# 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)

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 354 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.

**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*.

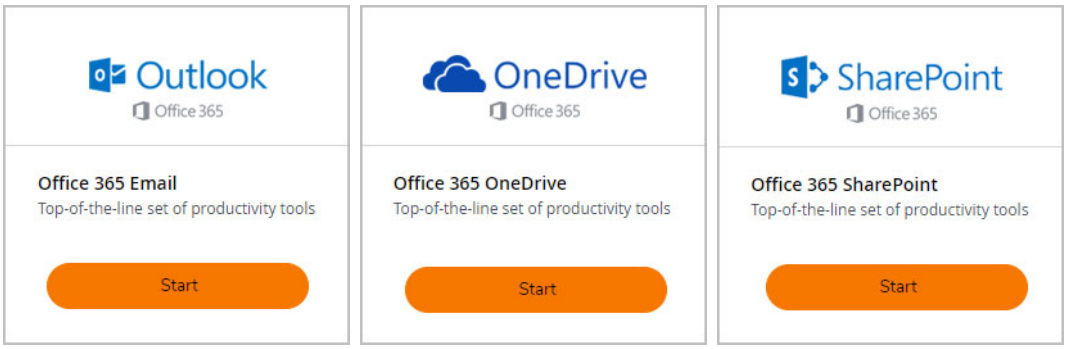
# Activating Office 365 for Cloud App Security

***To activate Office 365 for Cloud App Security:***

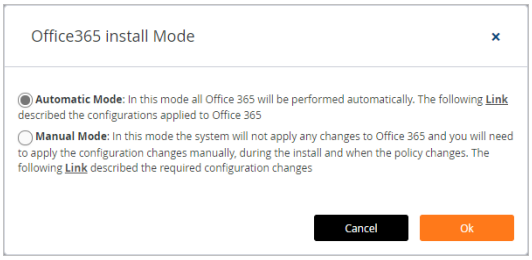
1 In Cloud App Security, navigate to either the:

- **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.

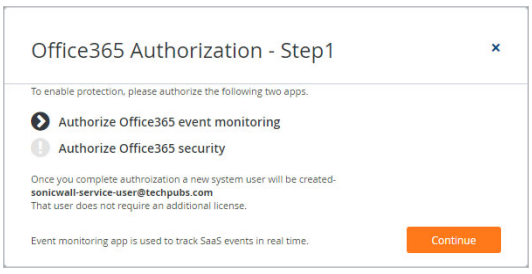



4 To automatically activate the Office365 cloud application, select **Automatic Mode** and click **Ok**.

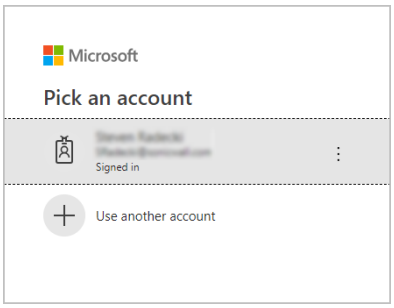
**NOTE: Automatic Mode** is the recommended activation mode and will work for most organizations. **Manual Mode** is intended for use by experienced Office 365 administrators.

For information on how to manually activate Office365 cloud applications using **Manual Mode**, see Manually Configuring Office 365 Cloud Applications During Activation.)

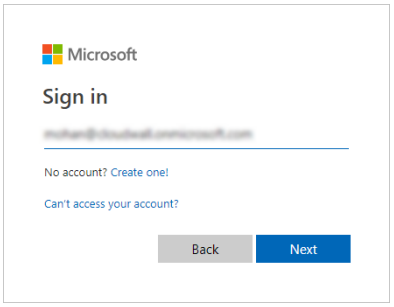
5 Click **Continue** to authorize any supporting applications.

