

# How to make sure ATP Safe Links protection is in place

## Office 365 ATP Safe Attachments

(To view the contributors to this article go to <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links?view=o365-worldwide>)

As a global administrator or security administrator, be sure to review your [ATP Safe Links policies](#) regularly. ATP Safe Links policies determine whether protection applies to hyperlinks in email messages only, or to URLs in Office documents as well.

After ATP Safe Links policies are in place, your organization's security team can see how ATP Safe Links protection is working for your organization by [viewing reports for Advanced Threat Protection](#).

## Example scenarios

The following table describes some example scenarios where ATP Safe Links protection might or might not be in place. (In all of these cases, we assume the organization has Office 365 Enterprise E5.)

Table 2

<b>Example scenario</b>	<b>Does ATP Safe Links protection apply in this case?</b>
Jean is a member of a group that has ATP Safe Links policies covering URLs in email and Office documents. Jean opens a PowerPoint presentation that someone sent, and then clicks a URL in the presentation.	Yes. The ATP Safe Links policies that are defined apply to Jean's group, Jean's email, and Word, Excel, PowerPoint, or Visio documents that Jean opens, so long as Jean is signed in and using Office 365 ProPlus on Windows, iOS, or Android devices.
In Chris's organization, no global or security administrators have defined any ATP safe links policies yet. Chris receives an email that contains a URL to a malicious website. Chris is unaware the URL is malicious and clicks the link.	No. The default policy that covers URLs for everyone in the organization must be defined in order for protection to be in place.
In Pat's organization, no global or security administrators have defined or edited any ATP Safe Links policies yet. Pat opens a	No. A policy that includes Office documents must be

Table 2

### Example scenario

Word document and clicks a URL in the file.

Lee's organization has a ATP Safe Links policy that has <https://tailspintoys.com> listed as a blocked website. Lee receives an email message that contains a URL to <https://tailspintoys.com/aboutus/trythispage>. Lee clicks the URL.

Jamie, Jean's colleague, sends an email to Jean, not knowing that the email contains a malicious URL.

### Does ATP Safe Links protection apply in this case?

defined in order for protection to be in place. See [Set up ATP Safe Links policies in Office 365](#).

It depends on whether the entire site and all its subpages are included in the list of blocked URLs. See [Set up a custom blocked URLs list using ATP Safe Links](#).

It depends on whether ATP Safe Links policies are defined for email sent within the organization. See [Set up ATP Safe Links policies in Office 365](#).

## Overview of Office 365 ATP Safe Attachments

View the contributors to this article by accessing the link below:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments?view=o365-worldwide>

- 05/17/2019

### In this article

1. [Overview of Office 365 ATP Safe Attachments](#)
2. [How to get ATP Safe Attachments](#)
3. [How to know if ATP Safe Attachments protection is in place](#)
4. [Submitting files for malware analysis](#)

## Overview of Office 365 ATP Safe Attachments

ATP Safe Attachments (along with [ATP Safe Links](#)) is part of [Office 365 Advanced Threat Protection](#) (ATP). The ATP Safe Attachments feature checks to see if email attachments are malicious, and then takes action to protect your organization. The ATP Safe Attachments feature protects your organization according to [ATP Safe Attachments policies](#) that are set by your Office 365 global or security administrators.

ATP protection can also be extended to files in SharePoint Online, OneDrive for Business, and Microsoft Teams. To learn more, see [Office 365 Advanced Threat Protection for SharePoint, OneDrive, and Microsoft Teams](#).

## How to get ATP Safe Attachments

First, make sure your subscription includes [Advanced Threat Protection](#). ATP is included in in subscriptions, such as [Microsoft 365 E5](#), [Microsoft 365 Business](#), Office 365 E5, Office 365 A5, etc. If your organization has an Office 365 subscription that does not include Office 365 ATP, you can potentially purchase ATP as an add-on. For more information, see [Office 365 Advanced Threat Protection plans and pricing](#) and the [Office 365 Advanced Threat Protection Service Description](#).

Next, make sure your ATP Safe Attachments policies are defined. (See [Set up Office 365 ATP Safe Attachments policies](#)) ATP Safe Attachments features are active when:

- ATP Safe Attachments policies are set up. (See [Set up ATP Safe Attachments policies in Office 365](#).)
- Users have signed into Office 365 using their work or school account. (See [Sign in to Office or Office 365](#).)

To define (or edit) ATP policies, you must be assigned an appropriate role. Some examples are described in the following table:

Table 1

<b>Role</b>	<b>Where/how assigned</b>
Office 365 Global Administrator	The person who signs up to buy Office 365 is a global admin by default. (See <a href="#">About Office 365 admin roles</a> to learn more.)
Security Administrator	Azure Active Directory admin center ( <a href="https://aad.portal.azure.com">https://aad.portal.azure.com</a> )
Exchange Online Organization Management	Exchange admin center ( <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a> ) or PowerShell cmdlets (See <a href="#">Exchange Online PowerShell</a> )

## How to know if ATP Safe Attachments protection is in place

After you have [defined \(or reviewed\) your ATP Safe Attachments policies](#), one good way to see how the service is working is by [viewing reports for Advanced Threat Protection](#).

The following table describes some example scenarios. In all of these cases, we assume the organization has an Office 365 subscription that includes Advanced Threat Protection.

Table 2

**Example scenario**

**Does ATP Safe Attachments protection apply in this case?**

Pat's organization has Office 365 E5, but no one has defined any policies for ATP Safe Attachments yet.

No. Although the feature is available, at least one ATP Safe Attachments policy must be defined in order for ATP Safe Attachments protection to be in place.

Lee is an employee in the sales department at Contoso. Lee's organization has an ATP Safe Attachments policy in place that applies to finance employees only.

No. In this case, finance employees would have ATP Safe Attachments protection, but other employees, including the sales department, would not until policies that include those groups are defined.

Yesterday, an Office 365 administrator at Jean's organization set up an ATP Safe Attachments policy that applies to all employees. Earlier today, Jean received an email message that includes an attachment.

Yes. In this example, Jean has a license for Advanced Threat Protection, and an ATP Safe Attachments policy that includes Jean has been defined. It typically takes about 30 minutes for a new policy to take effect across datacenters; since a day has passed in this case, the policy should be in effect.

Chris's organization has Office 365 E5 with ATP Safe Attachments policies in place for everyone in the organization. Chris receives an email that has an attachment, and forwards the message to others who are outside the organization.

ATP Safe Attachments protection is in place for messages that Chris receives. If the recipients' organizations also have ATP Safe Attachments policies in place, then the message that Chris forwards would be subject to those policies when the forwarded message arrives.

Jamie's organization has ATP Safe Attachments policies in place, and [ATP for SharePoint, OneDrive, and Microsoft Teams](#) has been turned on. Jamie assumes that every file in SharePoint Online has been scanned and is safe to open or download.

ATP Safe Attachments protection is in place according to the policies that are defined; however, this does not mean that every single file in SharePoint Online, OneDrive for Business, or Microsoft Teams is scanned. (To learn more, see [ATP for SharePoint, OneDrive, and Microsoft Teams](#).)