

# 1

## Getting Started

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Websense TRITON AP-EMAIL protects your organization against the threats of malware, spam, and other unwanted content in email traffic.

TRITON AP-EMAIL provides maximum protection for email systems to prevent malicious threats from entering an organization's network. Each message is analyzed by a robust set of antivirus and antispam filters to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

You configure and manage your services using the TRITON Cloud Manager. The manager provides a central, graphical interface to the general configuration, policy management, and reporting functions of your service, making defining and enforcing email security an easy, straightforward process. You maintain control over the system through on-demand statistics and reporting, but powerful self-service tools allow end users to manage quarantined mail, helping relieve the burden on IT staff.

### About this guide

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

This guide is intended for IT administrators who are responsible for setting up and operating TRITON AP-EMAIL cloud-based accounts.

It relates to all TRITON AP-EMAIL services, although the functionality available to you depends on licensing.

The layout of the Cloud TRITON Manager screens is similar for all services. Wherever possible this guide indicates where a feature or functionality is specific to a particular service.

## Initial steps

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Take the following steps to get started with TRITON AP-EMAIL.

1. Request an evaluation.
2. Register for the service.
3. Log on to the Cloud TRITON Manager.
4. Add inbound and outbound connections.
5. Add domains.
6. Set up outbound email routing.
7. Set up inbound email routing.
8. Restrict connections to your mail servers.
9. Set up users and groups.

It is likely that you have already completed these steps. If not please see the TRITON AP-EMAIL [Getting Started Guide](#).

## Logging on and portal security

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions



### Note

To use the Cloud TRITON Manager, your browser must be Javascript-enabled.

To access the Cloud TRITON Manager, visit <https://admin.websense.net/portal>.

The logon process uses cookies where possible. For the best user experience, we recommend that you accept cookies from the Cloud TRITON Manager. If your web browser is unable to, or is configured not to accept cookies from the Cloud TRITON Manager, an additional screen appears during logon reminding you of the benefits of securing your session.

If the Cloud TRITON Manager cannot use cookies to secure the session, it falls back to ensuring that all requests for the session come from the same IP address. This may cause problems for you if your company has several load-balanced web proxies, because the Cloud TRITON Manager perceives requests coming from several sources as a security breach. Companies with a single web proxy or a cooperating web proxy farm should not be affected.

To avoid problems, we recommend enabling cookies on your web browsers.

## Locking down your firewalls

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Getting Started](#)

If you have not already done so, we strongly recommend that you follow the advice provided in the TRITON AP-EMAIL Cloud [Getting Started Guide](#) and restrict connections to your email servers so that they only accept email from the IP address ranges used by Websense. These can be found on the [Service IP addresses](#), [page 43](#) page.

## Privacy statement

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Logging on and portal security](#)

The Cloud TRITON Manager uses 2 cookies during logon. The first is used to identify whether the user's Web browser is willing to accept and store cookies for the manager; it contains no information. If the first cookie is successfully stored, a second cookie is stored containing temporary information about the session. No personal information is stored in either cookie, and both cookies are used only for the duration of the session.

## Idle timeout

Cloud TRITON Manager Help | Cloud Email Protection Solutions

For security reasons, if you are logged on to the Cloud TRITON Manager and are inactive for a pre-defined period, you are automatically logged off. When you next attempt to perform an action, you are asked to log on again. Once you have done so, you are taken to the page that you requested. The inactivity timer is between 30 and 60 minutes.

## Customizable landing page

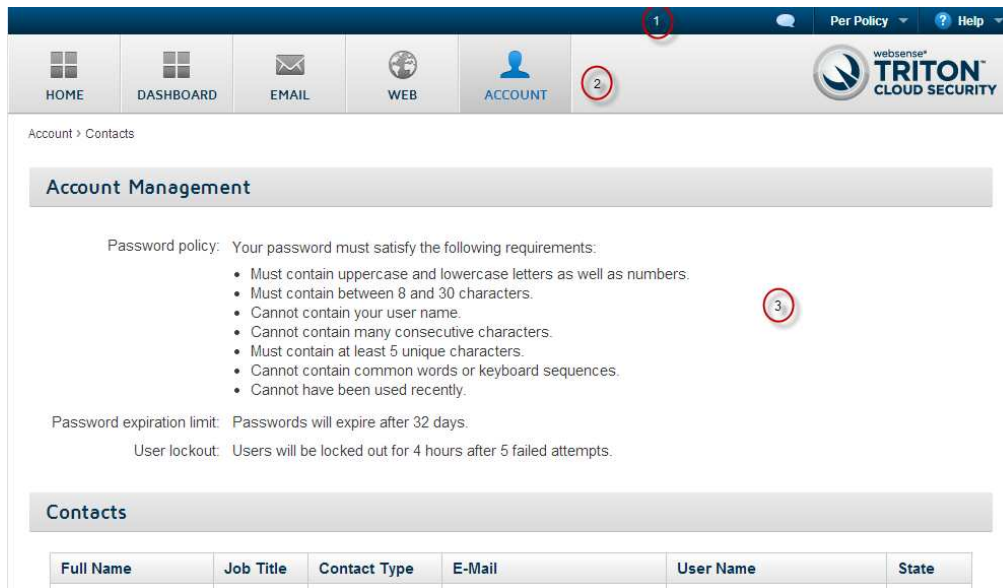
Cloud TRITON Manager Help | Cloud Email Protection Solutions

By default, when you first log on to the Cloud TRITON Manager, you land on the Dashboard page. You can change your landing page by navigating to what you would like your landing page to be and clicking the **Pin** option on the top menu bar. Note that some pages have been deliberately excluded from supporting this functionality.

# Cloud TRITON Manager Navigation

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The Cloud TRITON Manager interface can be divided into the following main areas:



1. Banner
2. Toolbar
3. Content pane

The **banner** shows:

- ◆ Any **Alerts** that are available for your account
- ◆ Your current **logon account**. When you're ready to end your administrative session, click the arrow next to the administrator name and select **Log Off**.
- ◆ The **Help** menu, from which you can access assistance for the page you are currently viewing, further product information, and Websense Technical Support resources.

The Help menu also includes the **Support PIN**. You must authenticate yourself with this PIN when calling Websense Technical Support.

Each PIN is unique per user, and is generated when a user logs on. The PIN is then valid for 24 hours after logon. After a 24-hour period has expired, a new PIN is generated at the next logon.



## Important

In order to preserve and maintain the security of your data, Support representatives will not be able to provide customer support without an accurate, up-to-date PIN.

The **toolbar** indicates which part of the Cloud TRITON Manager is currently active:

- ◆ **Dashboard** provides access to the Cloud Email Security dashboards.
- ◆ **Reporting** gives access to all reporting options, including email reports, account service reports, and your saved reports.
- ◆ **Email** contains all configuration settings relating to TRITON AP-EMAIL, including account-wide email settings, policy management, and the [Message Center](#).
- ◆ **Account** provides access to configuration options that apply to all cloud services. This includes administrator management, directory synchronization, licenses, and groups.

When you select an item in the toolbar, a **navigation pane** drops down, containing the available navigation choices for that item. Click the toolbar item again to close the navigation pane.

The **content pane** varies according to the selection you make in the navigation pane.

## Dashboard

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To view your main email dashboard, go to **Dashboard**. If you are a cloud web and email customer, select the **Email** tab. The dashboard provides a snapshot view of how your cloud email services are performing.

The panels you see depend on your subscription settings. You may see the following:

- ◆ Email activity overview - the number of inbound and outbound email requests processed for your account in the last 7 days.
- ◆ Inbound and outbound composition categories - reveals how TRITON AP-EMAIL categorized your inbound and outbound email. Examples of composition categories include Phishing, Commercial Bulk, and Backscatter
  - Phishing - attempts to acquire information, such as usernames, passwords, or credit card information by masquerading as a trusted or well-known entity
  - Commercial Bulk - solicited bulk email, such as newsletters
  - Backscatter - maliciously generated bounce messages (e.g., non-delivery report/receipt (NDR); delivery status notification (DSN); and non-delivery notification (NDN) messages) sent by spammers to spoofed return addresses
- ◆ Top 5 viruses - indicates the top 5 viruses seen in your account along with the number of email carrying each of these viruses.
- ◆ URL categories in email - reveals how TRITON AP-EMAIL classified all of the URLs found in your organization's email.

You have the option of viewing this data in either a bar graph or pie chart.





## Alerts

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Click the speech bubble icon in the toolbar to see alerts for your account.

Alerts are the primary means of communicating with customers to keep you fully informed of service issues. If you suspect that there may be a problem with the service, log on and check for new alerts. The number of alerts for your account is displayed with the alert icon.

You may see the following alert types:

	<b>Error.</b> Your service has been interrupted, and you must act on this alert immediately.
	<b>Severe.</b> You must act on this alert as soon as possible. If you do not act by the date given in the alert, it will be upgraded to Error and you risk interruption of your service.
	<b>Warning.</b> This alerts you to future events that might affect your service – for example portal outages, or license expiration.
	<b>Information.</b> This might be announcing a new release or upcoming maintenance work.

Select an alert summary in the left pane to see more detail, if available, in the right pane.





# 2

## Account Settings

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Click **Account** in the Cloud TRITON Manager toolbar to see the configuration options that apply to the complete account. Only administrators with account-level privileges can access these. The exact options available on the menu depend on the services you are licensed for.

- ◆ To change the password for your cloud service administrator account, select [My Account](#), [page 9](#).
- ◆ To view the configuration audit database for your account, choose [Audit Trails](#), [page 163](#).
- ◆ Choose [Contacts](#), [page 10](#) to view and modify the contact details of people in your organization who administer, support, and pay for the services. The administrator contacts can be given logons to the portal and their permissions restricted as necessary. You can also use this page to modify your password settings.
- ◆ To set up your own combinations of file types, MIME types, and file extensions for email attachment blocking, choose [Custom file types](#), [page 17](#).
- ◆ If you are using Choose [Directory Synchronization](#), [page 18](#) to configure directory synchronization for your account.
- ◆ Choose [End Users](#), [page 18](#) to search for end users so you can enable or disable their Web access, delete them, or change their policy assignments. (This option is available only to accounts enabled for directory synchronization.)
- ◆ When you define [Groups](#), [page 19](#), they are available in all your policies in all services. This allows you to define a consistent set of rules across the services for groups of end users.
- ◆

This chapter covers the configuration of account-level options. To configure the majority of email service options, click **Email** in the toolbar and then select the appropriate setting type or policy.

## My Account

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Use the My Account page if you need to change your password or generate a new one. Enter and confirm a password, then click **Submit** when done. The password must conform to your password policy, as described on the screen.

Optionally, you can also change your password question. Select a question from the drop-down list, then enter an answer to the question and click **Submit**.

See [Changing passwords](#), page 20 for more information about passwords.

## Contacts

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Adding a contact](#)
- ◆ [Password settings](#)

Use the **Contacts** page to define the password policy for administrators in your account, and to manage the contact list and administrator logons.

The Account Management area displays the current requirements for passwords in your account, as well as any expiration limit. For more information, see [Password settings](#), page 13.

The contact information in the **Contacts** area is created with the details supplied during enrollment. The initial contact assumes the role of Company Master User and has the highest rights and privileges for your account.

We use these contact details defined on this page when we need to communicate with you. You can specify a variety of contact addresses and numbers for each contact, plus a call order that specifies the order in which we should call them.



### Note

If the contact also has logon privileges, you must enter an email address to enable them to use the password reset function, if required.



### Note

It is your responsibility to administer the logon privileges for the contacts in your account, and to ensure access to the Cloud TRITON Manager is maintained or protected as appropriate. You are also responsible for any actions taken by the users of the administrator logons that you create.

---

## Adding a contact

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

To add a new contact:

1. Click **Add**.
2. Select the new contact's **Title**, and enter the first name and surname. The **Full name** field is automatically populated.
3. Select the **Contact type** from the drop-down list.
4. Optionally, enter further details for the contact, including the job title, department, and address.
5. Enter a telephone number, email address, or both. It is recommended that you provide at least one form of contact that Support can use if required.
6. Select a preference for each form of contact so that Support know the order in which your administrators should be contacted.
7. Click **Submit**.

### Adding logon details

To assign logon privileges to the contact you just created:

1. In the **User name** field, click the hyperlink in **No user name. Click here to add one**. This opens the Add User Name screen,



#### Note

You can also access this screen by clicking the contact's logon ID in the User Name column on the main Contacts screen.

---

2. By default, the email address is used as the contact's logon ID. To change this, edit the User Name field.
3. Enter and confirm a password for the user.

You can type a password for the user and confirm it. Alternatively, if you want to automatically generate a password that complies with the password policy, click **Create a password for me**. The password, which meets the stated password policy, populates into the Password field.
4. Define when the password should expire. By default this is the same as the expiration limit set as part of your password policy (see [Password expiration limit](#), page 15).

5. To force the user to change the password when they log on, mark **Change password next log on**. This is recommended.

**Note**

When the user first logs on, a screen is displayed giving them 8 days to select a password question from the list provided and enter an answer. This password question and answer is used if the user later forgets their password (see [Forgotten passwords, page 17](#)). If the user does not set a password question within the 8-day limit, they are forced to do so at their next logon.

---

**Configuring permissions**

By default, all rights are assigned to the Company Master User - the first contact established on your account. When this user creates a new user, by default only the **View All Reports** permission is assigned to the new user. This is the minimum permission a user needs to be able to log on; it grants permissions over only the Reporting tab on the main menu bar.

We provide flexible users' rights so you can create a hierarchy of administrators. For example, much of the functionality accessed from the portal is useful for help desk agents to aid with problem isolation; but they do not necessarily require control over policy configuration.

Likewise, you should assign Directory Synchronization privileges to the contact you set up for the Directory Synchronization Client (see [Set up authentication, page 34](#)), but no-one else should need this privilege.

Permissions are granted at an account and policy level. This lets you create multiple policies, and administrators can control their own policy but no one else's.

To modify an administrator user's permissions, click **Edit**. To refine policy-level permissions, click **Advanced**.

**Note**

The **Advanced** button does not show for contacts with Manage Users permissions, because they are assumed to have maximum account-level permissions.

---

The following are account-level permissions:

- ◆ **Manage Users** - User can create, edit, and remove user logons and permissions.
- ◆ **Directory Synchronization** - User can synchronize an LDAP directory with the cloud service.
- ◆ **View All Reports** - User can run all reports associated with the licensed services.

The following email permissions can be assigned at the account or policy level:

- ◆ **Modify Configuration** - User can modify all options within Account Settings except users' logons – for this, the user must have **Manage Users** permissions.

- ◆ **View Configuration** - User can view all configurations within Account Settings, but not make any changes.
- ◆ **View Configuration Audit Trail** - User can access and search the policy setup audit trail. User also has access to the black and white list search facility.
- ◆ **Quarantine Administration** - Same as “View Quarantine,” but the user can also perform actions on the messages.
- ◆ **View Quarantine** - User can use Message Center to search quarantined messages but cannot perform any actions on the messages.
- ◆ **View Quarantine Audit Trail** - User can access and search the Message Center audit trail. User also has access to the black and white list search facility.
- ◆ **View Quarantined Images** - User can access and search the Message Center for quarantined images. “View Quarantine” must also be enabled to use this option.
- ◆ **View Delivered Messages** - Same as “View Quarantine,” but the user can view message logs as well as quarantined email.
- ◆ **Black and White Listing** - User can access, search, and manage all black and white lists.
- ◆ **View Filtered Reports** - User can only view reports that can be filtered by the specified policy or policies. This option is not available if View All Reports is selected.

**Note**

The View Filtered Reports option may not be enabled in your account.

---

**Note**

If users are logged on to the portal when their permissions are changed, the changes do not take effect until they log off and then log on again.

---

## Password settings

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

Click **Account > Contacts > Edit** to define password settings for your account. On this screen, you can define an expiration limit for your users and also set up the user lockout option. If you have more than one password policy (a policy that defines how

“strong” your users’ passwords must be), you can also choose which policy to use on this screen. Click **Update** when you’re finished making your selections.

Note that you can override these settings for individual users on their permissions settings screen.

## Password policy

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

A password policy defines how “strong” your users’ passwords are required to be. (A strong password is a secure password.) The password policy in the cloud portal sets the minimum length, maximum length, password history, sequence rules, and unique character rules of a user’s password.

Following are the minimum requirements:

Parameter	Default policy value
Minimum length	8
Maximum length	30
Password history size (number of former passwords to check)	3
Maximum number of characters in sequence	4
Minimum number of unique characters	5

In addition, passwords:

- ◆ cannot contain the user’s logon ID.
- ◆ cannot contain common words or keyboard sequences.
- ◆ must include uppercase letters.
- ◆ must include lowercase letters.
- ◆ must include numbers.

## Password expiration limit

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

We recommend that you force users to change their passwords on a regular basis. Passwords can be set to automatically expire in a set time period. You configure this on the main setup screen for the account. You can override this setting for individual users on their permissions settings screen.

1. On the Contacts screen, click **Edit**.
2. From the **Password expiration limit** drop-down list, select one of the following from the expiration period: 30, 60, 90, 120, or 180 days, Custom days.  
When you click **Custom days**, a new field appears so you can enter any number of days you want. Periods longer than 365 days are not supported.
3. Click **Update**.

## User lockout

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Unlocking user accounts](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

If a user enters an incorrect password when attempting to log on, they have a limited number of further attempts before they are locked out for a period of time. You set up the number of further attempts and the lockout time period on the main setup screen for the user.

1. On the Contacts screen, click **Edit**.
2. From the **User lockout** drop-down list, select a lockout time period. The options are 15 minutes, 1 hour, 4 hours, 24 hours, or Forever.  
If you select **Forever**, an administrator with Manage Users permissions must unlock the user account before the user can log on again.
3. Select the number of permitted failed attempts from the drop-down list. This can be between 3 and 10.
4. Click **Update**.

## Unlocking user accounts

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [User logout](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

If a user is locked out because they failed to enter the correct password after the allotted number of attempts, an administrator with Manage Users permissions can unlock the user account before the lockout time period has ended. If the lockout time period is set to **Forever**, the user must be unlocked by an administrator.

1. Select **Account > Contacts**.
2. In the User Name column of the contact list, click the required user name.
3. Click **Edit** on the User screen.
4. Click **Unlock**.
5. Click **Submit**.

## Changing passwords

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Forgotten passwords](#)

Users are required to change passwords when they expire or when a change is forced by an administrator. Only administrators with Manage Users permissions can force a user to change his or her password. To force a change, select the **Change Password next logon** box on the user's contact screen. When users are required to change their passwords, they see a Change Password screen the next time they log on.

Users can also opt to change their password from **Account > My Account**, which displays the same Change Password screen.

If a user creates a password that does not meet the password policy standards, they receive an error message and are asked to try again. For example:

This password has been used recently. Please try another.

To implement the changed password, users should click **Save**. They should also make note of the password for future reference.



## Forgotten passwords

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)

If a user forgets their password, they can click the **Forgot your password?** link on the logon screen and follow the instructions to reset the password:

1. The user enters their portal user name and clicks **Submit**.
2. The cloud service sends an email to the email address listed in the contact details associated with that user name.



### Note

If the email address set up for the user name on the Contacts page is out of date or invalid, the user must contact their administrator to get their password reset.

---

3. The user clicks the link in the email to go to a secure page.
4. The user enters the answer to their password question, and clicks **Submit**.
5. When the question is answered correctly, the user can enter and confirm a new password. They also have the option to change their password question.



### Note

If a user forgets the answer to their password question, they must contact their administrator to get their password reset.

---

Should you need to generate a new password for a user, follow these steps:

1. Select **Account > Contacts**.
2. In the User Name column of the contact list, click the required user name.
3. Click **Edit** on the User screen.
4. Click **Create a password for me**.
5. Make note of the password.
6. Click **Submit**.

## Custom file types

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The cloud service provides a number of file formats and file types to enable you to manage messages containing attachments. File types allow you to quarantine attachments by specific formats, for example GIF files or HTML documents. File formats are more generic: for example, the Sound format includes anything related to sound files, including RealAudio, Windows Media Audio, MPEG Audio, and MIDI files.

If the available file formats and types do not meet your requirements, you can set up custom file types containing one or more file types and MIME types. You can then use the custom file types to quarantine or park messages with the attachments you specify.

For more information, see [Creating custom file types](#), page 94.

## Directory Synchronization

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Working with LDAP Directories](#)
- ◆ [What is LDAP?](#)
- ◆ [How the service works with LDAP](#)
- ◆ [Basic steps](#)

Click **Account > Directory Synchronization** when you want to configure your account for directory synchronization. See [Configure directory synchronization](#), page 31 for details on this screen and other LDAP considerations.

## End Users

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [End Users tab](#)
- ◆ [Managing registered users](#)

To view and manage user data, click **Account > End Users**. (This option is only available if you have directory synchronization enabled.) The resulting screen has 3 columns.

Column	Description
Criteria to use	Check the boxes on the left to indicate what search criteria to use.
Search Criteria	Narrow down the search by entering or selecting precise data in the middle column. Under source, you can choose whether to search <i>synchronized</i> users or <i>portal-managed</i> users.
Show in Results	Check the boxes on the right to indicate what information to include in the results.

Click **Search** when done. Please note that the search may be slow if there are a large number of users.

From the resulting data, you can make individual edits or bulk edits. For example, you can:

1. Undo the manual override (applies only to directory synchronization)
2. Delete user(s)

Using the drop-down list between the search box and the search results, select the action you want to make, then select the users on which to perform the action and click **Go**. All changes made on this screen override any group/policy assignments (existing or future ones).

You can view and manage user data at the policy level as well using the **End Users** screen for the policy. The account-level page shown here is available only to users with account-level privileges.

## Groups

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Downloading and uploading groups](#)

The groups functionality enables you to create policies using your organization's hierarchy.

Groups can contain:

- ◆ email addresses of users in your organization
- ◆ other groups

Groups are configured at the account level. To set up groups in the cloud service, click **Account > Groups**.

The resulting screen shows a list of groups currently defined for your account, an indication of whether they were added manually on the portal or automatically through the directory synchronization feature, and the web policy to which the group is assigned.

On this screen, you have the ability to create new groups and edit group membership. Click a group name to edit it, or click **Add** to add a new group. You can also change the order of groups in the list by dragging and dropping the group names.



### **Important**

Add or load groups only if you intend to use them for policy assignment or exceptions. You don't need them just because users are members of them.

---

## **Downloading and uploading groups**

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

If you are managing groups strictly in the cloud (in other words, you are *not* using directory synchronization), you have the option to upload or download a list of groups in a comma-separated values (CSV) file. You can then edit this using a simple text editor or a spreadsheet application such as Microsoft Excel.

If a policy includes a group that contains email addresses not on domains routed by the cloud email service, those email addresses are ignored.



### **Important**

If you already have groups in place for web users and there are dependencies between the groups and rules, replacing existing groups and addresses with uploaded versions could void exceptions to your rules. (For example, if a rule states that no one but the Accounting group can access [www.financialnews.com](http://www.financialnews.com), and then you upload a new Group list, it is possible that Accounting could lose access to that website.)

To maintain existing group/rule associations, make sure that group names in the CSV file match group names in the portal exactly. The best way to achieve this is to download existing group configurations to a PC, manipulate them as needed, then upload the changes to the cloud.

---

# Licenses

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Licenses screen](#)
- ◆ [License information](#)
- ◆ [Accepting licenses](#)

Our subscription model operates in a similar manner to many software vendors: to use the service, you must accept the terms of your agreement. Once you have done this, your services are automatically enabled, renewed, or upgraded depending upon the subscription type.

The purchase and billing systems are fully integrated with the Cloud TRITON Manager. Each cloud service has a subscription associated with it, and that subscription is applied to each customer account.

To view the subscriptions associated with your account, go to **Account > Licenses**. You can use this area of the portal to view and manage your rights to use cloud services.



## Note

If an alert indicates that your account is currently unlicensed, please check the **Licenses** screen for further information.

## Licenses screen

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [License information](#)
- ◆ [Accepting licenses](#)

The **Licenses** screen provides basic information about your account. Depending on the subscriptions associated with your account, you may see up to 3 sections:

1. Pending licenses: Licenses that require accepting.
2. Current licenses: Licenses that have been accepted and are currently valid.
3. Previous licenses: Licenses that have either expired or been replaced by another license.

## License information

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Subscriptions are generated automatically when you order a service. Each subscription contains the following information:

- ◆ **Contract:** The contract governing the license. This contains a link to a copy of the contract.
- ◆ **License type:** This provides information about the type of subscription (renewal, upgrade, etc.) and the contract type (for example, evaluation, SIB).
- ◆ **Services:** The services that your account is licensed to use.
- ◆ **Users:** The number of users or mailboxes for which your account is licensed.
- ◆ **Ordered by:** The name of the reseller that ordered the license for you.
- ◆ **Valid from / until:** Start and end dates of the license.
- ◆ **Billing period:** When you pay for your license – typically annual in advance or multi-year in advance.

## Accepting licenses

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The first time you log on to a new cloud service account, you are shown the licenses screen and must accept the terms of the agreement to activate your account and continue. If multiple subscriptions exist, you can accept them all at once.

Whenever a new subscription is ordered for you (for example, at renewal time or following an upgrade), it is added to your account in a pending state. You must accept this subscription to use the service. Each time you log on, you are taken to the licenses screen to remind you that a subscription requires accepting.



### Note

To ensure continuity of service, you should accept any pending licenses as soon as possible. This requires Modify Configuration permissions.

---

If your license expires before you have a chance to renew it, you receive a grace period. During that period, please order a new subscription as soon as possible.

## Important rules for configuring accounts

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

- ◆ Your account can enforce multiple policies on your email and web traffic.
- ◆ It is good practice to keep the number of policies to a minimum, because if a global change is required, you must make it across all policies.

- ◆ To prevent accidental changes, many configuration options are greyed out until you click the appropriate edit box.
- ◆ Each service has its own configuration screen accessed by clicking the appropriate tab on the main policy setup screen. Regardless of the services that you are licensed to use, you see all tabs. If you click the tab for a service that you are not licensed to use, you are informed of such.
- ◆ Where multiple email addresses, domains, or user names are entered into a screen, they should be separated by commas.
- ◆ You can click **Help** at any time to access online help information.
- ◆ All changes are made in real time and usually only take a few minutes to propagate across the cloud infrastructure.
- ◆ TRITON AP-EMAIL analyzes inbound and outbound email including both inbound and outbound spam. Analyzing outbound spam helps detect email that might be being sent by a botnet or otherwise compromised system at your site.
- ◆ Cloud web products Most settings in the policy screens are specified separately for inbound and outbound policy application. It is often not appropriate to set these identically for each direction. For example if a virus is detected in outbound email, then you probably do not want to send a notification to the intended recipient, whereas you might for an inbound email.
- ◆ Each TRITON AP-EMAIL policy applies to a domain or set of domains and specifies settings that TRITON AP-EMAIL uses to determine how to process your email.
- ◆ If you need to route email for different domains to different servers, you need to create a separate policy for each set of domains. Each policy includes its own routing table.

To access an email policy, click **Email**. Then go to **Policy Management > Policies**, and you are presented with a choice of service-specific policies.





# 3

## Working with LDAP Directories

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Maintenance](#)
- ◆ [Configure directory synchronization](#)

The cloud service allows you to make use of existing LDAP directories, such as Active Directory or Lotus Domino, so you don't have to re-create user accounts and groups for your email and web services or manage users and groups in two places.

The cloud service synchronizes with LDAP directories via a client-resident application known as the Directory Synchronization Client. Changes made to a directory, such as deleting a former employee or adding a new one, are picked up by the service on the next scheduled update. If you have more than one LDAP directory, the client can merge them together before synchronizing the data with the service.



