Symantec™ Data Loss Prevention Email Quarantine Connect FlexResponse Implementation Guide

Version 14.6

Symantec Data Loss Prevention Email Quarantine Connect FlexResponse Implementation Guide

Documentation version: 14.6

Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1 Introducing Email Quarantine Connect 6

About the Email Quarantine Connect integration 6
About email messages, remediation requests, and status updates 7
Workflow in reflecting mode 7
Workflow in forwarding mode 8
Flow of remediation actions for remediation initiated from Symantec Data Loss Prevention 9
Flow of remediation actions for remediation initiated from Symantec Messaging Gateway 11
About installing and configuring Email Quarantine Connect 12

Chapter 2 Installing and configuring Email Quarantine Connect 13

Before you install 14
System requirements 14
Installing Email Quarantine Connect 14
Configuring certificates and authentication 17
Creating a user and role for use by Symantec Messaging Gateway with Email Quarantine Connect 19
Installing the Email Quarantine Connect FlexResponse plug-in 21
Configuring the Email Quarantine Connect FlexResponse plug-in 22
Email Quarantine Connect FlexResponse plug-in properties 23
Creating response rules for Email Quarantine Connect 25
Configuring Symantec Messaging Gateway routing, policies, and filters 27
Configuring Network Prevent for Email for use with Email Quarantine Connect 29
Creating a user and role for a remediator 31
Testing the integration 31
Troubleshooting Email Quarantine Connect 32
Uninstalling Email Quarantine Connect 33

Chapter 3 Remediating Symantec Messaging Gateway incidents from the Enforce Server administration console 34

About remediating quarantined email incidents 34

Remediating email incidents from the Enforce Server administration console 37

Index 39

Chapter 1

Introducing Email Quarantine Connect

This chapter includes the following topics:

- About the Email Quarantine Connect integration
- About email messages, remediation requests, and status updates
- About installing and configuring Email Quarantine Connect

About the Email Quarantine Connect integration

Email Quarantine Connect is an integration between Symantec Messaging Gateway and Symantec Data Loss Prevention. The integration uses both Symantec Data Loss Prevention and Symantec Messaging Gateway for detection of sensitive messages and enables users to remediate the resulting incidents on either platform. Typically, the integration is intended for a workflow where Symantec Data Loss Prevention applies detection policies to email messages and sends suspect messages to Symantec Messaging Gateway where they are quarantined pending further remediation.

Using the Symantec Data Loss Prevention Enforce Server administration console, users can initiate remediation actions such as releasing the message from quarantine, deleting the message, encrypting the message, or performing other actions. Users can also initiate those remediation actions from the Symantec Messaging Gateway Control Center. Regardless of the platform where the remediation is performed, the incident details are updated on both platforms with messages about the remediation.

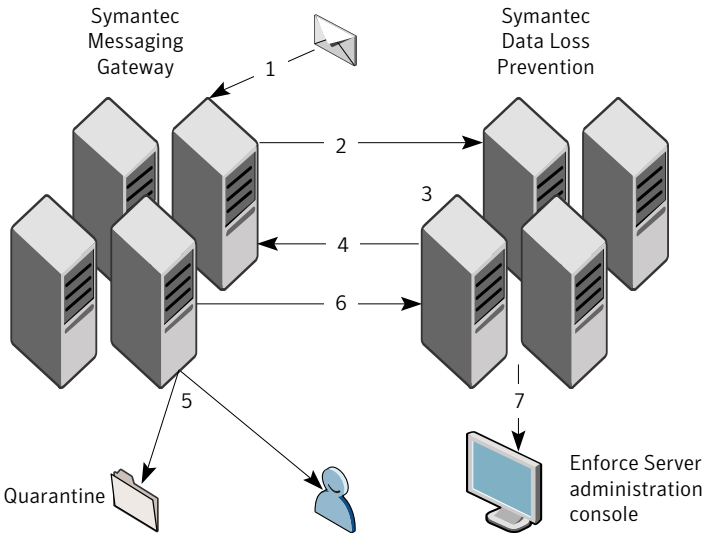
About email messages, remediation requests, and status updates

This section describes the sequence of events that occur in a typical email quarantine workflow. The sequence is different depending on whether Symantec Data Loss Prevention Network Prevent for Email is configured for reflecting or forwarding mode. Both sequences are described in this section.

Workflow in reflecting mode

Figure 1-1 describes the workflow when Network Prevent for Email is configured in reflecting mode.

Figure 1-1 Reflecting mode workflow



1 Email arrives at Symantec Messaging Gateway.

2 Symantec Messaging Gateway forwards the message to Symantec Data Loss Prevention.

3 Symantec Data Loss Prevention applies the policies and detection rules. If the message violates a policy, Symantec Data Loss Prevention adds x-headers to the message.

4 Symantec Data Loss Prevention sends the message back to Symantec Messaging Gateway.

5 Symantec Messaging Gateway applies the policies and filters to the message. One policy is configured to detect the x-header and to respond by quarantining the message.

If no x-header is detected, the email is forwarded to the recipient.

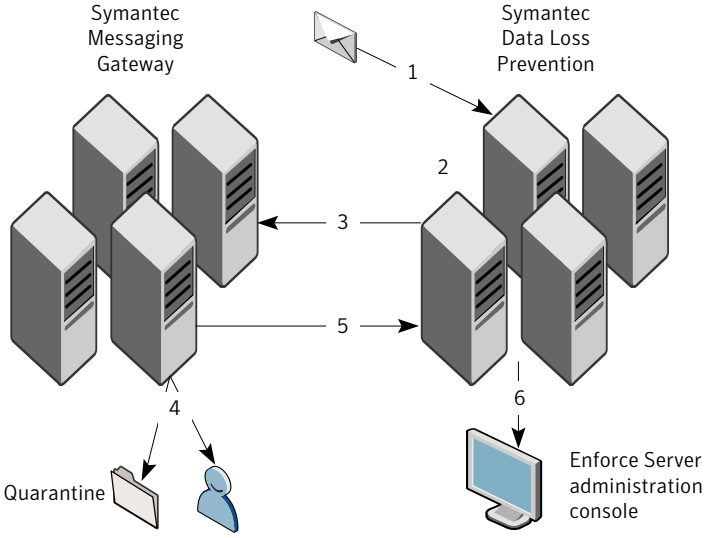
6 Symantec Messaging Gateway sends a status update to Symantec Data Loss Prevention.

