ok**.

14 On the **The SaaS Selection** page, verify that a green checkbox appears on the tile for the Office365 cloud application indicating that the application has been activated for Cloud App Security.

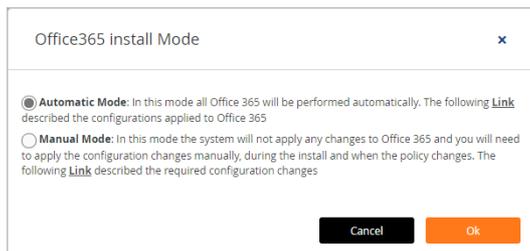
NOTE: If you have only activated Office 365 cloud application at this time, you will not need to reauthorize Cloud App Security again when you activate any additional Office 365 cloud applications.

NOTE: The Office 365 cloud application onboarding process could take several minutes. An email will be sent to your MySonicWall email address after the process has completed.

Manually Configuring Office 365 Cloud Applications During Activation

To manually configure Office 365 cloud applications during activation:

1 Select the installation mode you want to use to activate the Office365 cloud application.



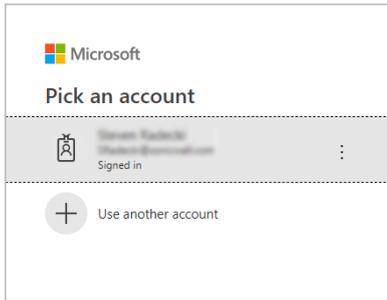
2 To manually activate the Office365 cloud application, select **Manual Mode** and click **Ok**. (For information on how to automatically activate the Office365 cloud application, see [Activating Office 365 for Cloud App Security](#).)

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

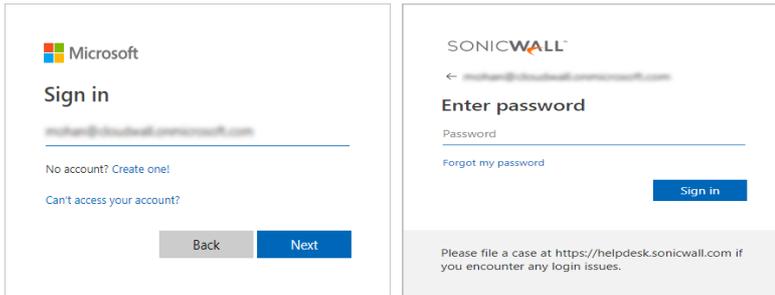


4 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

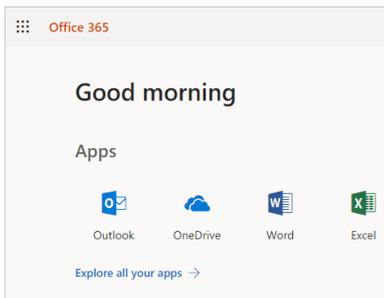
NOTE: Only Microsoft Office 365 Business Essentials, Office 365 Business, and Office 365 Business Premium accounts are supported by Cloud App Security.



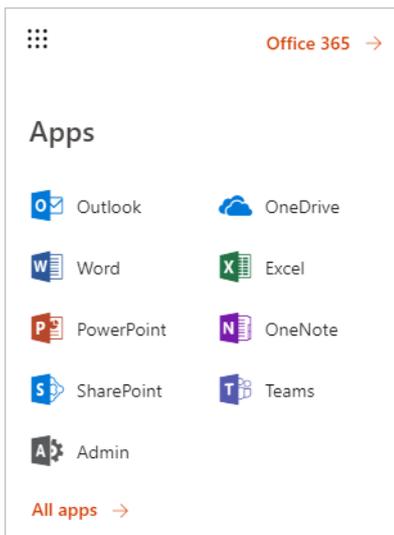
5 Sign into your Microsoft business account.



