Releasing blocked email in Data Security

IN-TopicInfo:Topic 41101/ Updated: 02-May-2011

Applies To:	Websense Data Security v7.1.x Websense Data Security v7.5.x Websense Data Security v7.6.x - v7.8x

SMTP violations with the quarantine action are held in the Data Security forensics repository. Depending on their role, administrators can release quarantined messages from TRITON - Data Security by clicking **Remediate > Release** on the Incident report's toolbar.

In addition, administrators can configure Data Security to notify users when email messages are blocked because of policy. It can be configured to notify administrators or end users.

If desired, you can allow recipients to release blocked messages by replying to the notifications they receive.

To activate this capability, you must create and configure a ***force release mailbox***.

To configure a force release mailbox, you must:

1. *Configure Data Security settings*.
2. *Configure the internal Exchange server* or other mail gateway. This document discusses Active Directory with Microsoft Exchange, but the concepts are universal.

Important

For notifications to be sent, you must select an action or action plan that specifies notifications when you configure a rule or attribute in a policy.

It does not matter which module detected the SMTP violation. The force release mailbox can be used to release incidents detected by the SMTP agent, protector in inline MTA mode, or Websense Email Security Gateway. If the Websense Exchange agent detected the incident—Data Security v7.5 and earlier—the force release mailbox is not required.

Configuring Data Security settings

On the Data Security Manager machine (v7.1) or Data Security Management Server (v7.5 and beyond), you must configure settings to prepare for the force release mailbox. You must:

1. Configure a release gateway.
2. Configure notifications.

How you configure these settings depends on your version of Websense Data Security. See:

- *Configuring Data Security Manager v7.1*
- *Configuring TRITON - Data Security v7.5Configuring TRITON - Data Security v7.6 - 7.8*

Configuring Data Security Manager v7.1

Configure the release gateway

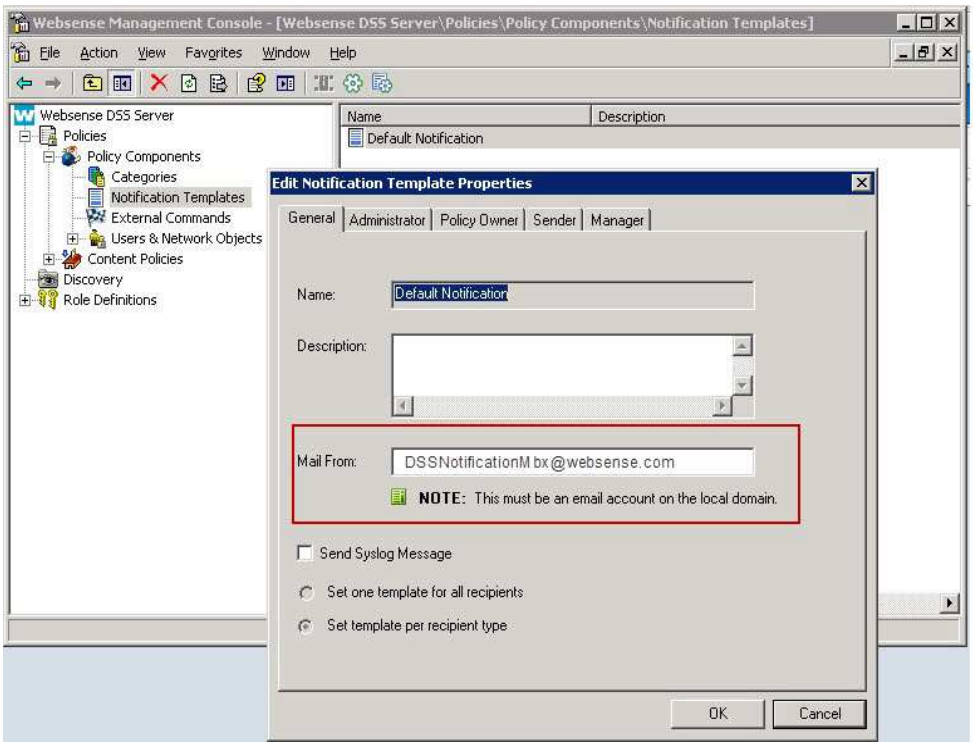
1. Open the **Microsoft Management Console** (MMC).
2. Navigate to **Configuration** > **System Modules** > **Global Properties**.

