

Email Monitoring Configuration

You can streamline many routine servicing workflows by setting up monitoring for generic email addresses (for example, *claims@youragency.com* or *sales@youragency.com*). Instead of moving items from external mailboxes into the system manually to be worked, you can route them to the appropriate accounts and employees or work groups directly from the [Unrouted Email](#) area. You can also configure the system to attach each received email message to the appropriate account or policy automatically if it meets specific matching conditions (see [Associate an email address and add server rules for monitoring](#)).

Microsoft Exchange Server Requirements

This functionality is only available to organizations using a *Microsoft Exchange Server 2016* backend for their email, or whose email provider uses a *Microsoft Exchange Server* backend (e.g. Hosted Exchange). Only *Microsoft Exchange Server 2016* is supported. While you may be able to use email monitoring with older versions of *Exchange Server*, Applied has not tested these versions and cannot guarantee full functionality.

Full Access Mailbox Configuration

Before you can set up email monitoring in Applied Epic, an administrator must access the *Microsoft Exchange Server* used for your agency's email to configure one mailbox with *Full Access* permissions for all generic email addresses to be monitored. You can either use an existing mailbox or create a new mailbox for this purpose. If you maintain your own email server or use a third-party server, you may need to work with your IT team to configure the appropriate mailboxes. If you use Applied Hosted Exchange, you may want to review the information in the *Mailboxes* section of the *Microsoft Exchange hosted by Applied Help File*.

To configure the mailbox through Applied Hosted Exchange, do one of the following:

- [Create a new mailbox with Full Access](#)

Once you create a mailbox and grant it *Full Access* permission to all of the generic email addresses you want monitored, you must return to *Configure > Attachment > Monitor Emails* in Applied Epic and enter the email address and password for the mailbox in the *Exchange Server Login* frame. Remember, you must add the mailbox whose credentials you will use in Applied Epic to the *Full Access* permissions list for each mailbox you want monitored.

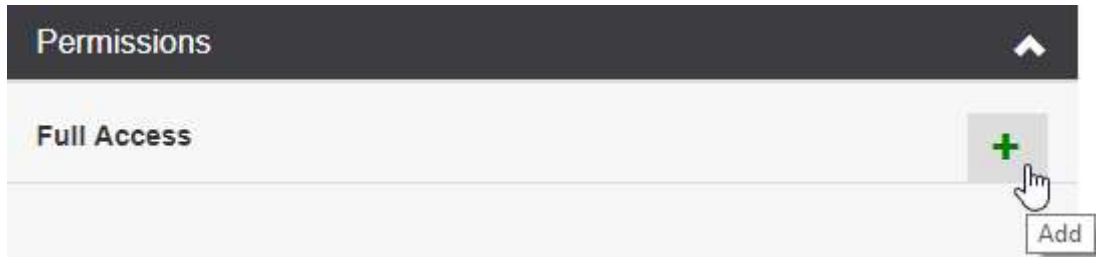
1. Log in to Applied Hosted Exchange through the *Admin Panel*.
2. Click the **Mailboxes** tab on the Hosted Exchange Home screen.



3. Click the **Add** button.
4. Select the **User** radio button.
5. Enter the **Display Name** that will display in the list of mailboxes.
6. Enter the local-portion of the **Email Address** (i.e. the text before the @ symbol).
7. Enter a unique **Password**.
8. Select **Account enabled**.
9. Click **Save** to create the new mailbox.
10. If you are not automatically redirected to the list of mailboxes, click the **Mailboxes** tab.
11. In the list, hover over a mailbox you want to be monitored and click **Edit Mailbox**



12. Click **Permissions** (depending on your screen resolution, you may need to scroll).
13. In the *Full Access* area, click the **Add** button.



14. Select the **mailbox** you created in a previous step and click **Add**.
15. Review the mailbox listed below *Full Access* and click **Save**.
16. Repeat steps 11-15 for each mailbox you want to be monitored.