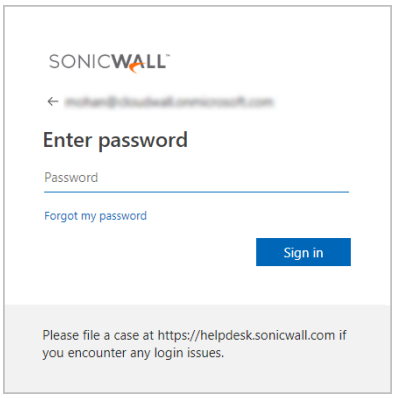


6 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

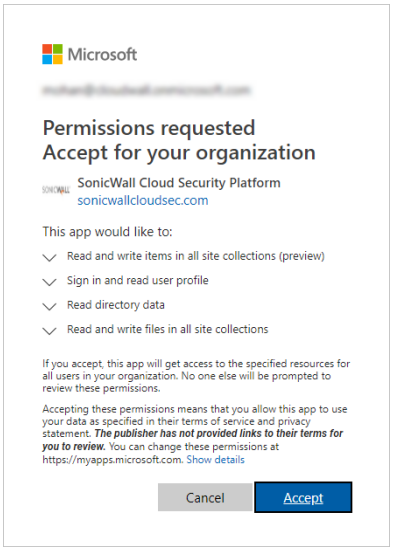



7 Sign into your Microsoft business account.

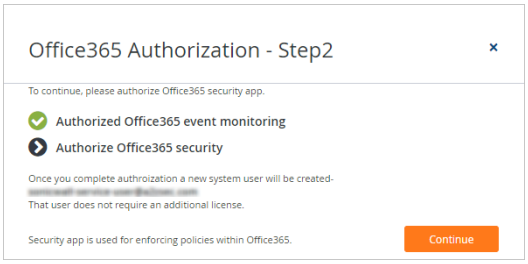



8 When prompted with a list of permissions to which to grant Cloud App Security access, click **Accept**.

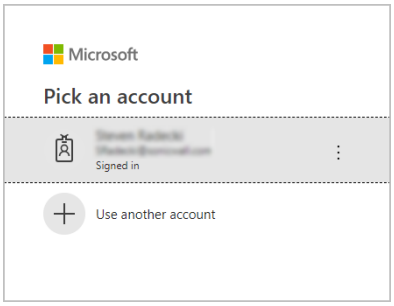


9 Click **Continue** to continue the activation process.



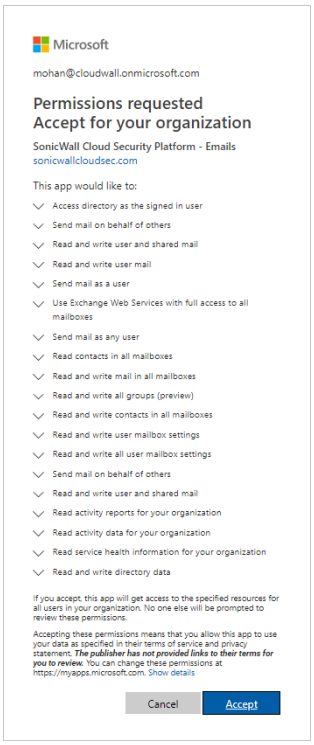

10 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

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

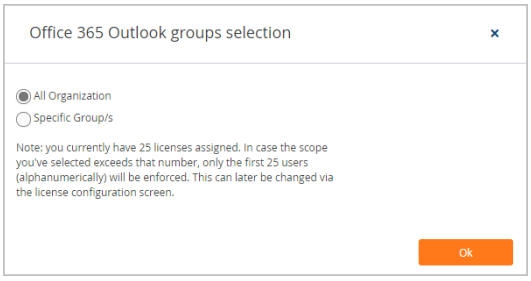



**NOTE:** Make certain that you select the same Microsoft account that you used in previous steps.

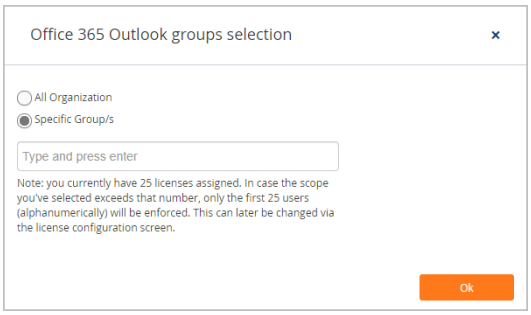
11 When prompted with a new list of permissions to which to grant Cloud App Security access, click **Accept**.



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 you Cloud App Security licenses for a specific subset of users within your organization.



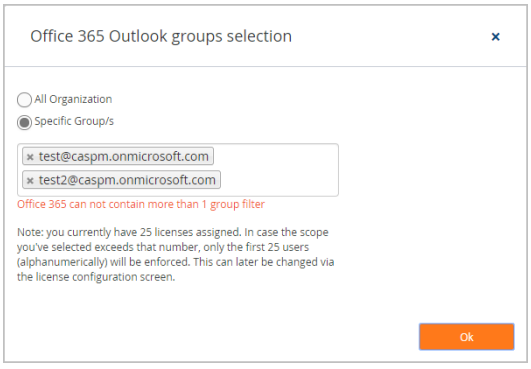

**NOTE:** Licenses are assigned in alphabetical order.

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

Refer to "Managing Cloud App Security (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.

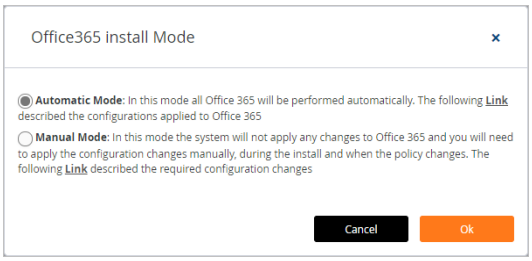
**NOTE:** If you have only activated Office 365 cloud application at this time, you will not need to reauthorize Cloud App Security again when you activate any additional Office 365 cloud applications.

**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

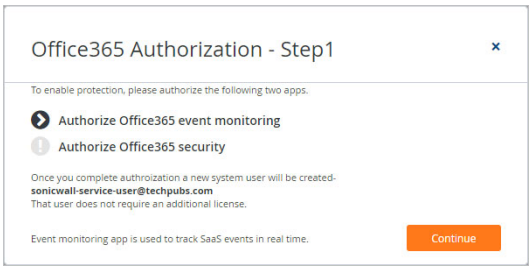
***To manually configure Office 365 cloud applications during activation:***

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



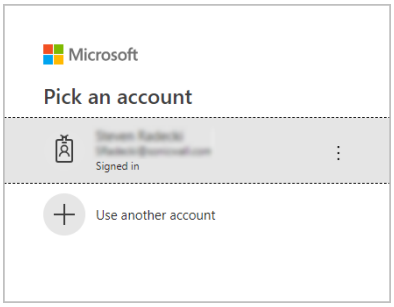

2 To manually activate the Office365 cloud application, select **Manual Mode** and click **Ok**. (For information on how to automatically activate the Office365 cloud application, see Activating Office 365 for Cloud App Security.

