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.



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.

DataSecuritySu	Username	admir
« Overview	Configuration > System Modules > Global Properties	
Incident Management	Release & Notification Gateways Encryption & Bypass IP Address Resolution Forensics Mail Release Gateway	
Reports	IP Address/Hostname: 127.0.0.1 Port: 10025	
Status & Logs	Notification Gateway IP Address/Hostname: 127.0.0.1 Port: 10025	
Configuration	Select notified recipients:	
Administration	Select	
Scheduler Settings		
External Commands Archive Change Password Organiza Exverites		
Brockshold, Annual Construction State		

- 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.

📸 Websense Management Console - [Websense D55 Server	Policies\Policy ([omponents\Notification Templates]	- 🗆 🗙
🚡 Eile Action View Favorites Wir	idow <u>H</u> elp			_ = = ×
← → 🖻 🖬 🗡 🙆 😫 😫	II 🛛 🔅 🔂			
Websense DSS Server Policies Notification Templates Websense DSS Server Notification Templates Websense Network Objects Content Policies Scovery Role Definitions	Name Default Noti fit Notification Templa General Administrator Name: Default Description: Mail From: DSS NO Send Syslog Messag C Set one template for	eation Properties olicy Owner Sen lotification otification totificationM bx (E: This must be a all recipients	Description ider Manager @websense.com an email account on the local domain.	
J	Set template per re	ipient type	0K Cancel	

- 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.

	F110 54004	User name: WebsenseAdministrator Access
Web Security	Data Se	curity Enail Security)
Hain Settings		
O Configuration		Remediation
System		Define the IP address and port number for the systog server and mail release gateway.
Authorization	2	Syslog Settings
Archive Policy Updates Dig Deployment System Nodules		Ender the IP address or host name and port number for the systog server. IP address or host name: Pactor best name: Pactor best name to know that part of the systog messages originate. Then choose that hose of message rou care about user messages, security/subtractor messages, or local-use messages. These messages and then anyn will appear in the systog.
Endpoint		Li Ste svidg ficht for these messages: [Local Local Lo
		Brite the P address or host name and portnumber of the mail reases pateriars. Data Becurty directs querantine final to this gateriary when the action is Quarantine & Release. P address or host name: 20,212,419. Port: 20025

- 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.

Release Gateway				
Enter the IP address or ho Quarantine & Release.	st name and port numbe	er of the mail relea	se gateway.	Data Security directs quarantined mail to this gateway when the action is
IP address or host name:	10.15.0.10	Port:	25	

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.

Save As		
lame:	Release G	ateway
escription:	Test of Re	lease Gateway
Votificatio	n Propert	les
General	Notiñ	cation Body
Sender nam	e:	DSSNotificationMbx Example: John Doe
Sender ema	il address:	DSSNotificationsMbx@mycompany.com Example: administrator@mycompany.com
Outgoing m	ail server:	10.203.18.10 Port: 25 💓
Subject:		Your message has been blocked
Recipients:		User: WebsenseAdministrator (egbson@websense.com) User: egbson2 (egbson2@sdteg.teg.websense.com)
		Additional email addresses:

- 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.

lanie: rescription:	Default notification	
votification	Properties	
Body Cor Display th V Logo V Action	stent following sections in the notification: ge to user:	
A pol Mess	cy breach was found and action "%Action%" was taken. Sender: "%Source%". age Subject: "%Details%".	
Tell Trailde	nt details	

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).

Disp	olay the following sections in th	e notification me	sage:	
V	Logo			
V	Action			
V	Message to user:			
	Message Subject: "%Subject?	*.		
V	Message Subject: "%Subject?	•.		
V	Message Subject: "%Subject? Incident details Violated rules	e .		

c. Click OK.

Configuring TRITON - Data Security v7.6 ! +",

Configure the release gateway

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

	INIFIED SECURITY CENTER				User name: adr	nin 🛛 Log Of
Web Security	Data Security	Email Security	-	Appliances	C TRITON Settings	2 Help
Main Settings			R	ole: Super /	Administrator 🖪	Deploy
🍥 General	* Remediat	tion				
System	> Define the	IP address and port number for the sys	slog server and mail release gate	way.		
Authorization	> Syslog	Settings				
Archive Policy Updates	Enter the IP address Select L	ne IP address or host name and port nu ess or host name:	mber for the syslog server. Port:	514	riginate	
🕼 Deployment	Then ch	noose which type of message you care a	bout: user messages, security/a	uthorization m	essages, or local-use messa	ges.
System Modules Endpoint	These n	nessages and their origin will appear in t syslog facility for these messages:	he syslog. Local use 3 (#19)	Ŧ		
	Tes	t Connection				
	Release	e Gateway				
	Select t Release	he mail release gateway. Data Security 8.	directs quarantined mail to this g	ateway when	the action is Quarantine &	
	Releter	ease gateway should be the agent whic	h detected the incident			
	O Use	the following gateway:				
	IP a	address or host name:	Port:			

- 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.