3. Click the **Release & Notification Gateways** tab.
4. In the **Mail Release Gateway** box, enter the IP address or host name and port number of the mail release gateway. The release gateway should be a mail hop that is used to route mail outside the organization.
5. In the **Notification Gateway** box, enter the IP address or host name and port number of the notification gateway.
6. Click **Select** to choose the recipients for notification messages.

Configure notifications

Follow these steps to set up the Data Security notification mailbox to send a notification:

1. Open the **Websense Management** console.
2. Navigate to **Policies** > **Policy Components** > **Notification Templates**. A list of notification templates appear in the right hand pane.
3. Double-click the desired notification. The **Edit Notification Template Properties** box appears.

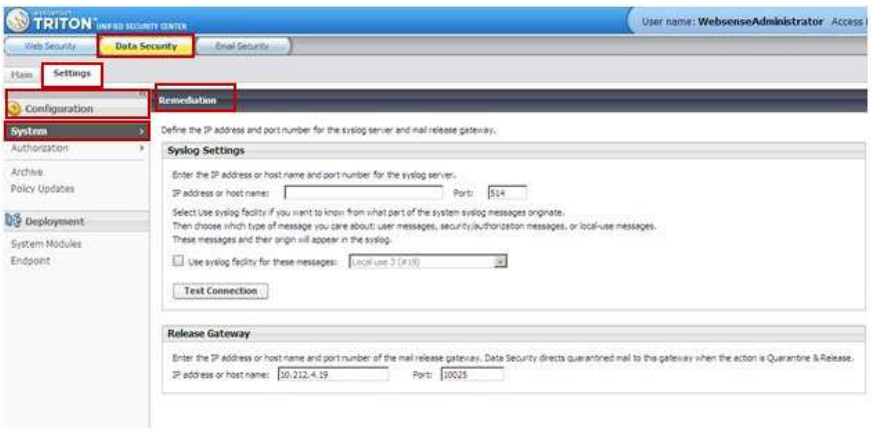


4. Click the **General** tab.
5. In the **Mail From** field, type the Exchange release mailbox (for example: DSSNotificationMbx@websense.com).
6. Click the relevant tab (**Administrator**, **Policy Owner, Sender**, or **Manager**) and depending on the role, mark the following checkboxes to include necessary information when you release the email:
   - Send Notification As (select **Plain Text** or **HTML**)
   - Add Incident Details (select either **Add to the notification body** or **Add as an attachment**)
   - Attach policy-breach content
   - Allow user to release policy-breach content.
7. Click **OK**.

Configuring TRITON - Data Security v7.5

Configure the release gateway

1. Log onto TRITON - Data Security.



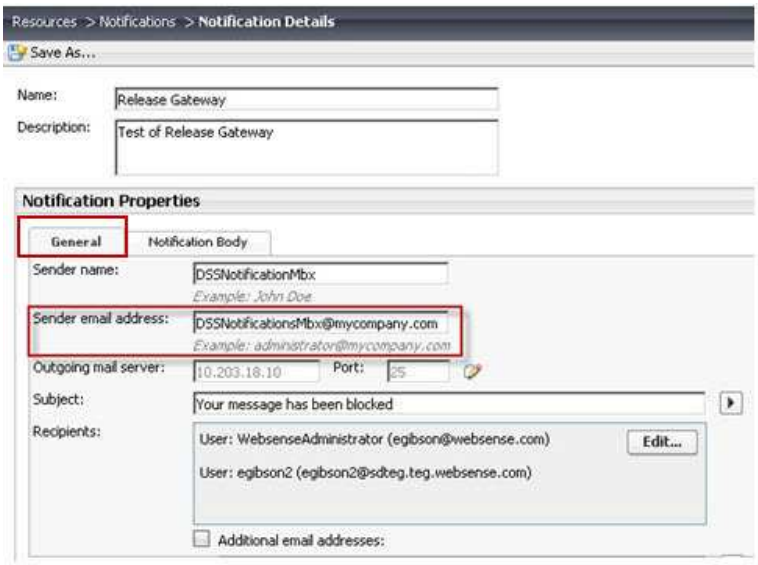
2. Navigate to **Settings > Configuration > System > Remediation**.
3. In the Release Gateway box, enter the IP address or host name and port number of the mail release gateway. The release gateway should be a mail hop that is used to route mail outside the organization.