### Important

The cloud service supports only one instance of the Directory Synchronization Client for each account. Using multiple synchronization configurations, or even using multiple installations of the Directory Synchronization Client, can cause data on the cloud service to be overwritten.

cloud web productsFor TRITON AP-EMAIL, you can synchronize primary and secondary email addresses and groups into the portal, improve spam detection, and improve the quality of reporting (less spam in the report). Directory synchronization makes it easier to manage groups as well.

## What is LDAP?

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [\*How the service works with LDAP\*](#)
- ◆ [\*Basic steps\*](#)
- ◆ [\*Cloud-based tasks\*](#)
- ◆ [\*Client tasks\*](#)
- ◆ [\*Maintenance\*](#)
- ◆ [\*Configure directory synchronization\*](#)
- ◆ [\*Set up authentication\*](#)

Lightweight Directory Access Protocol (LDAP) is a networking protocol for querying and modifying directory services. An LDAP directory contains data with similar attributes and organizes data in a directory tree structure. It is considered “lightweight” because it is a reduced version of the X.500 directory standard.

Active Directory (AD) is Microsoft’s LDAP-compliant directory service, and is an integral part of the Windows Server architecture. Active Directory is a hierarchical framework of resources (such as printers), services (such as email), and users (user accounts and groups). It allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization.

The cloud service integrates with LDAP directories and has been certified to work with Microsoft Active Directory. If you have enterprise information stored in AD, you do not have to enter it into the cloud portal manually.

## How the service works with LDAP

---

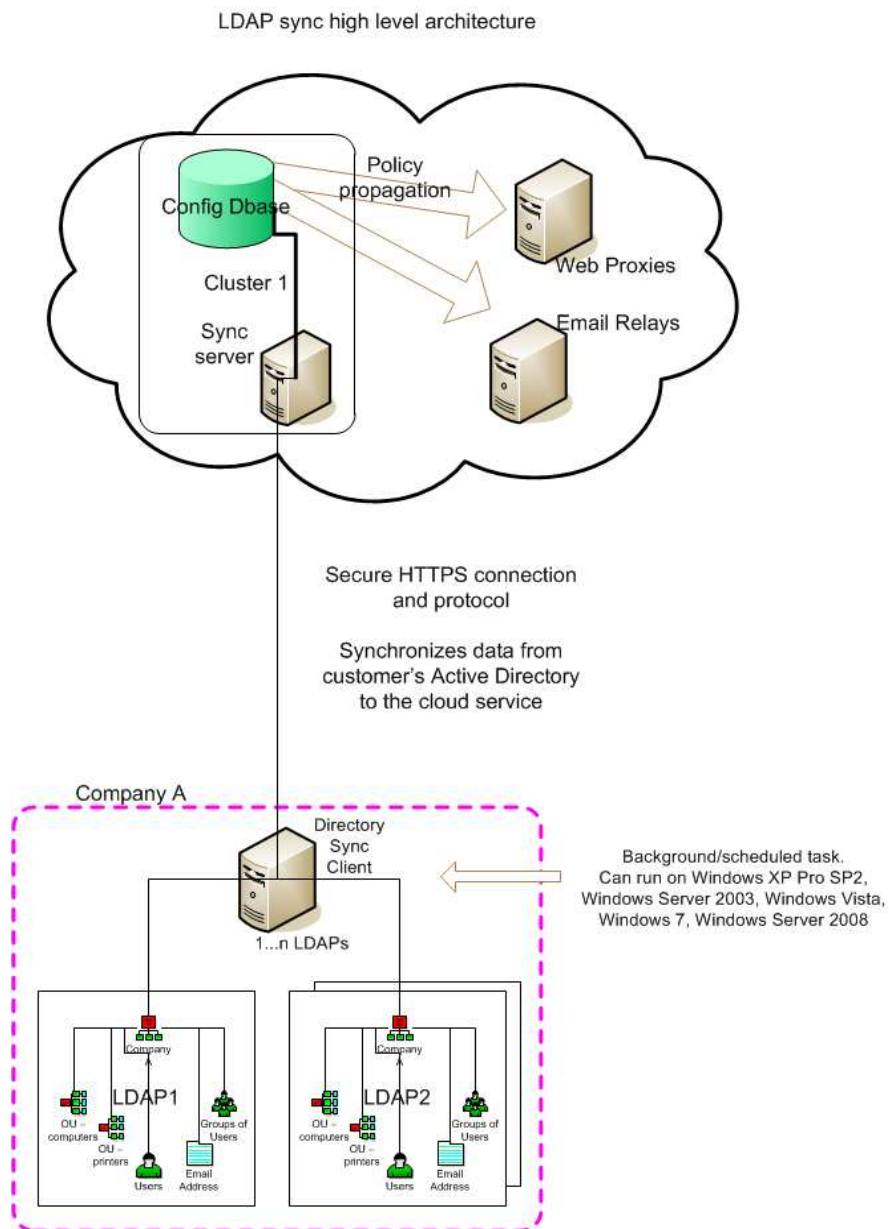
Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

For each data synchronization:

1. The Directory Synchronization Client communicates with the LDAP server and returns the selected data (users, groups, and email addresses).
2. The Directory Synchronization Client performs a synchronization and returns incremental changes to the portal via Secure Hypertext Transfer Protocol (HTTPS). You can force a full synchronization when necessary.
3. The uploaded data is stored in the cloud service along with users and group data managed through Cloud TRITON Managerthe administrator portal.

4. If both user and group data is required, the update occurs in 2 transactions. If one fails, the other can still succeed. Email addresses are a third transaction.
5. The client authenticates with the portal using a username and password that you establish manually on the **Contacts** page. (Consider an appropriate password expiration policy for that user so you don't have to regularly update the client application with the password changes.)
6. LDAP synchronized data is viewable but not editable through the portal.

The synchronization client resides on a computer at the customer's site and accesses one or more LDAP directories via the customer's network. If more than one LDAP directory is accessed, then this data can be merged together by the synchronization client before it is synchronized with the cloud service.



## Planning for your first synchronization

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

When you are setting up directory synchronization, it is important that you review the data you are about to synchronize before you synchronize it. The way that you structure data in your LDAP-compliant directory affects how you should structure groups and users in the portal for policies and exceptions. You should devise a synchronization strategy before you start.

To start, what data do you want to get out of your LDAP directory and what do you plan to do with it?

Second, how is that data organized?

Third, how do you need to structure users and groups in the portal to accommodate your security requirements?

In a typical directory, users are members of many groups. For example, users may be members of global groups like “All Sales;” they may be members of geographical groups like “London” or “New York;” and they may be members of a department such as “NY Telesales” and many others. When deciding on which groups to synchronize, select only groups that are going to be useful to the cloud service, typically for setting policy or group-based exceptions. See [Deciding what to synchronize, page 29](#) for more guidelines on this decision.

If you already have users and groups in the portal, then you’ll need to determine how and whether to adjust that structure to match the LDAP directory (or vice versa).

Following are the most common use cases. Follow the links to review considerations and checklists designed just for you.

- ◆ New web and/or email customers:
  - [Synchronizing users/groups with a single Web policy and exceptions](#)
  - [Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory](#)
- ◆ New and existing email customers:
  - [Synchronizing email addresses to provide a “white list” of valid email addresses](#)
  - [Synchronizing users/groups to provide per-user/per-group exceptions to email policies](#)
- ◆ Existing web and/or email customers:
  - [Wanting to manage users/groups from an LDAP directory](#)
  - [Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal](#)

## Deciding what to synchronize

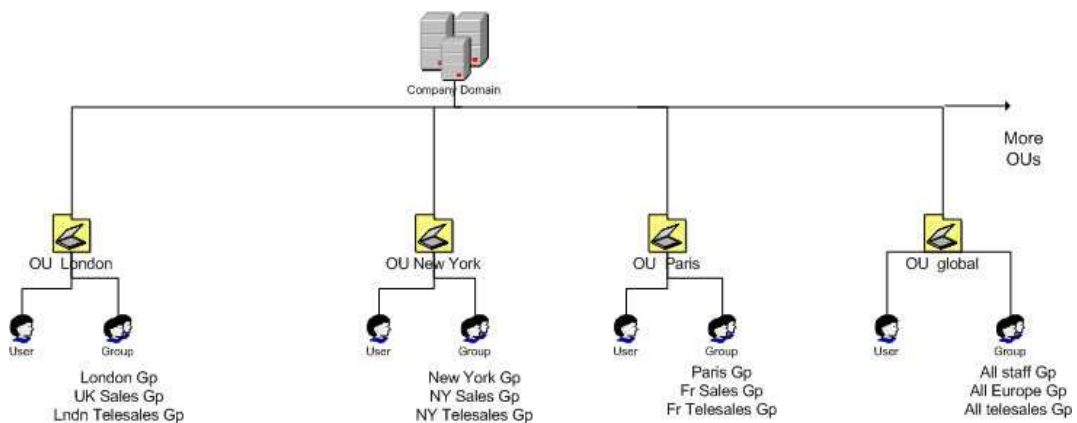
Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [What is LDAP?](#)
- ◆ [How the service works with LDAP](#)
- ◆ [Basic steps](#)
- ◆ [Cloud-based tasks](#)
- ◆ [Client tasks](#)
- ◆ [Set up authentication](#)

You do not need to synchronize all of the groups and users in your LDAP-compliant directory. Instead, synchronize only groups that are useful to the cloud service.

Consider this Active Directory (AD) example:



If you are going to set up a policy for members of a New York Telesales department that gives them special permission to access certain websites, you should synchronize the “NY Telesales” group. There is no need to sync the “London” group if you are not going to set up geographical policies in the cloud service, even if the London users are going to be using the service.

Sometimes when users are synchronized to the cloud service, they are members of multiple AD groups, but only a subset of those groups is synchronized. This is not a problem: the cloud service is designed to accept users with group references that are not on the service.

You specify which groups to synchronize using an LDAP search facility on the Directory Synchronization Client. There is great flexibility in selecting the appropriate data to synchronize. For example, you can use the *membership of an LDAP group*

attribute to select the users you want, even though you may not select that group in the group synchronization setup itself.



#### Note

If you add or change a group name in Active Directory or move a group from one organizational unit (OU) to another, be sure to add the new name to the group inclusion list on the Directory Synchronization Client before the next synchronization. Otherwise, the group is deleted from the portal.

Regardless of how many groups you synchronize, user detail must be sent as part of a separate user synchronization. When you synchronize a group, you transfer information about the group but not about its contents. User synchronizations include details of the group(s) to which users belong. When you apply a web policy or an email policy to a synchronized group, that policy is applied to all synchronized users who are members of that group.

Please refer to the [Directory Synchronization Client Administrator's Guide](#) in the Technical Library for more information on using the LDAP search feature to target only those users and groups that are required.

## Basic steps

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Although the steps for your use case may vary, the basic steps for setting up directory synchronization follow:

### In the cloud

1. [Configure directory synchronization, page 31](#), for your account.
2. [Set up authentication, page 34](#), for the client machine. The client should have its own username and password to gain access to the cloud service.

### On the client

1. Download the Directory Synchronization Client (see [Client tasks, page 35](#)) and install it on a network client machine. Download the client administrator's guide as well. This contains valuable information on helping you integrate your directory service with the cloud service.
2. Configure the client. Use the username and password established in the **Contacts** section of the portal to authenticate.
3. Test the Directory Synchronization Client to make sure it is returning the correct data from the LDAP server to the client. If you are an existing customer switching to directory synchronization for the first time, you should compare the data with that which already exists in the cloud.

4. Initiate a synchronization. The service updates its groups and users, including policy assignment where appropriate.

If a synchronization is unsuccessful, you can use the **Restore** feature to restore the directory information to a previous version. (See [Restore directories](#), page 37 for more information.)

5. Schedule automatic synchronization. You can update the cloud service several times a day if required.

Refer to the [Directory Synchronization Client Administrator's Guide](#) for instructions on items 2-5.

---

## Cloud-based tasks

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Maintenance](#)

To set up your account for directory synchronization, perform the following steps in the portal:

1. [Configure directory synchronization](#), page 31, for your account.
2. [Set up authentication](#), page 34, for the client machine.

## Configure directory synchronization

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

1. On the main menu bar, click **Account**.
2. Click **Directory Synchronization**.
3. Click **Edit**.
4. Check the **Enable directory synchronization** box. You cannot connect the Synchronization Client to the cloud without doing so, even if you have a valid username and password.

5. Fill out the rest of this screen as follows:

**General**

---

**Overwrite groups**

If you are a new customer with no group data in the cloud, leave this box unchecked.

If you have existing data and are migrating to LDAP, check this box if you want to overwrite current groups with the synchronized groups when there is a group name conflict.

Users, groups, and email addresses are overwritten by LDAP data of the same name. Once this occurs, they are manageable only by LDAP synchronization.

If you are switching to LDAP for the first time, take care to match your LDAP group names and membership to the existing setup. Doing so allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.

If you have duplicate names, you have 2 options: make sure the duplicate can be overwritten or don't allow overwriting and rename the duplicates to avoid a conflict.

If you don't select this option and duplicate names are found, the transaction is rejected. In the cloud, you receive the error "403: Attempt to overwrite portal-managed group 'nnnn'." On the client, you receive "Error communicating with the Hosted Service portal. Update abandoned."

---



**Web**

Assign users to policy	<p>Because you are synchronizing user and group data, you can manage policy membership through group membership.</p> <p>Select the web policy to which you want to assign users if they have no group-based policy assignment already. By default, the first policy in the list is chosen.</p>
User policy assignment	<p>Specify whether you want the user policy assignment to be fixed after the first synchronization, or if you want the service to check the group policy membership every time users are synchronized or group policy assignments are changed in the cloud.</p> <p>Select “Follow group membership” if you want users’ policy assignments to change automatically when there are changes to their group membership. If you move someone to another group, he or she moves to a different policy. This is the default.</p> <p>Select “Fixed” if you want to manage policy assignments in the cloud. When you select “Fixed,” the service makes a policy assessment for an individual user only when that user first appears in the system (in other words, is synchronized for the first time). It either assigns the user a group-based policy or the default policy specified above. If you want to move someone to a new policy, you need to do so in the cloud.</p>
Email new users	<p>Select one of the radio buttons to indicate whether you want email sent to new end users to notify them that they are now protected by the cloud service. You can send email to all new users, only those who do not have an NTLM identity, or no one.</p> <p>Be aware that sending to end users could flood your email servers with messages and slow down performance. You’re asked to confirm this decision. We recommend you do this at a quiet time.</p>
Email notification	<p>Choose which email you want to use to notify end users of their enrollment in the cloud service. Initially, only the default message is offered, but you can create custom notifications if desired. See <a href="#">Block and notification pages</a> for more information.</p> <p>For sender’s address, enter the address from which you want notification messages sent to new users.</p>

**Email**

(Quarantine/discard/bounce.)  
mail for unknown users

This determines what happens to email arriving at the cloud service that is sent to an unknown email address. By default it is quarantined.

Check this box if you want the message handled in this way. Leave it unchecked if you do not.

Only Websense Customer Services can modify the disposition of this option.

Occasionally customers cannot enable or disable this option. This happens when addresses have not been synchronized, a similar access control has been manually added to your policy, or Customer Services has explicitly turned it off.

6. Click **Save** when done.

**Note**

You can turn off directory synchronization any time and revert to managing all users, groups, and email addresses in the cloud. If you plan to do this, please see [Turn off directory synchronization](#), page 39 for possible considerations.

## Set up authentication

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

On the **Contacts** page, set up authentication for the client machine. We strongly recommend that the client have its own username and password to gain access to the cloud service. This keeps the synchronization process separate from your other administration tasks and enables you to establish longer password expiration policies.

Once you establish a contact for the client machine, you configure the client to pass these logon credentials when connecting to the service.

1. On the main menu bar, click **Account**.
2. Click **Contacts**.
3. In the Contacts section, click **Add**.
4. Enter identifying information for the client machine in the **First name** and **Surname** fields. For example, "Directory Sync" and "Client."
5. Click **Submit**.
6. In the User Name field, click [here](#) to add a user name.
7. Enter a password for the client machine. It must conform to the password policy on the main Contacts page.
8. Enter a password expiration date for the client. To avoid having to regularly update it, this should be different than the regular account settings; it should span a longer period.

9. Under **Account Permissions**, check the **Directory Synchronization** box, and any other permissions you want to give this “user”. You can act as an administrator from this logon.
10. Click **Submit**.

## Client tasks

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The Directory Synchronization Client is designed to run on a machine with at least 2GB of RAM, and requires approximately 10MB of disk storage. The following operating systems are supported:

- ◆ Windows XP Professional Service Pack 2
- ◆ Windows Server 2003
- ◆ Windows Vista
- ◆ Windows 7
- ◆ Windows Server 2008

To download the client:

1. From the client machine, log on to the portal.
2. Select **Account > Directory Synchronization**.
3. Under Download Directory Sync Client, download the directory synchronization client.  
Select a client tool to download it. If you already have a Java Runtime Environment (JRE), download the tool without a JRE. Otherwise, download the one that includes a JRE. A JRE is required to run the client software.
4. When the download is complete, run the executable file.
5. Navigate through the installation wizard as prompted, accepting the license agreement and indicating where to install the application. Review the installation instructions in the client administrator’s guide for assistance.
6. Configure the client as described in the client administrator’s guide. Provide the logon credentials that you established as part of the configuration.

## Maintenance

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

After directory synchronization is set up and running properly, you can perform the following tasks in the portal:

1. [View and manage user data](#). Note you cannot edit data that has been synchronized from your directory.

2. [View and print reports](#)
3. [View recent synchronizations](#)
4. [Restore directories](#) to previous version
5. [Troubleshoot synchronization failures](#)
6. [Turn off directory synchronization](#)

## View and manage user data

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

You can view account- or policy-level data about end users at any time. The portal provides a clear indication of which records are maintained in the service and which have been synchronized from your directory.

1. To view account-level data on users, select **Account > End Users**.
2. Check the boxes on the left to indicate which search criteria to use.
3. Narrow down the search by entering or selecting precise data in the middle column.
4. Check the boxes on the right to indicate what information to include in the results.
5. Choose how many results to show per page and click **Search**.
6. From the resulting data, you can make individual edits or bulk edits. For example, you can:
  - a. Undo the manual override
  - b. Delete user(s)

All changes made on this screen override any group/policy assignments (existing or future ones). To return to the automatic settings, manually undo your changes here.

You can view and manage user data at the policy level as well as using the End Users screen for the policy.

## View and print reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

You can view and print reports that show the history of synchronizations, including high-level statistics on success/failure and numbers of items synchronized.

The following reports are available:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

Click **Account > Reports > Services** to access them. See [Service reports](#), page 150, for more information.

## View recent synchronizations

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

### 1. Select **Account > Directory Synchronization**.

The Recent Synchronizations section shows your recent synchronization history.

Column Heading	Description
Date	The date and time that the synchronization was performed in coordinated universal time (UTC). Format YYYY- MM DD HH: MM SS.
Status	An indication of whether the synchronization completed or failed. Possible HTTP response codes include: <ul style="list-style-type: none"> <li>• 200 OK - Completed successfully.</li> <li>• &gt;400 - Synchronization failed <ul style="list-style-type: none"> <li>• 403 Error text - The client synchronization failed for reasons given in the error text. For example: <ul style="list-style-type: none"> <li>• 403 Groups contain circular references</li> <li>• 403 Transaction failed</li> <li>• 403 Attempt to overwrite cloud-managed group.</li> <li>• 403 Email address exists in another account</li> </ul> </li> <li>• 503 Service Unavailable.</li> </ul> </li> </ul>
Type	The type of record that was synchronized: Users, Groups, Addresses, or Test. Test indicates that the client connected to the cloud service to verify its settings, but did not synchronize.
Additions	The number of new records added during the synchronization. If the synchronization is not yet complete, "In progress" is displayed.
Deletions	The number of records deleted during the synchronization.

### 2. Click the timestamp in the date column to view details about a specific synchronization.

In the resulting screen, you can see the time that the connection started and ended in the local time zone of the client machine. (This lets you see how long the synchronization took). You can view the IP address of the source connection, the username of the client initiating the synchronization, and the number of records amended, added, or deleted. You can also see reporting and logging information.

## Restore directories

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

If necessary, you can undo the last directory synchronization and restore the system to its state before the synchronization.



### Important

It is not possible to undo the restore, so changes you made in the cloud between the last synchronization and the restore operation may be lost. You are warned of the potential impact and asked to confirm the action.

1. Select **Account > Directory Synchronization**.
2. Click **Restore**.
3. Click **Restore** to restore your directory to the current backup version or click **Cancel** to cancel.
4. Confirm your action when prompted, “Are you sure?”

## Troubleshoot synchronization failures

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Should a synchronization fail to complete, a record is saved by the cloud service along with your details, date/time stamps, and an error message. You can access this information by selecting **Account > Directory Synchronization**. See [View recent synchronizations](#), page 37, for more information. You can also view it in the Synchronization History log, available under **Account > Reports > Services**.

In the status column, any response code greater than 400 indicates a failed synchronization.

HTTP Response Code	Explanation	Recommended Action
403 Groups contain circular references	An attempt has been made to synchronize a hierarchy of groups that contain one or more circular references. For example, GroupA is a member of GroupB, but GroupB is a member of GroupA.	The list of groups forming the cycle are listed in the response code. Check these groups and fix the memberships to break the cycle.
403 Transaction failed	Further explanation is added to the response code to explain the problem. This is usually due to some uniqueness constraint failing--for example, if 2 users have the same email address or LDAP domain name.	Resolve the issue detailed in the full response code.
403 Attempt to overwrite portal managed group.	An attempt has been made to synchronize a group with the same name as a cloud-managed group, and the Overwrite Portal Groups option is off.	On the Configure Directory Synchronization screen, check the Overwrite Groups box to allow overwriting, or rename the duplicate groups to remove the conflict.

HTTP Response Code	Explanation	Recommended Action
403 Email address exists in another account	An email address in the LDAP directory already exists in another account.	Remove this email user from your directory if it is your error. If it is a valid address that you own, contact Customer Services to have the address removed from the other account.
503 Service unavailable.	<ul style="list-style-type: none"> <li>The cloud service is heavily loaded, so a synchronization is not currently possible.</li> <li>Synchronization is not enabled on the account</li> <li>Your account has exceeded its daily synchronization limit</li> </ul>	<ul style="list-style-type: none"> <li>No action. The client automatically re-tries later.</li> <li>Enable synchronization by selecting <b>Account &gt; Directory Synchronization &gt; Edit &gt; Enabled.</b></li> <li>Retry tomorrow (or when next scheduled).</li> </ul>

Partially transmitted and temporarily stored data remains in the cloud service for a few days as a possible debugging aid. This data is not used when you try to synchronize again.

## Turn off directory synchronization

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

You can turn off directory synchronization any time and revert to managing all users, groups, and email addresses in the portal. To do so:

1. Cancel any scheduled synchronizations on the client machine. For more information, see the section “Removing the synchronization schedule” in the [Directory Synchronization Client Administrator’s Guide](#).
2. Log on to the portal.
3. Choose **Account > Directory Synchronization > Edit**.
4. Clear the **Enable directory synchronization** check box.
5. Click **Save**



### Important

Ensure that a synchronization is not under way when you disable directory synchronization. If a synchronization is running, you may end up with an incomplete set of data: for example, your groups might have synchronized successfully, but your users might not.

When you turn off directory synchronization, Group and user IDs on previously synchronized items are retained, so you can easily re-enable synchronization at a later date.

Please note that changes made manually in the cloud to data items that were previously synchronized are lost if you later re-synchronize. When you re-enable synchronization, you are indicating that it is now the LDAP directory that holds the master data, and a full re-synchronization is performed.





# 4

## Configuring Email Settings

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [File sandboxing](#)
- ◆ [Aliases](#)
- ◆ [Service IP addresses](#)
- ◆ [Black and white lists](#)
- ◆ [End-user message reports](#)
- ◆ [Email notifications](#)
- ◆ [Phishing block pages](#)
- ◆ [Image white list](#)
- ◆ [Defining Email Policies](#)

Use the **Email > Settings** options to configure account-level settings for TRITON AP-EMAIL, including aliases, black and white lists, and end-user message reports for your account.

### File sandboxing

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [What does a file sandboxing transaction look like?](#)
- ◆ [URL Sandboxing tab](#)
- ◆ [URL Sandboxing Utility](#)



#### Note

You must have the Email Sandbox module to use this feature.

---

Use the **Email > Settings > File Sandboxing** page to send suspicious files received in email messages to a cloud-hosted sandbox for analysis. The sandbox activates the file, observes the behavior, and compiles a report. If the file is malicious, the message is either quarantined, or an email alert is sent to the administrator(s) that you specify, containing summary information and a link to the report.

A file that qualifies for sandboxing:

- Is **not** classified as “malicious” by virus scanning or the ThreatSeeker<sup>®</sup> Intelligence Cloud
- Fits the Websense Security Labs profile for suspicious files
- Is a supported file type for sandboxing.



#### Note

Because the file was **not** detected as malicious, it was **not blocked** and has been delivered to the email recipient.

---

1. File analysis is disabled by default. Select **On** to send qualified files to the cloud-hosted sandbox for analysis.
2. Select the analysis mode you wish to use:
  - **Monitor only** performs the file analysis; however, because the file was not originally detected as malicious, it is not blocked and is delivered to the email recipient regardless of the analysis results.
  - **Enforce** holds any messages with attachments sent for analysis, and then quarantines those messages found to contain malicious attachments.
3. Specify the email address of at least one person in your organization who will receive notifications.

Notifications are sent only for monitor mode. If you have selected the Enforce mode, you may still want to enter an email address in case a message pending analysis is released from quarantine with no further processing before analysis is complete. In this case, a notification will be sent if the attachment is found to be malicious.

The specified person does not have to be a TRITON AP-EMAIL administrator. If you specify multiple email addresses, ensure you enter one address per line.

4. Select the file types you want to submit for analysis from the **File types to scan** list.
5. Click **Save**.

## What does a file sandboxing transaction look like?

1. The cloud service receives an email message for an end user that explicitly or implicitly includes a file.

2. The message is not classified as malicious, and virus scanning or the ThreatSeeker® Intelligence Cloud does **not** find the attachment(s) to be malicious. However, the attached file matches the configured file types to be sent to the sandbox in the cloud for analysis.
3. If monitor mode is selected, the message with the attached file is delivered to the email recipient. If enforcement is selected, the message is held, pending analysis.
4. The sandbox analyzes the file, which may take as long as 5 to 10 minutes, but is typically much quicker.
5. If the file is found to be malicious, the cloud service sends a malicious file detection message to the configured alert recipient(s). The alert email includes a link to the report.  
If enforcement mode is in use, the message is quarantined.
6. Upon receipt of the message, administrators should:
  - a. Access and evaluate the report for the file
  - b. Assess the impact of the intrusion in their network
  - c. Plan and begin remediation
7. Separately, the file sandbox updates the ThreatSeeker Intelligence Cloud with information about the file and the source email message.
8. ThreatSeeker updates its rules and other security components, which are then pulled by Websense deployments.
9. The next time someone receives an email message containing this file, they and the organization are protected by their TRITON AP-EMAIL deployment.

## Service IP addresses

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

TRITON AP-EMAIL uses customer-specific DNS records to route email from the service to your email gateway, and from your email gateway back to the service. You can view your customer-specific DNS records by selecting **Email > Settings > Service IP addresses**. The records are listed under MX Record DNS entries.

Because TRITON AP-EMAIL is a managed service, we are responsible for managing system capacity. For this reason, we may occasionally choose to alter the route of your email within our service. To enable us to do this seamlessly without requiring you to make further changes, you must allow SMTP connections from all the IP ranges listed under Service IP Addresses on this page. To access the Cloud TRITON Managerportal, ensure that ports 80 and 443 are also permitted for these IP ranges.

## Aliases

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Adding or modifying an alias](#)
- ◆ [Downloading and uploading aliases](#)

TRITON AP-EMAIL can rewrite email addresses as email enters and leaves your system. Aliases must be to and from domains associated with your TRITON AP-EMAIL policies. Aliases let you rewrite email addresses both inbound from the Internet and outbound to the Internet. When an alias has been applied, email passes through the policy for the new address. Addresses in the SMTP envelope and in those header fields defined in the standard Internet message format (as defined in RFC 2822) are rewritten.

