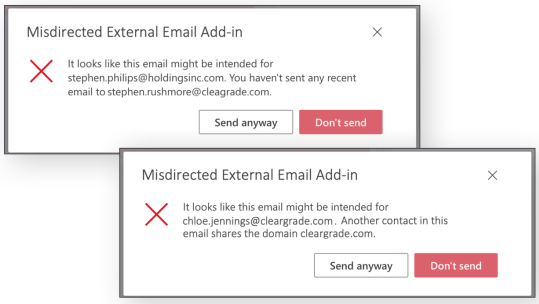
DARKTRACE/EMAIL MISDIRECTED EXTERNAL EMAIL ADD-IN

Introduction

Available for Microsoft Outlook, the Darktrace Misdirected External Add-in draws upon the 'pattern of life' of user-to-user, contact-to-contact, and business-to-business relationships developed by Darktrace/Email. Triggered when a user sends an email, Darktrace/Email Misdirected External Add-in warns the end user if the intended recipients may be incorrect - from a simple mistype to a confusion between two trusted contacts - and guides them towards correcting the addressees.



How Does It Work?

The add-in is available for Windows and MacOS Microsoft Outlook desktop clients and in Outlook when accessed from a browser. When a user clicks "Send" on an email, the Add-In will analyze the addressees for anomaly. End-users may briefly observe a status message that indicates that the Misdirected External Add-In is analyzing their email during this step - if no anomaly is found, this status will disappear and the message will send successfully. This scenario will apply to the majority of external email communications.

The Darktrace/Email Misdirected External Add-In will display a message to end-users under the following circumstances:

- The email address of the external recipient does not fit with the contextual profile of external contacts this user - or the wider organization - has recently communicated with. This may be due to a mistyped address or a confusion between contacts with similar names.

  In this case, the Add-In will also suggest the likely intended recipient of the email based upon a contextual understanding of normal contact-to-contact relationships.

- The email has multiple external recipients but one of the email addresses is not consistent with those contacts. For example, three recipients are `@holdingsinc.com` and one recipient is `@holding.com`.

  Here, the Add-In will also suggest the likely intended recipient of the email based upon both the other recipient domains, and a contextual understanding of normal contact-to-contact relationships.

These two scenarios are not mutually exclusive - multiple anomalies may be identified with the same message.

External Emails vs Internal Emails

Darktrace/Email Misdirected External Add-In supports external emails only. You may observe the Add-In analyzing outbound emails between internal contacts - this is a purely pre-analysis step where Darktrace/Email establishes whether the recipients are associated with internal or external domains.

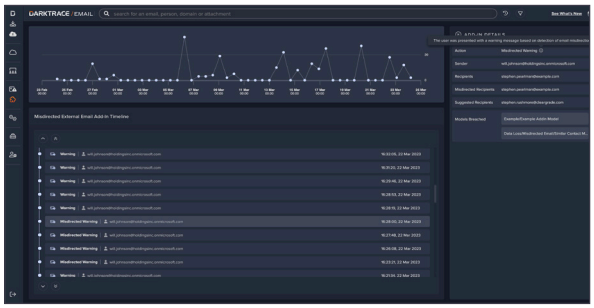
The Darktrace Misdirected External Add-in will not attempt to identify misdirected internal email communications, and will not prompt the user to correct these addresses.

Available Interactions

The message displayed to end-users has two interactions available:

- "Don't Send" will close the pop-up and return the user to their draft message to correct the discrepancies.
- "Send Anyway" will discard Darktrace/Email recommendations and send the message regardless.

Misdirected External Email Dashboard



If the Darktrace/Email Misdirected External Email is deployed in your Microsoft 365 environment, an additional dashboard will appear on the Email Console (**Add-In** > **Misdirected External**).

This dashboard includes a timeline of interactions between the Add-In and your end users which is filterable by user or action. These interactions are also displayed in the user timeline and by filtering the main email logs by the new "End User Interaction" filter.

Requirements

- Only Microsoft 365 environments are supported at this time(no additional license requirements). On-premises Microsoft Exchange and Gmail deployments are not supported.
- A user with Microsoft Global Admin permissions is required during setup to deploy the Add-in.
- A user with access to the Darktrace/Email Email Console and Config page is required during setup.

Deploying the Add-In

The Darktrace/Email Misdirected External Email Add-in can be deployed to multiple users via the Microsoft 365 Integrated Apps portal. Many organizations choose to deploy the add-in to a small group of users, then gradually increase the scope. The following process is essentially aligned with that described in the Microsoft documentation "Test and deploy Microsoft 365 Apps by partners in the Integrated apps portal".

The deployment process will require access to the Darktrace/Email console "Config" page and the Microsoft 365 Admin center. Deployment in the Microsoft 365 Admin center must be performed by a Global Admin user as it requires a user to consent to permissions on behalf of other users in the organization.

Deployment Process

1. In the Microsoft 365 Admin Portal, access the **Settings** > **Integrated Apps** section.

   A direct link to this page is also included on the Darktrace/Email Config page (**System** > **Config**) - click "Go to Portal" under **Misdirected External Email** > **Installation**.

2. Click **Upload custom apps**. The "Deploy New App" dialog will open.

3. Under the **App Type** subheading, select "Office Add-In" from the dropdown.

4. Under the **Choose how to upload app** subheading, choose "Provide link to manifest file".

5. In a new tab or window, access the Darktrace/Email console as user with permission to view the Config page.

   Navigate to this page (**System** > **Config**)

6. Click "Misdirected External Email" from the left hand options.

   Under the **Installation** subheading, copy the Manifest URL to the clipboard using the copy icon.

7. Returning to the Microsoft Admin Portal, paste the Manifest URL copied above into the "Provide link to manifest file" field.

   Click **validate**. After successful validation, click **Next** to proceed.

8. If you are deploying the app to a small group of users for testing, set "Is this a test deployment?" to **Yes**.

   This can be modified later.

9. Assign users who should receive the add-in. Many organizations choose to deploy the add-in to a small group of users, then gradually increase the scope.

   This can be modified later. Click **Next** to proceed.

10. On the next step - "Accept permissions requests" - review the permissions requested by the app and click **Accept Permissions**.

    A Microsoft 365 pop-up will open and you will be prompted to log in. The user who logs in to grant permission **must be a Global Administrator**, or Darktrace/Email will not be able to deploy the add-in to users other than the authenticating user.

    Accept the permissions on behalf of the organization, then click **Next** to proceed.

11. Review the Add-In configuration and click **Finish Deployment** - Microsoft 365 will now deploy the add-in to the chosen users.

    Click **Done** to close the deployment dialog. Deployment will continue in the background.

Darktrace provides a demo email address for testing purposes - any emails to this address will trigger the Darktrace Misdirected External Add-in. The email address can also be found on the config page under the **Misdirected External Email** > **Functionality** section.

Modifying the Add-In

If you wish to make changes to any of the settings, locate the **Misdirected External Email** entry in the list of **Integrated Apps** in the Microsoft Admin Center. Click on the name of the app to view or change settings.

The Add-In can also be disabled by turning off **Outbound Validation** on the Darktrace/Email Email Console Config page.

Please note that upon the expiry of any subscription to Darktrace/Email, the Darktrace Misdirected External Add-in (the "Add-in") will remain in the Microsoft 365 environment, but will not be functional. The Add-in is run every time a user sends an outbound communication from the Microsoft 365 environment, by using the Add-in, the user acknowledges and accepts the risk of any potential disruption caused to the flow of outbound email traffic, as intended by the Add-in or otherwise. The Add-in processes email metadata in accordance with the Darktrace Data Processing Addendum.