

Installation Instructions - Microsoft Exchange Button

<https://campus.barracuda.com/doc/75696051/>

The Microsoft Exchange Button is a server-side plugin for both Microsoft Exchange and Microsoft 365.

This article describes the various ways to install the Microsoft Exchange button.

Requirements

Client

The Microsoft Exchange button requires one of the following client platforms:

- **Windows Desktop** – Outlook 2013 and 2016
- **Mac Desktop** – Outlook 2016
- **Web** – The latest versions of Chrome, Safari, Firefox, Edge, Internet Explorer 11

Server

The Microsoft Exchange button requires a minimum of API.1.1 support for basic functionality, and API 1.3 for full functionality. This chart shows which client and server versions are compatible.

Client	Supported API Requirement Sets
Outlook 2016 (Click-to-Run) for Windows	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Outlook 2016 (MSI) for Windows	1.1, 1.2, 1.3, 1.4
Outlook 2019 for Mac	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Outlook 2016 for Mac	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Outlook 2013 for Windows	1.1, 1.2, 1.3, 1.4
Outlook on the Web (Microsoft 365 and Outlook.com)	1.1, 1.2, 1.3, 1.4, 1.5
Outlook client (2013 or later) connected to Exchange 2019 On-Premises	1.1, 1.2, 1.3, 1.4, 1.5
Outlook client (2013 or later) connected to Exchange 2016 On-Premises	1.1, 1.2, 1.3
Outlook client (2013 or later) connected to Exchange 2013 On-Premises	Not supported (Might have limited functionality.)
Exchange Online (OWA)	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9

The Microsoft Exchange button has different levels of functionality based on the version of Microsoft

Exchange you are using.

- Full functionality – Exchange 2019 or 2016 On-Premises; Outlook 365
- Limited functionality – Exchange 2013, based on what the Microsoft API 1.1 has available.
 - For an example of the different button views, refer to "What does the button look like?" at the end of this document.
- No functionality – Exchange versions lower than 2013 are not capable of using the Microsoft Exchange button from Security Awareness Training.
- No functionality – Hybrid implementations of Exchange (e.g., Exchange on-premise combined with Microsoft 365 acting as a front end) are not supported and might not work with the Microsoft Exchange button.

Server - Permissions Settings

Regardless of who hosts the button code – you or Security Awareness Training – the server administrator must set OAuthAuthentication to true on the Client Access Server EWS directory to enable the makeEwsRequestAsync method to make EWS requests. Refer to <https://docs.microsoft.com/en-us/office/dev/add-ins/outlook/web-services#authentication-and-permission-considerations-for-makeewsrequestasync> for details.

Ensure you have a valid certificate on your Exchange server. If you have a standalone EWS server, it requires its own valid certificate.

Exchange Button Components

The OWA button consists of Javascript, CSS, HTML, and images. It is hosted on a web server and installed on the Exchange Server by an administrator. No components must be installed on individual computers. You can host the OWA button either on Security Awareness Training's server or on your own server.

Option 1 (Recommended): Hosting on Security Awareness Training's Server - For All Users

Having Security Awareness Training host the button is the easiest deployment path available, and so it is recommended.

To host the button on Security Awareness Training's server:

1. Finish all configuration on the Outlook Plugin Configuration Manager screen as described in [Customization Options - Microsoft Exchange Button](#).
Make sure to leave the Custom Config URL field blank.
2. When you are satisfied with your configuration options, click the **Publish** button at the bottom of the page. Then, confirm your decision to publish on the pop-up screen.

The publish action can take several minutes. Wait until the the system notifies you that the publishing process is complete.

3. When the publish action is complete, close the confirmation window and scroll to the bottom of the configuration page. You will see a link to view your configuration. Click the link.
4. Confirm that you can view the XML file it shows you, your button has been published, and that you are ready to log into your Exchange Administrator account and install the add-in. If you cannot view the XML file, [contact Barracuda Networks Support](#).
5. Copy and paste the URL of the manifest XML file (`report-phish.xml`) into the Exchange Admin Center in the **Organization > Add-ins** section.

Important

Every time you make changes to your button configuration, you will need to remove the previous button installed, and then upload the new one. If you do not remove the old button when you upload the new one, you might see multiple buttons or have other inconsistencies.

After you have submitted the URL for the newly created button configuration, it might take several minutes for the button to propagate across servers.