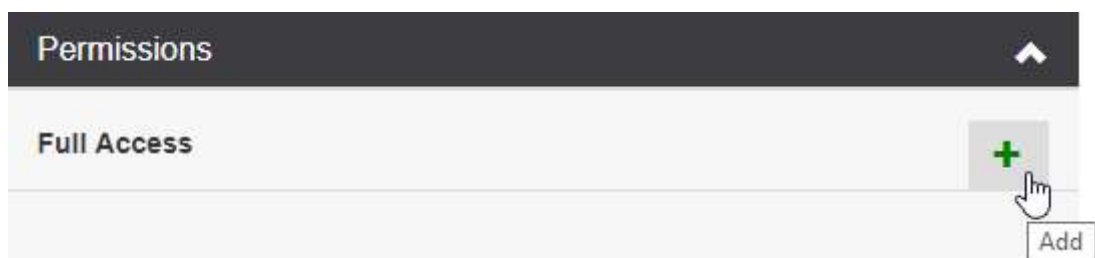
- [Configure Full Access for an existing mailbox](#)

Once you configure a mailbox with *Full Access* to all of your organization's generic email addresses, you must return to *Configure > Attachment > Monitor Emails* in Applied Epic and enter the email address and password for the mailbox in the *Exchange Server Login* frame. Remember, you must add the mailbox whose credentials you will use in Applied Epic to the *Full Access* permissions list for each mailbox you want monitored.

1. Log in to Applied Hosted Exchange through the *Admin Panel*.
2. Click the **Mailboxes** tab on the Hosted Exchange Home screen.
3. In the list, hover over a mailbox you want to be monitored and click **Edit Mailbox**



4. Locate and click **Permissions**.
5. Locate the *Full Access* area and click **Add**.



6. Select the **mailbox** you will use to enter the credentials in Applied Epic and click **Add**.
7. Review the mailbox listed below *Full Access* and click **Save**.
8. Repeat steps 3-7 for each mailbox you want to be monitored.

Exchange Server Login Configuration

Once you have followed the steps above to create or obtain an email address and password for the mailbox with *Full Access* permissions to all of the mailboxes you will be monitoring, you must enter these credentials in the Email Monitoring Configuration area of Applied Epic to connect the system to your Exchange Server before you can add or edit individual email addresses for monitoring. Follow these steps to access this area and set up monitoring for each mailbox.

1. From *Home*, do one of the following:

- Click **Configure** on the navigation panel.
- Click **Areas > Configure** on the menubar.
- Click the **down arrow** next to *Home* on the options bar and select **Configure**.

From any other area of the program, do one of the following:

- Click the **down arrow** to the right of the *Home* options bar button and select **Configure**.
- Click **Home > Configure** on the menubar.

2. Click **Attachment** on the navigation panel or **Areas > Attachment** on the menubar.

3. Click **Monitor Emails** in the navigation panel.

4. In the *Exchange Server Login* section, enter the email address for the *Full Access* mailbox in the **Login** field.

5. Enter the **Password** for the *Full Access* mailbox.

6. Click **Create Login**.


You can do the following from here:

- [Associate an email address and add server rules for monitoring](#)

You must enter each generic email address you want Epic to monitor individually (e.g., sales@youragency.com; claims@youragency.com). Assign either a work group or a specific employee to monitor email sent to each address. Make sure you have created the necessary [work groups](#) before assigning any email addresses to them. Each email address can be assigned to only one work group or employee. The *Automatically route email* option enables you to attach email to the appropriate account or policy if it meets specific matching conditions (see step d).

The *Status* column in the list of email addresses and the *Connection status* frame indicate whether Applied Epic has connected or is in the process of connecting to each mailbox. A *Not Connected* status indicates a failure to connect to a mailbox. If you see this status, ensure that autodiscovery is enabled on the Exchange Server and that the server (or your email service) is operational. An *Unavailable* status indicates a problem with the credentials entered for an email address (if you mistyped the address or password, for example). You can attempt to resolve the issue by deleting the email address from the list and then reentering the information for it. If either of these statuses continues to display after you have performed these troubleshooting steps, contact Applied Customer Support.