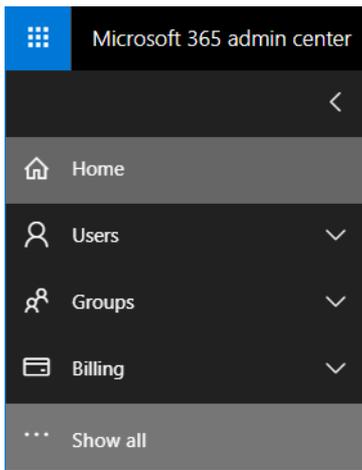
6 Click the  in the upper left area of the page.



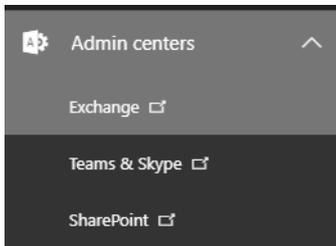
7 When the **Apps** area appears, select **Admin**.



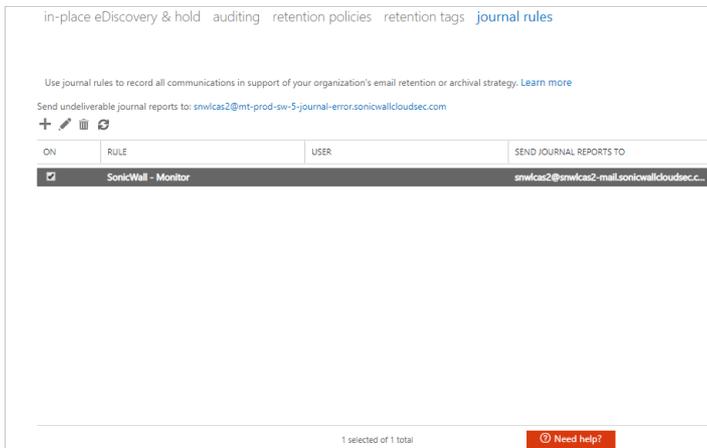
8 From the **Microsoft 365 admin center**, click **Show all**.



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



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



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

SonicWall - Monitor

Apply this rule...

*Send journal reports to:

 Name:

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

*Journal the following messages...

The journal rule is used for the monitoring mode. The journal rule configures O365 to send all emails to the system.

12 Click **Save**.

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

Exchange admin center

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

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

hybrid

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

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

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

0 selected of 2 total

[Need help?](#)

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

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

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

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

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

SonicWall Inbound

Mail flow scenario

From: Partner organization

To: Office 365

Description

SonicWall Inbound Connector

Status

On

[Turn it off](#)

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

Edit Connector

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

*Name:
SonicWall Inbound

Description:
SonicWall Inbound Connector

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

Next Cancel

- b Select **Turn it on** if you want to connector enabled after you complete its configuration.
- c Click **Next**.
- d Select where to the use the domain name or the IP address of the sender.

Edit Connector

How do you want to identify the partner organization?

Specify whether you want to use a domain or IP address to identify the partner organization. [Learn more](#)

Use the sender's domain
 Use the sender's IP address

Select this option to apply this connector to email messages that come from your partner's domains.

Back Next Cancel

- e Click **Next**.

- f Select the IP addresses you want to use to identify your sender.

Edit Connector

What sender IP addresses do you want to use to identify your partner?

Specify the sender IP address range.

+ ✎ -

192.178.148.100

Specify IP address ranges that this connector applies to.

Back Next Cancel

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

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

Edit Connector

What security restrictions do you want to apply?

Reject email messages if they aren't sent over TLS

And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or *.contoso.com

This option requires that all email messages from the partner organization be sent over Transport Layer Security (TLS), a secure channel. If a message isn't sent over TLS, it will be rejected by Office 365.

Back Next Cancel

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

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

Edit Connector

Confirm your settings
Before saving, make sure these are the settings you want to configure.

