TRITON AP-DATA Email Gateway Administrator Help

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

This Administrator Help describes the management component for the TRITON AP-DATA Email Gateway virtual appliance. When deployed in a Microsoft Azure environment, AP-DATA Email Gateway for Microsoft Office 365 allows outbound email from Exchange Online to be analyzed for data loss or theft. Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped. See the TRITON AP-DATA installation guide for detailed information about deploying the Email Gateway virtual appliance.

Topics:

Initial TRITON AP-DATA Email Gateway configuration

Some initial configuration settings are important for proper TRITON AP-DATA Email Gateway operation. See the topic titled *Configuring the appliance in the TRITON Manager* in the TRITON AP-DATA installation guide.

Viewing subscription information

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You should have received a TRITON AP-DATA subscription key after you purchased the AP-DATA Email Gateway. Enter and view this key in the TRITON AP-DATA module.

Navigating the TRITON Manager Email module

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The Email module user interface can be divided into 6 main areas:

- Banner
- Module tray
- Email module toolbar
- Left navigation pane
- Right shortcut pane
- Content pane

The TRITON Manager banner shows:

- Your current logon account
- A Log Off button, for when you want to end your administrative session

The module tray lets you launch the Data module of the TRITON Manager. Click Data to open that module.

An Appliances button in the module tray opens a Manage Appliances window, which lets you add and remove an appliance in your system.

The module tray also provides access to Explain This Page context-sensitive Help, complete Help system contents, and the Support Portal.

The Email module toolbar, just under the module tray, lets you switch between the Main and Settings tabs of the left navigation pane. Use the Main tab to access policy management features and functions. Use the Settings tab to perform system administration tasks. The toolbar also includes a drop-down list of system appliances.

The right shortcut pane contains a Find Answers portal that may include links to topics related to the active screen and step-by-step tutorials for specific tasks. A search function lets you find relevant information in the Forcepoint eSupport web site.

Both the left and right navigation panes can be minimized by clicking the double arrow (<< or >>) icon at the top of the pane. Click the reverse icon (>> or <<) to view the pane. Click a shortcut icon on the minimized left navigation pane to access various groups of email security functions without maximizing the pane.

Registering with TRITON AP-DATA

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

With TRITON AP-DATA Email Gateway, you can have your email analyzed for regulatory compliance and acceptable use and protect sensitive data loss via email by enabling DLP policies in the **Main > Policy Management > Policies** page. Data loss prevention policies are enabled by default.

See *Enabling data loss prevention policies*, page 16, for more information about activating DLP policies.

Email Data Loss Prevention policy options are configured in the TRITON Manager Data module (**Main > Policy Management > DLP Policies > Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See *Data Security Manager Help* for details.

If you plan to use email encryption functions, you must configure an email DLP policy with an action plan that includes message encryption. See *Data Security Manager Help* for details.

You must register email appliances with TRITON AP-DATA in order to take advantage of its acceptable use, data loss prevention, and message encryption features. Registration is automatic with a valid TRITON AP-DATA subscription key. See subscription information in the Data module. Subsequent appliances are registered when you add them to the TRITON Manager from the Email Gateway interface.

If the Status field in the Email module **Settings > General > Data Loss Prevention** page displays **Unregistered**, you must register with TRITON AP-DATA manually.

Use the following steps in the Email module **Settings > General > Data Loss Prevention** page to register an appliance manually with TRITON AP-DATA:

1. Specify the IP address used for communication with the email protection system in the **Communication IP address** drop-down list.

   Note
   The appliance IP address is the one assigned to the virtual appliance by the cloud service.

2. Select the **Manual** registration method to enable the Properties entry fields.
3. Specify the following data management server properties:
   - IP address
   - User name
   - Password
4. Click **Register**.

5. You must deploy DLP policies in the Data module to complete the process. Click the Data module and then click **Deploy**.

> **Important**
> You should wait until DLP policies are completely deployed before you register another appliance.