- ◆ An alias can apply both inbound and outbound. In this case, there is a one-to-one mapping of an internal address to an external address and vice-versa. This is often called masquerading an address.
- ◆ An outbound-only alias is also a one-to-one mapping.
- ◆ An inbound-only alias can be a one-to-one or a one-to-many mapping (a distribution list). To specify a distribution list, separate email addresses with commas.
- ◆ If an alias is neither inbound nor outbound, it is a disabled record.

To view the aliases that have been configured for your system, select **Email > Settings > Aliases**.

To search for all aliases in the system, enter an asterisk in the **Email address** field, check both the **Inbound** and **Outbound** check boxes, then click **Search**.

To narrow the list to specific entries, enter search criteria in the **Email address** field, such as “\*john\*”. Wildcards are supported.

## Adding or modifying an alias

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Aliases](#)
- ◆ [Downloading and uploading aliases](#)

1. Select **Email > Settings > Aliases > Add Alias**.

2. Enter the internal and external addresses for which you want to create an alias.
3. Specify whether the alias applies inbound or outbound mail, or both.
4. Click **Submit** to save your changes.

## Downloading and uploading aliases

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Aliases](#)
- ◆ [Adding or modifying an alias](#)

You can download the complete alias list as a comma-separated values (CSV) file. You can then edit this using a simple text editor or a spreadsheet application such as Microsoft Excel. If you are intending to upload aliases, be very careful not to change the format of the file. The first line of the file is a header line - it must always be exactly:

I nbound, O ut bound, E xt er nal , I nt er nal

Subsequent lines follow this format:

yes, no, addr 1@xt er nal . domai n. com addr 2@nt er nal . domai n. com

All values must be separated by commas and enclosed in double-quotes if they contain commas.

During the alias upload, TRITON AP-EMAIL performs a complete syntax check before it imports the aliases to the system configuration. If it finds any errors, it reports them and abandons the file import.

## Black and white lists

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Adding an entry to a white or black list](#)

1. Select **Email > Settings > Black & White Lists** to see which email addresses have been black- or whitelisted for your account.

2. Enter search criteria into the fields provided, then click **Search**.

Field	Description
<b>Address Pattern</b>	Enter a specific address for which to search, or use wildcards to expand your search. Enter an asterisk (*) to search for all addresses that have been black- or whitelisted.
<b>Action</b>	Select the type of search you want to perform. You can search for <b>Accept</b> actions (whitelist), <b>Reject</b> actions (blacklist), or both.
<b>Minimum policies contained in</b>	Indicate a policy threshold for your search. You can specify an interest in addresses that are black or whitelisted in at least <i>nn</i> policies.

The resulting screen shows black- or whitelisted addresses that appear in the specified number of policies for your account.

To manage black and white lists for your policies or end users, go to the Antispam tab for the policy. See [Adding an entry to a white or black list](#), [page 85](#) for more information.

## End-user message reports

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Subscriptions tab](#)
- ◆ [Settings tab](#)
- ◆ [Text and Language tab](#)
- ◆ [Bulk Upload tab](#)
- ◆ [Requesting a message report](#)
- ◆ [Understanding the report](#)

To configure the content of email message reports sent to end users, select **Email > Messages > End User Message Reports**. The end-user message report (EUMR) gives end users a summary of the messages that they have received and sent.

You can choose to subscribe your end users to the EUMR via the Cloud TRITON Managerportal. In this case, users receive a single report in the format that you configure, and the report contains a link that a user must click to receive the report on a weekly basis. Otherwise, to receive an EUMR, users must request it via a website. They can also subscribe to the report for automatic delivery. For information on the contents of the report and the request process, see [End-User Self Service](#), [page 155](#).

On the **End User Message Report** page, there are 4 tabs:

- ◆ Subscriptions
- ◆ Settings
- ◆ Text and Language
- ◆ Bulk Upload

## Subscriptions tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [End-user message reports](#)
- ◆ [Settings tab](#)
- ◆ [Bulk Upload tab](#)
- ◆ [Text and Language tab](#)

In the Subscriptions tab, you can see a list of the recipients of an end-user message report (EUMR) subscription, the email address(es) or account(s) covered in the EUMR, and a description of the subscription if provided. Optionally, you can filter elements in the list.

To create a new subscription for an end user to receive the EUMR:

1. Click **Add**.
2. Under Subscription, enter an email address for the **Recipient** of the EUMR, and optionally, enter a **Description**.
3. Under Manage Accounts, enter any other email aliases or accounts that you wish to consolidate into this EUMR.

Enter one email address at a time, clicking **Add Address** after each. If you choose to consolidate multiple email addresses into one report, the recipient gets a report containing details of all sent and received mail for all associated email addresses.

Note that any whitelist or blacklist entries associated with the email addresses are not merged – i.e. if a sender has previously been whitelisted for one address, it is not automatically whitelisted for other addresses in the same report subscription. However, if the report recipient later chooses to whitelist or blacklist an address by clicking the **Whitelist** or **Blacklist** buttons in the EUMR, it will apply to all email accounts or aliases associated with the report.

4. Under Report Options, define the following options:
  - Select the **Email types to include** in the report.

- Choose how information about quarantined and non-quarantined messages should be sorted: by status, date/time, subject, from, or to. You can then define ascending or descending order. Note that clean messages will always be shown by date and time.

**Note**

Subscriptions to the TRITON AP-EMAIL message report lapse after 93 days. 62 days after subscribing, each time users receive a report, they are reminded that they should renew their subscription. To see the expiration date for a subscription, go to **Reporting > Account Reports > Services**. In the **Show** drop-down list, choose **End User Message Report - Subscriptions**. Click **Generate Report**. The report includes the expiration date as well as recipient and subscriber addresses.

- Select the language and time zone you want reflected in the report.
5. Click **Submit**. This becomes the default configuration for all future message reports. You can change this configuration at any time.

To edit existing subscriptions, click on the pencil icon next to the recipient's name. The Edit Subscription box appears in which you can perform the same steps outlined above.

## Settings tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

**Related topics:**

- ◆ [End-user message reports](#)
- ◆ [Subscriptions tab](#)
- ◆ [Bulk Upload tab](#)
- ◆ [Text and Language tab](#)

The Settings tab shows the default settings for your end-user message reports, which are used when an end user first subscribes and if new subscriptions are created via LDAP synchronization. In Settings, you can perform actions, such as allowing end users to modify report content, and several other features described below. Report content that you create when adding a new subscription overrides the general settings.

Below is a summary of what you can do. Click **Apply** after you've made your selections.

### Fallback language

For Fallback language, specify the language to use when the end user's browser uses a language for which there are no translations available.

There are 14 languages available for the end-user message report:



- ◆ Czech
- ◆ Dutch
- ◆ English (U.K.)
- ◆ English (U.S.)
- ◆ French
- ◆ German
- ◆ Greek
- ◆ Italian
- ◆ Polish
- ◆ Portuguese
- ◆ Portuguese (Brazilian)
- ◆ Romanian
- ◆ Slovak
- ◆ Spanish
- ◆ Swedish

### **Fallback timezone**

Use the Fallback timezone drop-down to specify the default timezone used in the report.

### **Report frequency**

Select how often the message report should be delivered.

If you select **daily** or **weekdays**, you can also configure multiple reports to be sent each day by choosing the hours when the report should be generated. Note that the maximum frequency is every 3 hours, so if you click 6, for example, 7 and 8 are disabled and the next hour you can select is 9.

### **Report content**

Use the check boxes to indicate which of the 6 possible sections to include in the message report:

- ◆ suspicious messages that have been quarantined (received and sent)
- ◆ suspicious messages that have not been quarantined (received and sent)—for example discarded or bounced messages, or a message that has had its subject line tagged because it matched a lexical rule
- ◆ clean messages (received and sent)

In the **Sort by** area, indicate the order in which you want suspicious and clean messages to be sorted:

- ◆ Date/Time
- ◆ Subject
- ◆ Originator

- ◆ Recipient
- ◆ Status

Also indicate whether you want the quarantined or non-quarantined messages to be sorted in ascending or descending order.

### **Allow end users to modify report content**

Check this box if you want to allow end users to customize the content to include in their message reports and the order of that content. When this is checked, end users are given access to a customization page on their report. Any changes they make override your settings here.

### **Allow delivery of empty reports**

Check this box if you want to send reports to end users even when there is no content to include in the report. If you do not check the box, the report is not sent if there is nothing to go into it.

### **List previously released messages**

This box is checked by default. Check the box if you want to include in the report all messages that have already been released from quarantine, either by an administrator or the end user. Clear the box to remove all previously-released messages from the report.

### **Subscribe users from future user directory synchronizations**



#### **Note**

This option may not be available in your account. To enable the option, contact Support.

---

If you are synchronizing your end users with the cloud service using the Directory Synchronization Client, you can check the **Subscribe users from future user directory synchronizations** box to subscribe new end users to the end-user message report rather than asking them to subscribe themselves. After you have checked this box, whenever there is an update of users in the directory and the update is synchronized to TRITON AP-EMAIL, the new users are automatically subscribed to the report.

Optionally, you can click **Subscribe current users** to subscribe all of your synchronized end users currently in the cloud.

The subscribed end users get a report in the format defined on this page. The report includes a link that, when clicked, subscribes the end user to the report on a weekly basis.

## Text and Language tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [End-user message reports](#)
- ◆ [Subscriptions tab](#)
- ◆ [Settings tab](#)
- ◆ [Bulk Upload tab](#)

When a report is requested or scheduled for delivery, TRITON AP-EMAIL sends an email message that includes the end user message report. To edit the text that appears in the email message, select **Email > Messages > End-User Message Reports**, then go to the **Text and Language** tab.

Click **Add** to select a language that you wish to customize the text in. Then follow the steps described below.

On the resulting screen:

1. From the **Language** drop-down menu, select the language you wish to use.
2. To specify customized email subject lines:
  - Clear the **Use the default value** boxes.
  - Supply a subject line for normal circumstances, one that you would like to appear when a user's report subscription is about to expire, and one to appear after it has expired.
3. Click **Submit**.
 

If you do not have any report content selected, an error results. Return to the End User Message Reports page, click **Edit**, check some boxes under **Report content** and try again. If the submission is accepted, **Edit Source** buttons appear.
4. Click **Edit Source** to customize the message text that appears at the top or bottom of the message. This allows you to edit the HTML source code for the message.
5. Type in the text editor's entry field.
 

You can also include predefined keywords in the text (for example, `_TOTAL_RECEIVED_`). When the report is generated, keywords are substituted with data, such as the total number of messages received.

To view the keywords that are available for substitution, click **View available keyword substitutions**. Click a keyword to paste it into the cursor position in the active field.
6. Click **Submit**.
7. To view how the message looks to users, click **View Report**.

To put your customizations into effect, click **Enable this customization**, then click **Submit**. If you do not click **Enable this customization**, the text set for the default

account is used. Click **Edit** to go back and edit the check boxes for email subject and **Enable this customization**.

Choose another language to edit if desired and customize the message for that language in the same way. Be sure to enable it before you submit it if you want it to take effect.

New languages that you add appear on the Text and Language tab page with a check if enabled. You can click on the link to the language, such as “en-us - English (US)” to edit the email message text for that language.

## Bulk Upload tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [End-user message reports](#)
- ◆ [Subscriptions tab](#)
- ◆ [Settings tab](#)
- ◆ [Text and Language tab](#)

To upload multiple email aliases in CSV format, do the following:

1. Go to **Email > Messages > End User Message Reports**.
2. Open the **Bulk Upload tab**.
3. Browse to the CSV file that you wish to upload.
4. Click **Upload**.

Note that the uploaded CSV file updates existing subscriptions, adds any new subscriptions, and deletes existing subscriptions that are not in the CSV file. You can also download and edit current subscriptions from this page.

If you want to include the time zone for the report subscriptions in the bulk upload, you can download a list of all the supported time zones.

## Email notifications

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Adding notifications](#)
- ◆ [Editing notifications](#)

Notification messages can be sent when email is quarantined for any reason. Use the **Email > Policy Management > Notification Email** screen to view, edit, and delete notification messages.

Click **Add Notification** on the **Notification Email** screen to create a new notification message, or click the name of an existing notification message to edit the message contents and properties (See [Adding notifications](#), page 53, or [Editing notifications](#), page 55, for more information.) On this page, you can also set the time zone to use for dates that are included in notifications and park attachment annotations by clicking on the link next to **Time Zone**.

You can set up separate notification messages for different types of policy breaches and notifications to be sent to the intended recipient of an inbound email, the postmaster, and to other addresses of your choice within policies. You can also notify senders of outbound email but only if the outbound email is being sent from an address within your organization, not from an external address. Note that you cannot notify recipients of outbound messages.

Use the **General** and **Content Filter** policy tabs (navigate to **Policy Management > Policies** and click a policy name) to configure when notification messages are sent and which notification messages are used in each policy. (See [General tab](#), page 60, and [Content Filter tab](#), page 88, for more information.)



#### Note

By default, TRITON AP-EMAIL does not send a notification when email is quarantined as spam. A quarantine-notify disposition is available, but its use is not recommended.

## Adding notifications

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Email notifications](#)
- ◆ [Editing advanced encryption settings](#)

Click **Add Notification** on the **Notification Email** screen to write and configure a custom notification message from scratch, rather than using the default message.

1. Define a name and description for the notification message.
2. Select **Copy configuration from existing notification** to use an existing notification as a template for creating this one. Selecting this option copies the following data from the specified message:
  - Subject line prefix
  - Message body
  - Domain variations

3. Enter a subject line prefix (optional).

Note that if you type `_SENDER_` as part of the subject line prefix, this variable is replaced with the envelope sender address when the notification is generated.

4. If you want to change the character set used in the message (UTF-8 by default), select **Change character set** and select from the drop-down menu.
5. Enter the text for the notification in the message body field.

To view and use supported variables and tokens in notification messages, click **Variables/tokens** in the top toolbar.

Variables/tokens	Description
<code>_msgurl_</code>	Generates a partial URL that gives access to the message held in quarantine. Embed it using the syntax ....
<code>_NOTIFIED_RECIPIENTS_</code>	Generates a string if the intended recipients have been notified.
<code>_RECIPIENTS_</code>	The intended recipients of the message.
<code>_DATE_</code>	Displays the date TRITON AP-EMAIL received the email that generated the notification. The date is based on the time zone set on the Notification Email screen.
<code>_DISPOSITION_</code>	What happened to the message causing the notification. This usually takes the value "quarantined."
<code>_NOTIFIED_ADMIN_</code>	Generates a string if the specified postmaster has been notified.
<code>_MESSAGEID_</code>	The ID as specified in the message headers.
<code>_ENDIF_</code>	End of a <code>_IF_QUARANTINE_</code> or <code>_IF_ENCRYPT_</code> block
<code>_IF_ENCRYPT_</code>	Place this at the beginning of a section that is relevant only if the message has been encrypted. The section must end with <code>_ENDIF_</code> .
<code>_NOTIFIED_SENDER_</code>	Generates a string if the originator has been notified.
<code>_ADMIN_MAIL_</code>	The postmaster address for the policy.
<code>_DOMAIN_</code>	The domain associated with the currently active policy.
<code>_IF_QUARANTINE_</code>	Place this at the beginning of a section that is relevant only if the message has been quarantined. The section must end with <code>_ENDIF_</code> .
<code>_SENDER_</code>	The message originator.
<code>_SUBJECT_</code>	The subject of the message.

6. If you want to edit a separate plain text version of the notification message, select **Edit a separate plain text version**.

7. If you want to send a separate version of this message to specific domains when this notification is enabled, select **Send variations of this message for specific domains**. The **Add Domain Variation** screen appears.
  - a. Select or enter the intended domain in the **Domain** field.
  - b. Specify a **Subject line prefix** (optional).
  - c. Enter the text for the notification in the message body field.
  - d. Click **Save**.
  - e. If you want to add additional variations for other domains, you can repeat this process by selecting **Add variation** (the button will be disabled when all domains have a variation assigned to them).
8. Click **Save Changes** when done.

## Editing notifications

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Email notifications](#)
- ◆ [Adding notifications](#)

Click the name of a notification message on the **Notification Email** page to edit the contents of the notification, the character set used, and variations of the message for specific domains.

See [Adding notifications](#), page 53, for information on the configuration options.

## Phishing block pages

Cloud TRITON Manager Help | Cloud Email Protection Solutions



### Note

You must have the Email Sandbox module to use this feature.

Click **Email > Policy Management > Phishing Block Pages** to view or edit block page text that is displayed when your end users click a link in a suspected phishing email.

A default Phishing Attack Blocked page is included with TRITON AP-EMAIL. This page provides information about phishing emails, including a definition of phishing, some common tactics, and an example of a phishing email message. You can either modify this to suit your needs, or add your own page. The page is then used if a user clicks a link in an email that is classified as part of a phishing attack.

The pages are grouped for ease of navigation. Click a down arrow next to a group name to see a list of all the pages within that group. To see all available pages, click **All**.



#### Note

Pages that you create are listed under Custom. To delete a custom page, click the delete icon next to the page name. The delete icon is displayed only if the custom page is not used in any policies.

---

Click the name of a page to edit its contents.

To create a new notification page:

1. Click **New Page**.
2. Enter a **Name** for the new page.
3. Enter a short **Description** of the page. This appears under the page name in the Block & Notification Pages list, and should clearly identify the purpose of the page to any administrator.
4. Click **Save**.

The Page Details page is displayed, with the name and description at the top. You can now edit the page as required.

For information about editing the content of a new or existing block page, see [Editing phishing block pages, page 56](#).

If you are also a customer, you can configure default options for your block and notification pages. See [Default notification page settings, page 161](#).

## Editing phishing block pages

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Each phishing block page is a complete HTML page (unlike email notifications, which are HTML fragments to appear within an email message). The Page Details page presents a simple view of the page with editable sections, enabling you to customize the text and images.

To change the content of a notification page:

1. For custom pages, click **Edit** to update the page **Name** or **Description**. Click **Save** when done.
2. To change the page name that appears in the browser's title bar, edit the **Page title** field.
3. Hover your mouse over the page content to highlight the sections that are editable. To edit a line of text or block of content, click its section to open a text editor window.
4. Edit the text as required.



You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting. Hover over each text formatting button to see its function.

Click **OK** when done.

5. To edit the page footer:
  - a. Click the footer section to open a text editor window.
  - b. Enter the footer text to use for this notification page. You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting.
  - c. Click **OK** when done.
6. To edit an image on the page:
  - a. Click on the image. The Image Properties popup window is displayed.
  - b. To use one of the standard images provided by TRITON AP-EMAIL select **Standard images** and click on the image you want.
  - c. To use an image of your choosing, select **Custom images** and enter the URL of the image you want.

The image must be a JPEG, GIF, or PNG file. Click **Verify Image** to confirm the format and location of the image file.
  - d. Click **OK**.
7. To view and edit the HTML source, click **HTML Editing**. Any valid HTML may be used within a notification page.

**Note**

If you edit a page in the HTML view and then click **Basic Editing** to return to the basic editor, you will lose any changes made in the HTML view.

---

8. To see how the page appears to end users, click **Preview**. The page appears in a separate window.

**Note**

Your browser may warn you that you are switching to an unsecured connection.

---

9. Click **Save** when done.

If you wish to discard customizations to a standard page, click **Revert to Default**. This removes all changes that have been made to the page in your account, and reverts the page to the original one supplied in TRITON AP-EMAIL.

## Image white list

---

Select **Email > Settings > Image White List** to view and edit the list of images that are not analyzed by TRITON AP-EMAIL.



**Note**

You must have the Image Analysis module to use this feature.

---

Add images to the white list if they are known to be clean – for example, you might want to add acceptable images that have been quarantined to ensure they do not get blocked in future.



**Note**

You can whitelist images directly from the Message Center. See [Managing quarantined images](#), page 130.



---


The image white list can contain a maximum of 200 images. Images are displayed in the order they were added, with the most recent at the top.

To add an image on the Image White List page:

1. Click **Browse**, and navigate to the location of the image file on your network.
2. Select the image, then click **Open**.
3. Click **Upload**.

The image is added to the top of the white list.

4. To edit the image name, click the pencil icon under the image thumbnail and enter the new name. Click  to confirm the name, or  to cancel the edit.

To remove an image from the white list, click the  icon in the top right corner of the image thumbnail.

# 5

## Defining Email Policies

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [General tab](#)
- ◆ [Domains tab](#)
- ◆ [Connections tab](#)
- ◆ [Antivirus tab](#)
- ◆ [URL Sandboxing tab](#)
- ◆ [Antispam tab](#)
- ◆ [Content Filter tab](#)
- ◆ [Encryption tab](#)

To configure an email policy, select **Email > Policy Management > Policies**, then click the name of the policy to configure. If you have not previously configured a policy, click the policy named **DEFAULT**. You can rename the default policy to something more meaningful to your organization, especially if you plan to create multiple policies.

Notice that each policy has multiple tabs to configure:

- ◆ [General tab](#)
- ◆ [Domains tab](#)
- ◆ [Connections tab](#)
- ◆ [Antivirus tab](#)
- ◆ [URL Sandboxing tab](#)
- ◆ [Antispam tab](#)
- ◆ [Content Filter tab](#)
- ◆ [Encryption tab](#)

Click the link to learn how to configure each one of these settings. Standard account-level settings are shown in [Standard Email Configuration](#).

Use the **Policy Management > Notification Email** screen to configure notification messages sent when email is quarantined (see [Email notifications](#), page 52 for more information).

## General tab

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The **General** tab lets you perform general functions on your email account. There are 2 functional areas on this screen:

- ◆ [General policy information](#)
- ◆ [Notifications](#) and [Annotations](#)

To change a policy name or postmaster address for a policy, click **Edit** under the general policy information.

To enable notifications or annotations for inbound mail, click **Edit** in the Inbound box. To enable notifications or annotations for outbound mail, click **Edit** in the Outbound box.

On the resulting screen, use the check boxes to indicate whether you want to notify senders, recipients, or others, and whether you want to annotate messages. You can only notify senders of outbound email if the outbound email is being sent from an address within your organization, not from an external address. Note that you cannot notify recipients of outbound messages.

## General policy information

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To change a policy name or postmaster address for a policy, click **Edit** in the top section of the **General** tab.

Complete the fields as follows:

Field	Description
<b>Policy Name</b>	Enter a name for the policy.
<b>Postmaster</b>	Enter an email address for the postmaster. The postmaster address is used as the address from which system notifications are sent. Your users may occasionally reply to these notifications, so this should be an email address that is monitored by your IT staff or administrative contact.

Click **Submit** when you're done.

## Notifications

Notification messages can be sent when email is quarantined for any reason. Use the **Policy Management > Notification email** screen to view, edit, and delete notification messages. For more information, see [Email notifications](#), page 52.

In a policy, you can set up different notifications to be sent for inbound and outbound messages.

To define the notifications used in a policy:

1. On the General tab, click **Edit** under either Inbound or Outbound.
2. Specify who receives a notification message when an email is quarantined. You can select the recipient (for inbound messages only), the sender (for outbound messages only), the administrator, or others. If you select Others, enter the email address(es), separated by commas.
3. For each option that you specify in step 2, select a notification message from the drop-down list.
4. Click **Submit**.

## Annotations

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Editing an annotation](#)
- ◆ [Report this email as spam](#)

Annotations are added to messages as they pass through TRITON AP-EMAIL. By default, they are set up for entire policies; however, you can also set up more specific annotations.

Examples of annotations that you might add to inbound messages are, “Click [here](#) to report this message as spam,” and “This message has been analyzed for malware by TRITON AP-EMAIL.”

For inbound email, you can create annotations specific to each domain in your policy. For outbound email, you can create annotations specific to an arbitrary list of sender domains, sender email addresses, or groups.

If you have the Email Encryption module, you can also add specific annotations for decrypted messages. These annotations are created from the **Encryption** tab; see [Editing advanced encryption settings](#), page 118.

## Editing an annotation

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Adding annotations](#)

Because email can be sent as HTML or plain text, TRITON AP-EMAIL maintains two versions of each annotation. To edit an annotation:

1. On the **General** tab of a policy, click one of the **annotation** links (taking care to choose an Inbound or Outbound annotation).



### Note

If you are adding an annotation for a decrypted message on the **Encryption** tab, click **Edit**, then click the **annotation** link.

---

2. On the resulting screen, click the annotation name of interest, or click **.\* [default]** to view the default annotation.
3. Indicate where you want annotations to be placed in each message by selecting **Top** or **Bottom** from the **Position** drop-down list.
4. Choose a default character set from the drop-down list.
5. Click **Edit HTML**. For best results, use the most recent version of Internet Explorer available.
6. Make whatever changes you wish to the annotation. The limit is 64 KB. This allows a maximum of 64 thousand characters depending upon the character set being used.

If you want to embed a message in the annotation, use the substitution tag `_MESSAGE_`. When the `_MESSAGE_` tag is present, TRITON AP-EMAIL ignores the “Top” or “Bottom” setting and wraps the annotation around the message text. You can use this tag to add annotations to the top and bottom of messages at the same time.

7. Click **Submit** to save your changes. The HTML editor checks syntax and prompts you to make corrections if necessary.
8. Click **Edit Plain Text**.
9. Repeat your text changes. Plain text messages also have a 64 KB limit.
10. Click **Submit**.
11. Repeat for each annotation that you want to edit.



### Note

If your HTML annotation contains a block of text, it is recommended that you split up the lines with line breaks. Lines longer than 190 characters can cause unwanted exclamation marks to appear in the annotation.

---

Make sure that annotations are enabled for this policy by checking the annotation box on the policy page.

## Report this email as spam

Cloud TRITON Manager Help | Cloud Email Protection Solutions



### Important

If you choose to edit the default inbound annotation, you lose the **Report this email as spam** feature. See [Report this email as spam, page 63](#) for more information.

We strongly recommend that you apply the default inbound annotation “Click [here](#) to report this email as spam.” For new policies, this annotation is enabled by default. This gives users immediate feedback and helps us tune our spam filter for future releases. Here is the feedback that users receive when they click this link:

#### Report as Spam

Thank you for reporting this spam message.

We are committed to delivering the best possible spam protection and your action helps us achieve this. Please continue to report any messages which you believe to be spam in this way.

Although you will not receive any further update from us about this spam message, the anti-spam system is being automatically updated to treat similar messages with more suspicion in future. This will reduce the likelihood of your receiving them again.

Reporting this message will not automatically block all messages from this sender - if you want to do this you should add the sender to your blacklist. See the user guide or contact your email administrator for further instructions.

To aid in the process of spam tuning, when you use the “Report as spam” annotation, we recommend that you configure TRITON AP-EMAIL to keep a private copy of clean email messages for a short period, separate from the quarantine area (see [Keep messages, page 81](#)). If TRITON AP-EMAIL has the original message available, our operations staff and automated systems can analyze the message.

## Adding annotations

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If desired, you can write an annotation message from scratch rather than editing the default. Just click **Add** on the Inbound or Outbound Annotations screen.

On the resulting screen:

1. Choose the domain or address list to annotate.
2. Choose the position of the screen on which to put the annotation: bottom or top.
3. Choose the default character set to use.
4. Enter text into the text editor as desired.
5. Click **Submit** when done.

Make sure that annotations are enabled for this policy by checking the annotation box on the policy page. A check indicates enabled. An X indicates disabled.

## Domains tab

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

◆ [Adding domains](#)

Select the **Domains** tab on the policy to view or change domains for the policy.

Each TRITON AP-EMAIL policy applies to a set of domains. Before a domain is accepted by TRITON AP-EMAIL and processed according to your policy, it must first be checked to ensure that we can deliver mail for the domain to your mail server and that the domain does in fact belong to your company.

