Releasing Email Blocked by Forcepoint DLP

SMTP violations with the quarantine action are held in the Forcepoint DLP forensics repository. There are two ways to release messages from quarantine:

- Administrators with appropriate permissions can click Remediate > Release on Incidents report page in the Forcepoint Security Manager.
- Administrators or end users who receive notifications when email messages are blocked can be given permission to release the messages by replying to the notifications.
  This option requires a force release mailbox.

---

**Important**

To have notifications sent, select an action (or action plan) that specifies notifications when configuring a policy rule or attribute.

---

There are two steps involved in configuring a force release mailbox:

1. Configure Forcepoint DLP settings.
2. Configure Microsoft Exchange or another mail gateway.
   This document discusses Active Directory with Microsoft Exchange, but the concepts are universal.

It does not matter which component detected the SMTP violation. The force release mailbox can be used to release incidents detected by the protector in inline MTA mode or Forcepoint Email Security.
Configure Forcepoint DLP settings

To configure a release gateway:

1. Log onto the Data Security module of the Security Manager.
2. Navigate to the Settings > General > Remediation page.

3. In the Release Gateway box, select Use the following gateway.
4. Enter an IP address or hostname and Port to use for communicating with the mail release gateway. The release gateway should be a mail hop used to route mail outside the organization.

5. Click OK.

After configuring a release gateway, also configure notifications. Instructions can be found in the Forcepoint DLP Administrator Help.

To configure the mail server, see Configure Microsoft Exchange, page 3.
Configure Microsoft Exchange

There are three general steps to configuring Microsoft Exchange:

1. Create a new Exchange contact.
2. Create an Exchange mailbox.
3. Configure a forwarding address.

The procedures for configuring these settings vary by Microsoft Exchange version. See:

- Configuring Exchange 2007 and 2010, page 4
- Configuring Exchange 2003, page 6

**Note**

Although the following procedures apply to specific Exchange versions, this process can also be used with other mail gateways.

**Warning**

- If there are multiple notifications, configuration must be repeated for every sender email address.
- When the force release mailbox feature is used, the Notifications sender cannot be a real email address.
- The Active Directory-based process above can be used with other mail systems, as long as the protector or integrated Forcepoint Email Security is an MTA over outgoing email messages.
Configuring Exchange 2007 and 2010

Create a new Exchange contact

1. In the Exchange Management Console, under Recipient Configuration, right-click **Mail Contact** and select **New Mail Contact** from the pop-up menu.

2. Enter details for the contact.

3. Under External e-mail address, click **Edit**, then create a contact with an SMTP address like DLPNotificationMbx@mycompany.dlp.

   ![New Mail Contact](image)

   **Note**
   The new contact can have any name or email address, but the email domain should not be internal. The domain preferably should not be resolvable by DNS.

4. Click **Next** on the wizard.

5. Click **Finish**.

Create an Exchange mailbox

Create an Exchange mailbox and/or Active Directory user account as follows:

1. Open the Active Directory - Users and Computers console, open the Users folder.

2. Create a user with the email address of the notification sender that was configured in the Security Manager.

3. Follow the steps in the wizard to create an Exchange mailbox in the appropriate mailbox database.

Consult the Exchange administrator with any questions.
Configure a forwarding address

1. Right-click the user account and select **Properties**.
2. Select the **Mail Flow Settings** tab, then select the **Properties** checkbox.
3. Select **Delivery Options**, then mark the **Forward to** option.
4. Browse to the contact that was created in the steps above.
5. Click **OK** and complete the configuration.

---

**Configuring Exchange 2003**

**Create a new Exchange contact**

The contact created in this step can have any name and email address, but the email domain should not be internal. As a best practice, the name should be one that cannot be resolved by DNS.

1. In the **Active Directory - Users and Computers** console, right-click any OU or AD container, and select **Users > New > Contact**.
2. Enter a **First name**, **Last name**, and **Display name** for the contact, then click **Next**.
   The new contact can have any name.

3. Make sure **Create an Exchange e-mail address** is selected, then click **Modify**.
4. In the New E-mail Address window, select **SMTP Address**, then click **OK**.

![Image of New E-mail Address window]

5. On the General tab of the Internet Address Properties window, enter an **E-mail address** for the account.

---

**Note**

The email domain should not be internal, and preferably should not be resolved by DNS.

---

![Image of Internet Address Properties window]

6. Click **OK**.
Create an Exchange mailbox

To create an Exchange mailbox and/or Active Directory user account:

1. In the Active Directory - Users and Computers console, open the Users folder.
2. Create a user with the email address of the notification sender that was configured in the Security Manager.
3. Follow the steps in the wizard to create an Exchange mailbox for the user.
   Consult the Exchange administrator with any questions.

Configure a forwarding address

1. Right-click the user account that was just created select Properties. The Properties dialog box appears.

   ![Properties dialog box](image)

2. Select the Exchange General tab, then click Delivery Options.
3. In the Forwarding address pane, select Forward to.
4. Click Modify. The Select Recipient window displays.
5. Select or search for the contact that was created. This will be the destination for the forwarding.
6. Click OK to complete the configuration.