Configuring email system alerts

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Your email protection system can notify administrators via an email message that various system events have occurred. Use the **Settings > Alerts > Enable Alerts** page to enable and configure this notification method.

Mark the **Enable email alerts** check box to have alerts and notifications delivered to administrators by email. Then, configure the following email settings:

Field	Description
From email address	Email address to use as the sender for email alerts
Administrator email address (To)	Email address of the primary recipient of email alerts. Each address must be separated by a semicolon.
Email addresses for completed report notification	Email addresses for completed report notification recipients. Each address must be separated by a semicolon.

Setting system preferences

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You can accomplish the following email system preferences on the **Settings > General > System Settings** page:

- *Entering the fully qualified domain name*
- *Setting the SMTP greeting message*
- *Setting system notification email addresses*

Entering the fully qualified domain name

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The SMTP protocol requires the use of fully qualified domain names (FQDN) for message transfer. Enter the appliance fully qualified domain name in the **Fully Qualified Domain Name** field (format is appliancehostname.parentdomain.com).

Important

This setting is important for proper email security system operation. You must replace the default fully qualified domain name entry with the correct appliance name.

An incorrect fully qualified domain name may cause disruptions in email traffic flow.

Setting the SMTP greeting message

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The SMTP greeting message is the response to a connection attempt by a remote server. It can also be used to indicate that the system is working properly. For example, the default SMTP greeting is

```
The email security service is ready.
```

Change the default message by entering text in the **SMTP greeting** field.

Setting system notification email addresses

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The email system can automatically send notifications of system events to a predefined address, often an administrator address. Enter the desired recipient address in the **Administrator email address** field.

If you want notification messages sent to or from an administrator email address for other than system events, you must enter an address in this field as well. For example, configuring a notification to be sent to or from an administrator address when a message triggers a filter requires that this field on the System Settings page contain an administrator address.

User notification messages may be sent from a predefined address. Enter the desired sender address in the **Default sender email address** field.

Managing appliances

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Before you add an appliance to TRITON AP-DATA Email Gateway, you should have already created a virtual appliance in the cloud service and performed initial configuration steps to activate email security functions on the appliance and configured network interfaces for the appliance. See the TRITON AP-DATA installation guide for detailed installation and configuration information.

If you change either the appliance hostname or communication IP address on the appliance, you must make the same change in the **Settings > General > Email Appliances** page. TRITON AP-DATA Email Gateway does not detect this change automatically.

Appliances overview

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You can manage multiple email appliances from the **Settings > General > Email Appliances** page without having to log on to each machine separately. Email Gateway appliances operate in standalone mode.

The Email Appliances page lists all current system appliances in a table that shows the appliance hostname, platform, system communication IP address, system connection status, and mode. It also contains an Action column, with links that allow you to switch to a different appliance (**Launch**).

To add an appliance to the appliances list in the **Settings > General > Email Appliances** page:

1. Click **Add**.
2. In the Add Appliance dialog box, enter the IP address used for communication with TRITON AP-DATA Email Gateway in the **System Communication IP Address** field.
3. Click **OK**.

Important

Changing the system communication IP address of an appliance terminates the appliance connection with AP-DATA Email Gateway. In order to re-establish the connection, the IP address must also be changed in the **Settings > General > Email Appliances** page.

When you add an appliance, it is automatically registered with AP-DATA Email Gateway for data loss prevention (DLP). To complete the registration process and deploy DLP policies, click the Data module on the TRITON console toolbar and then click **Deploy**.

You can remove an appliance from the appliances list by selecting the appliance and clicking **Delete**. Note that you cannot delete an appliance that is being accessed by another user. Once you remove an appliance from the list, you cannot manage it from the Email Appliances page.

Editing appliance settings from the appliances list

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You can edit the appliance communication IP address by clicking the appliance name in the appliances list. Note that the system connection status and mode cannot be changed on this page.

Managing domain and IP address groups

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

A collection of domain names or IP addresses can be defined in a single group for use in email functions. For example, you can define a domain name group to establish domain-based delivery options, or you can define an IP address group for which some email analysis is not performed. IP address groups can also be used for the email encryption functions.