Configure notifications

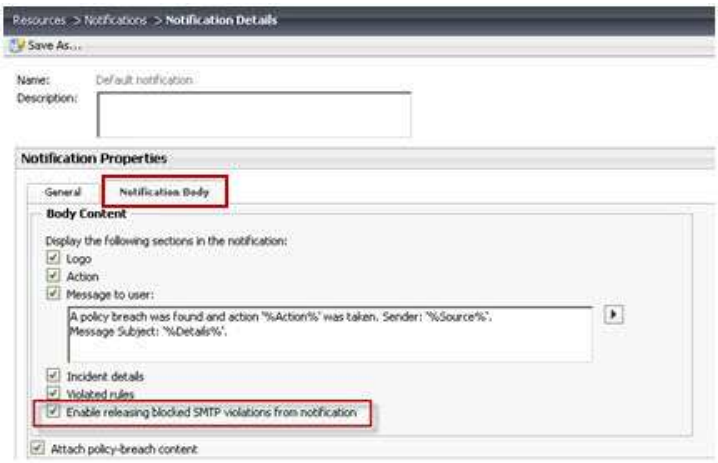
These instructions apply to TRITON - Data Security v7.5 and v7.6.

1. Navigate to **Main > Policy Management > Resources > Notifications**.
2. Edit an existing notification or click **New** to create a new notification. The **Notification Details** window displays.
3. On the **General** tab, enter the name and email address of the sender in the **Sender email address** field. This should be a valid internal email address. This is the name and address that is shown in the **From:** field of the notification email message.

In the example shown below, we have used DSSNotificationsMBX@mycompany.com.



4. Verify that the IP address and port listed for your outgoing mail server is correct. Click the pencil icon to edit the settings.
5. Enter a subject for the messages. Click the right arrow to select variables such as incident ID or action.
6. Click **Edit** to select the recipients for the notification messages. You can select administrators, directory entries (end users), or custom users.
7. Now configure TRITON - Data Security to allow the release of SMTP violations when they are blocked due to policy.
   a. Click the **Notification Body** tab.



   b. Complete the following step:

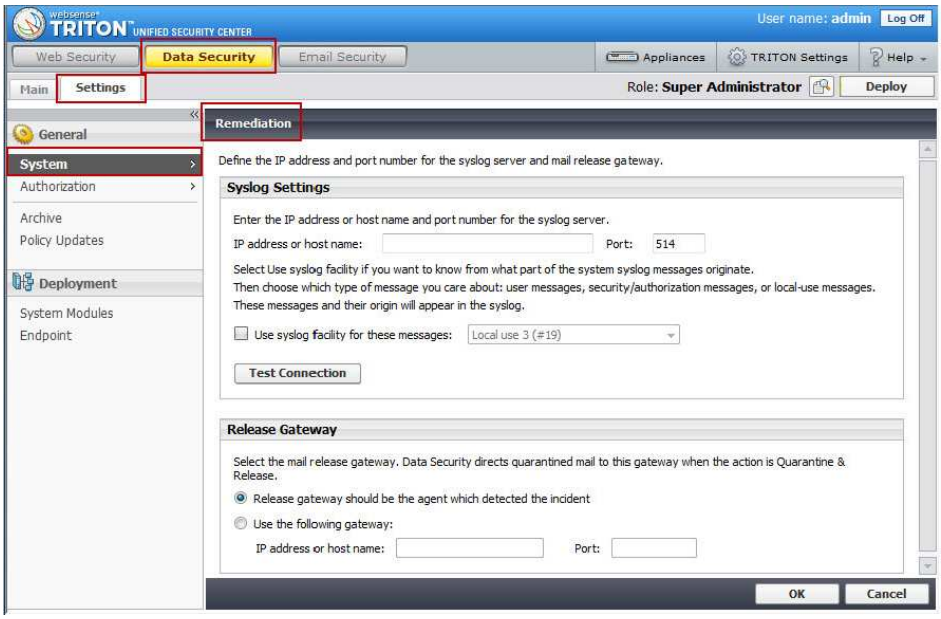
- In v7.5, select the **Enable releasing blocked SMTP violations from notification** checkbox, if it is not already selected (as shown above).
- In v7.6, select **Allow recipients to release blocked email from this notification** (shown below).

c. Click **OK**.