The **Route Status** column displays the result of the inbound route check. The **Ownership Status** column shows the result of each domain's ownership check. Status can be **Unchecked** (awaiting validation or check failed; unavailable for use within policy), or **Checked** (check passed; active within policy). To view more details of the domain and its status, click the domain name link. If your domain has failed one or both of its checks and the domain does belong to you, please contact Support.

When viewing a domain for a policy, click **Show MX records** to check the MX record configuration for the domain.

## Adding domains

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To add domains to any policy (including the default policy), you must first set up a valid inbound connection on the [Connections tab](#), [page 67](#) that will accept messages for the domain you plan to add. A valid inbound connection is one that accepts messages on port 25 for the domain. If it is behind the firewall, the firewall must allow email traffic from the IP address ranges listed on the [Service IP addresses](#), [page 43](#) page. The connection is checked as part of the validation.

To add a domain or sub-domains to the policy:

1. Click **Add** on the **Domains** tab.
2. Enter the domain name in the **Domain** field.
3. To apply the policy to all sub-domains in the current domain, select **Include sub-domains**.
4. Click **Submit**.



At this stage TRITON AP-EMAIL checks for a valid inbound connection for this domain and displays the result on the Add Domain screen. If it cannot find or validate a connection, an error message appears.

**Important**

The inbound connection checking does not guarantee the correct delivery of email messages. It is strongly recommended that you run your own testing on the inbound connection that you have specified.

---

The Add Domain screen also displays the following options for you to verify ownership of the domain you have entered. The ownership check initially displays as **Failed**, because it cannot succeed until you have done one of the following:

- ◆ Create a CNAME record in your DNS that aliases the character string shown on the screen to autodomain.mailcontrol.com. For more information, see [CNAME records and A records, page 65](#).
- ◆ Create an A record for the character string shown on the screen, pointing to the IP address of autodomain.mailcontrol.com. For more information, see [CNAME records and A records, page 65](#).
- ◆ Add your customer-specific DNS records into your MX records in your DNS. For more information about adding and editing MX records, see [MX records, page 66](#).

Once you have made one of the above changes, click **Check Now**.

**Important**

If you choose to use MX record verification, the service will accept email messages for this domain as soon as the MX records are set up.

---

If you return to the list of domains on the Domains tab before the required record has been added or successfully propagated, the details you entered appear in the domain list with the status **Unchecked**. Once you have created the required records, click the domain name to view the details, and then click **Check Now** again to retry the validation.

**Important**

Do not configure domains until you are ready to verify ownership, because all domains are marked **Rejected** after 7 days if ownership verification has not been completed. You must then call Support to edit or re-enable the domain.

---

## CNAME records and A records

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Contact your DNS manager (usually your Internet service provider) and ask them to set up either a CNAME record or an A record as directed on the Add Domain page.

### CNAME records

CNAME records are used to assign an alias to an existing hostname in DNS.

A CNAME record might look like this:

```
abcdef gh. mydomai n. com CNAME aut odomai n. mai l cont r ol . com
```

Where CNAME indicates that you are specifying a CNAME record.

Make sure you include the trailing period in the domain name. Both the domain name and the character string are provided on the Domains screen when you add a new domain.

The above example indicates that abcdefgh.mydomain.com is forwarded to autodomain.mailcontrol.com. This enables TRITON AP-EMAIL to confirm that you own mydomain.com.

## A records

An A record is the Address record which maps a domain or subdomain to a valid IP address. In this case, it is matching a character string provided on the Add Domain screen. The record indicates that the specified string can be reached at the given IP address.

An A record might look like this:

```
abcdef gh. mydomai n. com I N A 86. 111. 217. 190
```

Where

- ◆ IN indicates Internet
- ◆ A indicates the Address record.

The above example indicates that the IP address for abcdefgh.mydomain.com is 86.111.217.190.

## MX records

Cloud TRITON Manager Help | Cloud Email Protection Solutions

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route email through TRITON AP-EMAIL to your Internet mail gateway.

Your DNS records, which end in **in.mailcontrol.com**, are available on the [Service IP addresses](#) page.

Contact your DNS manager (usually your Internet service provider) and ask them to set up or replace your current MX records for the domain you have added with the customer-specific DNS records listed on the [Service IP addresses](#) page (the ones that end in **in.mailcontrol.com**). For example, they might change:

Change	From	To
MX Preference 1	mydomain.com. IN MX 50 mail.mydomain.com.	mydomain.com. IN MX 5 <b>cust0000-1.in.mailcontrol.com.</b>
MX Preference 2	mydomain.com. IN MX 51 mail.mydomain.com.	mydomain.com. IN MX 5 <b>cust0000-2.in.mailcontrol.com.</b>

Make sure they include the trailing period, and ask them to set both of these records to an equal preference value.

It can take up to 24 hours to propagate changes to your MX records across the Internet. During this time, you should keep your previous mail routing active to ensure all your mail is delivered: while your MX records are changing over, some mail will be delivered using your old MX information, and some mail will be delivered using your new MX information.

## Connections tab

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Select the **Connections** tab on the policy to view or change connections for the policy. Your policy must have at least one default inbound connection and one outbound connection in order to be active on the system.

The **Inbound Mail Routing Rules** section of the tab specifies rules that route inbound mail from TRITON AP-EMAIL to particular email servers depending on the recipients. The rules are applied in the order listed; you can change the order by dragging the priority numbers up and down the list, then clicking **Save Order**.

To add a new inbound mail routing rule, click **Add New Rule**, then see [Configuring inbound mail routing rules](#), page 67.

You can check which of your mail routing rules, if any, applies to a particular email address by clicking [mail routing test utility](#). See [Testing mail routing](#), page 69.

The **Default Inbound Routes** section defines where TRITON AP-EMAIL sends email that is not matched by an inbound routing rule after processing messages received from the Internet - these are the connections to your email servers.

The **Outbound** box specifies from which connections TRITON AP-EMAIL is prepared to accept email for your domains (for onward delivery to the Internet).

Note that TRITON AP-EMAIL always attempts to deliver or receive email messages over a TLS connection if the sending or receiving MTA supports it. If opportunistic TLS is not available, the data transfer is made via plain text, rather than encrypted text. In either case, the data transfer is successfully accomplished. If you wish to use mandatory TLS, see [Transport Layer Security](#), page 106.

## Configuring inbound mail routing rules

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Testing mail routing](#)

Click **Add New Rule** on the **Connections** tab to add an inbound routing rule that applies to specified users, groups, domains, or content types. This enables you to route mail to different mail hosts for certain groups of users in your network, useful if, for example, your organization has multiple mail servers for different locations or subsidiaries.

If a message is sent to a user who is in more than one group covered by your inbound routing rules, the first rule in the list that matches the user will be applied. A message sent to multiple users who have different routing rules will be split into multiple copies and routed as configured for each individual user.

If you set up a content type rule, the rule is applied to messages that are encrypted with PGP. You can apply that rule to all PGP-encrypted messages, or choose to apply it to messages for specific users, groups, or domains.

Before it can be enabled for mail routing, a rule must be checked to ensure the following:

- ◆ TRITON AP-EMAIL can connect to the specified inbound mail hosts.
- ◆ The mail hosts accept messages for all domains explicitly specified in the rule. This is required for the rule to be valid.
- ◆ The mail hosts accept messages for the domains contained in all email addresses explicitly specified in the rule. This is required for the rule to be valid.
- ◆ The mail hosts accept messages for at least one domain within the policy.

**Note**

If a group includes a domain that the mail hosts do not accept messages for, some mail may not be delivered. We recommend that you check your groups for domains not accepted by your mail hosts, and that you recheck your inbound mail routing rules if you change or resynchronize your groups in the portal.

---

The mail host checking takes place as you configure the inbound rule.

1. Enter a **Rule Name**. This is required.
2. In the **Apply To** field, enter one or more recipients for the rule to apply to. These can be individual email addresses, groups configured in TRITON AP-EMAIL, or domain names. You can enter multiple recipients, separated by commas.

This field is required unless you are creating a rule that routes by content type and select **PGP Encrypted only** as described below.


To edit an existing recipient, click the item. Press **Enter** to save your changes as a new entry in the Apply To list. To discard your changes, press **Esc**.

To remove an item from the Apply To list, click the Delete icon next to the item.

3. To apply the rule only to confidential messages encrypted with PGP, mark **PGP Encrypted only**.  
If you select this option, the **Apply To** field is no longer mandatory.
4. Optionally, select a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See [Encryption tab](#), page 106 for further information.
5. If you are enforcing security, select an **Encryption Strength**: 128 or 256.

6. Click **Add Mail Host** to add a receiving mail server to the rule.

You can add up to 10 mail hosts to a rule. If TRITON AP-EMAIL cannot deliver inbound email to the first mail host in the list, it tries the other servers in order until the message is delivered. To change the order of the mail hosts, click an order number and drag it up or down the list.

7. Enter a **Host Name** (for example mail.mycompany.com) for the server. If the host name cannot be resolved on the Internet, enter an **IP Address** for the server as well. Click the  icon to confirm.

TRITON AP-EMAIL checks the mail host and sets the **Status** to Passed or Failed.

If the route check failed, click Failed to open a popup window that displays details of the failure. Filter the results of the check to view domains that are required or optional for the rule, and those that passed or failed.

In this window, you can recheck all the domains in the rule, or just the domains that failed. You can also choose to **Ignore Failed** domains, which changes the mail host's **Status** to Passed. Be aware that if you ignore failed domains, some messages may be undelivered.


You can edit the server settings by clicking the pencil icon.

8. To enable the rule for use, mark **Enabled**.



#### Note

At least one mail host in the list must pass the check for the rule to be saved as enabled. If the check fails, you can still save the rule, but you must first clear the **Enabled** check box.

If you make changes to the rule, for example changing the recipients it applies to or editing the **Security** settings, each mail host must be rechecked. Click the  icon to run the check again.

9. Once you have finished configuring your rule, click **Save**.

## Testing mail routing

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring inbound mail routing rules](#)

The mail routing test utility enables you to check which inbound mail routing rules apply to specific email addresses.

Enter one or more email addresses, separated by commas. If you have defined mail routing rules that apply to PGP-encrypted messages, you can select **Show rules for PGP emails to these addresses** to include those rules in your test. Then click **Test Addresses**.

The Test Results section contains a line for each entered email address, displaying which groups the address is a member of, and which inbound routing rule or rules, if any, applies to the address. Click on a rule name to see and edit the rule details.

## Adding inbound and outbound routes

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To add an inbound route:

1. On the Connections tab, click **Add** under **Default Inbound Routes**.
2. In the **Server** field, enter a fully qualified host name or an IP address.  
If you enter an IP address you are asked to give this connection a name. The name you give your IP address connection is not important and can just be “inbound” or whatever you feel is appropriate.  
If you enter an invalid IP address such as one from the reserved, private range, an error results.
3. Enter a **Preference** value to specify the order in which connections should be used. (Connections with preference value 1 are used before all other connections.)
4. Optionally, choose a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See [Encryption tab](#), page 106 for further information.
5. If you have selected a Security value, select an **Encryption Strength**: 128 or 256.
6. Click **Submit**.

To add an outbound route:

1. On the Connections tab, click **Add** under **Outbound Routes**.
2. In the **Server** section, either:
  - Select Server name or IP address, and enter a fully qualified host name or an IP address.  
If you enter an IP address you are asked to give this connection a name. The name you give your IP address connection is not important and can just be “outbound” or whatever you feel is appropriate.  
If you enter an invalid IP address such as one from the reserved, private range, an error results.Or:
  - If your organization is using Microsoft Office 365 for email, select **Office 365**.Or:

- If your organization is using Google Apps for email, select **Google Apps**.

**Note**

If you select Office 365 or Google Apps, you must configure the outbound mail gateway in your Office 365 or Google Apps account to point to your customer-specific DNS records. These are the records ending in “out.mailcontrol.com” on the [Service IP addresses](#) page.

3. Optionally, choose a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See [Encryption tab](#), [page 106](#) for further information.

**Note**

If you have selected Office 365 or Google Apps in the **Server** section, you cannot set encryption options as part of the connection. To enforce encryption on your outbound route, configure your Office 365 or Google Apps account.

**Note**

If you have the Email Encryption module, all outbound connection routes must have a security value of Verify+CN. See [Advanced encryption](#), [page 115](#) for further information.

4. If you have selected a Security value, select an **Encryption Strength**: 128 or 256.
5. Click **Submit**.

## Disaster recovery

Cloud TRITON Manager Help | Cloud Email Protection Solutions

TRITON AP-EMAIL provides a number of features that can help in the event of a major disaster or a failure of your Internet connectivity or email server.

### Specifying secondary routes

If TRITON AP-EMAIL cannot deliver inbound email to the primary connection specified it looks to see if a secondary connection is configured. This can be to a backup email server or a disaster recovery site.

### Email queuing

If TRITON AP-EMAIL cannot deliver email to any of the specified inbound connections, it queues all email for up to seven days and attempts to deliver queued email to each route approximately every thirty minutes. The queue operates on a first-in first-out basis, so the oldest email is delivered first when a connection becomes available.

## Connectivity test

For an inbound connection, click **Test** to carry out a connectivity test to its destination from your TRITON AP-EMAIL clusters.

The connectivity test shows you the response TRITON AP-EMAIL received from the email server, plus information about the time taken to reach that destination. You can run this test from various clusters in order to troubleshoot local connectivity issues.

## Antivirus tab

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Editing inbound or outbound rules](#)

Select the **Antivirus** tab on the policy to set up rules for antivirus protection.

Listed are the inbound and outbound antivirus rules that have been set for this policy. To edit the inbound or outbound rules, click **Edit** in either the **Inbound Rules** or **Outbound Rules** box.

## Editing inbound or outbound rules

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Antivirus exceptions](#)

The majority of the antivirus functionality is the same for inbound and outbound email. Field descriptions are provided below.

### Virus

Check this box if you want viruses to be quarantined when detected. Viruses are software programs capable of reproducing themselves and usually capable of causing great harm to files or other programs on the computer.



## Phishing



### Note

You must have the Email Sandbox module to use this feature

This option is applicable to inbound email only. Define whether suspected phishing messages should be quarantined, or allowed with suspicious URLs replaced by a link to a block page that you specify.

To set up block pages for phishing messages, see [Phishing block pages](#), page 55.

## Content

### Filter active HTML content

This ThreatSeeker Network feature automatically analyzes HTML inside messages and disables any potential dangerous content (by disabling specific HTML tags). You can define how strictly the system applies this security feature. Available settings are:

Setting	Description
<b>Low</b>	Disable embedded scripts (<SCRIPT> and <OBJECT> tags) and disable unknown HTML tags that are deemed to be potentially dangerous.
<b>Medium</b>	As Low but also disable “Web bugs” (URLs that are referred to inside a message, excluding links to images) and HTML styles that contain code.
<b>High</b>	As Low but disable all “Web bugs” and all HTML styles.
<b>Very high</b>	Extremely strict: as High, but this also disables all hypertext links to protect against a number of known vulnerabilities in common email clients.

The recommended setting is **Medium**; setting the level higher than this may cause messages to display too poorly for general users.

### Block potentially malicious macros

This feature looks for potentially malicious macros in common Microsoft Office document formats. By changing the sensitivity, you can control how suspicious ThreatSeeker is when it carries out its analysis. We recommend setting this to **High** initially. You may need to amend this setting if you find that a lot of documents just over the threshold are being quarantined. Documents containing known viruses are quarantined by the antivirus engines, regardless of this setting.

### Strict checks on message structure

This feature runs extra checks on email messages to confirm they meet an accepted structure and satisfy the requirements of external penetration tests. For example, one of the attachment checks would quarantine a MIME attachment with a filename that ends in a period but has no file extension (such as “attachment1.”).

By default this option is disabled. We recommend leaving it as disabled unless you are running an old mail client or want to run external penetration tests on your messages, otherwise you may see an increase in false positives.

## Encrypted Messages

Encrypted email must be decrypted before it can be analyzed for viruses. TRITON AP-EMAIL does not have the necessary key to do this and therefore cannot analyze encrypted messages. Similarly, a message containing a password-protected archive file attachment such as ZIP or RAR cannot be analyzed, because the password is unknown. To protect against the possibility of a virus infection from such email, TRITON AP-EMAIL allows them to be quarantined. Administrators can open them later in a secure environment.

## Executables

TRITON AP-EMAIL uses commercial antivirus (AV) engines to identify known viruses and its own ThreatSeeker intelligent threat prevention technology to identify viruses for which the AV vendors have not yet released a patch. However, even with multiple layers of protection, it is impossible to predict the types of technology that may become available to virus writers. TRITON AP-EMAIL therefore provides a range of additional features to aid in the fight against viruses.

We recommend that, where possible, email containing executable attachments be quarantined. If this is not appropriate for all users, then enforce this policy globally and use the antivirus exceptions option to configure exceptions.

### Quarantining messages containing scripts and executables

If you choose to block scripts and executables, messages containing any file whose contents appear to be executable are blocked, along with those with the following potentially dangerous file extensions: A6P, AC, ACR, ACTION, AIR, APK, APP, APPLESCRIPT, AWK, BAS, BAT, BIN, CGI, CHM, CMD, COM, CPL, CSH, DEK, DLD, DLL, DRV, DS, EBM, ELF, ESH, EXE, EZS, FKY, FRS, FXP, GADGET, GPE, GPU, HLP, HMS, HTA, ICD, IIM, INF, INS, INX, IPA, IPF, ISU, JAR, JS, JSE, JSX, KIX, KSH, LIB, LNK, MCR, MEL, MEM, MPX, MRC, MS, MSC, MSI, MSP, MST, MXE, OBS, OCX, PAF, PCD, PEX, PIF, PL, PLSC, PM, PRC, PRG, PVD, PWC, PYC, PYO, PY, QPX, RBX, RGS, ROX, RPJ, SCAR, SCPT, SCR, SCRIPT, SCT, SEED, SH, SHB, SHS, SPR, SYS, THM, TLB, TMS, U3P, UDF, VB, VBE, VBS, VBSCRIPT, VCARD, VDO, VXD, WCM, WIDGET, WORKFLOW, WPK, WS, WSC, WSF, WSH, XAP, XQT.

## Antivirus exceptions

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

◆ [Antivirus tab](#)

Exceptions are available for the following options on the Antivirus tab:

- ◆ *Phishing*
- ◆ *Executables*

## Phishing

Click **Phishing Exceptions** to override the phishing settings for users, groups, or domains. You must have the Email Sandbox module to use this feature

Click the appropriate policy in the **Apply to** column of the resulting screen. You can then change the way phishing messages are handled for specific users, groups, or domains. For example, you can allow URLs to be replaced in messages for certain groups, for example Marketing, and quarantine messages for other groups.

To create an exception:

1. Click **Add phishing exception**.
2. Choose an email address, domain name, or group from the list. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
3. Define whether suspected phishing messages should be quarantined, or allowed with suspicious URLs replaced by a link to a block page that you specify.
4. Click **Submit**.

## Executables

Click **Executable Exceptions** to override the executable settings for users, groups, or domains.

Click the appropriate policy in the **Apply to** column of the resulting screen. You can then change the way executables are handled for specific users, groups, or domains. For example, you can deselect "Quarantine messages containing scripts and executables" for Developers receiving internal mail.

To create an exception:

1. Click **Add executable attachment exception**.
2. Choose an email address, domain name, or group from the list. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
3. Clear the **Quarantine messages containing scripts and executables** box.
4. Click **Submit**.

## URL Sandboxing tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [URL sandboxing exceptions](#)
- ◆ [URL Sandboxing Utility](#)
- ◆ [File sandboxing](#)

Use the **URL Sandboxing** tab in a policy to inspect uncategorized URLs in email by



### Note

You must have the Email Sandbox module to view and use this feature.

tagging them for additional real-time advanced security analysis. Doing so helps protect end users from accessing malicious websites.

With URL sandboxing, if users click on a link within an email and that link or elements associated with that link are suspicious, they receive a warning that “The link may not be safe.” The notification includes:

- ◆ The domain they are trying to access.
- ◆ The reasons the link is considered suspicious: for example, the sender email address may be unknown to our service or the sending mail server may have a suspicious reputation.
- ◆ The option to analyze the page further.

If they answer **No** to **Analyze the page?**, the suspicious link is not analyzed. They can then close the notification window. For their protection, they cannot access the page.

If they answer **Yes**, the page is analyzed using TRITON AP-EMAIL real-time advanced security analysis. They then receive one of the following messages:

Notification	Description
<b>The link appears to be safe</b>	No malicious threats found. The notification lists the URL and category or categories of the page. Users can proceed to view the page if they choose to do so.
<b>Access denied</b>	Malicious threats detected in the page. The notification lists any matched categories along with the sites suspected of being infected with a malicious link. Users cannot access the page.
<b>Access denied</b>	Users may also receive an <b>Access denied</b> notification if their organization does not permit them to browse uncategorized web pages.

Notification	Description
<b>Unable to access page</b>	The web server may be down or the link may be incorrect. They may want to try again later, or contact their administrator for more information.
<b>Unable to analyze URL</b>	The page could not be analyzed because its protocol is not supported. Supported protocols are HTTP and FTP. If you have selected the <b>Allow the recipient to follow links with an unsupported protocol</b> option, the user can proceed to view the page if they wish; otherwise, the user cannot access the page.

To modify rules for URL sandboxing:

1. Click **Edit**.
2. Under Default settings, select **Analyze suspicious URLs**.
3. To allow the user to click through to the site after looking at the category of the Web page, select **Allow the recipient to follow links to unclassified URLs**.
4. Links cannot be analyzed if TRITON AP-EMAIL does not recognize the network protocol used. Supported protocols are HTTP and FTP. To allow the user to click through to the site if it cannot be analyzed, select **Allow the recipient to follow links with an unsupported protocol**.
5. If required, enter customized text to display in email messages instead of suspicious URLs, such as “Danger, do not click!”.
6. Under Policy-wide settings, enter any trusted domains that you do not want to be inspected in email messages. Use this list with caution: if a site on the list is compromised, TRITON AP-EMAIL does not analyze the site and cannot detect the security problem.
7. Define whether to analyze suspicious URLs contained in signed messages.



#### Note

The options to whitelist domains and analyze suspicious URLs in signed messages apply to all users and groups in a policy, and cannot be over-ridden by exceptions.

8. Click **Submit**.

## URL sandboxing exceptions

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [URL Sandboxing tab](#)
- ◆ [URL Sandboxing Utility](#)

It is possible to tailor some URL sandboxing settings in TRITON AP-EMAIL for individual users or groups of users. These settings override the settings made on the URL Sandboxing tab for the policy.

1. On the URL Sandboxing tab, click **URL sandboxing exceptions**. This brings you to a list of URL sandboxing exceptions if you have created any.
2. Click **Add Exception**.
3. Enter the domain(s) or end-user email address(es), or select a group to which this policy applies. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
4. Define the URL sandboxing settings for these users or groups. For details of the settings, see [URL Sandboxing tab, page 76](#).
5. Click **Submit**.

## URL Sandboxing Utility

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [URL Sandboxing tab](#)
- ◆ [URL sandboxing exceptions](#)

To view details of a URL that has the URL sandboxing feature applied to it:

1. Go to **Email > Messages > URL Sandboxing Utility**.
2. Enter a sandboxed URL, and then click **Submit** to show the original URL and its recipient, security and policy settings. An administrator in the account that sandboxed the URL sees:

Sandboxed URL	Shows the sandboxed URL entered.
Original URL	Shows the original URL before sandboxing.
Block Policy Flags	Shows if the recipient is allowed to see unclassified URLs. Also shows if suspicious URLs are masked for the recipient.
Policy Name	Shows the name of the policy that owns the recipient domain.
Recipient	Shows the email address of the recipient of the message containing this URL.

An administrator in the account that did not sandbox the URL only sees:

- ◆ Sandboxed URL
- ◆ Original URL
- ◆ Block Policy Flags

- ◆ Recipient email address

## Antispam tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Antispam exceptions](#)
- ◆ [Commercial bulk email detection](#)
- ◆ [Adding an entry to a white or black list](#)
- ◆ [Uploading a white list or black list](#)

Select the **Antispam** tab on the policy to view or modify rules for spam protection and to configure your settings to detect commercial bulk mail.

By design, email is checked for spam under the following conditions:

- ◆ Email is inbound from the Internet.
- ◆ The email message is not stopped by some other rule, for example it contains a virus or a barred attachment type.
- ◆ The Antispam service is enabled for the policy (i.e., you are licensed for the service).

All such email is assigned a spam score (unless it is blocked by system-wide rules that identify bulk spam). This is visible in the message header and message tracking results. The higher the spam score, the more likely it is to be spam. Many rules are used to generate the spam score, including analysis of the words within the message, where it came from, its headers, and comparisons with other spam and non-spam email.

## Spam Options

Check **Filter for Spam** if you want email filtered for spam.

There must be at least one spam rule defined. By default two rules are set up:

1. Quarantine all email with a spam score greater than 6.
2. Discard any email with a spam score greater than 15.

You can define multiple rules for different spam thresholds and associate actions with each of these. For example, you can create a rule that forces all email with a spam score greater than 6.0 to be forwarded to an administrator, all email with a score greater than 7.0 to be quarantined, and all email with a score over 10.0 to be discarded.

Lower values detect more spam at the risk of false positives - email wrongly detected as spam. Higher values reduce the risk of false positives but could miss some spam.

TRITON AP-EMAIL aims to ensure that no false positives occur with spam scores over 6.0. This is the recommended default setting for quarantining email.

To define spam rules:

1. From the first **Spam scoring more than** drop-down list, select a spam threshold.
2. From the second **Spam scoring more than** drop-down list, select an action for that threshold.

The following actions are available:

Action	Description
<b>Quarantine-Notify</b>	Messages are quarantined as above and a notification is sent to an email address. This is not recommended, because you are simply replacing one email with another. It is included for those that wish to use notifications during an evaluation phase rather than the more widely used “tag” option.
<b>Quarantine</b>	Messages are kept in quarantine for up to 30 days. This is the normal setting used for messages identified as spam. Note that no notifications are sent for this action.
<b>Forward</b>	Messages are forwarded to one or more email addresses in a comma-separated list. You can use this setting to forward all spam to a single account for management purposes.
<b>Tag subject</b>	Message subjects are tagged with a prefix that you’ve assigned (in the <b>Tag subject prefix</b> box under <b>Existing Rules</b> ).
<b>Bounce</b>	Messages are bounced back to the sender.
<b>Discard</b>	Messages are discarded. This is often used to discard messages with a very high spam score.

3. Click **Add Rule>>** to create a rule based on these parameters.

Depending on the action you select, you may be prompted for additional information first, such as the email address to which to forward the message.

A list of existing rules is displayed. You can also delete rules here.



## Spoofed messages

Select **Filter spoofed messages of domains in this policy** to detect and act on messages sent from domains within the policy to recipient domains within the policy, where the sender address has been spoofed.

A sender address is considered to be spoofed if the following conditions are true:

- ◆ The IP address of the sending MTA does not match any of the outbound connections configured in the policy.
- ◆ Cloud service additional message authenticity checks fail.

Select **Verify “From” address displayed to end users** to check if both the address the message recipient sees in the From: field and the envelope sender address match domains defined in your policies. The envelope sender is used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces) and often matches the From: address, but not always. For example, the message might come from a mailing list, or from an organization authenticated to send messages on your company’s behalf.

If you select this option, one of the following happens:

- ◆ If the envelope sender address does not match one of your policies but the From: address does match, the cloud service performs message authenticity checks on the From: address.
- ◆ If the envelope sender address matches one of your policies, the cloud service performs message authenticity checks on the envelope sender only.

If this option is not selected, the From: address is ignored and authenticity checks are performed only on the envelope sender if it matches one of your policies.