7 Symantec Data Loss Prevention updates the incident status and history. Remediators can now remediate the incident from the Enforce Server administration console. The status update is asynchronous. It may take up to an hour for the remediation status updates to appear in the Enforce Server administration console.

Workflow in forwarding mode

Figure 1-2 describes the workflow when Network Prevent for Email is configured in forwarding mode.

Figure 1-2 Forwarding mode workflow



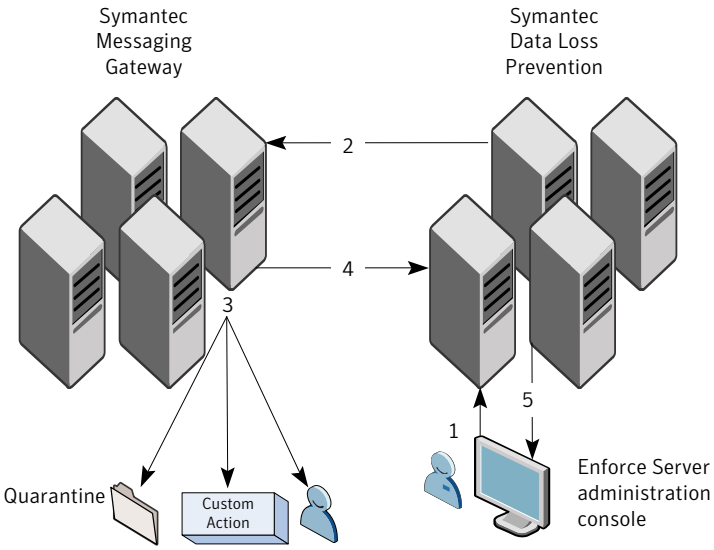
1. Email arrives at Symantec Data Loss Prevention.
2. Symantec Data Loss Prevention applies the policies and detection rules. If the message violates a policy, Symantec Data Loss Prevention adds x-headers to the message.
3. Symantec Data Loss Prevention forwards the email to Symantec Messaging Gateway.
4. Symantec Messaging Gateway applies the policies and filters to the message. One policy is configured to detect the x-header and to respond by quarantining the message.

   If the message does not violate a policy, Symantec Messaging Gateway forwards the message to its destination.
5. Symantec Messaging Gateway sends a status update to Symantec Data Loss Prevention.
6. Symantec Data Loss Prevention updates the incident status and history. Remediators can now remediate the incident from the Enforce Server administration console. The status update is asynchronous. It may take up to an hour for the remediation status updates to appear in the Enforce Server administration console.

Flow of remediation actions for remediation initiated from Symantec Data Loss Prevention

Figure 1-3 shows the workflow when remediation is initiated from the Enforce Server administration console.

Figure 1-3 Remediation from the Enforce Server administration console



1 A remediator uses the incident snapshot or incident list to apply one of the FlexResponse remediation actions.

2 Symantec Data Loss Prevention sets the "remediation attempted" status for the incident and sends a request to Symantec Messaging Gateway to execute the action.

3 Symantec Messaging Gateway executes one of the following requested actions:

- Quarantine the email.
- Perform a custom action (typically, encryption).
- Forward the email to its destination.

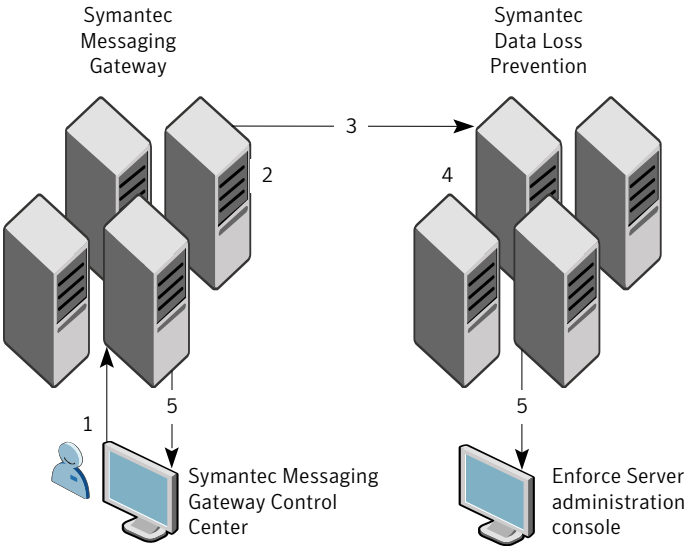
4 Symantec Messaging Gateway sends a status update to Symantec Data Loss Prevention that updates the incident status and history.

5 Remediators can view and remediate the incident in the Symantec Messaging Gateway Control Center or the Symantec Data Loss Prevention Enforce Server administration console.

Flow of remediation actions for remediation initiated from Symantec Messaging Gateway

Figure 1-4 shows the workflow when remediation is initiated from the Symantec Messaging Gateway Control Center.

Figure 1-4 Remediation from the Symantec Messaging Gateway Control Center



1 A remediator uses the Symantec Messaging Gateway Control Center to remediate a quarantined email.

2 Symantec Messaging Gateway performs the remediation.

3 Symantec Messaging Gateway sends a batch of status updates to Symantec Data Loss Prevention. As part of the Symantec Messaging Gateway configuration, an administrator configures the size of the batches and the interval at which the batches are sent to Symantec Data Loss Prevention for processing.

4 Symantec Data Loss Prevention updates the status and history of the incidents in the batch.

5 Remediators can view and perform further remediation from the Enforce Server administration console or the Symantec Messaging Gateway Control Center.

About installing and configuring Email Quarantine Connect

In the Symantec Data Loss Prevention environment, this integration requires that an administrator use the single Email Quarantine Connect installer to install three Email Quarantine Connect FlexResponse plug-ins. These plug-ins enable the remediation actions in the Enforce Server administration console. The administrator also configures the plug-ins, installs and configures SSL certificates, creates response rules and policies, and configures users, roles, and privileges for access.