Configuring TRITON - Data Security v7.6 - 7.8

Configure the release gateway

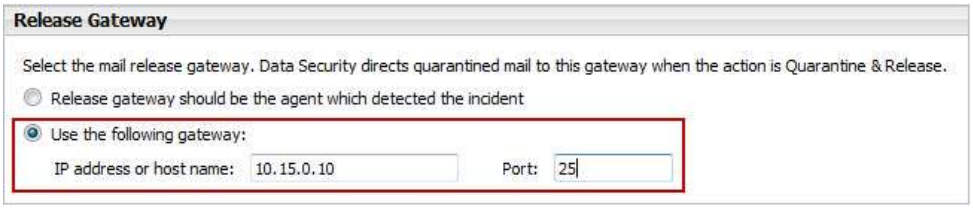
1. Log onto the TRITON Console. Click the **Data Security** tab.



a. Navigate to **Settings > General > System > Remediation**.

b. In the **Release Gateway** box, select the option **Use the following gateway**.

c. Enter an IP address or host name and port number of the mail release gateway. The release gateway should be a mail hop that is used to route mail outside the organization.



Configure notifications

The process for configuring notifications is the same for Websense Data Security v7.5.x and v7.6.x. Refer to *Configure notifications* for details.

Configuring Microsoft Exchange

To prepare for the force release mailbox feature, configure the following *common settings* in 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 your version of Microsoft Exchange. See:

- *Configuring Exchange 2003*

- *Configuring Exchange 2007 and 2010*

Note

Although the following procedures apply to Active Directory with Microsoft Exchange 2003, 2007, and 2010, 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.
- You cannot use a real address (for example, your CSO email) as the Notifications sender email address if you want to use the force release mailbox feature.
- The Active Directory-based process above can be executed with other mail systems as long as the protector/SMTP agent is an MTA over outgoing email messages.
- This setup is for inline MTA mode only.

Configuring Exchange 2003

Create a new Exchange contact

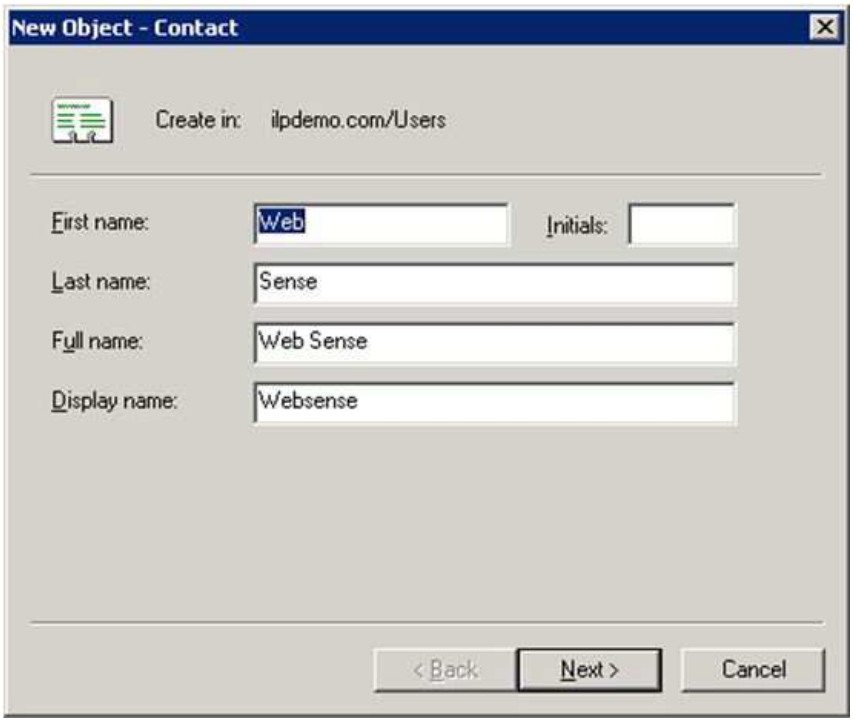
1. In the **Active Directory - Users and Computers** console, right-click any OU or AD container, and select **Users > New > Contact**.
2. Create a contact with an SMTP address like pa@pa.pa. The new contact can have any name.