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

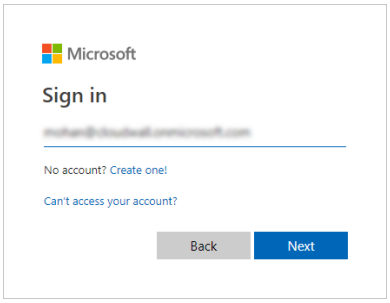


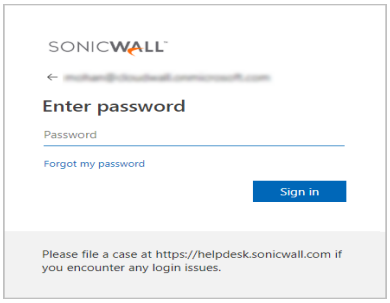

4 Select your Microsoft account from the list and, if prompted, log in using your Microsoft account username and password.

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

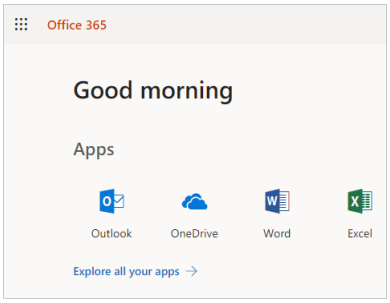



5 Sign into your Microsoft business account.

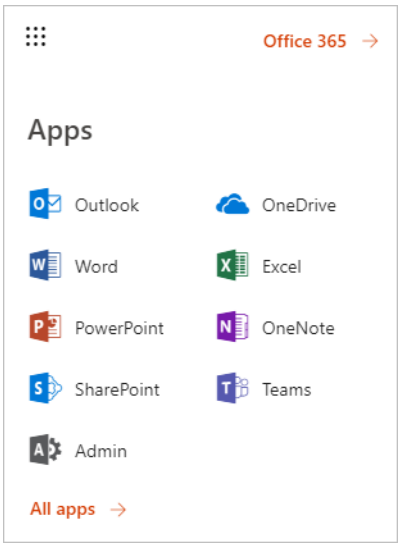


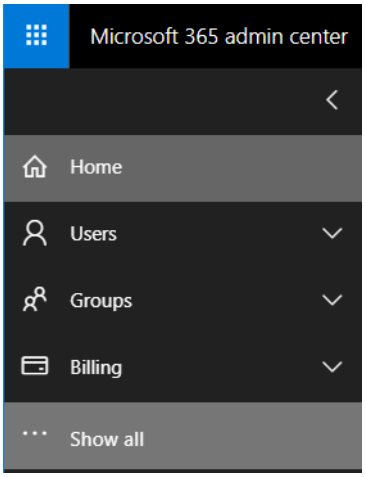

6 Click the ⠿ in the upper left area of the page.



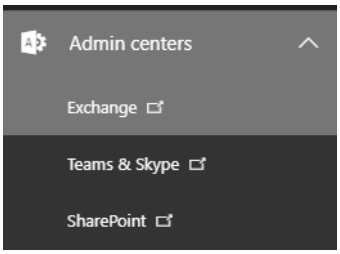

7 When the **Apps** area appears, select **Admin**.



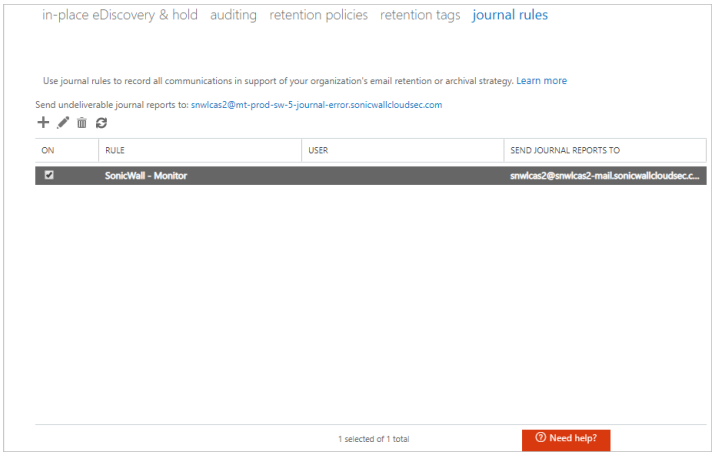
8 From the **Microsoft 365 admin center**, click **Show all**.



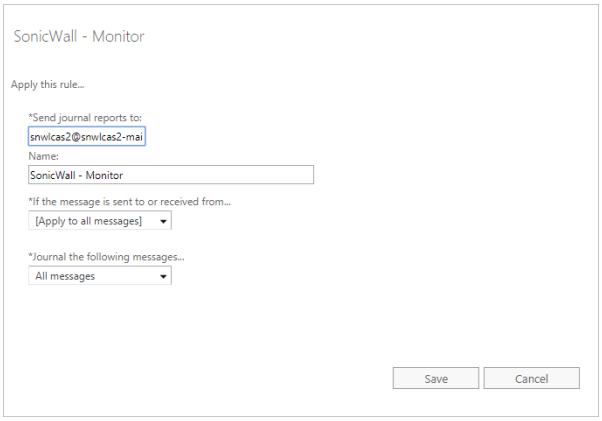

9 Scroll down to **Admin centers** and click **Exchange**.




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



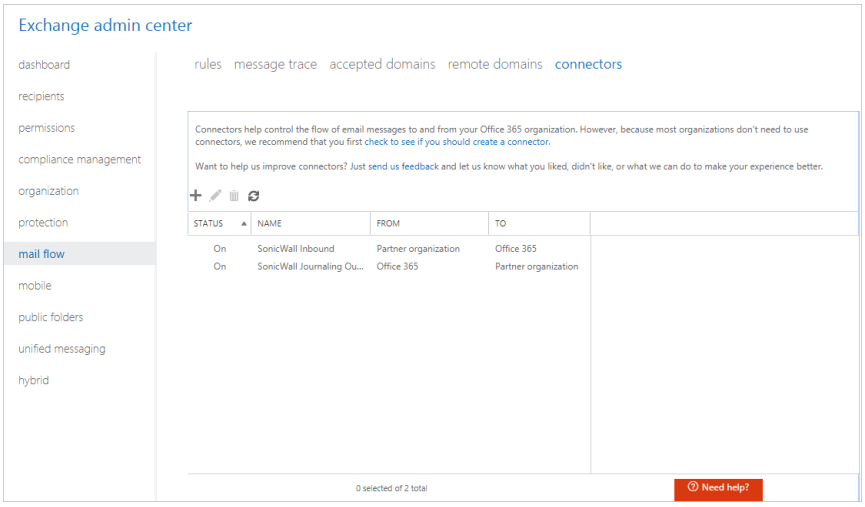

11 In the **Send journal reports to** field, enter the email address in your domain to which the journal reports should be sent.