Select the action to perform when spoofed messages are detected:

- ◆ **Quarantine.** This is the default option. Spoofed messages are kept in quarantine for up to 30 days.
- ◆ **Discard.** Spoofed messages are discarded. Note that no notifications are sent for this disposition
- ◆ **Tag subject with.** The subject headers of detected spoofed messages are tagged with “SPOOFED:” or a custom tag that you enter.

Click **Submit** when you are finished.

## Keep messages

By default, TRITON AP-EMAIL does not keep a copy of any messages unless they are quarantined, in which case they are held for 30 days before being automatically deleted. Checking **Keep a copy of clean messages** allows TRITON AP-EMAIL to keep a private copy of clean email messages, for a short period, separate from the quarantine area, to aid in the process of spam tuning when the “Report this email as Spam” link is used (see [Report this email as spam, page 63](#), for more details). If TRITON AP-EMAIL has the original message available, our operations staff and future automated systems can analyze it.

## Commercial bulk email detection

The TRITON AP-EMAIL service offers a way to configure your settings to detect commercial bulk email and to perform certain actions on them, such as quarantining them or tagging the message subject, so that you can easily identify which messages are commercial bulk email.

To enable commercial bulk email detection, do the following:

1. Under **Commercial Bulk Email Detection**, select **Analyze for commercial bulk email**.
2. Select the action you'd like performed when commercial bulk email is detected:
  - **Take no action.** No action is taken on the commercial bulk email detected.
  - **Tag the message subject.** The subject of detected commercial bulk email messages are tagged with "COMMERCIAL:" or a custom tag that you enter.
  - **Quarantine the message.** Commercial bulk email messages are kept in quarantine for up to 30 days. Note that no notifications are sent for this disposition.
3. Select the sensitivity level of the feature:
  - **Normal** detects email that comes from known commercial bulk email sources.
  - **High** detects email that comes from known commercial bulk email sources or email that contains commercial content.
4. Click **Submit** when you are finished.

Note that the subject tag that you select will also be used in all antispam exceptions.



### Note

If you wish to run a report that shows the number of commercial bulk email messages you have received, these messages will only be counted if you have selected **Analyze for commercial bulk email**.

---

## Whitelists and blacklists

Here you can configure whitelists and blacklists that affect the whole policy. White lists apply to sender addresses only, and list the email addresses that are permitted to send mail to you without spam filtering being applied.

Blacklists also apply to sender addresses only and are lists of addresses from which you do not want to receive email. Note that blacklists are often ineffective as a spam-prevention measure since spammers change email address frequently.

If you enable whitelisting, you can also configure the following options:

- ◆ **Apply whitelist matching on spoofed email addresses.** If TRITON AP-EMAIL detects a message is spoofed, whitelisting is not applied by default. However, you may wish to allow some messages that are legitimately spoofed, for example a message from an email distribution list that appears to come from a specific

person. Select this option if you want to allow spoofed addresses through if the address appears in your whitelist.

- ◆ **Do not apply whitelist matching on From: headers.** An email message has two addresses associated with it: the envelope sender, and the From: header. The envelope sender is used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces); the From: header is what the message recipient sees. The envelope sender and the From: header often match, but not always. There are a number of legitimate reasons why a envelope sender might not match the From: header, for example if the message comes from a mailing list, or from an organization that has implemented a specific address for bounced messages.

Email spammers can take advantage of this, by changing the From: header on a spam email to be a domain that you recognize, while the envelope sender remains related to a domain under their control.

By default, TRITON AP-EMAIL performs whitelisting on both the From: header and the envelope sender. If you select this option, whitelist matching applies only to the envelope sender.

To populate your white and blacklists, click the links in **Whitelist [these](#) addresses** or **Blacklist [these](#) addresses**. See *[Adding an entry to a white or black list](#)*, page 85 for more information.

**Note**

Whitelists always take priority over blacklists. If you have blacklisted an email address and also inadvertently whitelisted it, messages from that sender are not blacklisted.

---

## End user permissions

TRITON AP-EMAIL Antispam provides a range of end-user self-service options. These are all initiated using the TRITON AP-EMAIL end-user message report (see *[End-User Self Service](#)*, page 155).

Two self-service options that you can enable or disable are the ability for users to release a copy of quarantined spam to themselves, and the option to populate and manage their own individual black and white lists.

**Note**

A user can never prevent an email containing a virus from being quarantined and, regardless of these settings, can never release one.

---

White lists always take priority over black lists. If you have blacklisted an email address for the policy, a user can whitelist it and, assuming it has no other issues, such as containing a virus or contravening a Content rule, it is delivered. To prevent a user receiving certain types of email, we recommend that you configure a content filtering policy. TRITON AP-EMAIL Antispam is used to detect spam, not enforce email usage policy. Spam is subjective and if users want to receive messages from a source that they do not consider to be a spammer, they should be allowed to.

For new policies, this feature is enabled by default. We recommend that you check this box if you are using the spam reporting link.

## Spam detection methods

For information on the methods that TRITON AP-EMAIL Antispam uses to identify spam, go to the [Knowledge Base](#) to read the article, “[Detecting spam](#).”

## Antispam exceptions

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Antispam tab](#)
- ◆ [Adding an entry to a white or black list](#)
- ◆ [Uploading white and black lists in bulk](#)

It is possible to tailor some antispam settings in the TRITON AP-EMAIL service for individual users or groups of users. These settings override the domain-wide settings, although you can choose whether to have changes in the main policy synchronized with your exceptions.

1. Click **Antispam Exceptions**.
2. Click **Add**.
3. Enter the domain(s) or end-user email address(es), or select a group to which this policy applies. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user’s email address, not LDAP user name.
4. Check **Synchronize end-users settings with the [main policy name] policy** to ensure any future changes to end-user settings in the main policy are also applied to the exception.

When you check the **Synchronize...** box, the settings below it are greyed out. To specify which parts of the end-user settings are synchronized with the main policy, clear the **Synchronize...** box, then check the boxes for the exception sections that should inherit any future changes from the main policy, and clear the boxes for the sections that you want to be unaffected when the main policy is edited.

5. Click **Submit**.

Under exceptions, it is also possible to synchronize spam and commercial bulk email actions with the [default] policy.

1. Click **Antispam Exceptions**.
2. Click the email address for the individual or group of users for whom you wish to tailor a policy.

Check **Synchronize Spam and Commercial Bulk Email settings with the [main policy name] policy** to ensure that any future changes to the spam and commercial bulk email actions settings in the main policy are also applied to the exceptions. If you have existing white list and black list exceptions that you want to use in TRITON AP-EMAIL, you can use the Bulk Operations options to import those lists. See [Uploading white and black lists in bulk](#), page 86 for more information.

## Adding an entry to a white or black list

Cloud TRITON Manager Help | Cloud Email Protection Solutions

1. On the Antispam tab, click the link in **Whitelist these addresses** or **Blacklist these addresses**. A list of currently whitelisted or blacklisted addresses appears. You can sort the list in ascending or descending order by address name or description. You may need to click **Next** to see all of the addresses in the list. You can narrow the list by adding search criteria and clicking **Search**.
2. Click **Add** to add a new entry to the list.
3. In the **Address** field, enter the email address of interest. You can also enter an entire domain or sub-domain, but you must precede it with a wildcard. Wildcards have the following effects depending upon their use:

<b>*acme.co.uk</b>	Covers all email addresses at acme.co.uk and all email addresses at any sub-domain of acme.co.uk
<b>*@acme.co.uk</b>	Covers all email addresses at acme.co.uk but none at any sub-domain
<b>*.acme.co.uk</b>	Covers any address at any sub-domain but excludes the main domain

4. Enter a description if desired.
5. Click **Submit**.

## Uploading a white list or black list

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If you have permission to modify configurations, you can populate a white list or black list in a policy or exception by uploading an address list in a comma-separated value (CSV) file.

The header of the file must be this string exactly, "Address, Description" and every line must contain the following 2 fields separated by a comma:

- ◆ An email address or domain name (wildcards permitted).
- ◆ A description (free text, up to 255 characters).

The fields can be quoted or not. If a field contains a comma, it must be quoted. If 1 field is quoted, the rest of the line must be quoted. If a field contains a quotation mark, this character must be surrounded by additional quotation marks. If a line contains

only 1 field, it is interpreted as the email address and the description is omitted. If a line contains more than 2 fields, the file is rejected and an error message is displayed.

For example:

Address, Description

address1@domain1.com, Description of address1, containing comma

address1@domain1.com Description of address1 without comma

address1@domain1.com, Description of address1, containing quotes

domain2.com, Description of domain2

To upload the file:

1. Click the link, [Upload addresses from a CSV file](#).
2. Browse to the name of the file to upload.
3. Select an action:

Action	Description
<b>Append to current list</b>	Elements imported from the file are added to the existing elements. The resulting list is a union of all elements. If any of the entries in the file is already included in the list, it is not added again and a warning message is displayed. This does not stop the processing of the file.
<b>Replace current list</b>	Elements already existing in the list are deleted and replaced by the elements in the file. You are asked to confirm this action.

4. Click **Upload**. Note that large files take a while to transfer to the server. If the file is empty, too large, or cannot be opened, an error results. An error also results if any of the elements are invalid.

You can also download the current addresses into a CSV file for viewing in a spreadsheet, or you can delete entries from the white or black lists by checking the box next to the address and clicking **Delete**.

## Uploading white and black lists in bulk

Cloud TRITON Manager Help | Cloud Email Protection Solutions

You can upload white list and black list exception information in bulk if you have the black or white list exceptions for all of your users and groups in a single file.

The file must be in comma-separated value (CSV) format, and the header of the file must be this string exactly: "Apply To, Address, Description". Every line must contain 3 fields separated by commas:

- ◆ An email address, domain name, or group that the white or black list address applies to (no wildcards permitted).

- ◆ An email address or domain name (wildcards permitted).
- ◆ An optional description (free text, up to 255 characters).

The fields can be quoted or not. If a field contains a comma, it must be quoted. If 1 field is quoted, the rest of the line must be quoted. If a field contains a quotation mark, this character must be surrounded by additional quotation marks. If a line contains more than 3 fields, the file is rejected and an error message is displayed.

For example:

```

Appl y To, Address, Descri pt i on
"UK Sal es", "address1@domai n1. com", "Descri pt i on of
address1, cont ai ni ng comma"
john@exampl e. com address1@domai n1. com Descri pt i on of
address1 wi thout comma
"exampl e. com", "domai n2. com", "Descri pt i on of domai n2"
"Mar ket i ng", "address2@domai n1. com", "descri pt i on of
address2", "t hi s fi el d i s not processed"

```

To upload the file:

1. On the Antispam Exceptions page, do one of the following:
  - To upload a bulk white list, click the link [Upload addresses from a CSV file](#) under Whitelist Bulk Operations.
  - To upload a bulk black list, click the link [Upload addresses from a CSV file](#) under Blacklist Bulk Operations.
2. Browse to the name of the file to upload.
3. Select an action:

Action	Description
<b>Append to current list</b>	Elements imported from the file are added to the existing elements. The resulting list is a union of all elements.
<b>Replace current list</b>	Elements already existing in the list are deleted and replaced by the elements in the file. You are asked to confirm this action.

4. Click **Upload**. Note that large files take a while to transfer to the server. If the file is empty, too large, or cannot be opened, an error results. An error also results if any of the elements are invalid.

You can also download the current black and white lists into a CSV file for viewing and editing in a spreadsheet.

Note that if no exceptions are created, the default spam policy will apply.

# Content Filter tab

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Editing content rules](#)

Content filtering rules are typically different for inbound and outbound email, because the email usage policy that you want to enforce more than likely specifies different sets of rules for email entering the organization than it does for email leaving the organization.

Select the **Content Filter** tab on the policy to view or modify rules for filtering content.

## Editing content rules

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Click **Edit** in the **Inbound Attachment Rule** or **Outbound Attachment Rule** box to edit the content rules for your policy.

The majority of the content filtering functionality is the same for inbound and outbound email.

Section	Field
Attachments	<ul style="list-style-type: none"><li>◆ <a href="#">Masking attachments</a></li><li>◆ <a href="#">Quarantining messages with specific file types</a></li><li>◆ <a href="#">Parking attachments</a></li><li>◆ <a href="#">Attachment exceptions</a></li><li>◆ <a href="#">Image analysis and quarantining</a></li></ul>
Message Size	<ul style="list-style-type: none"><li>◆ <a href="#">Message Size</a></li></ul>
Content Filtering	<ul style="list-style-type: none"><li>◆ <a href="#">Filtering using lexical rules</a></li><li>◆ <a href="#">Quarantining messages where lexical analysis does not complete</a></li></ul>

## Attachments

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The following actions are available for email attachments:



- ◆ *Masking attachments*
- ◆ *Quarantining messages with specific file types*
- ◆ *Image analysis and quarantining*
- ◆ *Parking attachments*
- ◆ *Attachment exceptions*

## Masking attachments

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ *Inverting the quarantine action*
- ◆ *Image analysis and quarantining*
- ◆ *Attachment exceptions*
- ◆ *Parking attachments*
- ◆ *Message Size*
- ◆ *Filtering using lexical rules*

Masking an attachment renames attachments with the specified extensions. The renaming replaces the last character of the extension with an underscore ‘\_’. For example, if you mask “EML” attachments, a file named “test\_email.eml” is renamed “test\_email.em\_”.

This stops the attachment being automatically associated with its appropriate executable in Windows and therefore avoids dangerous actions being triggered automatically.

We recommend that you mask “EML” attachments, because these can cause email clients such as Outlook and Outlook Express to execute code automatically.

Click the link on **Mask attachments with** [these extensions](#) to specify which attachments to mask.

### Inverting the mask action

You can invert masking by extension. This enables you to specify that all extensions **except** those specified are subject to the Mask action. If you want to do this, select the radio button **Mask all extensions except these**.

## Quarantining messages with specific file types

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Masking attachments](#)
- ◆ [Attachment exceptions](#)
- ◆ [Parking attachments](#)
- ◆ [Image analysis and quarantining](#)
- ◆ [Creating custom file types](#)
- ◆ [Message Size](#)
- ◆ [Filtering using lexical rules](#)

You can quarantine messages containing attachments matching file types that you specify.

File types are grouped together into file formats. For example, if you select the Sound format, this quarantines anything related to sound files, including RealAudio, Windows Media Audio, MPEG Audio, and MIDI files.

You can expand a file format to select or remove specific file types from the quarantine list. For example, you can select the Standard Graphics format to block all standard image attachments, but then choose to clear the JPEG file type within that format to allow JPEGs to be delivered.

If the available file types do not meet your requirements, you can set up custom file types containing one or more file extensions and MIME types. For more information, see [Creating custom file types](#), page 94. The custom file types you create are available for all policies, and appear as part of a default custom file format on the same page as the supplied file formats.



### Note

Options on the Antivirus tab are the most effective way to block unsafe executables. For more information, see [Executables](#), page 74.

---

To quarantine attachments:

1. On the Content Filter tab, click the link in **Quarantine messages containing files with [these types](#)**.  
The page displays the file formats and types currently being quarantined.
2. Click **Edit**.
3. Check the boxes for file formats you wish to quarantine.
4. To select particular file types within a file format, click the + icon to expand the format.

If you have selected the file format, all of the subsidiary file types are also selected. You can select or clear as many file type options as you wish. The information next to each file format tells you how many are currently selected from that format.

5. Click **Submit**.

### Inverting the quarantine action

Inverting the quarantine action enables you to specify that all file types **except** those selected are quarantined. If you want to do this, select **that do not match the selected file types** from the drop-down list.

## Image analysis and quarantining

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If you have the Image Analysis module, you can choose to quarantine messages that have images attached to prevent potentially pornographic images from entering your organization. Messages are quarantined if they contain an image attachment considered to be inappropriate. This can be set up for inbound messages, outbound messages, or both.

To quarantine images, select **Quarantine messages containing inappropriate images**, and define how strictly the system applies this security feature by selecting a sensitivity level. By changing the sensitivity, you can control how suspicious the image scanner is when it carries out its analysis.

It is difficult to impose absolute thresholds on what constitutes an “inappropriate” image, as perceptions can vary. Therefore depending on the sensitivity level you select, you may see a proportion of messages containing acceptable images being quarantined. If there are images that you don’t want to be analyzed and quarantined, perhaps because they are repeatedly blocked, you can add them to the image white list. See [Image white list, page 57](#), and [Managing quarantined images, page 130](#).

If a message includes an image attachment that TRITON AP-EMAIL cannot analyze, perhaps because it is too large, you can select **Quarantine messages with images that could not be analyzed** to quarantine that message for further analysis.

## Attachment exceptions

Cloud TRITON Manager Help | Cloud Email Protection Solutions

You can override some of the attachment settings for users, groups, or domains. To do this:

1. Click **Attachment Exceptions** for either inbound outbound attachments.
2. Click **Add Exception**.

3. In the **Domain or address list** field, enter the address(es), domain(s), or select the appropriate group(s) to which this configuration applies. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
4. Make whatever changes you want to the policy for this user, group, or domain.
5. Click **Submit**.

To edit an existing attachment exception, click the appropriate policy in the **Apply to** column of the Attachment Exceptions page.

## Parking attachments

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Masking attachments](#)
- ◆ [Image analysis and quarantining](#)
- ◆ [Park attachments by file type](#)
- ◆ [Unknown attachment types](#)
- ◆ [Filtering using lexical rules](#)

Use the **Policy > Content Filter > Park Attachment Rules** page to park large message attachments on the TRITON AP-EMAIL system. The file is removed from the message and stored. An annotation is added to the message including the filename, its size, and a Web link from where the file can be retrieved over a secure HTTP (HTTPS) connection. The wording of the annotations is completely configurable.

To create a park attachment rule:

1. Click **Add Rule**.
2. Define whether the rule should be initially enabled or disabled.
3. Enter a **Rule name**.
4. Select an **Attachment size** and a **Message size** from the drop-down lists. For example, you might choose to park any attachment with a size of 2 MB or larger in messages that are 3 MB or larger in size.  

You can also select Ignore for either of these options, for example if you want all attachments larger than a certain size to be parked regardless of the message size.
5. Choose how long the parked message should be stored for. The default is 7 days.
6. Define whether the system should keep a copy of the original message.
7. Under **Apply To**, define who the rule affects. By default, the rule applies to all the senders (for an outbound rule) or recipients (for an inbound rule) in the policy. Alternatively you can apply the rule to only the senders or recipients that you specify. Enter the domains, addresses, or groups to include, separated by commas.

8. To exclude certain sender and recipients from your rule, select **Exclude these senders and recipients**, then list the domains, addresses, or groups to exclude, separated by commas. For example, you can specify that a rule does not apply if an email is from xyz@externaldomain.com or is sent to xyz@internaldomain.com. You can enter up to 65,535 characters.
9. Under **Annotations**, you can edit the annotation that appears in the original message sent to the recipient. A default annotation like the one below is included.  
The attachment attach1-2100.txt (2.1 MB) was parked. It can be retrieved from [here](#).

In addition, you can include the following variables:

Variables/tokens	Description
<b>_RECIPIENTS_</b>	The intended recipients of the message.
<b>_DATE_</b>	The date TRITON AP-EMAIL received the email that generated the annotation. This date is based on the time zone set on the Notification Email screen.
<b>_SENDER_</b>	The message originator.
<b>_SUBJECT_</b>	The subject line of the message that is being annotated.
<b>_ATTACH_TYPE_</b>	The file type of the attachment parked.
<b>_NAME_</b>	The name of the attachment parked.
<b>_RETRIEVE_END_</b>	Used in HTML annotations surrounding some text that displays as a link. For example, "It can be retrieved from _RETRIEVE_START_here_RETRIEVE_END."
<b>_RETRIEVE_START_</b>	Used in HTML annotations surrounding some text that displays as a link. For example, "It can be retrieved from _RETRIEVE_START_here_RETRIEVE_END."
<b>_RETRIEVE_LINK_</b>	Used to include a link to download the attachment. For example, "It can be retrieved from _RETRIEVE_LINK_."
<b>_SIZE_</b>	The size of the attachment parked.

Click on **Variables/tokens** to select these variables from the drop-down list.

10. Under **Notification Options**, select who should be notified about the parked attachment. In all cases, you have the option to include the original message with the notification.
11. Click **Submit** when done.

After a rule has been created and enabled, you have the option to add parking by file format or type. See *Park attachments by file type*, page 94.

## Park attachments by file type

Cloud TRITON Manager Help | Cloud Email Protection Solutions

You can add parking by file format or type to an existing, enabled park attachments rule.

You can combine attachment and message size checks with file types. For example, you can specify a rule that parks all video files larger than 5 MB.

To park attachments by file type:

1. From the Park Attachment Rules window, click the name of the rule you want to edit.
2. Select the **Park attachments by file type** check box to enable parking by file type.
3. Click the link in **Park attachments by file type** [Choose file types to specify file types for parking](#).
4. Check the boxes for file formats you wish to park. To select particular file types within a file format, click the + icon to expand the file format.
5. Click **Save**.

## Creating custom file types

Cloud TRITON Manager Help | Cloud Email Protection Solutions

You can set up custom file types to meet your organization's needs. For example, you might want to block a file extension not covered by the supplied file types, or create a type that groups a number of specific extensions.

You can also use custom file types to set up attachment blocking for MIME types.

To create a custom file type:

1. Go to **Account > Custom File Types**.
2. Click **Add**.
3. In the **Extensions** field, enter the file extensions to include in the custom type, separated by commas. For example, to block particular types of image file, you might enter JPG, GIF, PNG.
4. Enter any MIME types in the format content type/content subtype. For example, video/mpeg or text/csv.
5. Enter a description for your custom file type. This description appears in the **Custom File Type** list when you are selecting file types and formats for attachment quarantine.
6. Click **Submit**.

## Unknown attachment types

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If a message includes an attachment type that TRITON AP-EMAIL cannot identify, you can choose to quarantine that message for further analysis. This can be set up for inbound messages, outbound messages, or both.

To quarantine unknown attachment types:

1. On the **Content Filter** tab, click **Edit** for either inbound or outbound rules.
2. Select **Quarantine messages containing files of unknown type**.
3. Click **Submit**.

## Message Size

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Masking attachments](#)
- ◆ [Attachment exceptions](#)
- ◆ [Parking attachments](#)
- ◆ [Filtering using lexical rules](#)

There are 3 pre-defined actions available for application to 3 configurable message size thresholds:

1. You can set a global limit above which email should be discarded. By default this cannot exceed 50 MB. This is applicable only to inbound email. (Note that messages larger than 50 MB are subject to special terms. See your TRITON AP-EMAIL contract for further detail.)



### Note

When an email is discarded because it exceeds the maximum allowable size, TRITON AP-EMAIL does not issue a notification (see [Email notifications](#), page 52 for more details). A failed delivery code is returned to the sending email server.

---

2. You can quarantine email above a specified size.
3. You can defer email above a specified size for delivery within a configurable time window. Deferral of large email is useful when you have Internet bandwidth capacity limitations and the user impact of delivering large email is noticeable during the main working day.

## Filtering using lexical rules

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Managing dictionaries](#)
- ◆ [Creating a lexical rule in advanced mode](#)
- ◆ [Creating a lexical rule in simple mode](#)
- ◆ [Creating a compliance rule](#)
- ◆ [Phrase score and lexical rule thresholds](#)

The TRITON AP-EMAIL lexical rules feature provides a powerful content filtering capability to mitigate the risks associated with email. A lexical rule compares words in a dictionary to those in an email and performs an action when there is a match.

You can use this technology to analyze for profanity and other undesirable content entering your organization. Furthermore, because lexical rules can be applied outbound as well, you can stop email from leaving the organization if they contain phrases that should not be allowed out. This might be profanity or inappropriate words but could also include company confidential information, or communications that could cause embarrassment, loss of reputation, or business.



### Note

We do not recommend using this feature to attempt to block spam, because generating ad-hoc rules is both time-consuming and prone to the introduction of false positives.

---

To set up lexical filtering rules, select the **Content Filter** tab of your policy, then click the link under Inbound or Outbound content **Filter using** [these lexical rules](#).

From this screen you can do the following:

- ◆ To add new lexical rules, click one of the buttons under **Add Lexical Rule**.
- ◆ To edit an existing rule, click the rule you want to edit.

## Phrase score and lexical rule thresholds

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Filtering using lexical rules](#)
- ◆ [Creating a lexical rule in simple mode](#)
- ◆ [Creating a lexical rule in advanced mode](#)



Each word or phrase in a dictionary is assigned a score that is used to determine the disposition in a lexical rule. Typically a higher score indicates a worse contravention of the rule. For example, a higher score would be assigned to the most obscene words in a list of profane words.

A lexical rule specifies a set of thresholds and actions on each. When a message is compared to the phrases, it accumulates scores for each of the phrases on which it matches. The scores for the phrases within each dictionary are totaled. The greatest threshold that is breached causes an action to be taken on the message.

## Creating a lexical rule in simple mode

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Filtering using lexical rules](#)
- ◆ [Creating a lexical rule in advanced mode](#)

The simple mode for entering lexical rules enables you to set up a single action to take when a message matches a phrase from the list you specify. If you want to set up lexical rules to match against system or custom dictionaries, or want to include multiple actions depending on the number of phrases matched, see [Creating a lexical rule in advanced mode, page 98](#).

1. On the main Lexical Rules screen, click **Add Simple Rule**.
2. Enter a name for the rule and a description if desired.
3. In the **Apply To** field, enter the domain(s) or individual email address(es) or select the group to which this rule applies. Note that these must be domains or email addresses associated with your account: for an outbound rule, this would apply to senders, and for an inbound rule it would apply to recipients. If you do not enter any information in this field, the rule applies to everyone.
4. Select the **Exclude certain senders/recipients** checkbox to specify domains, email addresses, or groups to exclude from the rule. The **Excluded recipients** and **Excluded senders** fields appear.

In the exclude fields, enter any domains or individual email addresses, or select the group to be excluded from this rule. If you do not enter any exclusion information, nobody is excluded from the rule.



### Note

For inbound and outbound lexical rules, you can create a list that excludes certain senders and a list that excludes certain recipients. For example, you can specify that a lexical rule does not apply if an email is from xyz@externaldomain.com or is sent to xyz@internaldomain.com. In all exclusion lists, you can enter up to 65,535 characters, consisting of domains, addresses, or groups, separated by commas.

5. In the **Phrases** field, enter one or more phrases for the rule to match against.

6. Select an action from the drop-down list. The following actions are available:
  - Quarantine message (optionally notify recipients, the postmaster, and/or others, with the selected notification messages, and select whether end users can view or release messages that contravene the lexical rule).
  - Encrypt the message (optionally notify the sender and/or others). This option is only available for outbound lexical rules, and if you have the Email Encryption module (see [Advanced encryption](#), page 115).
  - Forward message to a specific address.
  - Tag the subject with a specified phrase and deliver the message.
  - Blind carbon copy the message to another address.
  - Tag the subject, deliver it, and send a blind carbon copy to another address.
  - Deliver the message without any tags and keep a copy for checking.

**Note**

There is a quota for the number of messages that can be retained with the Keep Copy action. When you select Keep Copy or manage a lexical rule that uses Keep Copy, the used and available quota is displayed. If you exceed this quota, messages matching the Keep Copy criteria are logged in the Message Center, but you cannot read the message contents. To free space, delete some messages in the Message Center and then contact Support to have the lexical rule(s) using Keep Copy checked and re-enabled.

7. Define whether the rule should match against the message headers, or the whole message body and subject.
8. Click **Submit**.

## Creating a lexical rule in advanced mode

Cloud TRITON Manager Help | Cloud Email Protection Solutions

**Related topics:**

- ◆ [Filtering using lexical rules](#)
- ◆ [Creating a lexical rule in simple mode](#)
- ◆ [Managing dictionaries](#)
- ◆ [Advanced dictionary configuration](#)
- ◆ [Creating a compliance rule](#)
- ◆ [Phrase score and lexical rule thresholds](#)

The advanced mode for entering lexical rules enables you to match against system or custom dictionaries, and include multiple actions depending on the number of phrases matched. If you want to specify a single action to take when a message matches a phrase from a list, see [Creating a lexical rule in simple mode](#), page 97.