Note

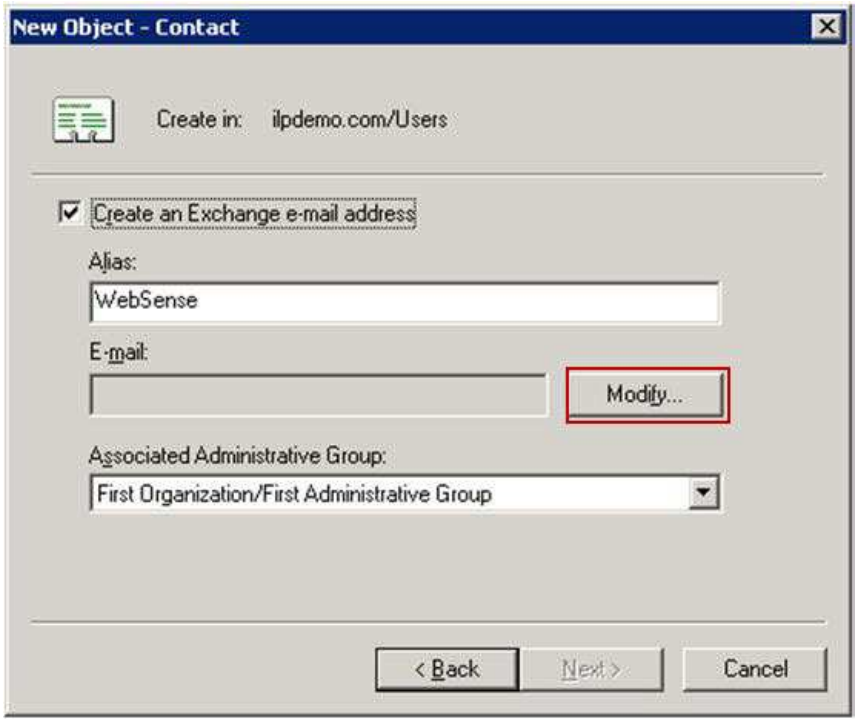
The new contact can have any name or email address, but the email domain should not be internal, and preferably should be one that cannot be resolved by DNS.

In other words, create an Exchange email address for the contact that can be routed out of the exchange and through the TRITON - Data Security SMTP agent to be processed.

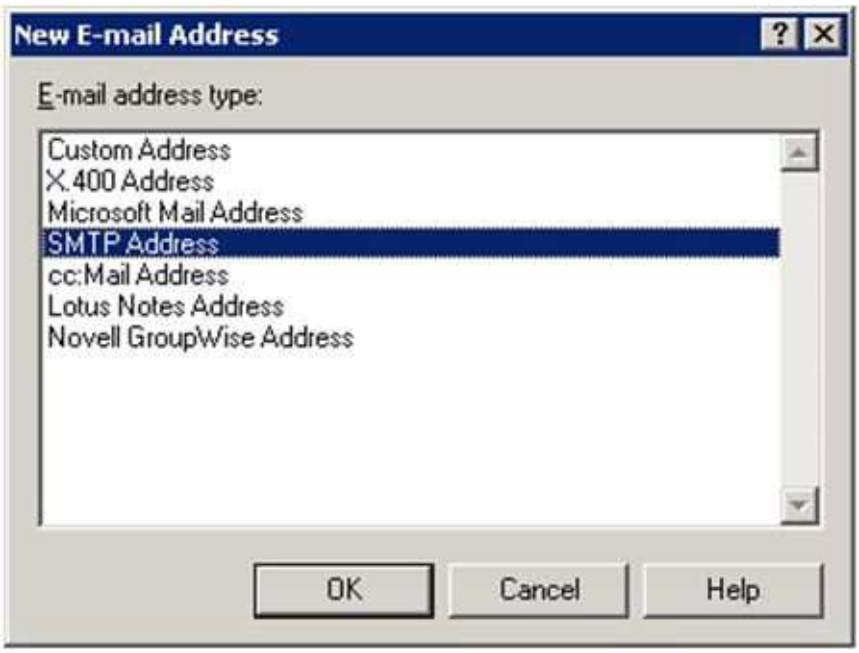
In this example, the new contact name is Web Sense with a display name of Websense. Our new contact Websense will be associated with the pa@pa.pa address.