Option 2: Hosting on Your Own Server - For All Users

To host the button code on your own server, you will need:

- A web server you control that can serve files with HTTPS
 - There must be a trusted certificate installed.
- The ability to upload a set of HTML, CSS, Javascript, and image files to that server

To host the button on your own server:

1. Finish all configuration on the Outlook Plugin Configuration Manager screen as described in [Customization Options - Microsoft Exchange Button](#). For the Custom Config URL field, enter the URL where you will host the button. The button XML manifest will be customized with that fully qualified URL.
2. When you are satisfied with your configuration options, click the **Publish** button at the bottom of the page. Then, confirm your decision to publish on the pop-up screen. The publish action can take several minutes. Wait until the the system notifies you that the publishing process is complete.
3. When the publish action is complete, close the confirmation window and scroll to the bottom of the configuration page.
4. At the bottom of the page, use the link to download the Installation Package: `InstallPhishLineOutlookJS.zip`.
5. Unzip and upload the contents of this file to your web server at the location you specified in the Custom Config URL field.
6. Confirm that you can access the `report-phish.xml` link, as listed in the CONFIGURL section of this

page. If you are able to visit the link, your files have been uploaded successfully, and you are ready to log into your Exchange Administrator account and install the add-in.

If you cannot view the XML file, [contact Barracuda Networks Support](#).

7. Copy and paste the URL of the manifest XML file (report-phish.xml) into the Exchange Admin Center in the **Organization > Add-ins** section.

Important: Every time you make changes to your button configuration, you will need to remove the previous button installed, and then upload the new one. If you do not remove the old button when you upload the new one, you might see multiple buttons or have other inconsistencies.


After you have submitted the URL for the newly created button configuration, it might take several minutes for the button to propagate across servers.

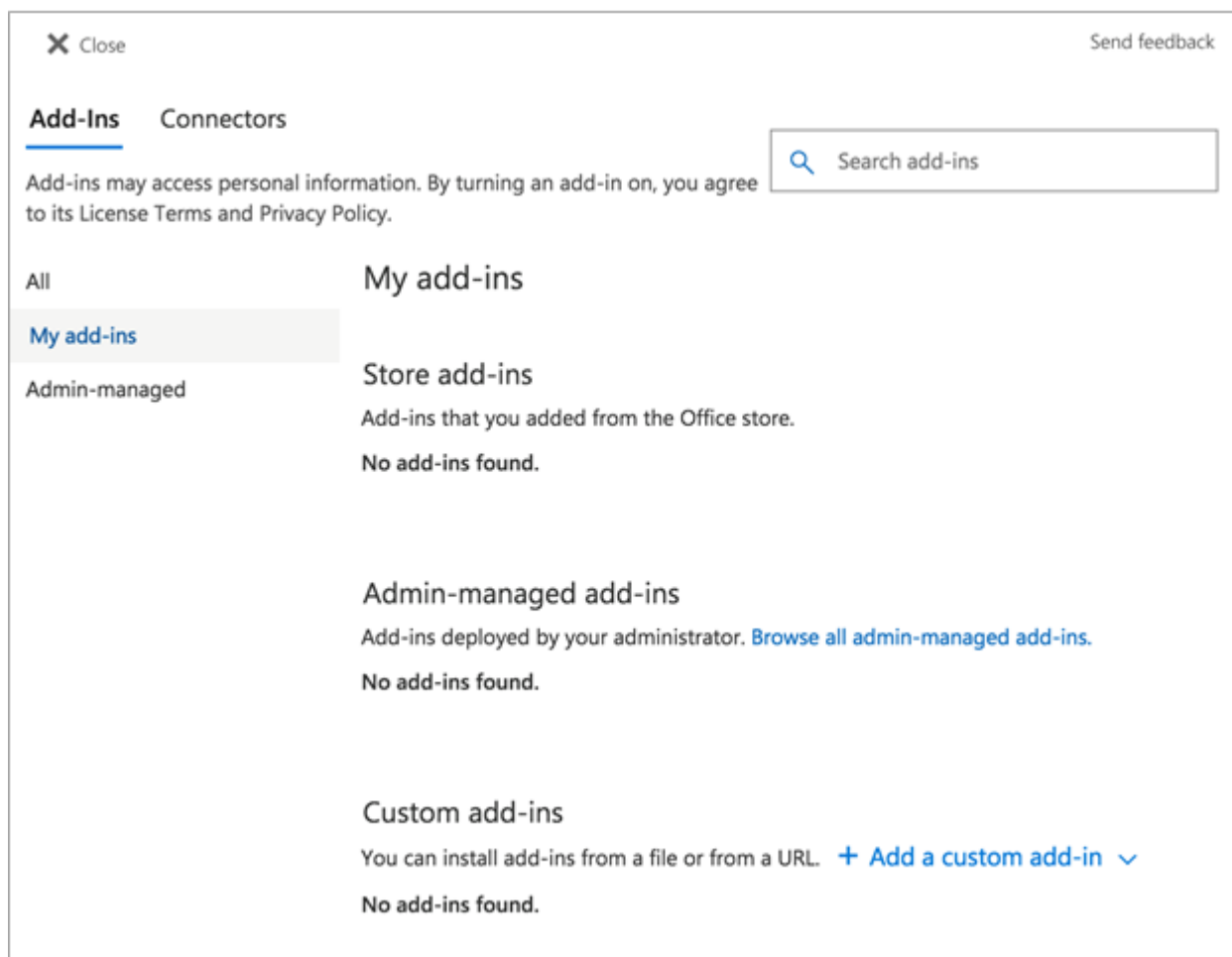
Installation Instructions for a Test Button - Single User or Group Installation