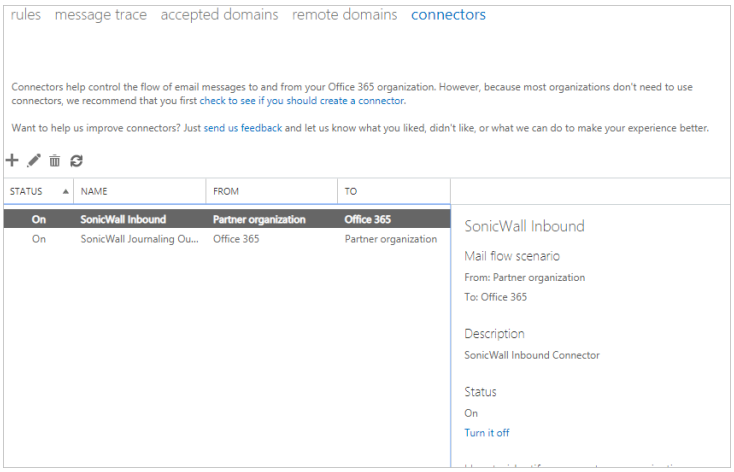

The journal rule is used for the monitoring mode. The journal rule configures O365 to send all emails to the system.

12 Click **Save**.

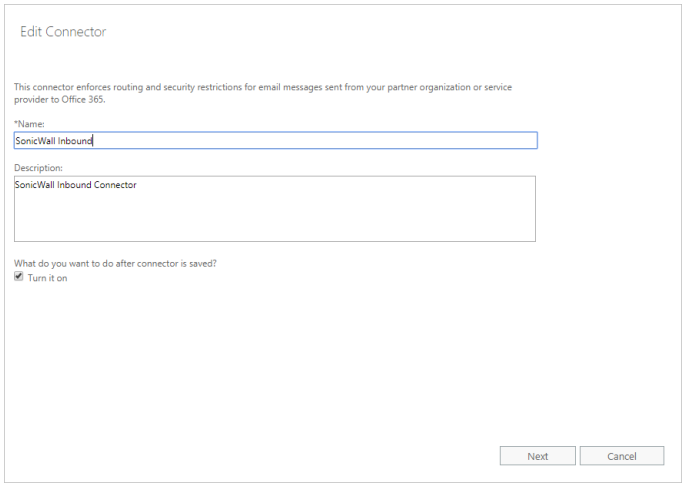
13 On the **Exchange admin center** page, click **mail flow > connectors**.




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



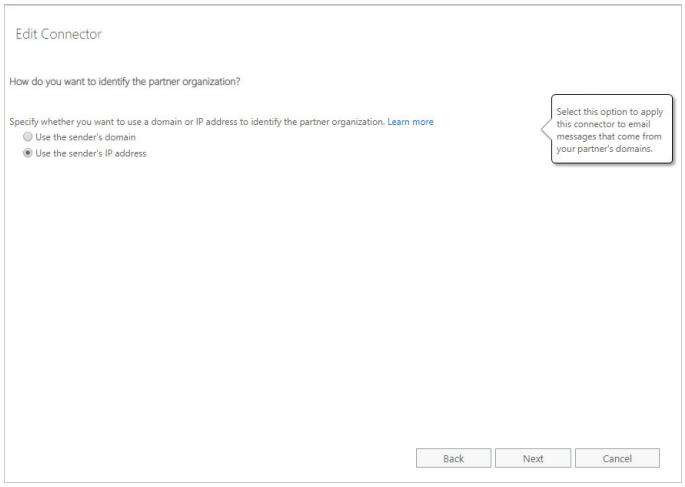
a Enter a **Name** and **Description** for the inbound connector.




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

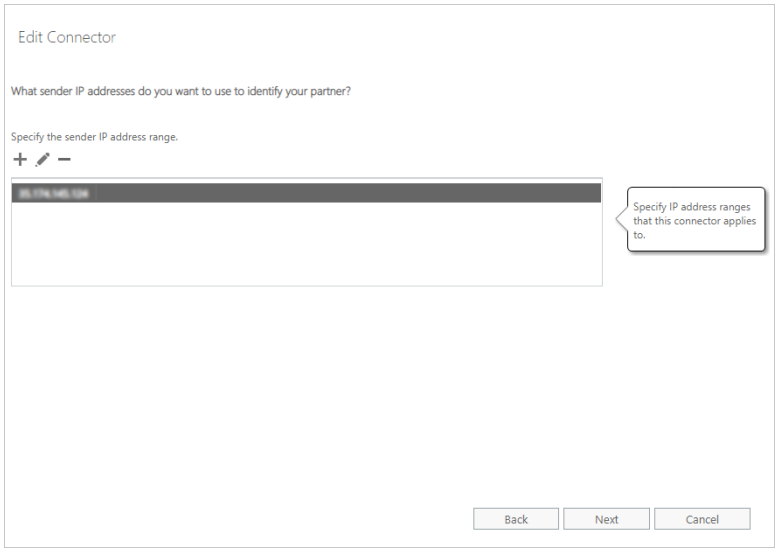
c Click **Next**.