Release Gateway				
Select the mail release gatewa	. Data Security directs o	quarantined mail to	this gateway	when the action is Quarantine & Release.
Release gateway should be	the agent which detect	ed the incident		
Ose the following gateway:			-	

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.



- 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.

Eirst name:	Web	Initials:
Last name:	Sense	
F <u>u</u> ll name:	Web Sense	
<u>D</u> isplay name:	Websense	

3. Click Next.

Cie	ate an Exchange e-	mail address		
Alia	6			
Iwe	Doense			
E·m	ail:			1
1			Modily	
Ass	ciated Administrativ	ve Group:		_
Firs	t Organization/First	Administrative Group	2	•

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

New E-mail Address	? ×
E-mail address type:	
Custom Address X.400 Address Microsoft Mail Address	*
SMTP Address cc:Mail Address Lotus Notes Address Novell GroupWise Address	
OK Canc	el Help

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.

Internet Address P	roperties	? ×
General Advance	1	
<u>E</u> -mail address:	pa@pa.pa	
OK	CancelAppl	y Help

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.
----	--------------------	----------------	--------	--------------

E-mail Addresses Exchange Feature	Exchange Advanced
ieneral Address Account Profile Terminal Services Profile COM+	Exchange General
vi silbov store:	
TEG/First Storage Group/Mailbox Store (TE	G
Alias:	
DSSNofificationMBX	
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
<i></i>	
Specify the mailbox warning and limit sizes and how long to keep deleted items.	St <u>o</u> rage Limits

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.

			Add
			Bemove
4		1.	
warding address			
C <u>N</u> one			
Eorward to:			
DSSNofificatio	onMBX		Modity
Deliver me	sages to both fr	warding addres	s and mailbox
1 o'Serer mo	sodyes to contro	Anatomy dubies	
ecipient limits			
C Line defend fer	0	lasimum recipier	da:
 Ose derark init 			

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

Select this object type:	
User or Other object	Object Types
Erom this location:	
Entire Directory	Locations
Enter the object name to select (<u>examples</u>):	
Enter the object name to select (<u>examples)</u> : Webßense	
Enter the object name to select (<u>examples</u>): WebSense	Check Names
Enter the object name to select (<u>examples</u>): Webßense	Check Names

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

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

and the second se				
Introduction	Contact Information			
Contact Information	Enter the account information	in that is required to cre	sate a new mail contact	t or to mail-enal
New Mail Contact	an existing mail contact.			
Completion	Organizational unit			
and a state specific terms	SDTEG teg websense.com	/Users		Browse.
	First name:	Initials	Last name:	
	DSSNothcationMbx			
	Name:			
	DSSNotificationMbx			
	Alias:			
	Income and the			

- 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.



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.

Account	Member Of	E-Mail Ad	dresses
General User Info	ormation Address	and Phone	Organizatio
Mailbox Settings	Mail Flow Setting	s Mailboo	Features
		10.00	
Properties			
Delivery Options			
Message Size Restri	ctions		
Message Delivery R	estrictions		
Description			
Description			
Description Delivery options control (delegated permissions ar	nd forwarding.	
Description — Delivery options control o	delegated permissions ar	nd forwarding.	
Description Delivery options control o	delegated permissions ar	nd forwarding.	
Description Delivery options control o	delegated permissions ar	nd forwarding.	
Description Delivery options control o	delegated permissions ar	nd forwarding.	
Description Delivery options control o	delegated permissions a	nd forwarding.	
Description Delivery options control o	delegated permissions a	nd forwarding.	
Description Delivery options control o	delegated permissions a	nd forwarding.	

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.

livery Options		
Send on behalf		
Grant this permission to:		
🕹 Add 🗡		
Forwarding address		
🔽 Forward to:		
DSSNotificationMbx	Browse	÷
 Derver message to com forwarding address 	ess and maildox	
Recipients limits		
Maximum recipients:		
	C	
	Line Lanc	- 1 C - 1

- 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.