By default, the Microsoft 365 Exchange Add-In web form will give all users access to an installed add-in. However, you can test the add-in by installing it for an individual user.

To install the add-in for a group of users, use the link at the bottom of this article to read Microsoft's documentation.

To install the button add-in for an individual user:

1. Create and publish a Security Awareness Training button, following the steps described above in Hosting on Your Own Server - For All Users.
2. Locate and copy the report-phish.xml URL from the button configuration screen.
3. Navigate to your web email URL. For example, <https://outlook.office.com/owa/>
4. Click the Settings icon  in the upper-right corner of the page. Click **Manage add-ins**. The Add-ins page displays. Click **My add-ins**.



5. Under **Custom add-ins**, click **+ Add a custom add-in**.
6. When prompted, paste the URL to the report-phish.xml button you want to install. Click **OK**.
7. When the warning message appears, click **Install**.
8. When the installation is complete, you will see the button listed as a Custom Add-in on your account.

You should now be able to use the add-in on this email account. It will appear automatically in any email client (Desktop Web, Mac, or Windows Outlook) for this account. It might take a few minutes to propagate to various servers before it is available. If it does not appear after a few minutes, or if you are prompted to, restart your email client.

Distributing to a Group of Users

You can also choose to use the Exchange Online Powershell. Use this link to read the Microsoft documentation:

[https://technet.microsoft.com/enus/library/jj943757\(v=exchg.150\).aspx](https://technet.microsoft.com/enus/library/jj943757(v=exchg.150).aspx)

Under **What do you want to do**, select **Limit availability to specific users** for an example of how

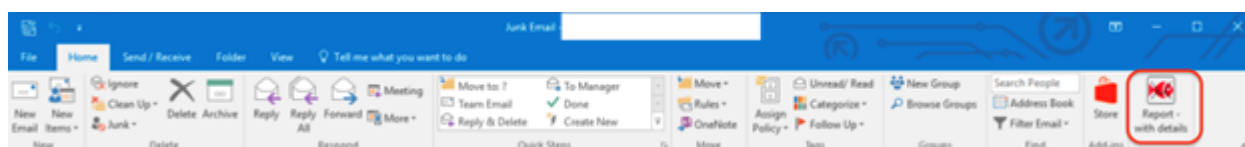
to use Exchange Online Powershell to assign a plugin to a distribution group.

What does the button look like?

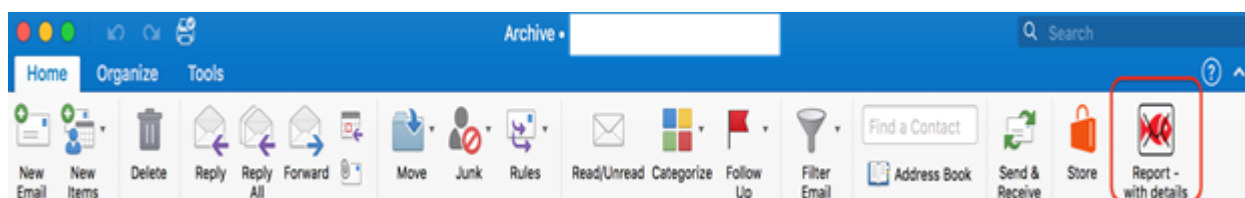
Note that the image and text on the button are customizable. The button will not necessarily look like those displayed in this section.