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




e Click **Next**.

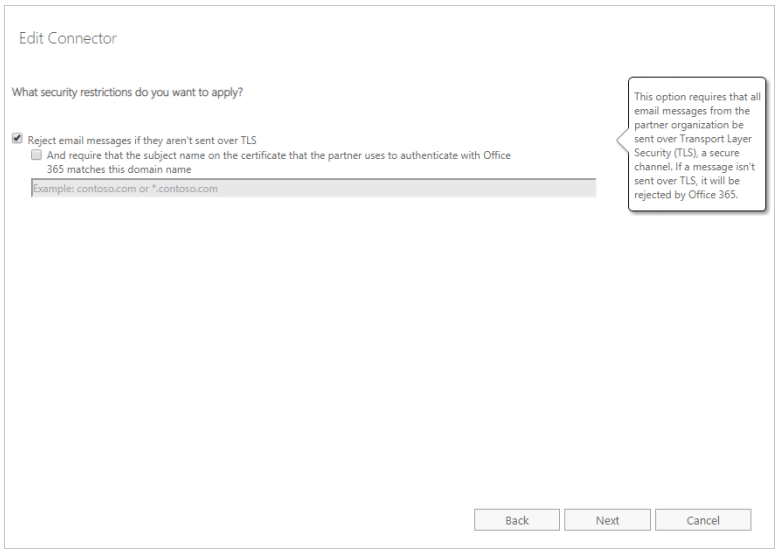
f Select the IP addresses you want to use to identify your sender.




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

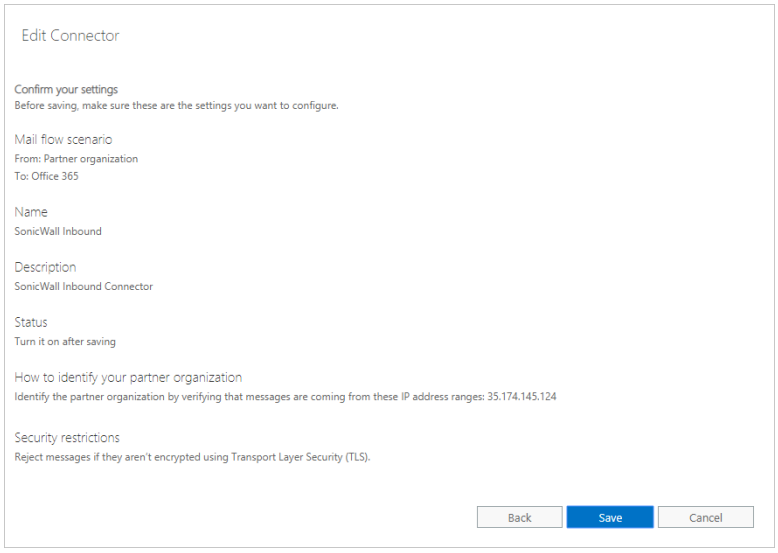
g Click **Next**.

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).

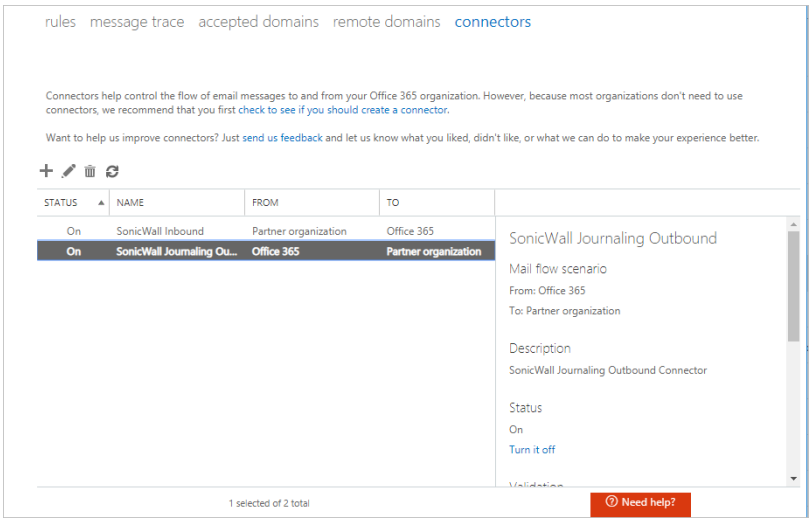



You can add an additional level of security by selecting **And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name** and specifying a required domain name.

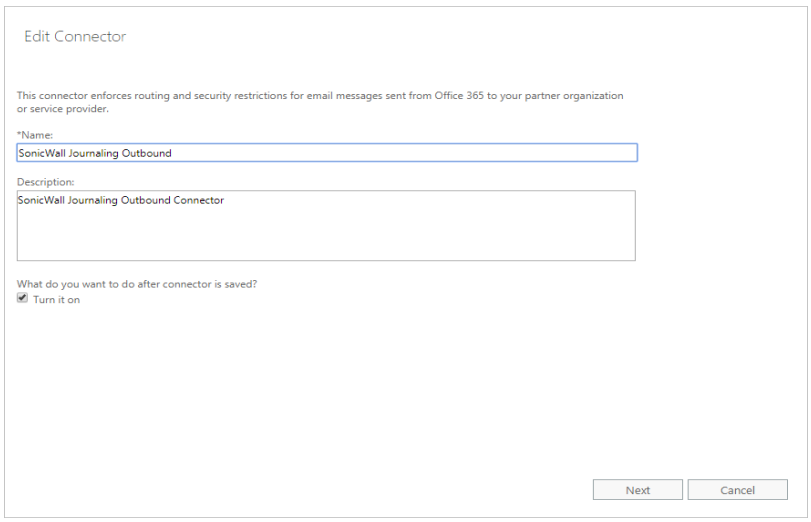
i Verify your settings for the inbound connector and click **Save**.