You can perform the following operations on domain or IP address groups:

- *Adding a domain group*
- *Editing a domain group*
- *Adding an IP address group*
- *Editing an IP address group*

You may delete a domain or IP address group from its respective list by selecting the check box to the right of the name and clicking **Delete**.

You should note the following two special default groups of domain or IP addresses:

- Protected Domain group
- Trusted IP Address group

See *Third-party encryption application*, page 14, for information about using the Encryption Gateway default IP address group. Default groups cannot be deleted.

Protected Domain group

The Protected Domain group should contain all the domains that an organization owns and needs the email system to protect. An open relay results when both the sender and recipient addresses are not in a protected domain.

The default Protected Domain group is empty after product installation. Domains may be added to or deleted from the Protected Domain group, but you cannot delete the Protected Domain group itself.

Important

Ensure that the Protected Domain group contains all the domains you want your email system to protect.

An open relay is created when mail from an unprotected domain is sent to an unprotected domain within your organization. As a result, all mail from any domain that is not protected may be rejected.

The Protected Domain group should not be used to configure email delivery routes (in the **Settings > Inbound/Outbound > Mail Routing** page) if you need to define domain-based delivery routes via multiple SMTP servers. See *Domain-based routes*, page 11, for information.

Trusted IP Address group

By default, the Trusted IP Addresses group is populated with all the IP addresses referenced in Microsoft Office 365. IP addresses may be added to or deleted from the Trusted IP Addresses group, but you cannot delete the Trusted IP Addresses group itself. The Trusted IP Addresses group may include up to 1024 addresses.

Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Mail from trusted IP addresses can bypass some relay controls (**Settings > Inbound/Outbound > Relay Control**).

Note

Mail from trusted IP addresses does not bypass policy and rule application.

Adding a domain group

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Click **Add** on the **Settings > Users > Domain Groups** page to open the Add Domain Group page. Use the following procedures to add a domain group:

1. Enter a name for the new domain group in the **Domain Group Name** field.
2. Enter a brief description of your domain group.

In the Domain Group Details section, add a predefined domain group by clicking **Browse** next to the **Domain address file** field and navigating to the desired text file. The file format should be 1 domain address per line, and its maximum size is 10 MB.

If a file contains any invalid entries, only valid entries are accepted. Invalid entries are rejected.

1. You can also create a domain group by entering an individual domain address in the **Domain Address** field and clicking the arrow button to add the information to the **Added Domains** box on the right. Use wildcards to include subdomain entries (e.g., *.domain.com).
2. Click **OK**.

After you finish adding your domain address entries, you can export the list to your local drive as a text file by clicking the Added Domains **Export** button.

Remove an individual entry by selecting it in the **Added Domains** box and clicking **Delete**.

Editing a domain group

Administrator Help | TRITON AP-DATA Email Gateway| Version 8.2.x

You can edit a domain group by clicking the domain group name in the **Settings > Users > Domain Groups** page Domain Groups List to open the Edit Domain Group page. Add or remove individual domains on this page. You can also edit the domain group description.

Note that if a domain is in use, you will be asked to confirm any changes that involve that domain.

Adding an IP address group

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Click **Add** on the **Settings > Inbound/Outbound > IP Groups** page to open the Add IP Address Group page. Use the following procedures to add an IP address group:

1. Enter a name for the new IP address group in the **IP Address Group Name** field.
2. Enter a brief description of your IP address group.
3. Add a predefined IP address group by clicking **Browse** next to the **IP address file** field and navigating to the desired text file. The file format should be 1 IP address per line, and its maximum size is 10 MB.

Note

The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

Subnet addresses may be entered for other default and custom IP address groups.

4. You can also create an IP address group by entering an individual IP address in the **IP Address** box and clicking the arrow button to add the information to the **Added IP Addresses** box on the right.
5. Click **OK**.

After you finish adding your IP address entries, you can export the list to your local drive as a text file by clicking the Added IP Addresses **Export** button.