See “Installing Email Quarantine Connect” on page 14.

In the Symantec Messaging Gateway environment, an administrator configures a user name, passwords, SSL certificates, and other settings that enable the integration.

See the *Symantec Messaging Gateway Administration Guide*, available with your Symantec Messaging Gateway software.

Chapter 2

Installing and configuring Email Quarantine Connect

This chapter includes the following topics:

- Before you install
- System requirements
- Installing Email Quarantine Connect
- Configuring certificates and authentication
- Creating a user and role for use by Symantec Messaging Gateway with Email Quarantine Connect
- Installing the Email Quarantine Connect FlexResponse plug-in
- Configuring the Email Quarantine Connect FlexResponse plug-in
- Creating response rules for Email Quarantine Connect
- Configuring Symantec Messaging Gateway routing, policies, and filters
- Configuring Network Prevent for Email for use with Email Quarantine Connect
- Creating a user and role for a remediator
- Testing the integration
- Troubleshooting Email Quarantine Connect
- Uninstalling Email Quarantine Connect

Before you install

Installing the Email Quarantine Connect integration requires that an administrator install and configure three FlexResponse plug-ins in the Symantec Data Loss Prevention environment. The integration also requires that an administrator configure Symantec Messaging Gateway to communicate with Symantec Data Loss Prevention. A user with administrative privileges must perform these tasks.

This chapter describes each task and indicates where the task is performed. For the tasks that are performed in the Symantec Data Loss Prevention environment, detailed steps are included in this document. For the tasks that are performed in the Symantec Messaging Gateway environment, a cross-reference is provided to a section of the *Symantec Messaging Gateway Administration Guide* that contains details on performing the task.

System requirements

Email Quarantine Connect requires the following components:

- Symantec Data Loss Prevention with a license for Network Prevent for Email
- Symantec Messaging Gateway
- If you install Email Quarantine Connect on a computer running the Linux operating system, a computer running Microsoft Windows is required during the installation process.

For specific version information about the supported platforms and for information about other requirements, see the following documents:

- *Symantec Data Loss Prevention System Requirements and Compatibility Guide*
- *Symantec Messaging Gateway Installation Guide*

Installing Email Quarantine Connect

Installing the Email Quarantine Connect integration requires a functioning deployment of Symantec Messaging Gateway and Symantec Data Loss Prevention. The details of these configurations are beyond the scope of this document.

For complete information, see the following documents, available with your Symantec software distribution:

- *Symantec Messaging Gateway Administration Guide*
- *Symantec Data Loss Prevention Administration Guide*

A system administrator who is familiar with the Symantec Messaging Gateway deployment and the Symantec Data Loss Prevention deployment should perform the installation and configuration tasks. Table 2-1 describes these tasks and the product or product component where each task is performed.

Table 2-1 Installing and configuring the Email Quarantine Connect integration

Step	Task	Product or component	Description
Step 1	Configure certificates and authentication.	Symantec Messaging Gateway and Symantec Data Loss Prevention	Configure the certificates that enable communication between Symantec Data Loss Prevention and Symantec Messaging Gateway. If a certificate has not yet been created, create a new certificate. See "Configuring certificates and authentication" on page 17.
Step 2	Configure a user account and role in Symantec Data Loss Prevention and configure Symantec Messaging Gateway to use the user account.	Symantec Data Loss Prevention and Symantec Messaging Gateway	Configure a user account and role in the Enforce Server administration console and configure Symantec Messaging Gateway to use this user account when it updates incident details on the Enforce Server. See "Creating a user and role for use by Symantec Messaging Gateway with Email Quarantine Connect" on page 19.
Step 3	Install and configure the Email Quarantine Connect FlexResponse plug-ins.	Enforce Server	Install and configure the FlexResponse plug-in that enables remediation of Symantec Messaging Gateway messages from the Enforce Server administration console. See "Installing the Email Quarantine Connect FlexResponse plug-in" on page 21.

Table 2-1 Installing and configuring the Email Quarantine Connect integration *(continued)*

Step	Task	Product or component	Description
Step 4	Create response rules.	Enforce Server	Create and configure three smart response rules that enable remediation from an incident snapshot or incident list in the Enforce Server administration console. You also create an automated response rule that adds x-headers to the email, and you add that response rule to one or more policies. See "Creating response rules for Email Quarantine Connect" on page 25.
Step 5	Configure Symantec Messaging Gateway routing, policies, and filters.	Symantec Messaging Gateway	Enable Symantec Messaging Gateway to communicate with Symantec Data Loss Prevention, and you set up folders and filtering policies. See "Creating a user and role for a remediator" on page 31.
Step 6	Configure Network Prevent.	Enforce Server	Enable Network Prevent for Email to forward messages to Symantec Messaging Gateway. See "Configuring Network Prevent for Email for use with Email Quarantine Connect" on page 29.
Step 7	Configure users and roles for remediators.	Enforce Server	Users who remediate email incidents using Email Quarantine Connect must have user accounts and must belong to a role with the correct privileges. See "Creating a user and role for a remediator" on page 31.

Configuring certificates and authentication

To enable secure communication between Symantec Data Loss Prevention and Symantec Messaging Gateway, you create, export, and import the required certificates. Then you configure a stored credential. Administrators perform these steps in both the Symantec Data Loss Prevention and Symantec Messaging Gateway environments. File system access is required for the steps that are performed on the Symantec Data Loss Prevention Enforce Server host.

To configure certificates and authentication

1. In the Symantec Messaging Gateway Control Center, export the same certificate that you use for the Control Center HTTPS interface to a temporary directory on the Symantec Data Loss Prevention Enforce Server host.

   If you have not yet created this certificate, add a new self-signed certificate. The certificate must reference the fully-qualified domain name of the Symantec Messaging Gateway server. For example: `mymailhost.mycompany.com`

   For more information, see the following topics in the *Symantec Messaging Gateway Administration Guide*:

   - "Exporting a TLS and HTTPS certificate"
   - "Requesting a Certificate Authority signed certificate"
   - "Assigning a user interface HTTPS certificate to the Control Center"

2. On the Enforce Server host, open a command (terminal) window.

3. Make sure that the `keytool` utility is included in your `PATH` environment variable. Consult your platform documentation for more information.