From this page, you can access the Dictionaries page to create or edit your custom dictionaries. For more information, see [Managing dictionaries](#), page 102.

**Note**

You can also manage dictionaries by going to **Email > Settings > Dictionaries**.

---

1. On the main Lexical Rules screen, click **Add Advanced Rule**. (To edit an existing rule, click the rule that you want to edit).
2. Enter a name for the rule and a description if desired.  
Note that the new rule is enabled by default. You can change this later if required.
3. From the **Dictionary** drop down box, select the dictionary you want to use for this rule.
4. In the **Include recipients or senders** field, enter the domain(s) or individual email address(es) or select the group to which this rule applies. Note that these must be domains or email addresses associated with your account: for an outbound rule, this would apply to senders, and for an inbound rule it would apply to recipients. If you do not enter any information in this field, the rule applies to everyone.
5. In the **Excluded recipients** and **Excluded senders** fields, enter any domains or individual email addresses, or select the group to be excluded from this rule. If you do not enter any exclusion information, nobody is excluded from the rule.

**Note**

For inbound and outbound lexical rules, you can create a list that excludes certain senders and one that excludes certain recipients. For example, you can specify that a lexical rule does not apply if an email is from xyz@externaldomain.com or is sent to xyz@internaldomain.com. In all exclusion lists, you can enter up to 65,535 characters consisting of domains, addresses, or groups, separated by commas.

---

6. Click **Submit**.  
The rule details are displayed. You can click **Edit** to change any of the details entered in the steps above, or to disable the rule.
7. Click **Add...** to tell TRITON AP-EMAIL what to do when a message matches entries in the dictionary. The Lexical Rule Action screen appears.
8. Specify a threshold, an action, and any notification options related to the selected action, then click **Add** to save your changes.

There are 7 different actions that can be performed on the email. You can therefore configure up to 7 different thresholds, each with a separate action:

- ◆ Quarantine message (optionally notify sender, recipients, and/or others with the selected notification messages).



---

**Note**

Once an email message is quarantined, no further actions can be performed on that message. Therefore, if you set a quarantine action at a certain threshold, any other action set at a higher threshold will fail.

---

- ◆ Encrypt the message (optionally notify the sender and/or others). This option is only available for outbound lexical rules, and if you have the Email Encryption module (see [Advanced encryption](#), page 115).
- ◆ Forward message to a specific address.
- ◆ Tag the subject with a specified phrase and deliver the message.
- ◆ Blind carbon copy the message to another address.
- ◆ Tag the subject, deliver it, and send a blind carbon copy to another address.
- ◆ Deliver the message without any tags and keep a copy for checking.



---

**Note**

There is a quota for the number of messages that can be retained with the Keep Copy action. When you select Keep Copy or manage a lexical rule that uses Keep Copy, the used and available quota is displayed. If you exceed this quota, messages matching the Keep Copy criteria are logged in the Message Center, but you cannot read the message contents. To free space, delete some messages in the Message Center and then contact Support to have the lexical rule(s) using Keep Copy checked and re-enabled.

---

For quarantined messages, you can also define whether end users can view or release any messages caught by this lexical rule from their end-user message report.

In the example above, inbound email is checked against a dictionary of offensive phrases to protect the intended recipient. Those that score 1.5 or above are quarantined. Email that scores 5 or above is likely to have matched multiple words or matched against words that have been allocated a higher score.

To help you choose an appropriate threshold for the actions you require, click **Show dictionary statistics** to display a statistical analysis of the selected dictionary. On the left side is a graphical representation of the distribution of scores in the dictionary. On the right side are a few statistics that may help you to choose a threshold.



---

**Note**

There is a limit on the number of regular expressions you can include in lexical rules for each policy. If your rules include a large number of regular expressions, it might restrict the ability of the service to process your email. A warning appears when you are nearing this limit, and once you exceed the limit, you cannot create or edit the lexical rule.

---

## Creating a compliance rule

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Filtering using lexical rules](#)
- ◆ [Phrase score and lexical rule thresholds](#)

TRITON AP-EMAIL includes dictionaries for 2 compliance standards:

- ◆ PCI Compliance isolates email messages that contain payment card information
- ◆ State Data Privacy Laws (SDPL) compliance isolates email messages that contain Social Security numbers

When you add a compliance rule, the dictionary, threshold score, and action are predefined. If you need to edit any of the default settings, you can do so after the rule has been created.

1. On the main Lexical Rules screen, click **Add Predefined Compliance**.
2. Select the compliance rule type you want to use.
3. To edit the rule's default settings, click the rule name.

From the resulting screen, you can edit the rule name, description, and the groups or users included in or excluded from the rule. You can also define different thresholds.

## Quarantining messages where lexical analysis does not complete

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Filtering using lexical rules](#)
- ◆ [Phrase score and lexical rule thresholds](#)

If lexical rule processing does not complete for a message, you can specify that it is quarantined immediately. This might occur if you have set up a large amount of lexical rules and regular expressions.

If you choose to quarantine a message of this type, you can examine it in the Message Center by searching for messages labeled Lexical Rule, with the subreason Analysis Failure. For more information, see [Message Center, page 121](#).

You can select different settings for inbound and outbound messages.

1. On the Content Filter tab, click **Edit** under either Inbound or Outbound.

2. Check the **Quarantine message if content analysis does not complete** box. If the box is not checked, any messages with incomplete lexical rule analysis are allowed through for further processing.
3. Click **Submit**.

## Managing dictionaries

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Excluding phrases from a dictionary](#)
- ◆ [Advanced dictionary configuration](#)
- ◆ [Phrase score and lexical rule thresholds](#)
- ◆ [Importing language packs](#)
- ◆ [Creating a lexical rule in advanced mode](#)

TRITON AP-EMAIL defines two types of dictionary: those that are pre-defined/published by Websense and your custom dictionaries. The former are maintained by Websense and include common profanities; dictionaries relating to categories such as finance, gambling, and shopping; and compliance rules for payment card information and Social Security numbers. You can exclude phrases from these lists (see [Excluding phrases from a dictionary](#), page 104) but you cannot include additional words or phrases; if you need to add phrases, system dictionaries can be embedded inside your own dictionaries.

Once defined, a phrase is available for use with both inbound and outbound lexical rules across all policies.

You can add 3 types of phrase to a custom dictionary:

- ◆ A simple string, for example “project rhine”.
- ◆ A complex multi-word search. This option searches on different variations of the phrase you define; for example if you enter “confidential email”, a lexical rule might match the exact phrase or any instances of the words “confidential” and “email” appearing close to each other in a message. See [Advanced dictionary configuration](#), page 104 for more examples.
- ◆ A regular expression.

Assign each phrase that you add a score. This is used to determine the disposition in a lexical rule: typically a higher score indicates a worse contravention of the rule. You can also select the following options instead of a numerical score:

- ◆ **Always trap this phrase** – assigns a score of +20 to the phrase, ensuring it always triggers the rule.
- ◆ **Always let through** – assigns a score of -20 to the phrase, ensuring that if it is matched, it never triggers the rule.

- ◆ **Ignore this phrase** – assigns a score of 0 to the phrase, ensuring it is never matched.

To add a new dictionary:

1. On the Dictionaries screen, click **Add Custom Dictionary**. (To view the contents of an existing dictionary or to edit a custom dictionary, click the dictionary name.)
2. Enter a name for the dictionary and a description if desired; then click **Add**. (If you are editing an existing name or description, click **Submit**.)
3. To include an existing dictionary:
  - a. Click **Attach dictionary**.
  - b. Select an existing dictionary from the drop-down list, then click **Submit**.

### Including simple phrases in a custom dictionary

1. Click **Attach phrase**.
2. In **Search type**, select **Simple substring search**.
3. Enter the phrase to add in the **Phrase** field, assign it a score, and indicate which parts of the message you want to apply it to.
4. Click **Submit**.

### Including complex searches

1. Click **Attach phrase**.
2. In **Search type**, select **Complex multi-word search**.
3. Enter the phrase to add in the **Phrase** field.
4. Assign a score to the phrase, and indicate which parts of the message you want to apply it to.
5. Click **Submit**.

### Including regular expressions

Regular expressions (Regex) are a powerful way of matching a sequence of simple characters. Using regular expressions in your dictionaries enables you to specify precise phrase matching for your email.



#### Note

Regular expressions are not case-sensitive.

---

For syntax and some examples, see [Standard Regular Expression Strings](#), page 179.

1. Click **Attach phrase**.
2. Click **Regex view**.
3. Enter the regular expression in the **Regex** field.
4. Enter a description for the regular expression. This description appears in the dictionary items list with “regex” next to it to signify that a regular expression was defined.

5. Assign a score to the phrase, and indicate which parts of the message you want to apply it to.
6. In the **Test against** field, enter some text that can test whether your regular expression is well-formed and meets your requirements, then click **Test regex**.
7. When you are happy with the regular expression, click **Submit**.

**Note**

To return to the simple substring search or complex multi-word search options, click **Simple phrase view**.

---

## Excluding phrases from a dictionary

Cloud TRITON Manager Help | Cloud Email Protection Solutions

You can exclude words or phrases from both system and custom dictionaries.

1. On the Dictionaries screen, click the dictionary name.
2. Under Dictionary Items, select the phrase you want to exclude.
3. Select a phrase exclusion option. If you choose to exclude the phrase within specific policies, select the policy or policies to apply the exclusion to.

You can select multiple items from each list by holding down the **Ctrl** key and clicking the items. To make selection easier, you can expand the list to appear in a larger window by repeatedly clicking on the **Grow list** link.

4. Click **Submit**.

The excluded phrase appears in the dictionary with a line through it.

## Advanced dictionary configuration

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Managing dictionaries](#)
- ◆ [Phrase score and lexical rule thresholds](#)

There are a number of techniques you can use for more advanced content filtering:

- ◆ If a pair of words must appear close to each other in the message, separate them with the NEAR keyword, for example, dear NEAR sir. By default, NEAR allows up to 8 words between the two phrases. To control the number of words allowed (the *nearness*), specify it inside square brackets after the NEAR keyword, for example, dear NEAR[2] sir.
- ◆ If the phrase consists of a set of words, on which any one can be matched, you can use the OR keyword. However, a better way of dealing with this situation is to



create a separate phrase for each word. For example, you can use bow OR bough but, more simply, you can create two phrases, one for bow and one for bough.

## Importing language packs

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Managing dictionaries](#)
- ◆ [Advanced dictionary configuration](#)

By default, you have access to the English language dictionaries. You can add other language dictionaries if you wish. Dictionaries are provided for the following languages:

- ◆ Dutch
- ◆ French
- ◆ German
- ◆ Italian
- ◆ Japanese
- ◆ Korean
- ◆ Portuguese
- ◆ Russian
- ◆ Spanish
- ◆ Traditional Chinese
- ◆ Simplified Chinese

To import an additional language pack or remove existing packs:

1. On the Dictionaries screen, click **Manage Language Packs**.
2. Select the language packs you want to use.
3. Click **Save**.



### Note

You cannot remove a language pack that is being used by a lexical rule. You must first remove all dictionaries in that language from your lexical rules.

---

## Encryption tab

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Standard encryption](#)
- ◆ [Advanced encryption](#)
- ◆ [Editing advanced encryption settings](#)

Select the **Encryption** tab to view or modify encryption policies.

Email encryption secures delivery of email by ensuring that it is not forwarded as plain text “in the clear.” TRITON AP-EMAIL Encryption encrypts the transport layer protocols being used to deliver the email at the edge of the network – the point where it leaves the secure environment of the local area network.

The following encryption functionality is available:

- ◆ Transport Layer Security (TLS) for secure enterprise-to-enterprise email communications (see [Transport Layer Security, page 106](#))
- ◆ Standard encryption rules for securing email to individuals (see [Standard encryption, page 112](#))
- ◆ Advanced encryption rules for secure identity-based encryption (see [Advanced encryption, page 115](#)). This option requires the Email Encryption module.

To add a secure transport policy setting or an encryption rule, click the relevant **Add** button.

## Transport Layer Security

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS for a connection or route](#)
- ◆ [Configuring TLS on your connections](#)
- ◆ [Configuring third-party TLS connections](#)
- ◆ [Testing an outbound connection](#)
- ◆ [When TLS fails](#)

TLS provides a transport layer encrypted “tunnel” between email servers or mail transfer agents (MTAs).

By default, TRITON AP-EMAIL always attempts to deliver or receive email using opportunistic TLS if the sending or receiving MTA supports it. With opportunistic TLS, if a connection attempt is made using the TLS protocol, the connection recipient must provide appropriate TLS credentials for an encrypted data transfer. If the TLS “handshake” fails, the data transfer is made via plain text, rather than encrypted text. In either case, the data transfer is successfully accomplished.

Alternatively, you can enforce TLS connections. There are 2 stages to configuring mandatory TLS:

1. Add security settings to the connections between your mail transfer agent (MTA) and the TRITON AP-EMAIL relays. See [Configuring TLS on your connections](#), page 108.
2. Add routes to the third-party MTAs with whom you want to communicate using TLS and add security settings to these.

When the conditions within the TLS policy are not met, TRITON AP-EMAIL does not deliver the email.

A full list of trusted certificate authorities and the encryption algorithms supported by TRITON AP-EMAIL are available as an article in the [Knowledge Base](#).

**Note**

TRITON AP-EMAIL can enforce TLS only on the immediate next SMTP hop. Situations may exist where TRITON AP-EMAIL does not deliver directly to recipients (e.g., they may be using a service similar to TRITON AP-EMAIL). In such situations, it is your responsibility to ensure that all intermediate SMTP hops support TLS. If this is outside of your control, we recommend you use the TRITON AP-EMAIL standard or advanced encryption functionality to provide secure delivery.

## Configuring TLS for a connection or route

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS on your connections](#)
- ◆ [Configuring third-party TLS connections](#)
- ◆ [Testing an outbound connection](#)
- ◆ [When TLS fails](#)

Similar configuration is required for both the connections between TRITON AP-EMAIL and your MTAs, and between TRITON AP-EMAIL and the third party MTAs that you wish to communicate with using TLS. These settings and the options are described below.

Each rule relates to a specific inbound or outbound connection and specifies whether TLS is enforced, a certificate is required and should be verified, and the encryption

strength. If an attempt is made to deliver an email and the specified criteria are not met, the email delivery fails and the sending MTA is notified.

## Configuring TLS on your connections

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS for a connection or route](#)
- ◆ [Configuring third-party TLS connections](#)
- ◆ [Testing an outbound connection](#)
- ◆ [When TLS fails](#)

The first stage of setting up a TLS policy is to configure the security settings on the connections between the TRITON AP-EMAIL relays and your email gateways. To do this:

1. Select the **Connections** tab.
2. Click the server name of the inbound or outbound email gateway that you want to configure.
3. Click **Edit**.
4. Add security and encryption strength settings to the connections on which you wish to enforce TLS. Typically these are the same inbound and outbound.



### Note

Inbound TLS settings apply to all inbound connections. If you have multiple MTAs receiving email from TRITON AP-EMAIL, all must be configured to use TLS.

---

## Configuring third-party TLS connections

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS for a connection or route](#)
- ◆ [Configuring TLS on your connections](#)
- ◆ [Testing an outbound connection](#)
- ◆ [When TLS fails](#)

You must add the connections to and from the businesses with whom you wish to communicate using TLS. To do so:

1. Select the **Encryption** tab.
2. Click **Add** in the Secure Transport section.

3. In the **Domain/Server** field, enter the IP address or fully qualified domain name of the business with whom you are establishing connection. For outbound connections, enter the recipient's domain. For inbound connections, enter a server name or IP address. Do not specify a server that is part of your MX records.  
Click **Check SMTP Connectivity** to confirm that you can connect to the domain name or IP address.
4. Select a direction for the connection: **Inbound** or **Outbound**.
5. Select a security level:

Security Level	Description
<b>Unenforced</b>	TRITON AP-EMAIL does not attempt to use TLS for this connection.
<b>Encrypt</b>	Delivery of a message fails (inbound or outbound) if the MTA with which it is communicating cannot use TLS to force an encrypted connection at the encryption strength configured for this connection or route. No certificate is required.
<b>Encrypt + CN</b>	As Encrypt but a certificate must also be presented on which the common name matches the MTA with which TRITON AP-EMAIL is communicating.
<b>Verify</b>	As Encrypt but the certificate must be from a trusted certificate authority (CA).
<b>Verify + CN</b>	As Encrypt + CN but the certificate presented must be from a trusted CA.

We recommend that you use Verify + CN, but you may opt to use Encrypt + CN if you want to use a self-signed certificate rather than paying for use of one from a CA. This may be acceptable for the connections between your MTA and TRITON AP-EMAIL.

6. Select a encryption strength:

Encryption Strength	Description
<b>128</b>	An encryption algorithm that supports a 128 bit key must be negotiated between TRITON AP-EMAIL and the MTA with which it is communicating.
<b>256</b>	An encryption algorithm that supports a 256 bit key must be negotiated between TRITON AP-EMAIL and the MTA with which it is communicating.



#### Note

You must ensure that the MTA supports the policy configured for its connections (certificate and encryption strength) and it must support an algorithm also supported by TRITON AP-EMAIL.

7. To enable the connection for TLS immediately, check **Enabled**.
8. Click **Save**

For outbound connections, we recommend that you check the TLS status of the server before enabling it. If you route mail to domains that do not support TLS, it will result in the non-delivery of your messages. For more information, see [Testing an outbound connection](#), page 110.

The companies with whom you want to communicate using TLS must ensure that their MTAs support one of the encryption algorithms supported by TRITON AP-EMAIL and the encryption strength that you configure in the policy. They must also be able to present a certificate appropriate to the policy that you configure.

**Note**

The third-party MTA must support the required configuration on the inbound and outbound connections or email delivery fails.

---

## Testing an outbound connection

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS for a connection or route](#)
- ◆ [Configuring TLS on your connections](#)
- ◆ [Configuring third-party TLS connections](#)
- ◆ [When TLS fails](#)

You can test an outbound TLS connection, because TRITON AP-EMAIL is responsible for initiating the connection.

1. Click a connection you have added to the Secure Transport section of the Encryption tab, then click **Check TLS status of server**. This brings up a test message using TLS. (Alternatively, click **Check** in the TLS Status column on the Encryption tab.)
2. Modify the test parameters if desired: the email address, the encryption strength, the security level.
3. From the drop-down list, select a service cluster from which to perform the test.
4. Click **Send**. The test results appear.

The response indicates whether or not TRITON AP-EMAIL was able to deliver the email in accordance with the configured policy. Note that if the service finds 2 MX records, it sends 3 messages. Check that all have arrived.

If the TLS check fails, check that the mail transfer agent (MTA) supports the settings in the policy.

## When TLS fails

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Configuring TLS for a connection or route](#)
- ◆ [Configuring TLS on your connections](#)
- ◆ [Configuring third-party TLS connections](#)
- ◆ [Testing an outbound connection](#)

TRITON AP-EMAIL does not deliver a message in the clear if the policy dictates that it should use TLS. If TLS cannot be used when dictated by the policy, TRITON AP-EMAIL rejects the message. The report that is returned to the sender is dependent upon their email server.

Condition	Action when TLS cannot be started	Message Center reporting for the log entry
You try to send email to TRITON AP-EMAIL from a connection specified as secure.	TRITON AP-EMAIL rejects the email with a permanent error. Your email server should send a non-delivery notification to the sender.	TLS (not verified) - message rejected
TRITON AP-EMAIL tries to send email to a third-party domain specified in the secure transport policy.	TRITON AP-EMAIL rejects the email with a reason “cannot start TLS”. Your email server should send a non-delivery notification to the sender.	Email is shown as “clean” because it was accepted from the customer, but the log indicates that onward delivery failed.
A third party tries to send email to TRITON AP-EMAIL from a connection specified in the secure transport policy.	TRITON AP-EMAIL rejects the email with a permanent error. The third party’s email server should send a non-delivery notification to the sender.	TLS (not verified) - message rejected
TRITON AP-EMAIL tries to send an email to you through a connection specified as secure.	TRITON AP-EMAIL rejects the email with a reason “cannot start TLS”. The third party’s email server should send a non-delivery notification to the sender.	Email is shown as “clean” because it was accepted from the third party, but the log indicates that delivery failed.

## Adding an encryption rule

Cloud TRITON Manager Help | Cloud Email Protection Solutions

There are 2 types of encryption rule available in TRITON AP-EMAIL:

*Standard encryption* is typically used to enforce encryption policy when the recipient’s MTA does not support TLS. This functionality relies on a TLS connection with you to secure communications between your MTA and TRITON AP-EMAIL. Recipients require a manually-generated password to access the encrypted email.

*Advanced encryption* uses identity-based encryption (IBE) to protect data without the need for certificates. Protection is provided by a key server that controls the mapping of identities to decryption keys. The recipient of an encrypted email authenticates against the key server to receive the decrypted version of the message.

To enable advanced encryption, you must have the Email Encryption module, and you must set the security on your outbound connection routes to Verify+CN. See *Connections tab*, [page 67](#).

## Standard encryption

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Password specification](#)
- ◆ [Notifications](#)
- ◆ [Accessing email](#)
- ◆ [Combining standard encryption with content filtering rules](#)
- ◆ [Advanced encryption](#)

Standard encryption comprises rules that, when matched, trigger the standard functionality process. This process is as follows:

1. Sender sends email that triggers the rule.
2. The email is saved to the Encryption service quarantine store.
3. The recipient is sent an email notification containing an encrypted link that when clicked allows access to the Encryption service quarantine store by HTTPS.
4. The sender is sent one or more notifications, depending on the number of recipients. Each notification contains a password that is required by a recipient to access the email. The sender needs to notify the recipient(s) of their password.

The criteria for the “parking” rules can include:

- ◆ Sender addresses
- ◆ Recipient addresses
- ◆ Messages marked as “sensitive” in the email headers
- ◆ Messages including a pre-defined prefix (trigger word) in the subject line.

To set up standard encryption, click **Add** in the Encryption section of the **Encryption** tab.

1. Enter a name for the encryption rule, and select **Standard Encryption** as the encryption type.
2. Define the password generation criteria (see [Password specification](#), [page 113](#)).



3. Optionally, enter one or more senders or recipients for the rule to apply to. These can be individual email addresses, groups configured in TRITON AP-EMAIL, or domain names. You can enter multiple senders or recipients, separated by commas.

To edit an existing sender or recipient, click the item. Press **Enter** to save your changes as a new entry in the sender or recipient list. To discard your changes, press **Esc**.

To remove an item from a sender or recipient list, click the Delete icon next to the item.

4. If you are including subject criteria in the encryption rule, select whether the message should match any of the criteria, or all of the criteria you select to trigger the rule.
5. To include messages with a sensitivity setting in the email headers for encryption, mark **The message contains a sensitivity header**, and select an option from the drop-down list. If you want the rule to match against all sensitivity headers, select **Any**.
6. To define a trigger word that appears at the beginning of the subject line for messages to be encrypted, mark **The subject starts with** box, and enter the trigger word.

**Note**

A trigger word is not case sensitive and **MUST** be followed by a space.

---

7. If required, edit the notifications sent to sender and recipient (see [Notifications](#), page 114).
8. Click **Submit**.

When an outbound email meets all of the specified criteria, the email is subjected to the standard encryption process.

## Password specification

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The password can be automatically generated by the system or specified in the subject of the email.

**Automatic password generation:** This occurs if **Allow sender to specify a password** is not checked.

If **Allow sender to specify a password** is checked, the user must include the password in the subject line of the email. There are two options for inclusion:

1. If the rule specifies a trigger word, the password follows this in the subject line.
2. If the rule does not specify a trigger word, you must add a prefix that is used to identify the password in the **subject prefix** field. Note this is different from the trigger in that it is not a criterion for rule execution.

Both the prefix and password must be followed by a space and the password must be enclosed in parentheses ( ). Both are stripped from the email by TRITON AP-EMAIL.

For example, to trigger standard encryption with a specified password from a message with the following subject:

TRI TON AP- EMAI L test of standar d encrypt i on

You would augment the message subject as follows:

ENCRYPT ( xyz987) TRI TON AP- EMAI L test of standar d encrypt i on

**Note**

The **subject prefix** field is available only when the **Where the subject begins with** box is not checked.

---

## Notifications

Cloud TRITON Manager Help | Cloud Email Protection Solutions

When an email is “parked,” the sender and recipient(s) are notified by email. The notification sent to the recipient(s) includes a link to the cloud service portal from where the message can be retrieved. The notification(s) sent to the sender includes a password that the sender must communicate to the recipient(s). The recipient(s) needs this password in order to retrieve the message. To set up notifications, open the standard encryption rule (click the name of the rule in the Encryption section of the **Encryption** tab), then edit the **Sender** or **Recipient** text under **Notifications**.

Both sender and recipient notifications can be fully customized on a per-rule basis, in both plain text and HTML format.

## Accessing email

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To access a parked message, the recipient clicks the link, accesses the cloud service portal using HTTPS, and is prompted to enter a password.

**Parked message**

Please enter the password supplied to you by the sender of this message.

Password:

Once recipients enter a password, a message is shown. They can access each part of the message and download any attachments. The message itself can be downloaded and viewed by an email client that supports a MIME type message/rfc822.

## Combining standard encryption with content filtering rules

Cloud TRITON Manager Help | Cloud Email Protection Solutions

To guard against end users inadvertently sending unsecured sensitive data outside your organization, you can set up a lexical rule that triggers standard encryption for any message that matches against that rule.

For example, from the **Content Filter** tab set up a predefined PCI compliance rule (see [Creating a compliance rule](#), page 101), and then edit it to include the Tag subject action at a threshold you choose. Tag the subject line with a phrase such as “Encrypt”.

Next, click **Add** in the Encryption section of the **Encryption** tab. In the **The subject starts with** field, enter the phrase you chose to tag the subject line.

When the standard encryption rule is set up, this ensures that a message matching against the compliance rule is parked for secure HTTPS retrieval by the recipient, with notifications going to the sender and recipient as configured in the encryption rule.

## Advanced encryption

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Editing advanced encryption settings](#)

If you have the Email Encryption module, you can send messages that use identity-based encryption, with no need for users to manually exchange passwords. You can also customize the email notification that the recipient sees before decrypting the message.

- ◆ [Prerequisites for advanced encryption](#)
- ◆ [How advanced encryption works](#)
- ◆ [Adding an advanced encryption rule](#)

### Prerequisites for advanced encryption

To use advanced encryption, you must have a TLS certificate on the server designated as an outbound connection. This certificate must meet the following requirements:

- ◆ The certificate is issued by a supported certificate authority. For a list of supported CAs, see the Knowledge Base article “What are the trusted Certificate Authorities?”.
- ◆ Wildcard certificates are supported, but Subject Alternative Name (SAN) certificates are not.
- ◆ The Subject CN of the certificate must match the outbound connection’s fully-qualified domain name (FQDN).

In addition, note the following requirements for your TLS connection:

- ◆ The sending IP address must resolve to the outbound connection’s FQDN.
- ◆ The outbound connection’s FQDN must resolve to the sending IP address.

- ◆ Your MTA's sending HELO string must match the outbound connection's FQDN.

For more information about TLS, see [Transport Layer Security](#), page 106.

## How advanced encryption works

When an advanced encryption rule is matched, the following process takes place:

1. Sender sends email that triggers the rule.
2. The email is encrypted by TRITON AP-EMAIL using identity-based encryption, and sent on to the recipient's MTA for delivery.
3. The recipient is sent an email notification containing an HTML attachment. When opened in a browser, the attachment displays a button that the recipient clicks to access to the secure encryption network via HTTPS. The recipient must register their email address and a password with the secure encryption network if this is the first time they have received an encrypted message via TRITON AP-EMAIL. The recipient then uses this password to access all subsequent encrypted messages sent to their email address.
4. If the recipient replies to the encrypted message, the message is decrypted by TRITON AP-EMAIL and then analyzed in the same way as other inbound mail before delivery.