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



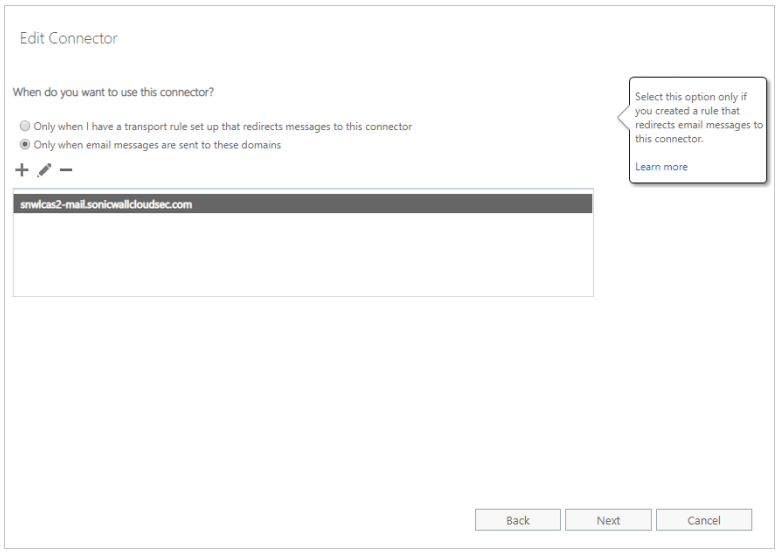

a Enter a **Name** and **Description** for the inbound connector.



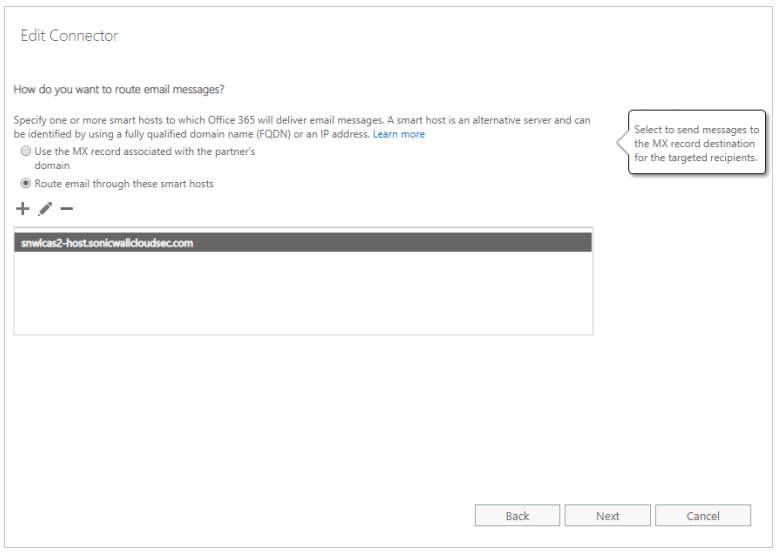

b Select **Turn it on** if you want to connector enabled after you complete its configuration.

c Click **Next**.

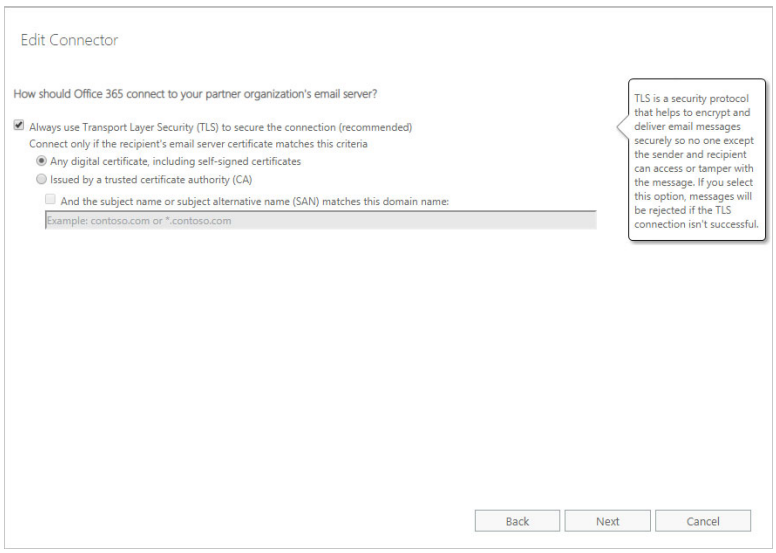
d Set when you want the connector to be used.




e Set how you want the email messages routed.