4. Create an Enforce Server keystore and client certificate by running the following command:

   Linux:

   ```
   SymantecDLP/jre/bin/keytool -genkeypair -alias client
   -keystore certstore.jks -keyalg RSA -dname "CN=enforce_host,
    OU=organizational  unit, O=organization,
    L=location, S=, C=country"
    -keypass password -storepass password
   ```

   Windows:

   ```
   SymantecDLP\jre\bin\keytool -genkeypair -alias client
   -keystore certstore.jks -keyalg RSA -dname "CN=enforce_host,
    OU=organizational  unit, O=organization,
   ```

```
L=location, S=, C=country"
-keypass password -storepass password
```

Where:

- *enforce_host* is the host name of the Enforce Server. For example. enforce.mycompany.com.
- *organizational unit* is the name of the organization unit. (Optional)
- *organization* is the name of the organization. (Optional)
- *location* is the location of the organization. (Optional)
- *state* is the name of the state where the organization is located. (Optional)
- *country* is the name of the country where the organization is located. (Optional)
- *password* is a password you create to control access to the keystore. Use the same password for both the -keypass and -storepass arguments. Do not lose this password. You use this password in a later step to configure an Enforce Server credential.

5 Export the client certificate you created in the previous step by running the following command:

Linux:

```
SymantecDLP/jre/bin/keytool -exportcert -alias client
-keystore certstore.jks -file client.crt -rfc -storepass password
```

Windows:

```
SymantecDLP\jre\bin\keytool -exportcert -alias client
-keystore certstore.jks -file client.crt -rfc -storepass password
```

6 In the Symantec Messaging Gateway Control Center import the Enforce Server client certificate you created in step 4.

See "Importing an application certificate" in the *Symantec Messaging Gateway Administration Guide*, available with your Symantec Messaging Gateway software.

7 On the Enforce Server host, import the server certificate that was created on the Symantec Messaging Gateway Control Center into the client keystore by running the following command:

Linux:

```
SymantecDLP/jre/bin/keytool -importcert -alias server
 -keystore certstore.jks -file server.crt
  -storepass <password> -v -noprompt
```

Windows:

```
SymantecDLP\jre\bin\keytool -importcert -alias server
 -keystore certstore.jks -file server.crt
 -storepass <password> -v -noprompt
```

8 Copy the certificate store file (`certstore.jks`) to the following directory:

(Linux) `SymantecDLP/Protect/plugins/EmailQuarantineConnect`

(Windows) `SymantecDLP\Protect\plugins\EmailQuarantineConnect`

The `protect` user (the `protect` user is defined during Symantec Data Loss Prevention installation) must have read and write access to this file.

9 Open the Enforce Server administration console and log in as a user with Administration privileges.

10 Navigate to **System** > **Credentials**.

11 Click **Add Credential**.

12 Type a **Credential Name**. You type this credential name in the configuration files for the three FlexResponse plug-ins in a later step.

13 In the **Access Username** field, type the name of the keystore file. For example: `certstore.jks`

14 In the **Access Password** field, type the password for the keystore file.

See "Creating a user and role for use by Symantec Messaging Gateway with Email Quarantine Connect" on page 19.

Creating a user and role for use by Symantec Messaging Gateway with Email Quarantine Connect

In the following procedure, you configure a user name and role in the Enforce Server administration console. Symantec Messaging Gateway uses this name when it accesses Symantec Data Loss Prevention web services to update incident details.

After you create the user and role, you configure Symantec Messaging Gateway to use this user to communicate with Symantec Data Loss Prevention.

To create a role and user for Email Quarantine Connect

1. Log on to the Enforce Server administration console as an administrator.
2. Select **System > Login Management > Roles**.
3. Click **Add Role**.
4. Type a name for the new role in the **Name** field. For example, type **dlp-remediator-role**.
5. In the **User Privileges** section of the screen, select the following items:

Incidents: View	Select **View** and then select **Network Incidents**.
Incidents: Actions	Select the **Remediate Incidents** privilege.
Incidents: Incident Reporting and Update API	Select the following user privilege: **Incident Update**

6. Click **Save**.
7. Select **System > Login Management > DLP Users**.
8. Click **Add DLP User**.
9. Type values for the **Name**, **New Password**, and **Re-enter New Password** fields.
10. In the **Roles** section of the

    screen, select the new role you created in step 4. For example, select **dlp-remediator-role**.
11. Select the same role in the **Default Role** menu.
12. (Optional) Click the **Incident Access** tab and add conditions to limit the incidents that Email Quarantine Connect may act on. The condition must not exclude Network incidents.
13. Click **Save**.
14. In the Symantec Messaging Gateway Control Center, specify the Enforce Server user and password.

    See "Configuring Symantec Messaging Gateway to update data with Enforce Server" in the *Symantec Messaging Gateway Administration Guide*.

See "Installing the Email Quarantine Connect FlexResponse plug-in" on page 21.

Installing the Email Quarantine Connect FlexResponse plug-in

The following procedure describes the steps that are required to install the Email Quarantine Connect FlexResponse plug-in in the Symantec Data Loss Prevention environment. In this procedure, you install and configure three FlexResponse plug-ins, one for each action available with the Email Quarantine Connect integration.

To install the Email Quarantine Connect FlexResponse plug-in

1. Obtain the Email Quarantine Connect installer from the Symantec FileConnect website.
2. Copy the `Symantec_DLP_Plugin_Email_Quarantine_Connect_2.0.0.19.exe` file to a temporary directory on a Windows computer. (If you are running the Enforce Server on a Windows computer, you can copy the file to a temporary directory on the Enforce Server host.)
3. Double-click the installer file. When the installer prompts you, type the name of a temporary destination folder.
4. Choose the temporary folder and click **Next**.