There are 3 ways to use advanced encryption:

- ◆ **Content-based.** Set up lexical rules so that a message will automatically be encrypted if it contains certain phrases. See [Creating a lexical rule in advanced mode](#), page 98.

Note that if a message triggers a lexical rule with a Quarantine action and a rule with an Encrypt action, the Quarantine action will take precedence and the message will be quarantined without encryption.

If a message triggers a rule with the Encrypt action and a rule with either Forward, Tag Subject, BCC, or BCC and Tag Subject, the Encrypt action will take precedence and the other action(s) will not be applied.

If a message triggers lexical rules with the Encrypt and Keep Copy actions, both actions will be applied.

- ◆ **Sender/recipient-based.** Set up an advanced encryption rule that encrypts a message sent from or to specific users.
- ◆ **Subject and content-based.** Set up an advanced encryption rule that encrypts a message with a certain trigger word in the subject header, a particular sensitivity header, or specific phrases in the message headers or body.

You can combine these methods to configure the encryption policy that you require.

Advanced encryption integrates with other aspects of your email policy as follows:

- ◆ If you have set up attachment parking, an attachment that meets the parking criteria will be parked before the message is encrypted. The decrypted message will contain a link to retrieve the attachment. See [Parking attachments](#), page 92.

- ◆ If you have outbound aliases, the aliases will be applied before the message is encrypted. The resulting encrypted message will always show the external address.

## Adding an advanced encryption rule

To set up sender/recipient-based or subject and content-based advanced encryption, click **Add** in the Encryption section of the **Encryption** tab.

1. Enter a name for the encryption rule, and ensure **Advanced Encryption** is selected as the encryption type.
2. To notify the message sender when a message has been encrypted, mark **Notify sender**. You can also notify others by entering a comma-separated list of email addresses.
3. Optionally, enter one or more senders or recipients for the rule to apply to. Recipients can be either specifically included in or excluded from the rule.  
  
You can enter individual email addresses, groups configured in TRITON AP-EMAIL, or domain names. You can enter multiple senders or recipients, separated by commas.  
  
To edit an existing sender or recipient, click the item. Press **Enter** to save your changes as a new entry in the sender or recipient list. To discard your changes, press **Esc**.  
  
To remove an item from a sender or recipient list, click the Delete icon next to the item.
4. If you are including subject criteria, content criteria, or both in the encryption rule, select whether the message should match any of the criteria, or all of the criteria you select to trigger the rule.
5. To include messages with a sensitivity setting in the email headers for encryption, mark **The message contains a sensitivity header**, and select an option from the drop-down list. If you want the rule to match against all sensitivity headers, select **Any**.
6. To define a trigger word that appears in the subject line for messages to be encrypted, mark **The subject** box, and select whether the trigger word is at the start of the subject or is contained anywhere in the subject line. Then enter the trigger word.



### Note

A trigger word is not case sensitive and **MUST** be followed by a space.

---

7. To specify phrases that trigger encryption if contained in a message, mark **The message contains any of the following phrases**, and select whether the phrases appear in the message body or headers.  
  
Enter each phrase on a new line, by pressing **Enter** after each phrase. The phrases are not case sensitive.
8. Click **Submit**.

## Editing advanced encryption settings

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Use the Advanced Encryption Settings area of the **Encryption** tab to fine-tune the content of the email notification template delivered to recipients. For example, you might want to include your organization name, and a contact method in case the recipient has trouble accessing the message.

A Websense logo appears in the email notification by default. You can replace this logo with a custom version, for example the logo of your organization. The logo must be hosted at a URL that will be accessible by all encrypted message recipients, such as your company website.

You can also add annotations to the decrypted message, and define the action to take on messages that have already been encrypted before being sent through TRITON AP-EMAIL.

1. Under Advanced Encryption Settings, click **Edit**.
2. To include an annotation at the end of the decrypted message, select **Add annotations to the inbound decrypted message**.  
Click the **annotations** link to edit the annotation (see [Editing an annotation](#), page 62).
3. Select **Quarantine messages that are already encrypted** if you want to quarantine outbound messages that have been encrypted using a different method, for example S/MIME.  
If you do not select this option, outbound messages that have been encrypted using a different method are processed without adding advanced encryption.
4. To replace the Websense logo in the notification template, select **Use custom logo**, and enter the URL where the custom logo is located.
5. Select **Add custom text to encrypted message template** to include your own text in the email notification sent to recipients.  
Enter the text in the field below the check box. Note that HTML tags are not supported. The text appears in the email notification in addition to the standard text that explains how to access the encrypted message.
6. If required, specify the language in which to display the standard text of the email notification. The following languages are available:
  - Czech
  - Dutch
  - English
  - French
  - German
  - Greek
  - Italian
  - Polish
  - Portuguese (Brazilian)

- Portuguese
- Romanian
- Slovak
- Spanish
- Swedish

7. Click **Submit**.





# 6

## Message Center

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Understanding your results](#)
- ◆ [Performing actions on the results](#)
- ◆ [Viewing message details](#)

The TRITON AP-EMAIL Message Center is a powerful message tracking and management tool that provides access to all quarantined messages and message logs for your account.

It is available only if you are licensed for .

To access the Message Center, select **Email > Messages > Message Center**. You are presented with a search form.

The search form lets you search for messages based on several layers of search criteria, such as the From, To, or Subject fields, the date sent, whether the message contained spam or a virus, and much more. The check box controls allow a granular search for clean email and/or those with an issue that caused TRITON AP-EMAIL to perform an action.



### Note

Enter as much detail as possible to minimize the data returned and so reduce the time that the search takes. This is especially important for large accounts.

## Search

Select the type of message for which you are looking. If you search for accepted messages, only clean messages are returned; if you search for quarantined messages, only quarantined messages are returned. You can also search for messages that have had certain actions performed on them, for example messages that have been released, forwarded, or deleted from quarantine. Information on deleted messages still appears

in the search results, even though they have been deleted from the quarantine itself and cannot be viewed.



#### Note

To display deleted messages you must search for them specifically from the search drop-down list, or check the **Show deleted messages** box.

---

## Show

Once a message is viewed by an end user or administrator, it is marked as reviewed. If an end user has viewed a multi-recipient message, it is shown as partially reviewed. If an administrator views a multi-recipient message, it is shown as reviewed for all recipients.

## Date sent

You must specify a date range to search. The more exact the date range, the faster a search completes. The default drop-down list allows you to choose common ranges; for more exact time ranges, click **more** and use the calendar picker.

Clicking **more** reveals the date range. From here you can specify exact dates and times (by the hour) to search. Click the calendar icon to open the calendar picker. Choose the date of interest by clicking the relevant date link. This closes the pop up and populates the appropriate field with the date. You can select the To and From hour from the drop-down lists. The default is to search all hours in the selected day.

## From

The sender of the email; you can include a wildcard in the search by entering an asterisk (\*) character to denote multiple characters.

## To

The recipient of the email; you can include a wildcard in the search by entering an asterisk (\*) character.

## Subject

The email subject; you can include a wildcard in the search by entering an asterisk (\*) character.

## Email direction

Select the direction to search: Inbound, Outbound, or Both.

When you select Outbound, the *Delivery status* drop-down appears if TLS reporting is enabled for your account.

## Results per page

The number of results to display per page.

## Show deleted messages

Indicate whether you want deleted messages to be included in the search results.

## Delivery status

Select the delivery status for outbound messages. The default is to search for all messages; you can filter on messages delivered with TLS, delivered without TLS, pending delivery, or delivery failed.

This option only appears if TLS reporting is enabled for your account and you select Outbound for the email direction.

## Clean

Indicate whether you want uninfected, non-spam messages to be included in the search results.

## General

<b>Access control</b>	Messages blocked by an access control policy. This applies only to customers that have been asked to implement access controls by TRITON AP-EMAIL operations.
<b>Operational</b>	Messages blocked by controls set up by TRITON AP-EMAIL operations in response to a virus outbreak.
<b>Message loop</b>	Messages stopped automatically because they are part of a message loop caused by auto-forwarding or auto-replying.
<b>System</b>	Messages that could not be processed, for example, messages that contravene email protocols.

## Antivirus

<b>Virus</b>	Messages that contain known viruses as identified by one of the commercial antivirus engines used in the TRITON AP-EMAIL service.
<b>Macro</b>	Messages that contain highly suspicious Microsoft Office document macros that operate outside the document, that you have chosen to quarantine under your policy.
<b>Blocked executable</b>	Messages that contain an executable file attachment that you have chosen to quarantine under your policy.
<b>Phishing</b>	Messages that are suspected to be phishing emails.

## ThreatSeeker

<b>Format</b>	Messages that deliberately attempt to expose vulnerabilities in email software with unusually formatted headers or body.
<b>Dangerous content</b>	Messages that contain potentially dangerous content.
<b>Greylisted</b>	Messages that contain executable content that is temporarily quarantined awaiting confirmation that it is safe for automatic release.
<b>Potential viruses</b>	Messages that contain potential viruses, identified by ThreatSeeker but not yet identified by one of the commercial antivirus analyzers used within the TRITON AP-EMAIL service.
<b>Confirmed viruses</b>	Messages that contain a virus, identified by the ThreatSeeker Network and subsequently confirmed by one of the commercial antivirus analyzers.
<b>ThreatScope</b>	Messages that have been analyzed by ThreatScope. You can refine this further by selecting a ThreatScope status from the drop-down list: choose from All, Clean, Malicious attachment(s), Malicious and pending further analysis, and Pending analysis.

## Antispam

<b>Spam</b>	Unsolicited bulk messages. You can select a maximum and minimum spam score range to narrow this search further.
<b>Blacklisted</b>	Messages that have been blacklisted by the default or per-user policy.
<b>Whitelisted</b>	Messages that have been whitelisted by the default or per-user policy.
<b>Bulk</b>	Outbound messages that have been classified as bulk messages.
<b>Commercial bulk email</b>	Inbound messages that have been classified as commercial bulk email by the default or per-user policy.

## Content Filter

<b>Too large</b>	Messages that exceed any size limits defined by the policy.
<b>Extension masked</b>	Delivered messages that contain an attachment whose file extension was masked as specified in the content filtering policy. You can restrict searches to one or more specific extensions by listing them in the associated field, separated by commas.
<b>Blocked attachment</b>	Messages that have been quarantined due to their file type being specified in the content filtering policy. You can restrict searches to one or more specific extensions by listing them in the associated field, separated by commas.

<b>Lexical rule</b>	Messages that have contravened a lexical rule in the content filtering policy. You can restrict searches to specific subreasons - either messages caught by the lexical filter or messages that have experienced analysis failure - by selecting the relevant option from the drop-down list.
<b>Blocked images</b>	Messages that contain an image attachment that has been analyzed and is considered inappropriate. Messages with this status may also have been quarantined because the image could not be analyzed, for example because it was too large. This option only appears if you are licensed for image analysis.
<b>Copy kept</b>	Messages marked as available for delivery, but with a copy kept for review by administrators. If you have exceeded your quota for this type of message, the message delivery is logged, but you cannot view the content. To free quota space, delete some messages. Note that messages with this status may also have been caught by the lexical filter and quarantined for other reasons.

## Encryption

<b>TLS</b>	Messages that policy dictates should be delivered using TLS whose delivery failed because the sender attempted to send them in the clear.
<b>Ad hoc</b>	Messages that triggered a standard encryption policy rule.
<b>Advanced</b>	Messages that triggered an advanced encryption policy rule. This option only appears if you have enabled advanced encryption.

## Understanding your results

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The query is hidden once a search has returned results. To show the query again, click **Show Query** near the top left of the page. The search results are explained below:

<b>Field</b>	<b>Description</b>
<b>From</b>	The sender of the email.
<b>To</b>	The recipient of the email. If there is more than one recipient, the number of recipients is shown and, if you hover your mouse over the area, a popup appears listing up to 10 recipients. Open the message to see all the recipients.
<b>Subject</b>	The subject of the email. If the subject is long, it is truncated by ellipses (...). If you hover your cursor over the area, a pop-up appears. Click the subject to view a detailed log for the message.
<b>Date / Time</b>	The date and time of the email in your local time zone. If you hover your cursor over the area, a pop-up shows you the time in UTC.
<b>Spam Score</b>	The score assigned by TRITON AP-EMAIL .

Field	Description
<b>Issue</b>	The issues applicable to the email. If you hover your cursor over the area, a pop-up gives more information on the issues.
<b>Action</b>	The action(s) applied to the message. If you click the <b>Action</b> link for a message, you can view other actions that may have been applied to the message. Possible actions are listed below this table.

### Possible Actions

- ◆ **Accepted** - The email was accepted and delivered.
- ◆ **Quarantined** - The email was quarantined for the reason described by the issue.
- ◆ **Released** - The email was quarantined, but a copy of the email has since been released to the recipients.
- ◆ **Release-pending** - The email was quarantined and a copy of the email has been requested to be released to the recipients.
- ◆ **Release-failed** - The email was quarantined and a release action was requested but it has failed.
- ◆ **Forwarded** - The email was quarantined, but a copy has since been forward to a specified email address.
- ◆ **Forward-pending** - The email was quarantined and a copy has been requested to be forwarded to a specified email address.
- ◆ **Forward-failed** - The email was quarantined and a forward action was requested but it has failed.
- ◆ **Multiple** - The email was quarantined and has had multiple actions performed on it; to see a description of these actions, hover your mouse over the multiple text and a pop-up appears. Multiple actions might include “released” and “forwarded”.
- ◆ **Deleted** - The email was quarantined and has now been deleted. It still appears in the search results, but the message itself has been deleted from the system. Clicking the message reveals the message log, rather than the message itself.
- ◆ **Discarded** - TRITON AP-EMAIL discarded the message but did not report this to the sending email server which believes the message was delivered.
- ◆ **Rejected** - TRITON AP-EMAIL rejected the message and reported this to the sending email server.

## Reviewed and Not Reviewed Messages

Messages that have been reviewed are displayed differently from those that have not been reviewed. Reviewed messages appear in a slightly lighter shading and have an open envelope icon by them. Messages that are not reviewed have a darker shading and a closed envelope icon next to them. Messages can also be partially reviewed by end users from their end-user message report (EUMR). These messages are shown as a partially opened envelope icon.

## Downloading CSV results

You can download a comma-separated values (CSV) file of results from your query for use by other programs such as Excel to generate graphs or analyze the results in greater detail. The CSV download includes all instances of the messages per recipient.

**Note**

CSV downloads are limited to 50,000 lines.

## Performing actions on the results

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If you have permission, you may perform actions on the messages. The message center allows you to review, release, forward, and delete one or more messages.

To select a message, select the checkbox next to the envelope icon for that message. To select all messages on the page, click **Select All** in the header bar of the search results. Messages on other pages of the result set are not affected.

Having selected a set of messages, you can select the required action from the action bar drop-down list and click **Go**. When the operation is complete, the “Action” column for the message is updated; and if the message was previously marked as “Not Reviewed,” its status changes to “Reviewed.” If any errors occur during the action, they are displayed at the top of the page.

You can also perform actions on a message from the message’s details page. For more information, see [Viewing message details, page 129](#).

The available actions are explained below.

Action	Description
<b>Release</b>	Releases a copy of the message to continue processing.
<b>Release (no further processing)</b>	Releases a copy of the message directly to the intended recipient, bypassing any further rules that you have set up for your inbound or outbound mail. We recommend that you review the message carefully before selecting this action.
<b>Forward To</b>	Forwards a copy of the message to the email address you specify. Note that this sends the message for further processing before delivery.
<b>Forward (no further processing)</b>	Forwards a copy of the message to the email address you specify, bypassing any further rules that you have set up for your inbound or outbound mail.
<b>Mark as Reviewed</b>	Indicates this message has been reviewed.

Action	Description
Mark as Not Reviewed	Use this to indicate that you have not yet read this message.
Delete Message	Deletes the message from the message center.

## Release and forward actions

Release and forward actions performed on a message via the Message Center are executed asynchronously by a separate process. All other actions execute immediately. For example, if a release action is requested, the message is marked as **release-pending** until the request is completed. It is then be marked as **released**. If the release fails it is marked as **release-failed**. Similar action states apply to forward actions. This functionality can be applied to multiple messages.

In order to view pending or failed requests, it is possible to search for these states via the **Search** drop-down list. Possible action states are as follows:

- ◆ Released
- ◆ Release-pending
- ◆ Release-failed
- ◆ Forwarded
- ◆ Forward-pending
- ◆ Forward-failed



### Note

Actions can be performed only on messages that are in quarantine and have not been marked as deleted.

---

## Action limitations

You cannot request a new forward action on a specific message until the previous forward action has completed. Similarly, you cannot request a release action for a specific message until the previous release action has completed.

In order to check for successful completion of an action, you must perform a fresh search.

## Message actions page

Cloud TRITON Manager Help | Cloud Email Protection Solutions

A **Message Actions** page displays the actions applied to an individual message. This is accessed by clicking the **Action** for a message on the **Message Center Results** screen.



The Message Actions screen shows general information about the message and details of actions that have been applied to the message and the order in which they were applied.

## Viewing message details

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Click on a message subject to view details for that message.

This page explains why a quarantined message was blocked or if a message was classified as commercial bulk email and includes the message headers, message text, and details of any attachments. If the message has been analyzed by ThreatScope and found to be suspicious, the page includes a link to the ThreatScope report. From this page you can perform the actions described in [Performing actions on the results](#).

If you want to release or forward a message from this page, clicking **Release** or **Forward** sends the message for any further processing before delivery. If you want to bypass any other processing rules that you have set up and deliver the message directly to its recipient, check the **No further processing** box before releasing or forwarding. We recommend that you review the message carefully before doing this.

For quarantined messages, you can also choose to whitelist or blacklist the sender's email address or domain. When you do this, the black- or whitelisted item becomes a per-user antispam policy within the email policy that applies to the intended message recipient. For more information, see [Antispam exceptions](#), page 84.

## Viewing logs

Click **View log** to see full details of the message processing and results. The log appears at the bottom of the message details page.

For a quarantined message, the log details provide the exact reasons for the quarantine. For example:

- ◆ For messages quarantined due to a virus, the log lists the virus name.
- ◆ For blocked attachments, the log includes the file type or class that matched against the attachment.
- ◆ For blocked images, the log includes a thumbnail of the image. See [Managing quarantined images](#), page 130.
- ◆ For lexical rule failures, the log lists the phrase that triggered the quarantine.

If email is classified as commercial bulk email, the message details page may also contain log lines indicating the action taken:

- ◆ Commercial bulk message subject tag added for <recipient>.
- ◆ Commercial bulk message quarantined for <recipient>.

- ◆ Commercial bulk message detected and allowed due to policy settings for <recipient>.



**Note**

You cannot view logs for discarded messages.

---

## Managing quarantined images

---



**Note**

You must have the Image Analysis module to use this feature.

---

If a message has been quarantined due to an inappropriate image attachment, a thumbnail of the image appears under Blocked Images at the end of the message log details. Note that you must have the “View Quarantine Images” permission to access these images.

If you consider a quarantined image to be acceptable, you can add it to the image white list by clicking **Add to white list** under the thumbnail. If the image is already in the white list and you wish to remove it, click **Remove from white list**.



**Note**

We recommend that you only add images to the white list that are likely to cause the repeated quarantining of messages.

---

The image white list can contain a maximum of 200 images; if you have already reached this limit, the **Add to white list** option is greyed out.

For more information on the image white list, see [Image white list](#), page 57.

# 7

## Email Reporting

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Downloading report results](#)
- ◆ [Reporting periods](#)
- ◆ [Categorized reports](#)
- ◆ [Email report list](#)
- ◆ [Account Reports](#)

The TRITON AP-EMAILreporting functionality provides you with the tools to report on security and usage.

Go to **Reporting > Email Reporting** to see the email reports that are available. Depending on your subscriptions, you may see: Volumes, Inbound, Outbound, Address, Virus, Spam, and Content.

For more information on these specialized reports, refer to [Categorized reports](#), page 133. To see what a specific email report contains, see [Email report list](#), page 136.

Reporting allows you to:

- ◆ Monitor service performance
- ◆ Monitor traffic volumes and patterns for capacity planning purposes
- ◆ Identify areas for potential future investment in other communication technologies
- ◆ Enforce your email acceptable use policy
- ◆ Isolate and resolve problems

All reports are generated in real time using the Cloud TRITON Managerportal. Most include charts and tables that are presented in an easy to read, printable format.



### Note

For larger accounts, where a lot of data is to be retrieved, the reports may take some time to generate. As soon as the relevant data has been retrieved it is displayed while the remainder of the report is being compiled.

Commonly-used report criteria can be saved for easy access. For more information, see [Saving reports](#), page 134. Saved reports can be scheduled for regular delivery to one or more recipients as described in [Scheduling categorized reports](#), page 135.

## Reporting periods

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Reports can be generated for periods of hours to years. When accessing a report, you can drill down from within the report to a shorter time period. For example, an email volumes report for 7 days returns a table of volumes by day and a corresponding bar chart. By clicking a link on the relevant day on the table or chart, the report drills down and provides an hourly table and chart for that day. This allows not only the creation of management reports, but also reactive tracking of day-to-day issues.

You can select the reporting period from the drop-down list or you can click **more** to select absolute From and To dates and times. The available dates and times are dependent on the type of report and the availability of the data.

## Downloading report results

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

On each report, you have the option to download the data as a PDF or CSV file.



### Note

You can also download charts as image files or in PDF format. To download a chart, right-click the chart and select the format to download (PDF, PNG, or JPEG).

---

## Downloading a CSV file

You can download the statistics for the majority of reports as a comma-separated values (CSV) file. This allows you to import it into a third-party application, such as Microsoft Excel, for viewing and manipulation. On each table of results, click **Download CSV** to begin the download.



### Note

For some email reports, the totals in the CSV file might be higher than the totals in the report on screen. This is because the generated reports contain 1 line per email message, whereas the CSV version contains 1 line per recipient which means that a single email message might appear several times.

---

## Downloading a PDF file

Report results can be output to Portable Document Format (PDF) for easy distribution or printing. The PDF report is generated by clicking the **Download PDF** button on a table of results.

## Categorized reports

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Saving reports](#)
- ◆ [Scheduling categorized reports](#)

To access an email report:

1. Go to **Reporting > Email Reporting**.
2. Select a report category from the navigation pane.
3. Select a report from the **Show** drop-down list.

The reports you see depend on your subscriptions.

Initially you can access only the **Selection** tab to enter selection criteria. Once you have generated a report, you can click the **Chart** and **Table** tabs to view the results in chart or table form.

For most reports, you can select filtering criteria that restricts the report results. Next to each of the filtering criteria is a note describing in more detail how to use that option.



### Note

If your account is enabled for filtered reporting, you may only be able to view reports that filter on certain policies. See [Configuring permissions](#), page 12.

When you select a report, you are shown a list of the time periods for which the report is available. Alternatively you can select a specific time period (from and to) for the report by clicking **more** next to the period list.

To make selection from some criteria lists easier, you can expand the list to appear in a larger window by repeatedly clicking on the **Grow list** link.

Once you have decided on the report and the appropriate criteria, click **Generate report**. You may receive feedback at this point advising that the report might take some time to generate. Typically this is due to the amount of data that must be

searched. You can often avoid this by adding more criteria to narrow the search. Click **Back** if you want to cancel the report.

## Report results

Most report results are displayed in chart and table format in the relevant screen. Note that not all reports are available in both formats.

## Drilling down

Many of the reports contain links to more detailed reports. For example, for time-based reports, clicking the chart column or data table entry for a day generally displays the hourly report for that day, using any filtering criteria that applied to the original report.

Some reports allow you to drill down into the data in a more flexible way. If this is the case, there is a drop-down list above the chart and data table listing the available views. Select the view required from the list and then click the chart or table to display the new report.

## Saving reports

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Scheduling categorized reports](#)

You can choose to save any categorized report. Use this option to identify the reports you generate most frequently and want to be able to locate quickly.

To see the list of reports that you have saved, select **Reporting > Account Reports > Saved Reports**.

To save a report:

1. Select the email report you want.
2. Use the **Selection** screen to enter your report criteria as described in [Categorized reports](#), page 133.
3. Click **Save report**.
4. Enter a name for the report, and click **Save**.

The Saved Reports list is displayed, and the report you entered is now listed.

As well as accessing the report from this screen, you now have the option to delete the saved report or schedule it for regular delivery.

## Scheduling categorized reports

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

◆ [Saving reports](#)

You can run reports as they are needed, or you can define a schedule for running one or more saved reports.

Reports generated by scheduled jobs are distributed to one or more recipients via email. The reports can be in HTML, PDF, or CSV format. There is a limit on the number of reports you can schedule for delivery: the Saved Reports list displays the remaining number you can schedule in addition to any existing deliveries.



### Note

You cannot schedule reports that have defined start and end dates, or that span periods of less than 24 hours.

To schedule a report:

1. Select **Reporting > Account Reports > Saved Reports**.
2. You can schedule an existing saved report by clicking the report you want to schedule on the Saved Reports list. If you do this, skip to step 5 below.  
Otherwise, to create a new report for scheduling, click the **Generate a new report** link. The page that appears includes only reports that are eligible for scheduling.
3. Create and save your report as described in [Saving reports](#), page 134.
4. On the Saved Reports list, click the name of your new report.
5. Click **Schedule email report**.
6. Enter the email address of the report recipient. Multiple email addresses should be separated by commas or spaces.  
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
7. Enter a subject for the report email, and the text you want to appear in the body of the email.
8. Select the report format.
9. Set one of the following delivery periods for your reports:
  - daily
  - weekdays
  - weekly
  - every other week (biweekly)
  - monthly (the default option)

If you want to stop the a scheduled report temporarily, select **suspend delivery**.

10. Click **Save**.

You are returned to the Saved Reports list. Reports that have been scheduled display the recipient list in the **Email to** column. Click an item in this column to open the schedule, where you have the option to edit or delete the report delivery.

## Email report list

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The tables below show the email reports that are available. Note that some reports appear in more than one report category.



### Note

You may not see all of the reports listed here, depending on the features enabled in your account.

- ◆ [Address reports](#)
- ◆ [Content reports](#)
- ◆ [Inbound reports](#)
- ◆ [Outbound reports](#)
- ◆ [Spam reports](#)
- ◆ [Virus reports](#)
- ◆ [Volume reports](#)

## Address reports

Report	Available Periods	Formats	Description
Outbound Senders	Daily	Table CSV Link PDF Link	Senders of email originating from your mail servers. Note that this can include senders of email that was auto-forwarded by your mail system and was originally from outside your organization.
Top Sources of Viruses	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses by volume of inbound viruses.



