Releasing Email Blocked by Forcepoint DLP

Releasing Email Blocked | Forcepoint DLP | v8.9.x

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.

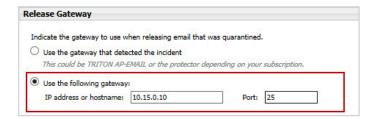
Configure Forcepoint DLP settings

To configure a release gateway:

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

₩-	Define the IP address and port number for the syslog server and mail release gateway.					
atus	Syslog Settin	gs				
	Enter the IP ad	dress or hostname and port n	number for the syslog se	rver.		
4	IP address or h	ostname:		Port:	514	
orting	Select Use sys	log facility if you want to k	now from what part of th	he system s	syslog me	essages originate.
						tion messages, or local-use messages
≡,∕	These message	es and their origin will appear	in the syslog.			
olicy	Use syslog	facility for these messages:	Local use 3 (#19)		Ŧ	
gement	Reporting	L				
		n				
>	Backup					
ogs						
0	Incident Export					
tings 🔺	Endpoint	ay to use when releasing	g email that was quaran	tined.		
		ay that detected the inci	dent			
\$	Mobile	RITON AP-EMAIL or the protector depending on your subscription.				
neral	ing gateway:					
nerut		iostname:	P	ort:		
		jostname:				

- 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 <u>Forcepoint DLP Administrator Help</u>.

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 varies 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.

and the second	1.2.0.0.2.0.0.0.0					
Introduction	Contact Information					
Contact Information	Enter the account information that is required to create a new mail contact or to mail-enable an existing mail contact.					
New Mail Contact						
Completion	Organizational unit					
	SDTEG teg websense.con	Browse.				
	First name:	Initials:	Last name:			
	DSSNotificationMbx					
	Name:					
	DSSNotificationMbx					
	Alias:					
	DSSNotificationMbx					

- 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.



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.

In other words, create an Exchange email address for the contact that can be routed out of the exchange and through the Forcepoint DLP MTA to be processed.

- 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.

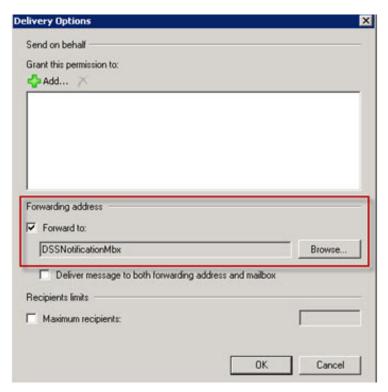
Consult the Exchange administrator with any questions.

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.

Account	Member Of	E-Mail Addresses
General User	Information Address and	Phone Organizatio
Mailbox Settings	Mail Flow Settings	Mailbox Features
Properties		
	_	
Delivery Options		
Message Size Re		
Message Delivery	Restrictions	
Description		
	ol delegated nermissions and for	warding
	ol delegated permissions and for	warding.
	ol delegated permissions and for	warding.
	ol delegated permissions and for	warding.
	ol delegated permissions and for	warding.
	ol delegated permissions and for	warding.
	ol delegated permissions and for	warding.

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.

New Object - Contact
Image: Create in: ilpdemo.com/Users

Eirst name:
Initials:

Last name:
Initials:

Full name:
Image: Image:

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**, and then click **OK**.

New E-mail Address	? ×
E-mail address type:	
Custom Address X 400 Address Microsoft Mail Address	<u>^</u>
SMTP Address cc:Mail Address Lotus Notes Address Novell GroupWise Address	
	*
OK Cancel	Help

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.

nternet Address Propertie	:5	?)
General Advanced		
<u>E</u> -mail address:		
OK	Cancel	Help

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.

NotificationMBX Properties	? ×
Member Of Dial-in Environment E-mail Addresses Exchange Features General Address Account Profile Terminal Services Profile COM+	, i 7 i
Mailbox store:	
TEG/First Storage Group/Mailbox Store (TEC Alias:	<u> </u>
NotificationMBX	
Set the maximum message size and specify the messages accepted by this mailbox.	Delivery Restrictions
Designate delegated permissions and a forwarding address.	D <u>e</u> livery Options
Specify the mailbox warning and limit sizes and how long to keep deleted items.	St <u>o</u> rage Limits
OK Cancel	Apply Help

- 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.

©2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owner.