   The installer extracts the plug-in files to the temporary folder.
5. Navigate to the temporary folder containing the extracted files.
6. Copy the following items to the `SymantecDLP\protect\plugins\` folder on the Enforce Server host:
   - `EmailQuarantineConnectApproved.jar`
   - `EmailQuarantineConnectApproved.properties`
   - `EmailQuarantineConnectCustom.jar`
   - `EmailQuarantineConnectCustom.properties`
   - `EmailQuarantineConnectRejected.jar`
   - `EmailQuarantineConnectRejected.properties`
   - `EmailQuarantineConnect` folder and its contents.
7. Open the following file in a text editor:

   `SymantecDLP\Protect\config\Plugins.properties`
8. Locate the following property in the `Plugin.properties` file:

`com.symantec.dlpx.flexresponse.Plugin.plugins`

If the property begins with a comment character (`#`), remove it.

This line lists all of the deployed plug-ins. Add the following entries, each separated by commas:

- `EmailQuarantineConnectApproved.jar`
- `EmailQuarantineConnectCustom.jar`
- `EmailQuarantineConnectRejected.jar`

For example:

```
com.symantec.dlpx.flexresponse.Plugin.plugins = MyPlugin.jar,
EmailQuarantineConnect-Approve.jar,
EmailQuarantineConnect-Custom.jar,
EmailQuarantineConnect-Reject.jar
```

9 Save the `Plugin.properties` file.

See "Configuring the Email Quarantine Connect FlexResponse plug-in" on page 22.

Configuring the Email Quarantine Connect FlexResponse plug-in

Each of the three FlexResponse plug-ins defines a separate action. Each of these actions displays a smart response link in the incident snapshot display.

To configure the Email Quarantine Connect FlexResponse plug-in

1 Open each of the following plug-in properties files in a text editor:

- `EmailQuarantineConnect-Approved.properties`
- `EmailQuarantineConnect-Custom.properties`

- `EmailQuarantineConnect-Rejected.properties`

2 In each file change the following properties as indicated:

`email-gateway-server-host`	Type the host name of the Symantec Messaging Gateway host. Symantec recommends that this property contain a fully-qualified domain name that is resolvable by DNS. You can also enter an IP address.
`email-gateway-server-port`	Type the port number of the Symantec Messaging Gateway host. The default value is `8443`.
`certificates-store.credential`	Type the name of the stored credential that you created in a previous step. See "Configuring certificates and authentication" on page 17.
`dlp-remediator-user`	Type the user name of the Symantec Data Loss Prevention remediator. This user is used to identify log and history entries that are stored in the Symantec Messaging Gateway environment. The user does not have to be a user that defined in either Symantec Data Loss Prevention or Symantec Messaging Gateway.
`dlp-remediator-action`	This property has already been configured.

See "Email Quarantine Connect FlexResponse plug-in properties" on page 23. for more information on the plug-in properties.

Do not change any other properties in the files.

3 Save the properties files.

4 Restart the Vontu Manager and Incident Persister services.

Email Quarantine Connect FlexResponse plug-in properties

Table 2-2 lists the properties that you must configure for the Email Quarantine Connect FlexResponse plug-in.

Table 2-2 Email Quarantine Connect FlexResponse plug-in properties

Property	Description
`email-gateway-server-host`	The host name of the computer running Symantec Messaging Gateway. Symantec recommends that this property contain a fully-qualified domain name that is resolvable by DNS. You can also enter an IP address. This property is required and there is no default value.
`email-gateway-server-port`	The port number where the Symantec Messaging Gateway web service is available. The default value is `8443`.
`certificates-store.credential`	The name of the stored credential that is used to access the certificate store for this FlexResponse plug-in. You created this credential in an earlier step. See "Configuring certificates and authentication" on page 17. This property is required and there is no default value.
`dlp-remediator-user`	The name of the Symantec Data Loss Prevention remediator user. This user is used to identify log entries that are stored in the Symantec Messaging Gateway environment. This property is required and there is no default value.

Table 2-2 Email Quarantine Connect FlexResponse plug-in properties *(continued)*

Property	Description
`dlp-remediator-action`	The remediation action that the Symantec Messaging Gateway server performs for this plug-in. This property is preconfigured for each of the three Email Quarantine Connect FlexResponse plug-ins so that each plug-in performs one of the actions. The possible actions are: ■ `REVIEW_STATE_APPROVED` ■ `REVIEW_STATE_REJECTED` ■ `REVIEW_STATE_CUSTOM` This property is required and there is no default value. See "About remediating quarantined email incidents " on page 34.

See "Creating response rules for Email Quarantine Connect" on page 25.

Creating response rules for Email Quarantine Connect

After you install the plug-ins, you configure three **Smart Response** rules, one for each action that the plug-in performs. You also configure an **Automated Response** rule that adds x-headers to the message before Symantec Data Loss Prevention forwards the message to Symantec Messaging Gateway.

To create response rules for Email Quarantine Connect

1. Open the Enforce Server administration console.
2. Navigate to **Manage** > **Response Rules**.
3. Click **Add Response Rule**.
4. Select **Smart Response** and click **Next**.

5 Type a **Rule Name** for the response rule.

This rule name displays in the incident snapshot and incident lists as the name of the smart response action. You may want to name the response rule with descriptive names, such as **Approve**, **Reject**, or another name that represents the functionality that is configured in the Symantec Messaging Gateway environment.

See "Creating a user and role for a remediator" on page 31.

6 (Optional) Type a description of the response rule.

7 In the **Actions** drop-down list, select **Server FlexResponse** and click **Add Action**.

The **All Server FlexResponse** action displays.

8 In the **FlexResponse Plug-in** drop-down list, define the appropriate action for the rule by selecting one of the following three actions:

- SMG Custom Action
- SMG Approve Action
- SMG Reject Action

See "Configuring Symantec Messaging Gateway routing, policies, and filters" on page 27.

9 Click **Save**.

10 Repeat steps 3 – 9 for each of the remaining actions.

11 Click **Add Response Rule**.

12 Select **Automated Response** and click **Next**.

13 Type a name for the response rule in the **Rule Name** field.

14 In the **Actions** drop-down list, select **Network Prevent** > **Modify SMTP Message** and click **Add Action**.

15 In the **Network Prevent: Modify SMTP Message action** box, select **Enable Email Quarantine Connect**. Do not select or enter anything else in the **Network Prevent: Modify SMTP Message** area.