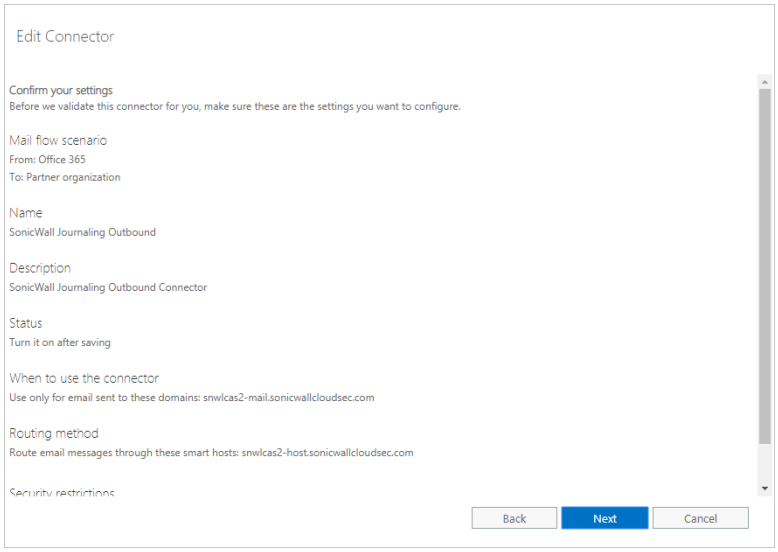


f Select **Always use Transport Layer Security (TLS) to secure the connection (recommended)** to only connect to the email server of the email recipient is TLS is used to secure the connection. (This option is selected by default.)



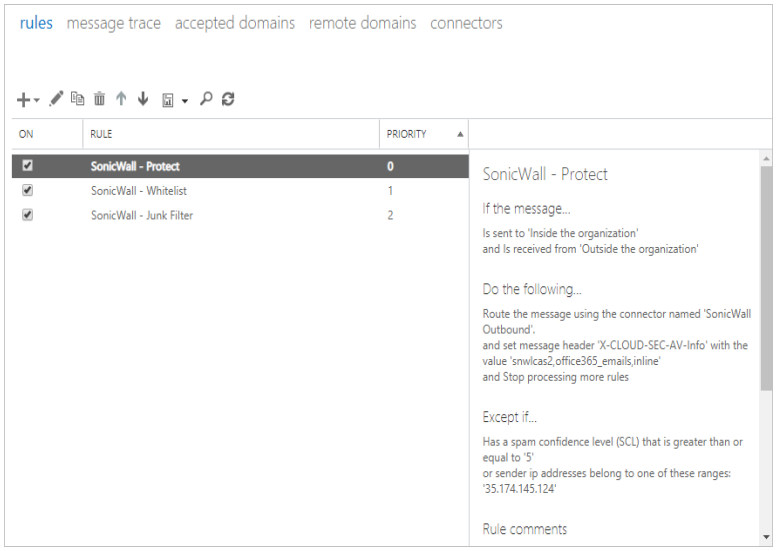

You can also increase the security of the connection by requiring the presence of an email server certificate, either self-signed or issued by a recognized certificate authority.

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

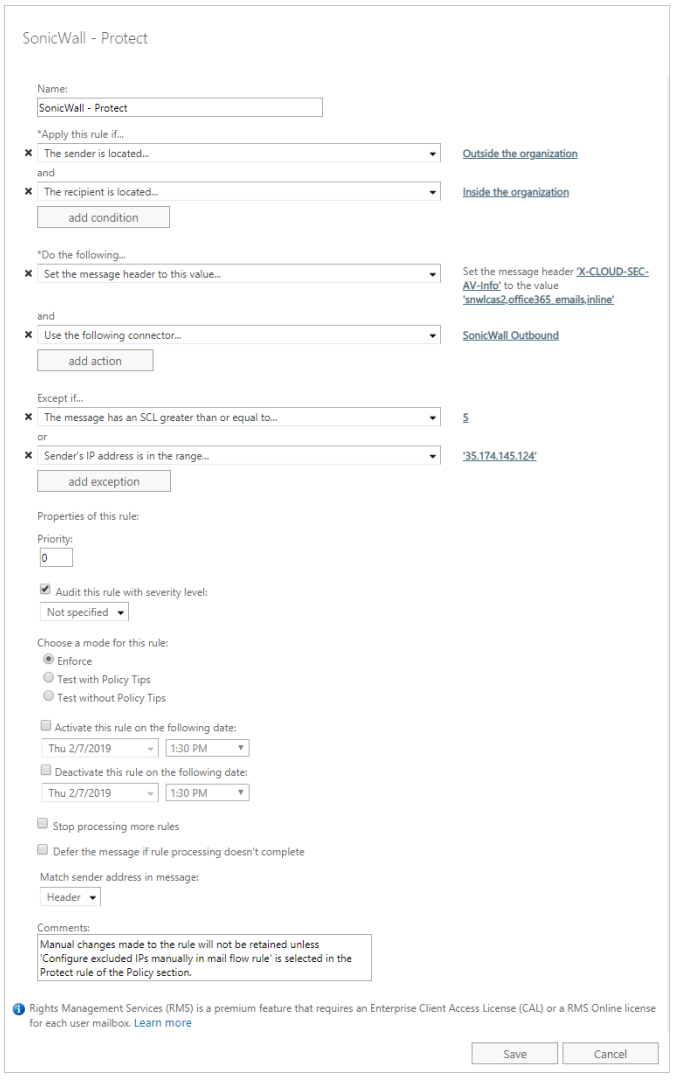



16 Navigate to **mail flow > rules**.

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




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



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

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

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

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

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

  **IMPORTANT:** One of your exceptions should include **Sender's IP address is in the range…** that includes the IP addresse(s) 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.

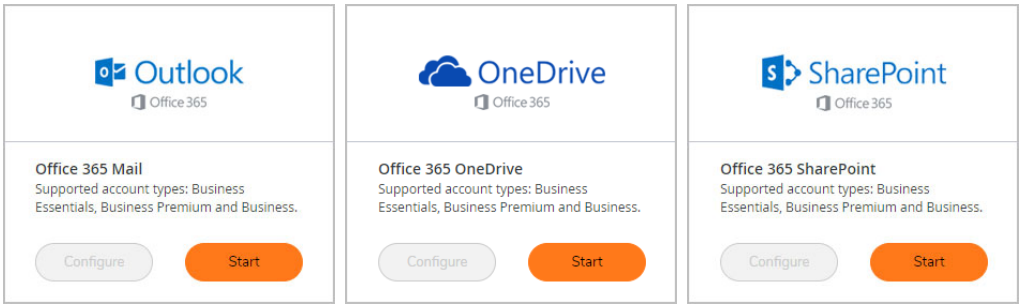
17 Click **Save**.

