Customization Options - Microsoft Exchange Button

https://campus.barracuda.com/doc/75696046/

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

This article describes how to create and customize the Microsoft Exchange button.

To create a new button:

1. Navigate to **System > Button Plugin Config**.
2. On the **Button Configuration Manager** page, click **New**.
3. Enter a **Configuration Name**, a user-friendly name you will use for this button configuration. This name is not visible to users.
4. Select a **Code Version** to specify the type of button you want to create – **Microsoft Exchange** – and the software version used for this configuration. Be sure to select the newest version available. Other configurations are described in other articles.
5. Click **Save**.
6. Specify the configuration based on the descriptions below, then click **Save** again.

General

- **Configuration Name** – The name you specified above is copied here. You can change it at this point if you choose.
- **Button Is Published** – If selected, the button is already published to the Security Awareness Training servers. This field is not editable.
- **Last Publish Request** – If the button is published, displays the last time a Button Publish was requested.
- **Last Publish Completed** – If the button is published, displays the l ast time a Button Publish request was completed.

Code Version

- **Code Version** – Version of the software code you chose for this configuration in Step 4 above.
- **Button Code Type** – Displays the type of source code for the selected **Code Version**.
- **Code Description** – Displays the description of the selected **Code Version**.

Button Image

- **Button Image** – Select and upload a graphics file to display on the button. Recommendation: Select a GIF or PNG file. If needed, the system will automatically resize the image to approximately 80 x 80 pixels.
- **Button Image File Type** – Displays the type of file you uploaded for the **Button Image**

(GIF or PNG).
- **Button Image File Size** – Displays the s ize of the image file you selected and uploaded.

Instructions

This section includes the ZIP file needed to install the Exchange button. For details, refer to Installation Instructions - Microsoft Exchange Button.

> **Note** – This ZIP file is not required if you are deploying the button to Security Awareness Training servers, which is the recommended deployment method. The ZIP file is only needed if you are hosting the button on premises.

General Settings

- **Add Header Details to Wrapper Email Body** – Most emails are <1MB and are reported as attachments, so all data is included. For rare emails >1MB, select this option to include header data in forwarding wrapper email.
  - Selecting this option adds the following to the message:
    - plain text version of the email
    - email headers
    - URLs present in the email
    - reporting button version information
    - reported-from folder
  - If you do not select this option, only the Phishing/Mock/Not Internal or Mock Body Text displays, followed by a base64-encoded version of the original message.
- **Are you sure - Enable** – Select this option if you want to prompt users if they really want to report the selected email.
- **Set Are you sure buttons to OK/Cancel instead of Yes/No** – Select this option to change the **Are you sure** button options to **OK** and **Cancel**.
- **Are You Sure - Title** – Optionally customize the title on the prompt asking if the user wants to report the selected email.
- **Are You Sure - Prompt Text** – Optionally customize the prompt asking if the user wants to report the selected email.
- **Disable Internal Delete** – Select this option if you do not want internal emails to be deleted when they are reported. Emails are considered internal if they originate from a domain name you have listed under the **Internal Message** section. See the **Internal Message** section below for more details.

Phishing

- **Phishing Button Label** – Enter a text label for the phishing button.
- **Phishing Button Tool Tip Title** – Enter text for the title and text of the tool tip that appears when a user hovers over the phishing button.
- **Phishing Report Email Subject** – Emails reported with the phish button that are less

than 1 MB are forwarded as email attachments. Specify the subject line for these emails. Larger reported emails are forwarded with the original subject. Use {0} to insert the original subject.
- **Phishing Body Text** – Enter text for the body of an email used to report a suspect email that is *not* a mock phishing test or an internal message.

To view reported email information within Security Awareness Training, include your Security Awareness Training email address (*phishline_<Instance_Name>@phishline-incident-response.com*) in the **Send To** fields in one or more of the sections below.
Message detail is available in **Results > Inbox Analysis** and **Results > Incident Response**. For more information, refer to Inbox Analysis and Incident Response.
Users who report campaign emails receive credit, shown in **Results > Outbound Analysis**. For more information, refer to Outbound Analysis.

Internal Message

- **Internal Send To** – Enter one or more email addresses to notify of reported emails from the internal domains. Separate multiple email addresses with semicolons or commas. For visibility within Security Awareness Training, include `phishline_<Instance_Name>@phishline-incident-response.com`. See note above.
- **Internal Reporting Success Pop Up Message** – Optional. Enter text to appear to users when they report a phishing message from an internal domain.
- **Reported Internal Body Text** – Enter the body text for the reported phishing email when it is recognized as Internal. Use {0} to insert the matching internal domain.
- **Internal Domains** – Enter a list of domains that the plugin will use to identify reported emails that came from your internal domains. Enter one domain per line in the format *example.com*.

Mock Message

- **Mock Send To** – Enter one or more email addresses to notify of reported emails recognized as Mock Phishing tests. Separate multiple email addresses with semicolons or commas. For visibility within Security Awareness Training, include `phishline_<Instance_Name>@phishline-incident-response.com`. See note above.
- **Mock Success Pop Up Message** – Optional. Enter text to appear to users when they report a mock phishing message.
- **Reported Mock Body Text** – Enter the body text for the reported email when it is recognized as a mock phishing test. Use {0} to insert header information.
- **Mock Phishing Headers** – Enter a list of X-Headers, one per line, to identify mock phishing emails. Configure custom X-Headers in **System > Global Settings**. X-Headers can be any string of alphanumeric characters. Choose a string that does not identify the

function of the X-Header and is unique enough not to be duplicated by another process. An example of an X-Header for this use is `X-AEDE112EDA`.

Not Internal Or Mock

- **Phishing Report Send To** – Enter one or more email addresses notified when a user clicks the phishing button, but the suspect emails are neither Mock nor Internal. Separate multiple email addresses with semicolons or commas. For visibility within Security Awareness Training, include `phishline_<Instance_Name>@phishline-incident-response.com`. See note above.
- **Phishing Success Message** – Enter an optional message that will be shown to users for every reported phishing message that is not Mock or Internal.

2-Step Button

This feature is not available with the Exchange button due to Microsoft 365 system limitations.

Spam

This feature is not available with the Exchange button due to Microsoft 365 system limitations.

Advanced

- **Custom Config URL** – Enter the URL, if you are hosting your own code.

Regardless of whether you or Security Awareness Training is hosting the button code, 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/reference/objectmodel/requirement-set-1.5/office.context.mailbox for more details.

- **Last Modified** – Displays the last time this configuration was modified.