16 Click **Save**.

17 Create one or more Symantec Data Loss Prevention policies and detection rules to detect policy violations for email. Add the Automated Response rule you created in step 13 to the policies.

See "Implementing policies" in the *Symantec Data Loss Prevention Administration Guide*.

See “Configuring Symantec Messaging Gateway routing, policies, and filters” on page 27.

Configuring Symantec Messaging Gateway routing, policies, and filters

Perform the following steps in the Symantec Messaging Gateway Control Center. For detailed procedures, see the referenced sections in the *Symantec Messaging Gateway Administration Guide*.

To configure Symantec Messaging Gateway routing, policies, and filters

1. Route outbound email to Data Loss Prevention Network Prevent and configure Symantec Data Loss Prevention Network Prevent for Email to route email back to Symantec Messaging Gateway. If you have multiple outbound scanners, you can route outbound mail to Data Loss Prevention Network Prevent servers differently for each scanner. Alternatively, you can apply the same settings to all outbound scanners.

   See "Configuring email connections to and from Data Loss Prevention Network Prevent" in the *Symantec Messaging Gateway Administration Guide*.

2. Create incident folders to capture the messages that violate content filtering policies and hold for remediation or review.

   In the Symantec Messaging Gateway Control Center, select the folder type **Hold for Review (Content Quarantine)** to hold incidents for remediation. Or you can choose **Informational Incidents** to hold incidents for review.

   See "Creating content incident folders" in the *Symantec Messaging Gateway Administration Guide*.

3 Create content filtering policies to detect the x-headers that the Symantec Data Loss Prevention automated response rule inserts into email messages. The x-headers take the following form:

```
X-dlp-uniquemsgid: <message ID>
X-dlp-policyid: <policy ID>
```

For example:

```
X-dlp-uniquemsgid: 3984736A-2964-437D-A0EC-67E62D4C187F
X-dlp-policyid: 23
```

Symantec Messaging Gateway filters messages for these headers. Based on the policy actions that you specify, it creates incidents in quarantine incident folders or informational incident folders.

Specify the policy action **Create a quarantine incident** to hold these incidents for remediation. Or you can specify the policy action to **Create an informational incident** to hold these incidents for review.

See "Creating a content filtering policy" in the *Symantec Messaging Gateway Administration Guide*.

4 Add specific content filter policy actions for the Approve, Reject, and Custom actions, as described in Table 2-3. You can configure any available action. These actions map to the three FlexResponse remediation actions you configured previously. (See "Configuring the Email Quarantine Connect FlexResponse plug-in" on page 22.)

Table 2-3 describes the three remediation actions you configure for the FlexResponse plug-ins. The Description column describes a typical workflow for remediating quarantined emails. You can configure other actions if desired by mapping these properties to other Symantec Messaging Gateway remediation actions.

Table 2-3 FlexResponse actions

Symantec Messaging Gateway action	Symantec Data Loss Prevention FlexResponse `dlp-remediator-action` property	Description
Approve	`REVIEW_STATE_APPROVED`	This action signals that the quarantined email has been approved for delivery. For a typical quarantine workflow, set this action to: `Deliver Message Normally`.

Table 2-3 FlexResponse actions *(continued)*

Symantec Messaging Gateway action	Symantec Data Loss Prevention FlexResponse `dlp-remediator-action` property	Description
Reject	`REVIEW_STATE_REJECTED`	This action signals that the quarantined email has not been approved for delivery. For a typical quarantine workflow, set this action to: `Delete message`
Custom	`REVIEW_STATE_CUSTOM`	You can set this action to any user-defined action. For a typical quarantine workflow, configure this action to encrypt and then deliver the message. You can also configure this action to archive the message.

See "Configuring Network Prevent for Email for use with Email Quarantine Connect" on page 29.

Configuring Network Prevent for Email for use with Email Quarantine Connect

Before configuring Network Prevent for Email to work with Email Quarantine Connect, you should begin with a fully configured and functional Network Prevent for Email Server.

See "Monitoring and preventing data loss in the network" in the *Symantec Data Loss Prevention Administration Guide*.

In the following procedure, you configure how a Network Prevent for Email detection server operates with Symantec Messaging Gateway. Select one of the following modes:

Reflecting mode	In reflecting mode, the Network Prevent for Email detection server receives messages from a Mail Transfer Agent (MTA). It analyzes them, and then returns them to the same MTA (with instructions to block the messages or process them downstream). In essence, the server returns messages to the same IP address from which they arrived.
Forwarding mode	In forwarding mode, the Network Prevent for Email detection server receives messages from an upstream MTA. It analyzes them, and then sends them on to a downstream MTA or hosted email service provider. You can specify a list of IP addresses or host names for the next-hop mail server in the Network Prevent for Email server configuration.

For more information on configuring reflecting mode or forwarding mode, see:

- "About Mail Transfer Agent (MTA) integration" in the *Symantec Data Loss Prevention Administration Guide*
- "How Symantec Messaging Gateway and Data Loss Prevention Network Prevent interact" in the *Symantec Messaging Gateway Administration Guide*

To configure Network Prevent for Email

1. Open the Enforce Server administration console and navigate to **System** > **Servers** > **Overview**.
2. Click on a Network Prevent for Email detection server.
3. Click **Configure**.
4. For production systems, deselect **Trial Mode**. For testing purposes, you may want to leave **Trial Mode** selected so that actual messages are not blocked.

   When trial mode is selected, the server detects incidents and creates incident reports, but does not block any messages.
5. To configure Reflecting mode, select **Reflect** in the **Next Hop Configuration** section and skip to Step 7.

   To configure Forwarding mode, select **Forward** and **Disable MX lookup** in the **Next Hop Configuration** section.
6. In the **Next Hop Configuration** section of the page, type the host name of the Symantec Messaging Gateway server in the text box.
7. Click **Save**.

8 Click **Server Settings**.

9 Set the **RequestProcessor.MTAResubmitPort** property to the port number used by Symantec Messaging Gateway. The default value is **10026.**

10 Click **Save**.

11 Click **Done**.

12 Repeat steps 2 - 7 for each Network Prevent for Email detection server.

See "Creating a user and role for a remediator" on page 31.