Mail flow scenario
From: Partner organization
To: Office 365

Name
SonicWall Inbound

Description
SonicWall Inbound Connector

Status
Turn it on after saving

How to identify your partner organization
Identify the partner organization by verifying that messages are coming from these IP address ranges: 35.174.145.124

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

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

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

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

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

+ ✎ 🗑️ ↻

STATUS	NAME	FROM	TO	
On	SonicWall Inbound	Partner organization	Office 365	<div style="border: 1px solid #ccc; padding: 5px;"> <p>SonicWall Journaling Outbound</p> <p>Mail flow scenario From: Office 365 To: Partner organization</p> <p>Description SonicWall Journaling Outbound Connector</p> <p>Status On Turn it off</p> </div>
On	SonicWall Journaling Ou...	Office 365	Partner organization	

1 selected of 2 total

[Need help?](#)

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

Edit Connector

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

*Name:

Description:

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

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

- c Click **Next**.
- d Set when you want the connector to be used.

Edit Connector

When do you want to use this connector?

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

Only when email messages are sent to these domains

+ ✎ -

snwicas2-mail.sonicwallcloudsec.com

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

Back Next Cancel

- e Set how you want the email messages routed.

Edit Connector

How do you want to route email messages?

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

Use the MX record associated with the partner's domain

Route email through these smart hosts

+ ✎ -

snwicas2-host.sonicwallcloudsec.com

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

Back Next Cancel

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

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

How should Office 365 connect to your partner organization's email server?

- Always use Transport Layer Security (TLS) to secure the connection (recommended)
Connect only if the recipient's email server certificate matches this criteria
 - Any digital certificate, including self-signed certificates
 - Issued by a trusted certificate authority (CA)
- And the subject name or subject alternative name (SAN) matches this domain name:
Example: contoso.com or *.contoso.com

A callout box on the right explains: "TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful."

Buttons: Back, Next, Cancel

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

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

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

Confirm your settings
Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario
From: Office 365
To: Partner organization

Name
SonicWall Journaling Outbound

Description
SonicWall Journaling Outbound Connector

Status
Turn it on after saving

When to use the connector
Use only for email sent to these domains: swwlcs2-mail.sonicwallcloudsec.com

Routing method
Route email messages through these smart hosts: swwlcs2-host.sonicwallcloudsec.com

Security restrictions

Buttons: Back, Next, Cancel

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

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

The screenshot shows the 'rules' page in the Exchange Admin Center. A table lists three rules:

ON	RULE	PRIORITY
<input checked="" type="checkbox"/>	SonicWall - Protect	0
<input checked="" type="checkbox"/>	SonicWall - Whitelist	1
<input checked="" type="checkbox"/>	SonicWall - Junk Filter	2

The configuration for the selected 'SonicWall - Protect' rule is shown on the right:

- If the message...**
 - Is sent to 'Inside the organization' and Is received from 'Outside the organization'
- Do the following...**
 - Route the message using the connector named 'SonicWall Outbound'.
 - and set message header 'X-CLOUD-SEC-AV-info' with the value 'snwicas2.office365_emails.inline'
 - and Stop processing more rules
- Except if...**
 - Has a spam confidence level (SCL) that is greater than or equal to '5'
 - or sender ip addresses belong to one of these ranges: '35.174.145.124'

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

The screenshot shows the configuration dialog for the 'SonicWall - Protect' rule. The fields are set as follows:

- Name:** SonicWall - Protect
- *Apply this rule if...**
 - The sender is located... **Outside the organization**
 - and
 - The recipient is located... **Inside the organization**
- *Do the following...**
 - Set the message header to this value... Set the message header 'X-CLOUD-SEC-AV-info' to the value 'snwicas2.office365_emails.inline'
 - and
 - Use the following connector... **SonicWall Outbound**
- Except if...**
 - The message has an SCL greater than or equal to... **5**
 - or
 - Sender's IP address is in the range... **'35.174.145.124'**
- Properties of this rule:**
 - Priority: **0**
 - Audit this rule with severity level: **Not specified**
 - Choose a mode for this rule:
 - Enforce
 - Test with Policy Tips
 - Test without Policy Tips
 - Activate this rule on the following date: Thu 2/7/2019 1:30 PM
 - Deactivate this rule on the following date: Thu 2/7/2019 1:30 PM
 - Stop processing more rules
 - Defer the message if rule processing doesn't complete
 - Match sender address in message: **Header**
- Comments:** Manual changes made to the rule will not be retained unless 'Configure excluded IPs manually in mail flow rule' is selected in the Protect rule of the Policy section.