3. Click **Next**.



4. Click the **Modify** button. The **New E-mail Address** window appears.



5. Select **SMTP Address** and click **OK**. The **Internet Address Properties** window displays.

6. In the **General** tab, type **pa@pa.pa** in the **E-mail address** field.

7. Click **OK**.

Create an Exchange mailbox

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

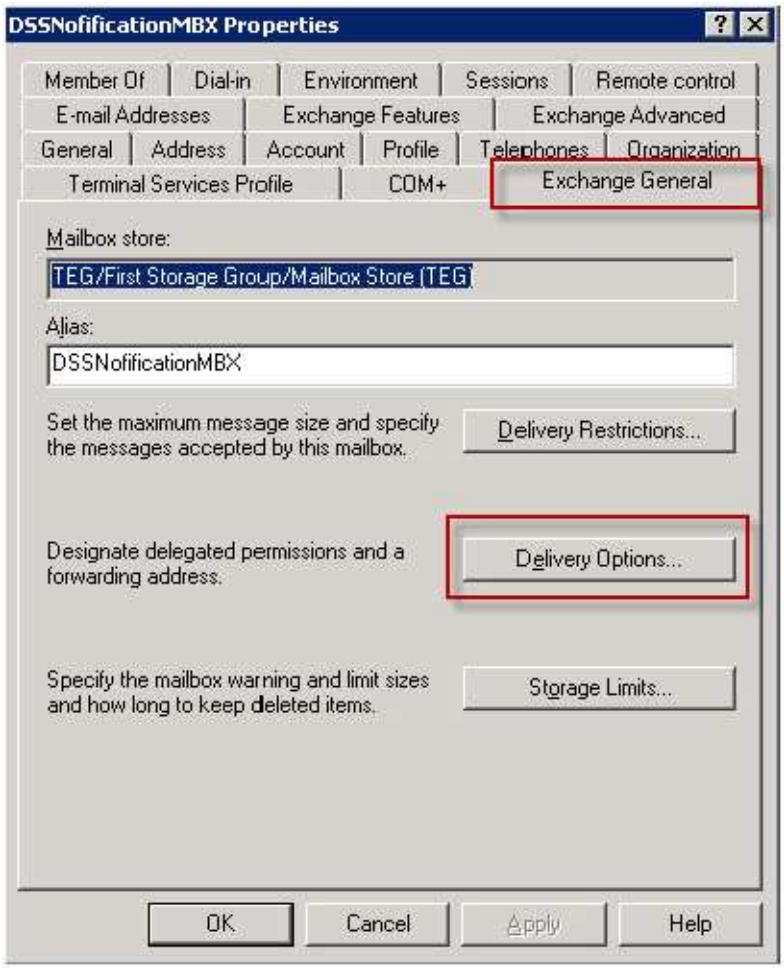
1. In the Users folder of the **Active Directory - Users and Computers** console, create a user with the email address of the notification sender that was configured in the TRITON -Data Security.

   In this example we will use DSSNotificationsMBX@mycompany.com. Substitute mycompany.com with your organization's domain.
2. Follow the steps outlined by the wizard and create an Exchange mailbox for the user. Consult the Exchange administrator if you have any questions.

Configure a forwarding address

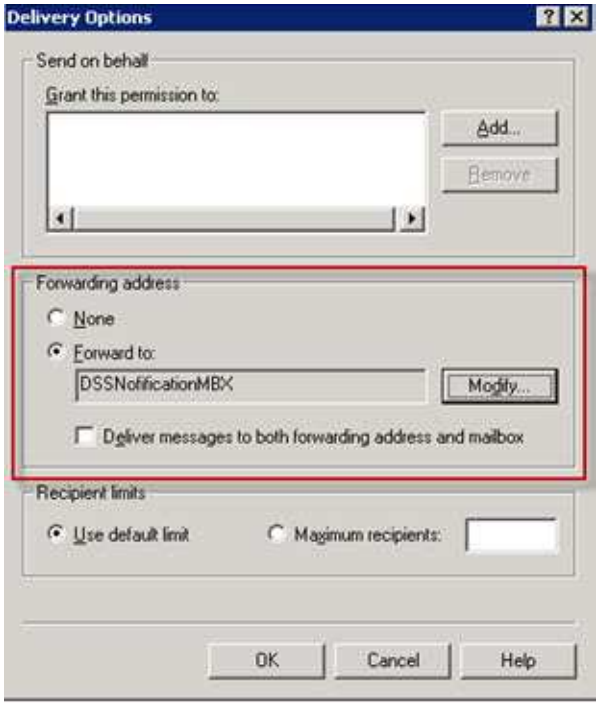
1. Right-click the user account that was just created and a pop-up menu appears.