Creating a user and role for a remediator

Each user who remediates email incidents using Email Quarantine Connect must have a user account configured in the Enforce Server Administration console. The user account must belong to a role that allows users in that role to execute the smart response rules that you configured for use with Email Quarantine Connect.

See "Creating response rules for Email Quarantine Connect" on page 25.

For more information on configuring user accounts and roles, see "Managing roles and users" in the *Symantec Data Loss Prevention Administration Guide*.

See "Testing the integration" on page 31.

Testing the integration

Follow the steps in the following procedure to test your integration of Symantec Data Loss Prevention and Symantec Messaging Gateway.

To test Email Quarantine Connect

1 Complete the installation and configuration of Email Quarantine Connect that is described in this document.

2 Create emails that violate a Symantec Data Loss Prevention policy and send the emails to a recipient where the email is routed through Symantec Messaging Gateway.

3 Open the Enforce Server administration console and navigate to a Network Prevent for Email incident report.

4 Click on an incident to open the incident snapshot.

5 Attempt to remediate the incident by clicking one of the FlexResponse actions.

6 View the incident again in the Enforce Server administration console. Note that the incident history contains entries relating to the remediation action you used to remediate the incident.

Note: Depending on the Symantec Messaging Gateway configuration, it may take up to an hour before updates to the incident history appear.

7 Open the Symantec Messaging Gateway Control Center and view the details on the incident.

8 If the remediation does not occur in the way that you expect, check the following:

- Check the log files for error messages.
  See "Troubleshooting Email Quarantine Connect" on page 32.
- Re-check the plug-in configuration.
  See "Configuring the Email Quarantine Connect FlexResponse plug-in" on page 22.
- Re-check the Symantec Messaging Gateway configuration.
  See "Creating a user and role for a remediator" on page 31.

See "Troubleshooting Email Quarantine Connect" on page 32.

Troubleshooting Email Quarantine Connect

Table 2-4

Problem	Possible action
Remediation of incidents does not occur as you expect.	Check the following log file for error messages: `SymantecDLP\Protect\logs\tomcat\localhost_<date>.log` There are additional log files in the Symantec Messaging Gateway environment. See the *Symantec Messaging Gateway Administration Guide*.
Response rules do not execute.	Check the ordering of response rule actions in the response rules you configured for Email Quarantine Connect. Note that a Block response rule action executes before any Server FlexResponse actions. See "Creating response rules for Email Quarantine Connect" on page 25.

See "Uninstalling Email Quarantine Connect" on page 33.

Uninstalling Email Quarantine Connect

To uninstall Email Quarantine Connect, remove the three FlexResponse plug-ins and their configurations from the Symantec Data Loss Prevention Enforce Server host.

To uninstall Email Quarantine Connect

1. Make sure that all plug-in remediation actions have completed for this plug-in.
2. Stop the Vontu Manager and Incident Persister services.
3. Remove the following files from the plug-ins directory on the Enforce Server:
   - `EmailQuarantineConnectApproved.jar`
   - `EmailQuarantineConnectApproved.properties`
   - `EmailQuarantineConnectCustom.jar`
   - `EmailQuarantineConnectCustom.properties`
   - `EmailQuarantineConnectRejected.jar`
   - `EmailQuarantineConnectRejected.properties`
   - `EmailQuarantineConnect` folder and its contents.

   `SymantecDLP\Protect\plugins\`
4. Open the file `SymantecDLP\Protect\config\Plugins.properties` in a text editor.
5. Remove the three plug-ins from the list of plug-ins that is specified with the following property:

   `com.symantec.dlpx.flexresponse.Plugin.plugins=`
6. Delete the response rules you created for this integration.

   See “Creating response rules for Email Quarantine Connect” on page 25.
7. Remove the Next Hop configurations for the Network Prevent for Email detection server(s).

   See “Configuring Network Prevent for Email for use with Email Quarantine Connect” on page 29.
8. Delete the credential you created for this integration.

   See “Configuring certificates and authentication” on page 17.
9. Restart the Vontu Manager and Incident Persister services.

Chapter 3

Remediating Symantec Messaging Gateway incidents from the Enforce Server administration console

This chapter includes the following topics:

- About remediating quarantined email incidents
- Remediating email incidents from the Enforce Server administration console

About remediating quarantined email incidents

When Symantec Data Loss Prevention uses Email Quarantine Connect to integrate with Symantec Messaging Gateway, users can remediate incidents in the Symantec Data Loss Prevention Enforce Server administration console. The section is directed to remediators and describes how to remediate email incidents using the Enforce Server administration console. Users can also remediate incidents from the Symantec Messaging Gateway Control Center. For more information, see the *Symantec Messaging Gateway Administration Guide*.

Note: Remediators must have properly configured user accounts and roles to remediate incidents in the Enforce Server administration console.

See "Creating a user and role for a remediator" on page 31.

Installation and configuration of the Email Quarantine Connect FlexResponse plug-in enables the remediation actions that display in the incident reports or snapshots. Email Quarantine Connect provides three actions a user can choose from to remediate these incidents. The display name of these actions is defined when an administrator configures the plug-in. The actual action that Symantec Messaging Gateway performs in response to these FlexResponse actions is configurable in the Symantec Messaging Gateway environment.

Table 3-1 describes the actions that are used in a typical deployment. The actions that are configured in your deployment may be different. Consult your Symantec Data Loss Prevention and Symantec Messaging Gateway system administrators to learn the exact actions that have been configured. See Table 2-3 on page 28.

Table 3-1 Remediation actions

Action (As defined by the FlexResponse rule name)	Description
SMG Custom Action	The remediation that is performed by this action is defined in the Symantec Messaging Gateway environment.
SMG Approve Action	Approves the email for delivery. The message is released from quarantine and is sent to the recipients.
SMG Reject Action	The email is not approved for delivery and is deleted.

Table 3-2 describes several special cases that may arise due to the different ways Symantec Data Loss Prevention and Symantec Messaging Gateway manage incidents.

Table 3-2 Incident remediation special cases

Remediation issue	Description
Updates to incident status do not appear immediately.	When you remediate an incident from the Enforce Server administration console, the incident status and history are not updated until Symantec Messaging Gateway executes the remediation action and sends a notification to Symantec Data Loss Prevention. This notification does not happen synchronously and there can be a delay before the update is viewable in the incident snapshot or list.