Buttons: Save, Cancel

- **Apply this rule if...:** Set the condition(s) under which the rule should be applied.

In this example, the rule is only applied to emails that originate outside the organization/domain and the email address of the recipient is within the organization/domain.

- **Do the following...:** Specify the action(s) to be taken when the rule is applied.

In this example, the header of the email message is assigned a specific value so that processed email messages can be more easily detected and then forwarded to the outbound connector that you created.

- **Except if...:** Specify any exceptions for when the rule’s actions should not be taken.

IMPORTANT: One of your exceptions should include **Sender’s IP address is in the range...** that includes the IP address(es) specified in your inbound connectors to prevent the email messages from being processed in an endless loop.

In this example, the actions are not taken if the email message has already been classified by Microsoft as spam (an Spam Confidence Level [SCL] greater than 5) or is a message that is identified as having been processed.

- Select **Stop processing more rules** to end the processing if the email message was processed by this rule.

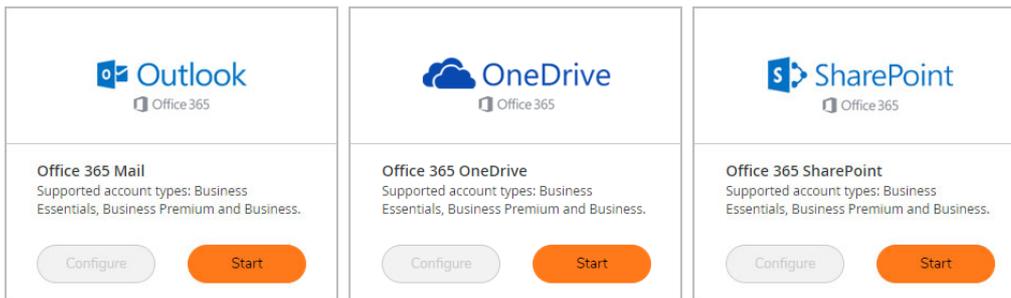
NOTE: Every time you change the scope of the inline policy (such as when you add or remove users or groups), you will need to edit the **“Apply this rule if... The recipient is ...”** section.

17 Click **Save**.

Configuring Office 365 for Cloud App Security

To configure Office 365 for Cloud App Security:

- 1 In Cloud App Security, navigate to the **Configuration > Cloud App Store** page.
- 2 Click **Configure** on the tile for **Outlook, OneDrive, or SharePoint**.



- 3 Set the options you want for the Office 365 applications.

Configure Office 365 Email Security ✕



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

Re-Authorize SonicWall CAS Office365 Emails App

Quarantine and workflow:

Dedicated quarantine mailbox:

Restore requests approver:

▶ Advanced

Cancel **Ok**

Configure Office 365 OneDrive Security ✕



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

Authorize SonicWall CAS Office365 OneDrive App

Quarantine Options: Create Quarantine folder in the root directory
 Quarantine to existing directory

Enable Remove Action:

Cancel **Ok**

Configure Office 365 SharePoint Security ✕



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

Authorize

Quarantine Options: Create a folder in the quarantine user's root directory
 Quarantine to existing directory

Force Site Admin:

▼ Advanced

Authorization Scope:

Authorize for all sites
 Authorize for specific sites only

Cancel **Ok**

- 4 Click **Ok**.

Testing Your Integration

If your Office 365 applications are properly activated for Cloud App Security, you will see them listed on the Cloud App Security Dashboard as secured cloud applications.



For More Information

For more information about configuring and using SonicWall Cloud App Security, refer to the *SonicWall Cloud App Security (SaaS Security) Administration Guide*.

Copyright © 2020 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. 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>.

Legend

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

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

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 1/31/20