2. Select **Properties**. The **Properties** dialog box appears.

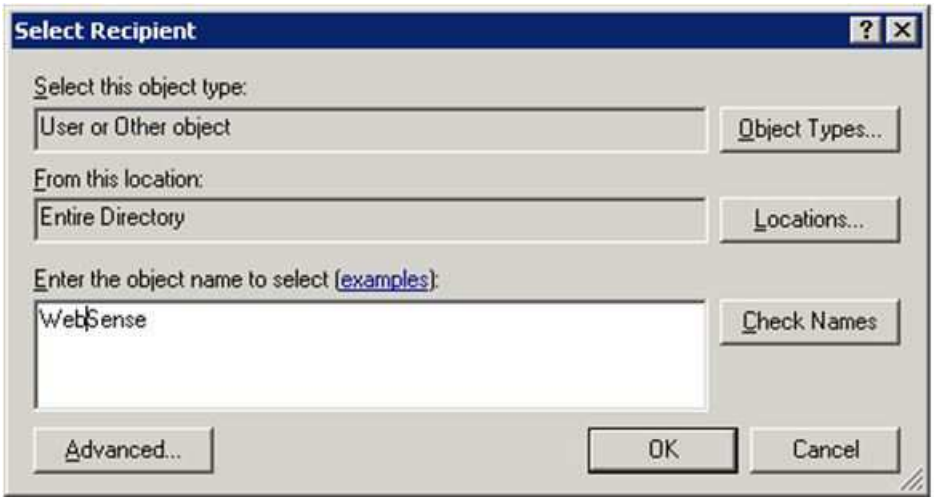


3. Click the **Exchange General** tab. (Active Directory must be integrated with the Exchange server for this tab to be present.)

4. Click the **Delivery Options** button. The **Delivery Options** window appears.



5. In the **Forwarding address** pane, select **Forward to**.
6. Click **Modify**. The **Select Recipient** window displays.



7. Select or search for the contact that was created. This will be the destination for the forwarding.

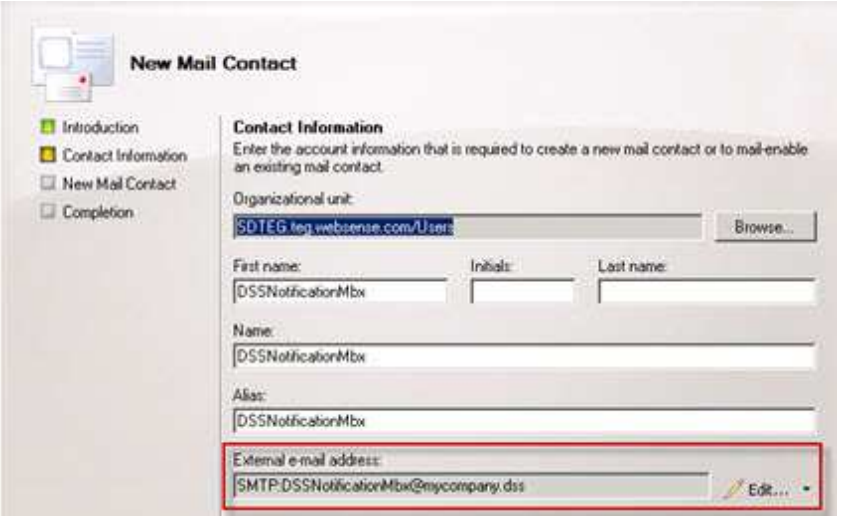
8. Click **OK** to complete the configuration.

> **Note**
>
> This Active Directory-based process can be executed with other mail systems as long as the Protector/SMTP agent is an MTA over outgoing email messages.
>
> Example configuration (for Websense.com):
>
> 1. Create an Active Directory contact: DSSNotificationMbx@wbsn.dss.
> 2. Create a notification mailbox: DSSNotificationMbx@websense.com.
> 3. Forward all email for DSSNotificationMbx@websense.com to DSSNotificationMbx@wbsn.dss.

Configuring Exchange 2007 and 2010

Create a new Exchange contact

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



2. Enter details for the contact.
3. Click the **Edit** button under the **External e-mail address** field, and create a contact with an SMTP address like DSSNotificationMbx@mycompany.dss.

> **Note**
>
> The new contact can have any name or email address, but the email domain should not be internal, and preferably should be one that cannot be resolved by DNS.

In other words, create an Exchange email address for the contact that can be routed out of the exchange and through the TRITON - Data Security SMTP agent 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:

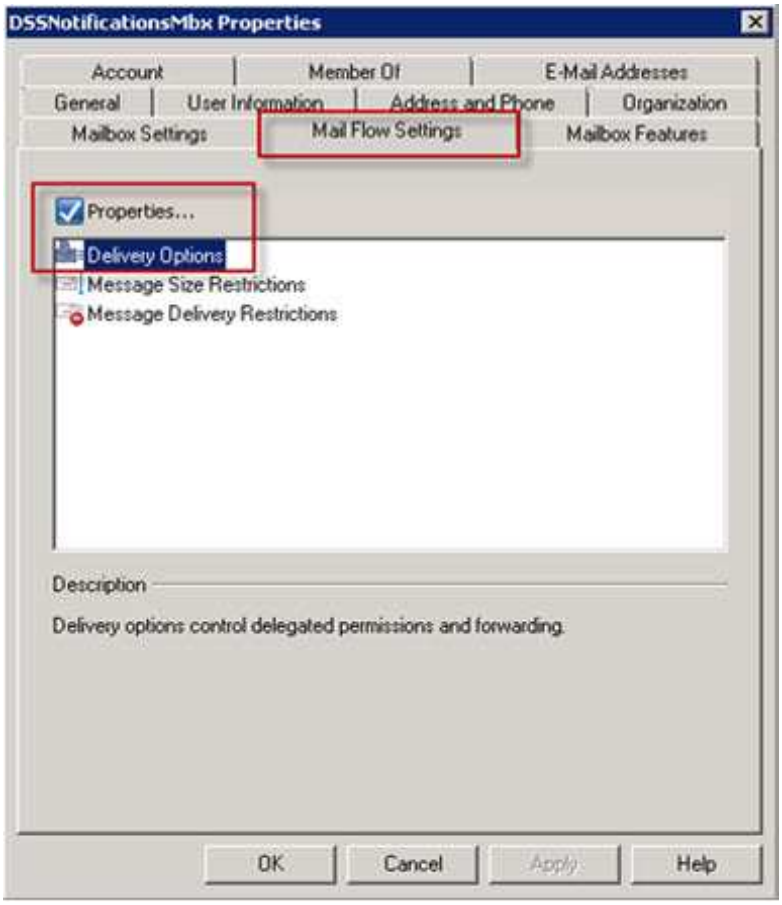
1. In the Users folder of the **Active Directory - Users and Computers** console, create a user with the email address of the notification sender that was configured in the TRITON -Data Security.

   In this example we will use DSSNotificationsMBX@mycompany.com. Substitute mycompany.com with your organization's domain.
2. Follow the steps outlined by the wizard and create an Exchange mailbox in the appropriate mailbox database. Consult the Exchange administrator if you have any questions.

Configure a forwarding address

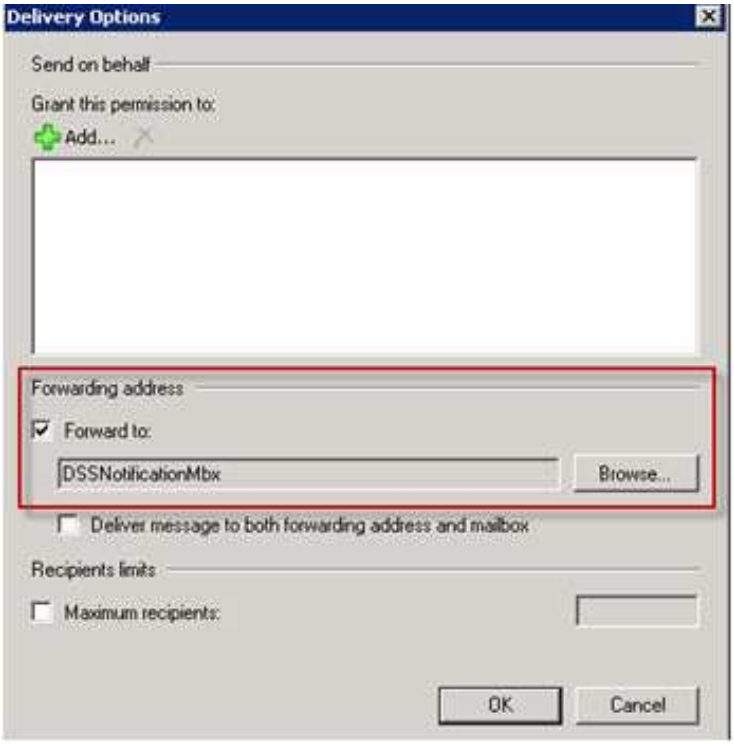
1. Right-click the user account that was just created and a pop-up menu appears.

2. Select **Properties**. The **Properties** dialog box for the user appears.



3. Select the **Mail Flow Settings** tab.
4. Check the **Properties** checkbox.

5. Select **Delivery Options**. The Delivery Options window appears.



6. Check the **Forward to** option in the **Forwarding address** pane.
7. Browse to the contact that was created in the steps above.
8. Click **OK** and complete the configuration.