Table 3-2 Incident remediation special cases *(continued)*

Remediation issue	Description
You need to remediate an email incident with multiple recipients that creates an incident for each recipient.	An email that has multiple recipients creates a single incident in Symantec Data Loss Prevention. However, Symantec Messaging Gateway creates an incident for each recipient. When you remediate an incident with multiple recipients from the Enforce Server administration console, all incidents that are created by Symantec Messaging Gateway are remediated using the same remediation action.
You need to remediate an email message that violates multiple policies and creates multiple incidents.	An email message may violate more than one policy. When an email violates multiple policies, Symantec Data Loss Prevention creates an incident for each violation. However, Symantec Messaging Gateway creates only a single incident. When you remediate one of these incidents from the Enforce Server administration console, the remediation action is not applied to the remaining incidents that are associated with the violation.
You need to remediate an email message that creates multiple incidents and that has multiple recipients.	If a message violates more than one policy and has multiple recipients, when you remediate the incident from the Enforce Server administration console, the incidents that Symantec Messaging Gateway creates for each recipient are also remediated using the same action. The incidents that Symantec Data Loss Prevention creates for each policy violation are not automatically remediated. There can be a delay before the remediation results are viewable in the incident snapshot.
The Symantec Messaging Gateway server cannot find the email that the remediation request references.	If an incident remediation request is sent to Symantec Messaging Gateway and Symantec Messaging Gateway cannot find the message, an entry in the incident history indicates that the message cannot be found.
For at least one Symantec Messaging Gateway incident, the Symantec Messaging Gateway server finds the email referenced by the request, but the email has already been released.	If a user initiates a remediation action from Symantec Data Loss Prevention on an email message that has already been remediated, the incident snapshot indicates that the server rejected the remediation request. The incident history also contains an entry indicating that the email has already been released.

Table 3-2 Incident remediation special cases *(continued)*

Remediation issue	Description
For at least one Symantec Messaging Gateway incident, the Symantec Messaging Gateway server fails to execute the remediation for any internal reason.	If the Symantec Messaging Gateway server fails to remediate an incident for any reason, a message is added to the incident history indicating that the email could not be remediated.

See "Remediating email incidents from the Enforce Server administration console" on page 37.

Remediating email incidents from the Enforce Server administration console

This section describes the steps that are required to remediate incidents from the Enforce Server administration console. You can remediate incidents from either an incident report or from an incident snapshot.

Note: Depending on how Symantec Messaging Gateway is configured, there may be a delay of up to an hour after a remediation action is initiated in the administration console before the incident status, history, and notes are updated.

To remediate incidents from an incident report

1. Open the Enforce Server administration console and navigate to **Incidents** > **Network**. You can also select any previously saved report that lists Network Prevent incidents.
2. Select the incidents you want to remediate, either manually, or by using the Filter and Advanced Filters to display the incidents you want to remediate.
3. Click **Incident Actions**.

   A drop-down list of incident actions displays.
4. Select **Run Smart Response** and then select one of the remediation actions that displays. You should see the three remediation actions that are associated with Email Quarantine Connect. You may also see other FlexResponse remediation actions that have been defined in your Symantec Data Loss Prevention deployment. Choose the appropriate action.

   The action is applied to all selected incidents.

To remediate email incidents from an incident snapshot

1. Open the Enforce Server administration console and navigate to **Incidents** > **Network**. You can also select any previously saved report that lists Network Prevent incidents.
2. Click on the incident you want to remediate.

   The incident snapshot for the incident displays.

   Note that the FlexResponse smart actions appear in a banner above the snapshot. Each action displays the following icon:

3. Click the FlexResponse action for the remediation you want to perform.

   The remediation action is executed for this incident.

Index

A

authentication 19
  configuration of 17
  credential 19
automated response rule
  configuration 25

C

certificates
  configuration of 17
certificates-store.credential 24
configuration
  Network Prevent for Email 29
  Symantec Messaging Gateway 27
credential 19
  configuration 24

D

dlp-remediator-action 25
dlp-remediator-user 24

E

Email Quarantine Connect
  about 6
  installation 13–14
  system requirements 14
  uninstalling 33
  workflow 7
email-gateway-server-host 24
email-gateway-server-port 24
EmailQuarantineConnect directory 21
EmailQuarantineConnectApproved.jar 21
EmailQuarantineConnectApproved.properties 21
EmailQuarantineConnectCustom.jar 21
EmailQuarantineConnectCustom.properties 21
EmailQuarantineConnectRejected.jar 21
EmailQuarantineConnectRejected.properties 21

F

FlexResponse actions 22
FlexResponse plug-in
  actions 25, 29
  configuration of 22
  configuring response rules 25
  installation 21
  Plugins.properties file 21
FlexResponse plug-in properties
  certificates-store.credential 24
  dlp-remediator-action 25
  dlp-remediator-user 24
  email-gateway-server-host 24
  email-gateway-server-port 24
forwarding mode 8, 30

I

Incident Update privilege 20
installation 13
  FlexResponse plug-in 21
installation overview 14

K

keystore 17
keytool 17

N

Network Prevent for Email
  configuration 29
Network Prevent: Modify SMTP Message action 26
Next Hop Configuration 30

P

Plugins.properties file 21

R

reflecting mode 7, 30
remediation
  about 34
  actions 35
  from Enforce Server 37

remediation *(continued)*
from Enforce Server administration console 9
from incident report 37
from incident snapshot 38
from Symantec Messaging Gateway Control Center 11
multiple incidents 37
multiple recipients 37
special cases 37
response rule
configuration 25
privileges 31
role 31
roles 19

S

smart response rule
configuration 25
SMG Approve Action 35
SMG Custom Action 35
SMG Reject Action 35
Symantec Messaging Gateway
configuration 27
Symantec_DLP_Plugin_Email_Quarantine_Connect_2.0.0.19.exe 21
system requirements 14

T

testing 31
troubleshooting 32

U

uninstalling
Email Quarantine Connect 33
user account 19, 31
user privileges 19–20

X

x-header 28