Remove an individual entry by selecting it in the **Added IP Addresses** box and clicking **Remove**.

Editing an IP address group

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You can edit an IP address group by clicking the IP address group name in the IP Address Groups List to open the Edit IP Address Group page. Add or remove individual IP addresses on this page. You can also edit the IP address group description.

Note that if an IP address is in use, you will be asked to confirm any changes that involve that address.

Configuring relay control options

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

You can prevent the unauthorized use of your mail system as an open relay by limiting the IP address groups for which your server is allowed to relay outbound mail. Configure relay control settings in the **Settings > Inbound/Outbound > Relay Control** page

In the Outbound Relay Options section, select the relay setting for senders in protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**. When you use this option, the sender domain must be included in the Email Gateway Protected Domains group (**Settings > Users > Domain Groups**).

Note that allowing all outbound relays may create a security vulnerability in your system.

Configuring delivery routes

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Configure domain-based delivery routes in the **Settings > Inbound/Outbound > Mail Routing** page. See *Domain-based routes*, page 11, for details.

Change the order of a domain-based route by marking its associated check box and using the **Move Up** or **Move Down** buttons.

Copying a route

Use the following steps to copy a route in the **Settings > Inbound/Outbound > Mail Routing** page:

1. Select a route in the route list by marking the check box next to its name.
2. Click **Copy**. A new route appears in the route list, using the original route name followed by a number in parentheses. The number added indicates the order that copies of the original route are created (1, 2, 3, etc.).
3. Click the new route name to edit route properties as desired.

Removing a route

If you want to remove a route, select the route by marking the check box next to its name and click **Delete**.

Note that the default domain-based route cannot be deleted.

Domain-based routes

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The Protected Domain group defined in the **Settings > Users > Domain Groups** page should not be used to configure delivery routes if you need to define domain-based delivery routes via multiple SMTP servers. Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

Use the following steps to add a domain-based delivery route on the **Settings > Inbound/Outbound > Mail Routing** page:

1. Click **Add** to open the Add Domain-based Route page.
2. Enter a name for your new route in the **Name** field.
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.
4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to edit your selected domain group, click Edit to open the Edit Domain Group page. See *Editing a domain group*, page 9, for details.
5. Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host). If you select this option, an SMTP Server List opens.
     a. Click **Add** to open the Add SMTP Server dialog box.

b. Enter the SMTP server IP address or hostname and port.

c. Mark the **Enable MX lookup** check box to enable the MX lookup function.

Important

If you entered an IP address in the previous step, the MX lookup option is not available.

If you entered a hostname in the previous step, this option is available.

- Mark the **Enable MX lookup** check box for message delivery based on the hostname MX record.
- If you do not mark this check box, message delivery is based on the hostname A record.

d. Enter a preference number for this server (from 1 - 65535; default value is 5).

If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

You may enter no more than 16 addresses in the SMTP Server List.

6. Select any desired security delivery options.

   a. Select **Use Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

   b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Configuring message exception settings

Administrator Help | TRITON AP-DATA Email Gateway| Version 8.2.x

The **Settings > Inbound/Outbound > Exceptions** page specifies how messages that cannot be processed for some reason are handled. Configure message exception settings as follows:

1. Specify whether a message should be delivered when an exception is caused by a data loss prevention policy.
2. If you want a notification sent regarding the unprocessed message, mark the **Send notification** check box to enable the Notification Properties section.
3. Specify the notification message sender from the following choices:
   - Original email sender (the default)

- Administrator. If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 5).
- Custom. Specify a single email address in this field.

4. Specify 1 or more notification message recipients from among the following choices:
   - Original email sender
   - Original email recipient
   - Administrator (the default). If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 5).
   - User specified. Enter 1 or more email addresses, separated by semicolons, in this field.
5. Specify the subject line of your notification message in the **Subject** field.
6. Enter the body of your notification message in the **Content** field.
7. If you want the original message to be attached to the notification message, mark the **Attach original message** check box.