To add an email address for monitoring, do the following:

- a. Click the **Add** button , or press **[Ctrl] + [Insert]** with focus on the list.
- b. In the *Details* section, enter the complete **Email Address**.
- c. Do one of the following:
 - To make emails sent to this address accessible to all members of a work group, select the **Work Group** radio button and select the **group** from the dropdown menu.
 - If a specific individual is responsible for processing emails sent to this address, select the **Employee** radio button and select the **employee** from the dropdown menu.
- d. Select the **Automatically route email checkbox** if you want incoming emails to be attached to the appropriate policy or account and routed to the selected *Work group* or *Employee* automatically when they [meet specific matching conditions](#).


If you select this option, the @REA (Email Routed Automatically) background system event defaults in the *Activity Code* dropdown to ensure that automatically routed emails remain

trackable in your system. If necessary, you can [configure this system event](#) to add additional activity codes or turn off this background event.

- e. In the *Emails left on Exchange Server* section, select one of the following options to determine what the system does with email messages in the mailbox after they populate in the *Unrouted Emails* area of Applied Epic:
 - **Delete:** Messages are deleted from the server, and the only record of them is in Applied Epic. If you select this option, no manual management of the mailbox outside of Epic is necessary.
 - **Mark as read:** The server retains a copy of each email message but marks it as read once it is received by Epic. If you select this option, someone must manage the mailbox on the server and delete, move, or archive messages manually to ensure that it does not exceed its storage limit.
- f. Click **Finish** to save the email address or **Cancel** to discard your changes.



- [Edit an email address association and server rules](#)

You can easily update monitoring options for a mailbox, such as the [work group](#) or employee responsible for monitoring it in the [Unrouted Email](#) area, as well as the system's handling of email messages left on the Exchange Server. However, you cannot edit the email address associated with any existing entry. If you need to modify the email address association, you must delete the entry and create a new one.

- a. Select the **email address** in the list.
- b. Click the **Edit** button .
- c. In the *Details* section, do one of the following:
 - To make emails sent to this address accessible to all members of a work group, select the **Work Group** radio button and select the **group** from the dropdown menu.
 - If a specific individual is responsible for processing emails sent to this address, select the **Employee** radio button and select the **employee** from the dropdown menu.
- d. Select the **Automatically route email checkbox** if you want incoming emails to be attached to the appropriate policy or account and routed to the selected *Work group* or *Employee* automatically when they [meet specific matching conditions](#).

If you select this option, the @REA (Email Routed Automatically) background system event defaults in the *Activity Code* dropdown to ensure that automatically routed emails remain trackable in your system. If necessary, you can [configure this system event](#) to add additional activity codes or turn off this background event.

- e. In the *Emails left on Exchange Server* section, select one of the following options to determine what the system does with email messages in the mailbox after they populate in the *Unrouted Emails* area of Applied Epic:
 - **Delete:** Messages are deleted from the server, and the only record of them is in Applied Epic. If you select this option, no manual management of the mailbox outside of Epic is necessary.
 - **Mark as read:** The server retains a copy of each email message but marks it as read once it is received by Epic. If you select this option, someone must manage the mailbox on the server and delete, move, or archive messages manually to ensure that it does not exceed its storage limit.
 - f. Click **Finish** to save your changes or **Cancel** to discard them.
- [Delete a Monitored Email Address](#)
 - a. Select the **email address** in the list.
 - b. Do one of the following:

- Click the **Delete** button  to the left of the list.
 - Click **File > Delete** on the menubar.
 - Press **[Delete]** on your keyboard.
- c. You are prompted to confirm the deletion. Click **Yes** to delete the email address or **No** to retain it.
- Print the list of Monitored Email Addresses
 - a. To print the list of generic email addresses, do one of the following:
 - Click the **Print** button  to the left of the list.
 - Click **Print > Listview** on the options bar.
 - Click **File > Print > Listview** on the menubar.
 - b. Print this list as you would any other document.