Button Views for Servers Supporting API version 1.3

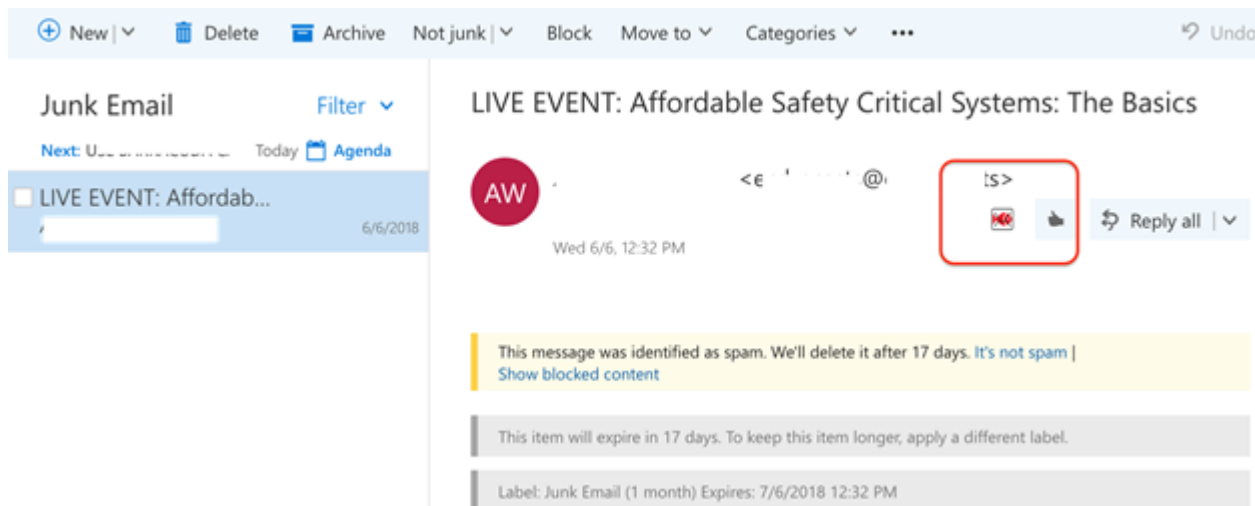
- Windows, Exchange 2013 or 2016



- Mac, Exchange 2016



Web-Based Mail, Microsoft 365

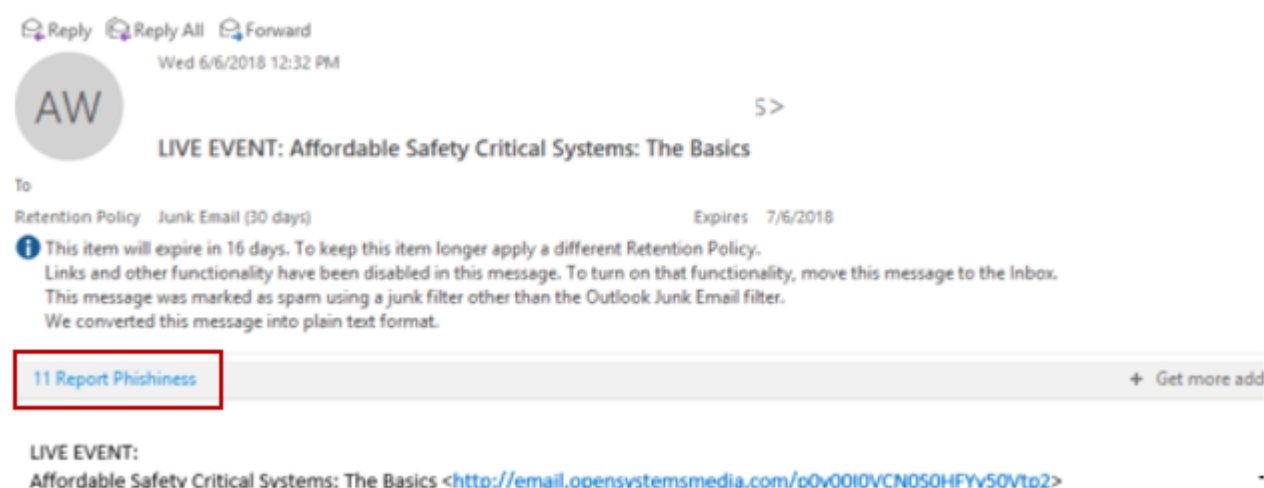


Button Views for Servers Supporting API version 1.1

If your server only supports API version 1.1, the ribbon is not available. The button appears above the body of the email you are viewing, as shown here:

Before clicking:

Click the reporting button to reveal the reporting section.



After clicking:

After you click the reporting button, the rest of the reporting section displays. Click the lower reporting button to report the suspect spam to the system.

Reply Reply All Forward

Wed 6/6/2018 12:32 PM



LIVE EVENT: Affordable Safety Critical Systems: The Basics

To

Retention Policy Junk Email (30 days)

Expires 7/6/2018

i This item will expire in 16 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk Email filter.
We converted this message into plain text format.

11 Report Phishiness ^

+ Get more add-ins

Report Phish

Click to report as a phish

LIVE EVENT:

Affordable Safety Critical Systems: The Basics <<http://email.opensystemsmedia.com/p0v00I0VCN050HfYv50Vtp2>>

Figures

1. owaSettings.png
2. myAddIns.png
3. button13b.png
4. Button13a.png
5. button13c.png
6. beforeClick.png
7. afterClick2.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.