If you do not specify either the delivery option or the notification option, the message that triggered the data loss prevention exception is dropped.

Handling encrypted messages

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

An email content policy configured in the Data module may specify that a message should be encrypted for delivery. If you want to encrypt specific outbound messages, you must create an email DLP policy that includes an encryption action plan in the Data module (**Main > Policy Management > DLP Policies**).

The following types of message encryption are supported:

- *Mandatory Transport Layer Security (TLS) encryption*
- *Third-party encryption application*

Use the **Settings > Inbound/Outbound > Encryption** page to specify the type of encryption you want to use.

Mandatory Transport Layer Security (TLS) encryption

TLS is an Internet protocol that provides security for all email transmissions. The client and server negotiate a secure “handshake” connection for the transmission to occur, provided both the client and the server support the same version of TLS.

In the Email Gateway, if you select only TLS for message encryption and the client and server cannot negotiate a secure TLS connection, the message is sent to a delayed

message queue for a later delivery attempt. Select **Transport Layer Security (TLS)** in the **Encryption method** drop-down list and the **Use TLS only (no backup encryption method; message is queued for later delivery attempt)** option to use only TLS for message encryption.

If you select TLS for message encryption, you can designate a third-party application as a backup method, in case the TLS connection fails. Specifying a backup option allows you a second opportunity for message encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

Select the **Transport Layer Security (TLS)** option in the **Encryption method** drop-down list to enable TLS encryption. Then mark **Use third-party application as backup encryption method** to use that backup method.

Third-party encryption application

The email protection system supports the use of third-party software for email encryption. The third-party application used must support the use of x-headers for communication with the email system.

You can also specify third-party application encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 13, for details.

The email protection system can be configured to add an x-header to a message that triggers a DLP encryption policy. Other x-headers indicate encryption success or failure. These x-headers facilitate communication between the email system and the encryption software. You must ensure that the x-header settings made in the Encryption page match the corresponding settings in the third-party software configuration.

X-header settings are entered on the **Settings > Inbound/Outbound > Encryption** page. Select **Third-party application** in the **Encryption method** drop-down list to configure the use of external encryption software. Use the following steps to configure third-party application encryption:

1. Add encryption servers (up to 32) to the Encryption Server List:
   a. Enter each server's IP address or hostname and port number.
   b. If you want to use the MX lookup feature, mark the **Enable MX lookup** check box.
   c. Click the arrow to the right of the Add Encryption Server box to add the server to the Encryption Server List.

   If you want to delete a server from the list, select it and click **Remove**.
2. In the **Encrypted IP address group** drop-down list, specify an IP address group if encrypted email is configured to route back to the email software. Default is Encryption Gateway.

3. If you want users to present credentials to view encrypted mail, mark the **Require authentication** check box and supply the desired user name and password in the appropriate fields. Authentication must be supported and configured on your encryption server to use this function.
4. In the **Encryption X-Header** field, specify an x-header to be added to a message that should be encrypted. This x-header value must also be set and enabled on your encryption server.
5. In the **Encryption Success X-Header** field, specify an x-header to be added to a message that has been successfully encrypted. This x-header value must also be set and enabled on your encryption server.
6. In the **Encryption Failure X-Header** field, specify an x-header to be added to a message for which encryption has failed. This x-header value must also be set and enabled on your encryption server.
7. Select any desired encryption failure options:
   - Mark the **Send notification to original sender** check box if you want to enable that option.

     In the Notification Details section, enter the notification message subject and content in the appropriate fields. Mark the **Attach original message** check box if you want the original message included as an attachment to the notification message.
   - Select **Deliver message** (default) if you want the message that failed the encryption operation delivered.
   - Select **Drop message** if you do not want the message that failed the encryption operation delivered.

Managing a filter

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

A predefined disclaimer filter is available for AP-DATA Email Gateway. The disclaimer filter automatically adds defined text to the beginning or end of a message. Specify the desired text in the Filter Properties section of the Edit Filter page for the Disclaimer filter. See *Disclaimer filter*, page 15, for information.