# Configuring Office 365 for Cloud App Security

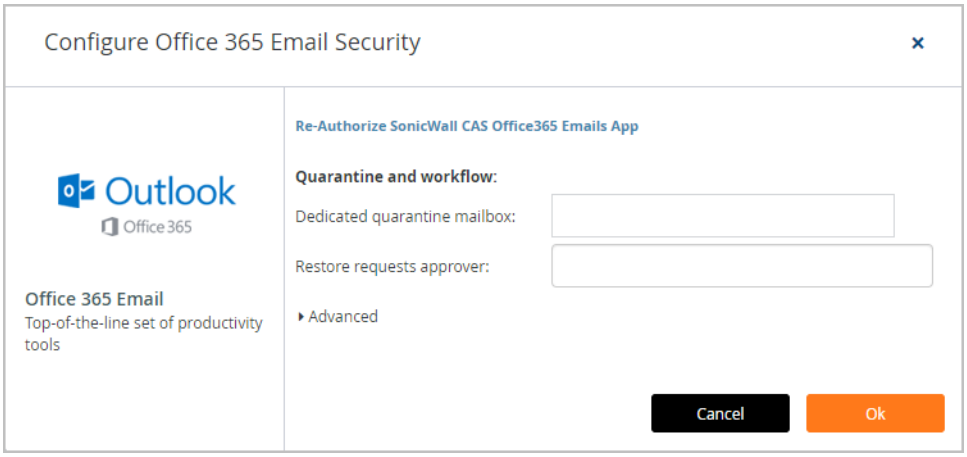
***To configure Office 365 for Cloud App Security:***

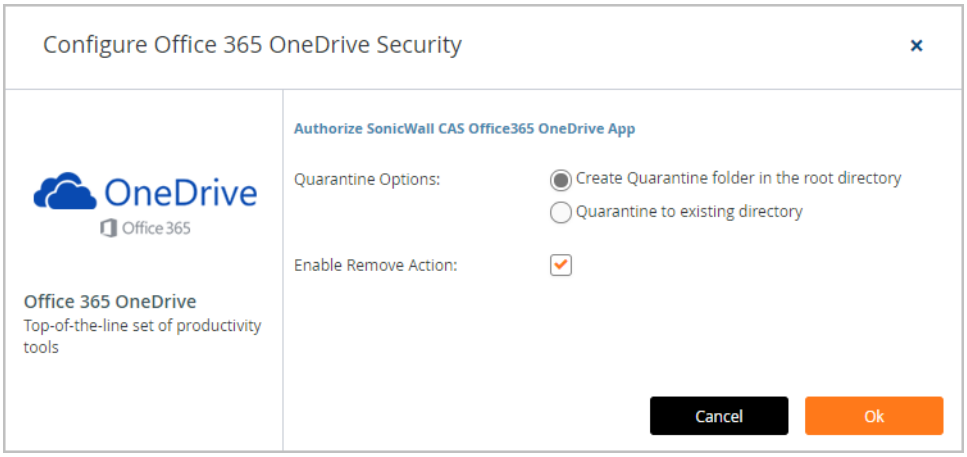
1 In Cloud App Security, navigate to the **Configuration > Cloud App Store** page.

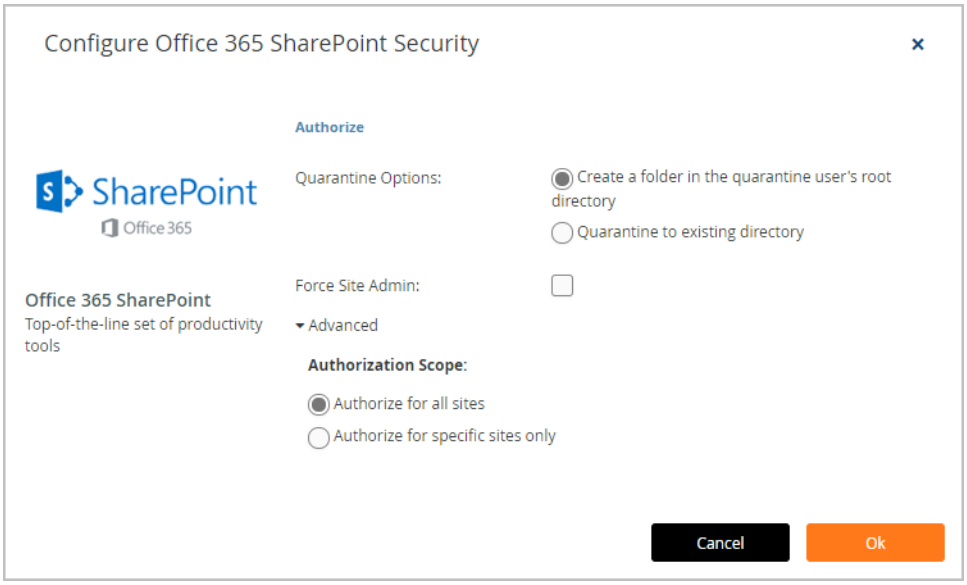
2 Click **Configure** on the tile for **Outlook**, **OneDrive**, or **SharePoint**.



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




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 Dasboard 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*.

**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