Cisco XDR

Cisco XDR connects Cisco security products into an integrated platform. Secure Email Threat Defense is integrated with Cisco XDR and Cisco XDR ribbon.

- XDR allows you to view and act on Secure Email Threat Defense information alongside data from your other Cisco security products.
- XDR ribbon allows you to navigate between Cisco security products, access casebook, search observables, and view incidents.

For details on XDR not provided in this document, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

XDR

Secure Email Threat Defense provides the following tiles that can be viewed in a Cisco XDR dashboard:

- Messages by Direction: Shows your total email traffic by direction. Mail is divided into Outgoing, Internal, and Incoming.
- Threats: Shows a snapshot of messages that were determined to be BEC, Scam, Phishing, or Malicious.
- Spam: Shows a snapshot of messages that were determined to be Spam.
- Graymail: Shows a snapshot of messages that were determined to be Graymail.

For information on the XDR dashboard, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

Authorize Cisco XDR for Secure Email Threat Defense

Before you can authorize Cisco XDR for Secure Email Threat Defense, you must have a Cisco XDR account and be part of a Cisco XDR organization. For more information, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

Note: A Secure Email Threat Defense account can only be integrated with one Cisco XDR organization at a time.

Secure Email Threat Defense super-admin and admin users can authorize the Cisco XDR module for their Secure Email Threat Defense instance:

1. Select **Administration** > **Business**.
2. Under **Preferences** > **Extended Detection and Response**, click **Authorize XDR Integration**.
3. Complete the authorization flow.

A banner appears, stating that XDR configuration was successful.

You can now add Secure Email Threat Defense tiles to your XDR dashboard. For information on how to do this, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm

Revoke XDR Authorization for Secure Email Threat Defense

Note: Any super-admin or admin user can perform this task. It does not have to be performed by the user who authorized XDR for the Secure Email Threat Defense instance.

To revoke XDR authorization:

1. Select **Administration** > **Business**.
2. Under **Preferences** > **Extended Detection and Response**, click **Revoke Authorization**.

A banner appears, stating that XDR configuration was successfully updated.

XDR Ribbon

The XDR ribbon is located in the lower portion of the page, and persists as you move between Secure Email Threat Defense and other Cisco security products in your environment. Any Secure Email Threat Defense user can authorize the XDR Ribbon for their use. Use the ribbon to navigate between your Cisco security applications, access casebook, search observables, and view incidents.

For information on XDR Ribbon, see the Cisco XDR documentation:
https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm

Pivot Menu

When you authorize the ribbon, XDR pivot menus are added within the Secure Email Threat Defense message report. These menus give you a central point of access to additional information about each observable, depending on which Cisco security products you have purchased.

Similarly, Secure Email Threat Defense’s integration with XDR allows you to use the pivot menu to access Secure Email Threat Defense from XDR. Observables you can pivot from include:

- Email Address
- Email Message ID
- Email Subject
- File Name
- Sender IP
- SHA 256
- URL

Use the pivot menu to:

- Quarantine messages with a specific observable directly from the pivot menu. Secure Email Threat Defense will indicate these messages as manually remediated by an XDR user.
  - **Note:** Quarantine from the pivot menu is limited to 100 messages.
- Move the messages you quarantined back to the inbox. Secure Email Threat Defense will indicate these messages as manually remediated by an XDR user.
  - **Note:** Moving from quarantine to the inbox is limited to 100 messages.

For more information on XDR pivot menus, see the XDR documentation:
https://docs.xdr.security.cisco.com/Content/pivot-menu.htm

Authorize XDR Ribbon

XDR ribbon is authorized at the user level. You can authorize the ribbon from within the ribbon or from the User Preferences menu.

Note: Your XDR account needs to be activated before you can authorize the ribbon. You can do this by following the instructions in Authorize Cisco XDR for Secure Email Threat Defense, page 61 or by integrating any other modules in XDR.

Authorize from within XDR Ribbon

To authorize your XDR ribbon from within the ribbon:

1. Click **Get XDR** in the XDR ribbon.
2. In the Grant Application Access dialog, click **Authorize Secure Email Threat Defense Ribbon**.

Your XDR ribbon is now authorized. A banner appears, stating that XDR configuration was successfully updated.

Authorize from Secure Email Threat Defense User Settings

To authorize your XDR ribbon from the User Settings menu:

1. Select **User** (profile icon) > **User Settings**.
2. Under **Preferences** > **XDR Ribbon**, click **Authorize XDR Ribbon**.
3. In the Grant Application Access dialog, click **Authorize Cisco Secure Email Threat Defense Ribbon**.

Your XDR ribbon is now authorized. A banner appears, stating that XDR configuration was successfully updated.

Revoke XDR Ribbon Authorization

XDR ribbon is authorized at the user level. You can revoke authorization from within the ribbon or from the User Preferences menu.

Revoke Authorization from within XDR Ribbon

To revoke your XDR ribbon authorization from within the ribbon,

1. Select **Settings** > **Authorization** > **Revoke** in the XDR ribbon.
2. In the Revoke dialog, click **Confirm**.

XDR ribbon is no longer authorized for your Secure Email Threat Defense user account.

Revoke Authorization from Secure Email Threat Defense User Settings

To revoke your XDR ribbon authorization from the User Settings menu:

1. Select **User** (profile icon) > **User Settings**.
2. Under **Preferences** > **XDR Ribbon**, click **Revoke Authorization**.

XDR ribbon is no longer authorized for your Secure Email Threat Defense user account. A banner appears, stating that XDR configuration was successfully updated.