Disclaimer filter

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

A primary disclaimer may be written in any language, as long as the email message supports the same character set.

The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set.

Disclaimer text may be between 4 and 8192 characters in length. A line break uses 2 characters.

Specify where the disclaimer should appear in the email:

- **Beginning of message**
- **End of message**

The default disclaimer filter is combined with the default disclaimer action to form the Disclaimer policy rule.

Managing policies

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

One predefined default policy is available for outbound email, in which the sender address is from a protected domain in your organization and the recipient address is not in a protected domain. This policy cannot be modified.

A data loss prevention (DLP) policy is also available. Data loss prevention policies are configured in the Data module of the TRITON Manager and can only be enabled or disabled in the AP-DATA Email Gateway. You need to register the Email Gateway with the Data module and click **Deploy** in the Data module for the policies to be active.

Enabling data loss prevention policies

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

In addition to creating and enabling a policy that protects your email system from email threats, you can enable DLP policies that can detect the presence of sensitive data in your organization's email and execute appropriate actions to prevent data loss.

Email DLP policies must be configured in the TRITON Manager Data module (**Main > Policy Management > DLP Policies > Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See *Data Security Manager Help* for detailed information.

You should create a DLP policy in the Data module if you want to use message encryption. Ensure the policy has an action plan of "encrypt." See *Handling encrypted messages*, page 13, for information about email encryption options.

Data loss prevention policies are enabled by default in the Email Gateway. However, the Email Gateway must be registered with the Data module before the policies are applied to email. See *Registering with TRITON AP-DATA*, page 3, for instructions on how to register with the Data module.

If you need to enable DLP policies for some reason, click the DLP policy name on the **Main > Policy Management > Policies** page, and set the following options in the Edit Policy page:

- **Status:** Enabled or Disabled. Enable or disable the DLP policy. Data loss prevention policies are enabled by default.
- **Mode:** Monitor or Enforce. Select **Monitor** if you want the data loss prevention function to simply monitor your email, and select **Enforce** if you want to apply DLP policies to your email.
- **Notification.** Add a notification to a message when an email attachment to that message has been dropped as a result of a DLP policy.
  1. Mark the **Send notification when attachment of the message is dropped** check box to enable the sending of notifications.
  2. Enter the notification message text.
  3. Determine whether the notification text appears above or below the message body of the mail whose attachment was dropped.

Editing a policy

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

Click the outbound policy name on the **Main > Policy Management > Policies** page to edit the default policy. You can change the description of the policy in the Description field, and toggle its status between **Enabled** and **Disabled**.

Edit the disclaimer rule by clicking the link in the Rule Name column of the Rules table. See *Editing a rule*, page 17, for more information.

Editing a rule

Administrator Help | TRITON AP-Data Email Gateway | Version 8.2.x

Click **Edit** on the Edit Rule page to open the Edit Filter page. You can perform the following activities on this page:

- Enter or modify the filter description.
- Enter or modify the primary disclaimer text.
- Enter or modify the secondary disclaimer text.
- Specify whether the disclaimer appears at the beginning or end of a message.

See *Disclaimer filter*, page 15, for more information.

Configuring Log Database options

Administrator Help | TRITON AP-DATA Email Gateway | Version 8.2.x

The Log Database stores appliance configuration and management data. It is not used to store message logs when used with the AP-DATA Email Gateway.

Making changes to Log Database settings on 1 appliance applies those changes to all the appliances in your network.

A Log Database Location section at the top of the page lets you enter the IP address\instance or hostname\instance of your Log Database server. By default, the Log Database created at installation is entered. It must be the IP address assigned to the Log Database when it was added to the VPN. If you chose to encrypt the database connection at product installation, the **Encrypt connection** check box is marked. If you did not select the encryption option during installation, you can encrypt the database connection by marking the check box here.

Other settings created at installation and displayed here include the designated authentication method (Windows or SQL Server), user name, and password.

Click **Check Status** to determine the availability of the server.