Report	Available Periods	Formats	Description
Top Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of messages regardless of direction
Top Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of messages regardless of direction
Top Inbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of inbound messages
Top Inbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of inbound messages
Top Inbound Sources	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent source IP addresses by volume of inbound messages
Top Outbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of outbound messages
Top Outbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of outbound messages
Top Transit Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of messages that were sent to and from the service
Top Transit Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent senders by volume of messages that were sent to and from the service
Top Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently used spamtraps

Report	Available Periods	Formats	Description
Top Senders to Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent senders by volume of messages sent to spamtraps
Top Sources to Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses by volume of messages sent to spamtraps
Top Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for recipients
Top Senders blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for senders
Top Sender/Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for pairs of senders and recipients

## Content reports

Report	Available Periods	Formats	Description
Most Frequent Lexical Rules	Hourly Daily	Chart Table CSV Link PDF Link	The lexical rules that most frequently matched
Top Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for recipients
Top Senders blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for senders
Top Sender/Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for pairs of senders and recipients
Parked Attachments	Minutes Hourly Daily	Table CSV Link PDF Link	Lists email messages that had attachments parked

Report	Available Periods	Formats	Description
Parked Attachments Summary	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Summarizes parked attachments over specified period
Lexical Analysis Failure Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email messages failing lexical analysis
Inbound Lexical Analysis Failure Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages failing lexical analysis
Outbound Lexical Analysis Failure Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages failing lexical analysis

## Inbound reports

Report	Available Periods	Formats	Description
Inbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of inbound messages
Top Inbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of inbound messages
Top Inbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of inbound messages
Top Inbound Sources	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent source IP addresses by volume of inbound messages

## Outbound reports

Report	Available Periods	Formats	Description
Outbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of outbound messages
Outbound Senders	Daily	Table CSV Link PDF Link	Senders of email originating from your mail servers. Note that this can include senders of email that was auto-forwarded by your mail system and was originally from outside your organization.
Top Outbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of outbound messages
Top Outbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of outbound messages
Encrypted Messages	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of encrypted messages sent in the selected time period
Encrypted Messages by Domain	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most popular domains for sending encrypted messages in the selected time period
Encrypted Messages by Policy	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most used policies for sending encrypted messages in the selected time period
Encrypted Messages by Encryption Rule	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most frequently-used encryption rules for sending encrypted messages in the selected time period
Opportunistic TLS	Hourly Daily	Chart Table CSV Link PDF Link	Shows the number of delivered messages that used, or did not use, opportunistic TLS

## Spam reports

Report	Available Periods	Formats	Description
Inbound Spam Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages detected as spam
Outbound Spam Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of outbound email messages detected as spam
Inbound Spam Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of inbound email detected as spam
Outbound Spam Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of outbound email detected as spam
Inbound Spam Bandwidth Saved	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Estimates the bandwidth saved for your company due to the filtering of inbound spam. The estimate is based on the number of inbound messages for your account in the selected time period, the approximate number of blocked messages for your account, and the average size of spam messages as calculated from the overall spam data for all TRITON AP-EMAIL accounts.
Spam False Positives and Negatives	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of false positives and false negatives generated during spam message processing.
Inbound Commercial Bulk Email Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages detected as commercial bulk email
Top Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequently used spamtraps

Report	Available Periods	Formats	Description
Top Senders to Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequent senders, by volume, of email messages sent to spamtraps
Top Sources to Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses associated with messages sent to spamtraps

## Virus reports

Report	Available Periods	Formats	Description
Most Common Viruses	Hourly Daily Monthly	Chart Table List CSV Link PDF Link	The most commonly-detected viruses
Zero-day viruses caught by ThreatSeeker	Hourly Daily Monthly	Chart Table Text CSV Link PDF Link	Recent viruses caught by ThreatSeeker before any virus signature updates within your account
Largest windows of exposure closed by ThreatSeeker	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Recent viruses caught by ThreatSeeker by largest window of exposure in your account
Virus Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email detected as containing viruses by all techniques including ThreatSeeker
Inbound Virus Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of inbound email detected as containing viruses by all techniques including ThreatSeeker.
Outbound Virus Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of outbound email detected as containing viruses by all techniques including ThreatSeeker.

Report	Available Periods	Formats	Description
Top Sources of Viruses	Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses, by volume, associated with inbound viruses
Sandboxed URLs	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of messages containing sandboxed URLs.
Clicked Sandboxed URLs	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of times sandboxed links were clicked in messages, and the action the user took after clicking.
Targeted Phishing Attacks	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Phishing topics that are part of a targeted attack, directed multiple recipients, listed by number of recipients.
Top Phishing Attacks	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most frequently seen phishing topics by number of recipients.
Top Repeat Phishing Victims	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The end users who have most frequently clicked a link in a phishing email.
Top Phishing Recipients	Hourly Daily Monthly	Table CSV Link PDF Link	The end users who have most frequently received phishing email messages.
Phishing Topic Details	Hourly Daily Monthly	Table CSV Link PDF Link	A list of phishing topics for specified recipients.
Phishing Recipient Details	Hourly Daily Monthly	Table CSV Link PDF Link	A list of recipients for specified phishing topics.

## Volume reports

Report	Available Periods	Formats	Description
Total Messages	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email processed (both inbound and outbound)
Total Message Size	Up to 12 hours	CSV Link PDF Link	How much mail in megabytes, has been processed or stopped by the service.
Inbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of inbound messages
Outbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of outbound messages
Transit Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of messages in transit (both to and from your account, i.e., internal messages)
Unprocessed Message Volumes	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Messages discarded because of access control rules
Largest Messages	Minutes Hourly	Table CSV Link PDF Link	The largest messages
Message Size Distribution	Minutes Hourly	Chart Table CSV Link PDF Link	The distribution of message sizes
Top Inbound Policies	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The policies receiving the most mail
Top Outbound Policies	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The policies sending the most mail



Report	Available Periods	Formats	Description
Top Inbound Receiving Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains receiving the most mail from the Internet
Top Inbound Sending Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains sending the most mail from the Internet
Top Outbound Receiving Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains receiving the most mail from this account
Top Outbound Sending Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains sending the most mail to the Internet
Message Analysis Delay	Hourly	Chart Table CSV Link PDF Link	The time taken in seconds (rounded up) to analyze email, i.e., excluding any delivery attempts
Top Mandatory TLS Failures	Hourly Daily	Chart Table CSV Link PDF Link	The volume of email messages that failed to be delivered due to TLS being unavailable.
Top Mandatory TLS Domains	Hourly Daily	Chart Table CSV Link PDF Link	The volume of email messages sent using mandatory TLS.



# 8

## Account Reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Account Summary report](#)
- ◆ [Service reports](#)
- ◆ [Downloading report results](#)
- ◆ [Saving reports](#)
- ◆ [Scheduling reports](#)

Go to **Reporting > Account Reports** to see the account-level reports available to you.

- ◆ The account summary report provides a summary of the email traffic that has been processed for your account during a defined time period.
- ◆ If you have directory synchronization enabled for your account, you can generate synchronization statistics for the service.
- ◆ If you have the cloud email service, you can report on the end users who are subscribed to the end-user message report (EUMR).

All reports are generated in real time using the cloud manager. Most include charts and tables that are presented in an easy to read, printable format.



### Note

For larger accounts, where a lot of data is to be retrieved, the reports may take some time to generate. As soon as the relevant data has been retrieved it is displayed while the remainder of the report is being compiled.

Commonly-used report criteria can be saved for easy access. For more information, see [Saving reports](#), page 152. Saved reports can be scheduled for regular delivery to one or more recipients as described in [Scheduling reports](#), page 153.

the current endpoint status.

- ◆
- ◆

## Account Summary report

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

- ◆ [Scheduling Account Summary reports](#)

The Account Summary report is a combination of reports that can be obtained elsewhere in the service. Select the time period, click **Go**, and you are presented with a summary of the email traffic that has been processed for your account during the selected time period. (If you have a lot of mail flowing through the system, this may take a while.) The report is organized by section and preceded by a table of contents with hyperlinks into specific data. Click the links to view the report, or scroll down the page using the scroll bar.

## Scheduling Account Summary reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

If you would like non-graphical versions of the Account Summary reports to be sent to one or more email addresses on a regular basis:

1. Select **Reporting > Account Reports > Account Summary**.
2. Click the **click here** link on the Account Summary Report page to set up report delivery.
3. Enter one or more email addresses to which you want the report sent.  
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
4. Set up a subscription schedule by specifying one of the following delivery periods for your reports:
  - daily
  - weekdays
  - weekly
  - every other week (biweekly)
  - monthly (the default option)If you want to stop the a scheduled report temporarily, select **suspend delivery**.
5. Click **Save**.

Your schedule details are then shown on the Account Summary page. You can edit or delete your details from the **click here** link.



### Note

You must renew your subscription to the Account Summary report every 3 months or your subscription expires.

## Printing Account Summary reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

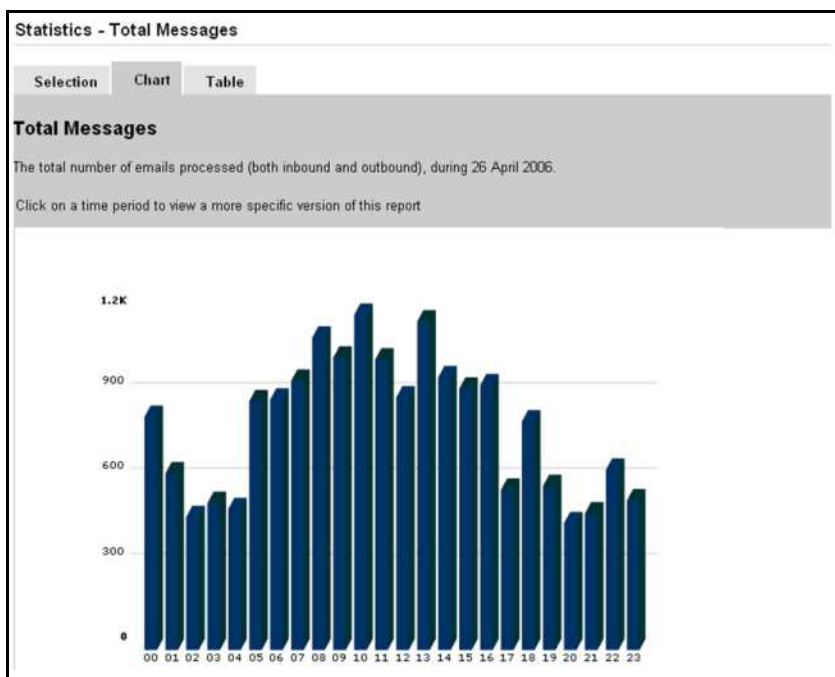
Once you have generated the Account Summary report, click **Click here to print this page** to get a printer-friendly version of the report. After a few seconds a printer selection dialog box appears.

Please leave plenty of time for the graphics to appear before printing. We recommend that you select “Landscape” format.

## Viewing detailed information

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

To view detailed daily information, click the relevant bar in the chart or the date in the table. The result of doing so is shown below.



You can expand each section in the Account Summary report in this manner.

## Service reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The Service reports provide data that relates to directory synchronization and to end user message report subscriptions.

### Directory synchronization reports

If you have directory synchronization enabled on your account, you can view and print reports on the portal that show the history of directory synchronizations, including high-level statistics on success/failure and numbers of items synchronized.

1. Select **Reporting > Account Reports > Services**.
2. From the **Show** drop-down list, select a report to show:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

3. From the **during** drop-down list, select the time period for the report. Click **more** to select a specific date or time.



#### Note

The 'last 6 full hours' period does not include a synchronization just performed. You must wait for the hour to pass for it to appear in this report. You can view the very latest synchronization history in the Manage Directory Synchronization page on the **Setup** tab.

4. Click **Generate report**. Following is a sample Synchronization History Log:

Selection

Chart

Table

Synchronization History Log

connection history (limited to 1,000 rows), during the last 7 days.

Date (UTC)	SourceIP	Type	Status	Additions	Deletions
2008-10-21 10:56:53	10.5.21.32	test	200 OK		
2008-10-21 10:57:21	10.5.21.32	Addresses	200 OK		
2008-10-21 10:59:15	10.5.21.32	test	200 OK		
2008-10-21 10:59:54	10.5.21.32	Addresses	200 OK	27	0
2008-10-21 11:01:13	10.5.21.32	Groups	200 OK	8	0
2008-10-21 11:01:43	10.5.21.32	Users	403 SQL command failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:07:06	10.5.21.32	Groups	200 OK	8	0
2008-10-21 13:07:18	10.5.21.32	Users	403 SQL command failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:10:19	10.5.21.32	test	200 OK		
2008-10-21 13:10:40	10.5.21.32	Groups	200 OK	0	0
2008-10-21 13:10:50	10.5.21.32	Users	200 OK	0	0
2008-10-22 09:16:14	10.5.21.32	test	200 OK		
2008-10-22 09:16:39	10.5.21.32	Addresses	200 OK	27	0
2008-10-22 09:16:52	10.5.21.32	Groups	200 OK	0	0
2008-10-22 09:17:05	10.5.21.32	Users	200 OK	0	0

You can download the report to a CSV or PDF file. You can also print the report.

## Subscriptions report

The End User Message Report Subscriptions report lists the end users who are subscribed to the EUMR for the criteria you specify.

1. Select **Reporting > Account Reports > Services**.
2. From the **Show** drop-down list, select End User Message Report - Subscriptions.
3. From the **during** drop-down list, select the time period for the report. Click **more** to select a specific date or time.
4. Select the policy or policies for the report.
5. Select the domain(s) for the report.



### Note

You can use the **Shift** and/or **Ctrl** keys to select multiple domains and policies.

---

6. Click **Generate report**.



### Note

You can see the expiration date of each subscription, as well as subscriber and recipient addresses, in the report that is generated. The latter may be useful for consolidated end user message reports (one report for multiple email accounts).

---

## Downloading report results

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

On each report, you have the option to download the data as a PDF or CSV file.



### Note

You can also download charts as image files or in PDF format. To download a chart, right-click the chart and select the format to download (PDF, PNG, or JPEG).

---

## Downloading a CSV file

You can download the statistics for the majority of reports as a comma-separated values (CSV) file. This allows you to import it into a third-party application, such as

Microsoft Excel, for viewing and manipulation. On each table of results, click **Download CSV** to begin the download.

**Note**

For some email reports, the totals in the CSV file might be higher than the totals in the report on screen. This is because the generated reports contain 1 line per email message, whereas the CSV version contains 1 line per recipient which means that a single email message might appear several times.

---

## Downloading a PDF file

Report results can be output to Portable Document Format (PDF) for easy distribution or printing. The PDF report is generated by clicking the **Download PDF** button on a table of results.

---

## Saving reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

◆ [Scheduling reports](#)

You can choose to save any Services report. Use this option to identify the reports you generate most frequently and want to be able to locate quickly.

To see the list of reports that you have saved, select **Reporting > Account Reports > Saved Reports**.

To save a report:

1. Under **Reporting > Account Reports > Services**, select the report you want.
2. Use the **Selection** screen to enter your report criteria.
3. Click **Save report**.
4. Enter a name for the report, and click **Save**.

The Saved Reports list is displayed, and the report you entered is now listed.

As well as accessing the report from this screen, you now have the option to delete the saved report or schedule it for regular delivery.



# Scheduling reports

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Related topics:

◆ [Saving reports](#)

You can run reports as they are needed, or you can define a schedule for running one or more saved reports.

Reports generated by scheduled jobs are distributed to one or more recipients via email. The reports can be in HTML, PDF, or CSV format. There is a limit on the number of reports you can schedule for delivery: the Saved Reports list displays the remaining number you can schedule in addition to any existing deliveries.



## Note

You cannot schedule reports that have defined start and end dates, or that span periods of less than 24 hours.

To schedule a report:

1. Select **Reporting > Account Reports > Saved Reports**.
2. You can schedule an existing saved report by clicking the report you want to schedule on the Saved Reports list. If you do this, skip to step 5 below.  
Otherwise, to create a new report for scheduling, click the **Generate a new report** link. The page that appears includes only reports that are eligible for scheduling.
3. Create and save your report as described in [Saving reports](#), page 152.
4. On the Saved Reports list, click the name of your new report.
5. Click **Schedule email report**.
6. Enter the email address of the report recipient. Multiple email addresses should be separated by commas or spaces.  
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
7. Enter a subject for the report email, and the text you want to appear in the body of the email.
8. Select the report format.
9. Set one of the following delivery periods for your reports:
  - daily
  - weekdays
  - weekly
  - every other week (biweekly)

- monthly (the default option)

If you want to stop the a scheduled report temporarily, select **suspend delivery**.

10. Click **Save**.

You are returned to the Saved Reports list. Reports that have been scheduled display the recipient list in the **Email to** column. Click an item in this column to open the schedule, where you have the option to edit or delete the report delivery.

# 9

## End-User Self Service

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Related topics:

- ◆ [Requesting a message report](#)
- ◆ [Understanding the report](#)
- ◆ [Accessing quarantined email](#)
- ◆ [Changing subscription details](#)
- ◆ [Consolidating end-user message report data](#)

TRITON AP-EMAIL allows end users to review personal lists of suspicious and clean email based on criteria that the user chooses, see details about each message, and decide whether to release a message or white or blacklist it. The service does this by providing an end-user message report (EUMR). As an administrator, you can configure what the report contains, how it is sorted, and whether or not you want end users to be able to customize certain aspects of the report. You also specify the default language, time zone, and schedule for the report. This is all done by clicking **Email > Messages > End User Message Reports**. (See [End-user message reports](#), page 46 for specifics.)

You can choose to subscribe your end users to the EUMR via the cloud portal. In this case, users receive a single report in the format that you configure as described above, and the report contains a link that a user must click to receive the report on a weekly basis.

Otherwise, end users are not set up to receive the message report by default. To receive an EUMR, users must request it from a cloud service website. The *TRITON AP-EMAIL End User's Guide* and the *TRITON AP-EMAIL End User's Quick Start Guide* provide instructions for your users.

### Requesting a message report

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Users can request an EUMR by going to the following website and entering their email address.

[www.websense.com/SupportPortal/1843.aspx](http://www.websense.com/SupportPortal/1843.aspx)

The report is emailed to the email address entered. This normally takes no longer than a few seconds depending on the amount of data included.



## Understanding the report

Cloud TRITON Manager Help | Cloud Email Protection Solutions

**Messages processed from: 2 Dec 2008 - 8 Dec 2008** A

Accounts: jcuevas@cuevas.com, jcuevas@cuevasout.com B

Please contact your administrator for further information: [mo@ppp.com](mailto:mo@ppp.com)

C Suspicious: 97  
Clean: 0

D Show 7 days E Display

If you want to receive this report regularly by email, please click [here](#).

G [Change Subscription](#) H [Manage White/Black Lists](#)

**Suspicious mail**

Select for action: F All: Quarantined, Spam  
Clear

Action to take: F

I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV	BW	BX	BY	BZ	CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ	CK	CL	CM	CN	CO	CP	CQ	CR	CS	CT	CU	CV	CW	CX	CY	CZ	DA	DB	DC	DD	DE	DF	DG	DH	DI	DJ	DK	DL	DM	DN	DO	DP	DQ	DR	DS	DT	DU	DV	DW	DX	DY	DZ	EA	EB	EC	ED	EE	EF	EG	EH	EI	EJ	EK	EL	EM	EN	EO	EP	EQ	ER	ES	ET	EU	EV	EW	EX	EY	EZ	FA	FB	FC	FD	FE	FF	FG	FH	FI	FJ	FK	FL	FM	FN	FO	FP	FQ	FR	FS	FT	FU	FV	FW	FX	FY	FZ	GA	GB	GC	GD	GE	GF	GG	GH	GI	GJ	GK	GL	GM	GN	GO	GP	GQ	GR	GS	GT	GU	GV	GW	GX	GY	GZ	HA	HB	HC	HD	HE	HF	HG	HH	HI	HJ	HK	HL	HM	HN	HO	HP	HQ	HR	HS	HT	HU	HV	HW	HX	HY	HZ	IA	IB	IC	ID	IE	IF	IG	IH	II	IJ	IK	IL	IM	IN	IO	IP	IQ	IR	IS	IT	IU	IV	IW	IX	IY	IZ	JA	JB	JC	JD	JE	JF	JG	JH	JI	JJ	JK	JL	JM	JN	JO	JP	JQ	JR	JS	JT	JU	JV	JW	JX	JY	JZ	KA	KB	KC	KD	KE	KF	KG	KH	KI	KJ	KK	KL	KM	KN	KO	KP	KQ	KR	KS	KT	KU	KV	KW	KX	KY	KZ	LA	LB	LC	LD	LE	LF	LG	LH	LI	LJ	LK	LL	LM	LN	LO	LP	LQ	LR	LS	LT	LU	LV	LW	LX	LY	LZ	MA	MB	MC	MD	ME	MF	MG	MH	MI	MJ	MK	ML	MM	MN	MO	MP	MQ	MR	MS	MT	MU	MV	MW	MX	MY	MZ	NA	NB	NC	ND	NE	NF	NG	NH	NI	NJ	NK	NL	NM	NN	NO	NP	NQ	NR	NS	NT	NU	NV	NW	NX	NY	NZ	OA	OB	OC	OD	OE	OF	OG	OH	OI	OJ	OK	OL	OM	ON	OO	OP	OQ	OR	OS	OT	OU	OV	OW	OX	OY	OZ	PA	PB	PC	PD	PE	PF	PG	PH	PI	PJ	PK	PL	PM	PN	PO	PP	PQ	PR	PS	PT	PU	PV	PW	PX	PY	PZ	QA	QB	QC	QD	QE	QF	QG	QH	QI	QJ	QK	QL	QM	QN	QO	QP	QQ	QR	QS	QT	QU	QV	QW	QX	QY	QZ	RA	RB	RC	RD	RE	RF	RG	RH	RI	RJ	RK	RL	RM	RN	RO	RP	RQ	RR	RS	RT	RU	RV	RW	RX	RY	RZ	SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK	SL	SM	SN	SO	SP	SQ	SR	SS	ST	SU	SV	SW	SX	SY	SZ	TA	TB	TC	TD	TE	TF	TG	TH	TI	TJ	TK	TL	TM	TN	TO	TP	TQ	TR	TS	TT	TU	TV	TW	TX	TY	TZ	UA	UB	UC	UD	UE	UF	UG	UH	UI	UJ	UK	UL	UM	UN	UO	UP	UQ	UR	US	UT	UU	UV	UW	UX	UY	UZ	VA	VB	VC	VD	VE	VF	VG	VH	VI	VJ	VK	VL	VM	VN	VO	VP	VQ	VR	VS	VT	VU	VV	VW	VX	VY	VZ	WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ	WR	WS	WT	WU	WV	WW	WX	WY	WZ	XA	XB	XC	XD	XE	XF	XG	XH	XI	XJ	XK	XL	XM	XN	XO	XP	XQ	XR	XS	XT	XU	XV	XW	XX	XY	XZ	YA	YB	YC	YD	YE	YF	YG	YH	YI	YJ	YK	YL	YM	YN	YO	YP	YQ	YR	YS	YT	YU	YV	YW	YX	YZ	ZA	ZB	ZC	ZD	ZE	ZF	ZG	ZH	ZI	ZJ	ZK	ZL	ZM	ZN	ZO	ZP	ZQ	ZR	ZS	ZT	ZU	ZV	ZW	ZX	ZY	ZZ
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

## Information included on the EUMR

Section	Contents
<b>A</b>	The date range for which the report was processed
<b>B</b>	Your email address. Note that if you have consolidated end-user message report data from multiple email accounts into one EUMR, you will see all the email addresses included in that subscription.
<b>C</b>	The number of suspicious and clean messages that were processed for you during the period
<b>D</b>	An option to change the number of days shown in the report
<b>E</b>	A link to receive this report by email on a regular basis
<b>F</b>	The ability to select all quarantined and/or spam message and take actions on them, such as delete or release
<b>G</b>	A link to change your report subscription
<b>H</b>	A link to manage your personal white lists and black lists
<b>I</b>	<p>A list of your email arranged in the following order (list depends on user and account configuration):</p> <ul style="list-style-type: none"> <li>• Suspicious messages you received or sent</li> <li>• Clean messages you received or sent</li> </ul> <p>If you are viewing the online version of your report, you can change the order of the messages by clicking a column heading link. For example, you can sort by the <b>From</b> or <b>To</b> column, the <b>Date/Time</b> column, or the <b>Status</b> column.</p>
<b>J</b>	An indication of whether a message has been received or sent.
<b>K</b>	<p>The actions you can take action on a message. (Select a message by clicking in the check box on the left.) Options include:</p> <ul style="list-style-type: none"> <li>• <b>Details</b> - Access details about the message</li> <li>• <b>Release</b> - Release the message from quarantine. (Inbound messages only. This is not possible for all messages, such as those containing known viruses.) If the message to be released was originally sent to a distribution list address that is included in a consolidated EUMR, you are given the option to release the message to the whole list or a specific email address.</li> <li>• <b>Whitelist</b> - Send this message or domain to your personal white list. This tells the cloud-based service to always allow messages from this sender or domain.</li> <li>• <b>Blacklist</b> - Send this message or domain to your personal black list. This tells the cloud-based service to never allow messages from this sender or domain.</li> </ul>

## Information included on the message summary line

Information included on the message summary section:

- ◆ An indication of whether the message was inbound or outbound
- ◆ The message sender

- ◆ The message recipient
- ◆ The time and date that TRITON AP-EMAIL logged the email
- ◆ The status of the email - what action TRITON AP-EMAIL took on the email
- ◆ The subject line of the message

## Default information included

The first time a user requests an EUMR, it contains a maximum of 50 lines and covers the period of the last 7 days.

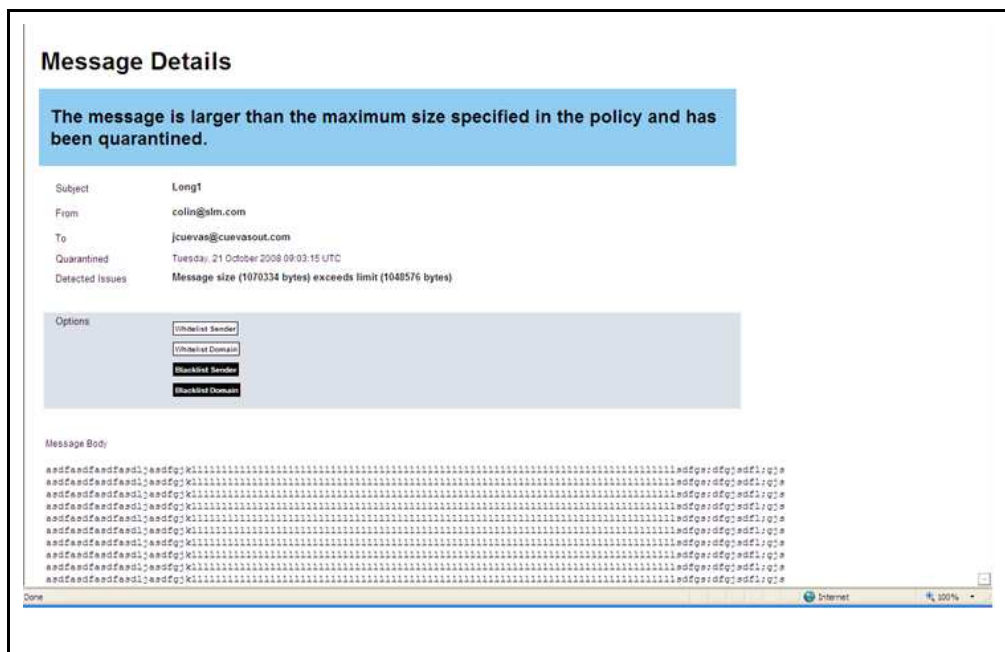
## Accessing quarantined email

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If users want to view the content of a particular quarantined message, they select the message (by clicking in the check box on the left), then click **Details**. They then have options of what to do with the message.

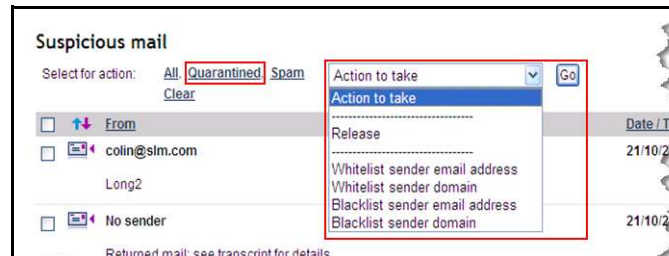
The details of a message may look something like this:



In this example, a message was quarantined, because it exceeded the maximum size specified in the policy. (This message is over 1 GB.) The administrator is allowing the user to add the sender or sending domain to a white list or black list. If these features were not enabled by the administrator, the buttons would not be on the screen. In some cases, users may be allowed to release a message or send a copy to themselves. If the email was quarantined because it contains a virus or offensive words, however, they would not be able to release a copy regardless of how the administrator has configured the service.

To view a list of quarantined messages, end users can sort on the **Status** column in their report, then scroll to the quarantined section.

When looking at the online version of their report, users can take action on all of the messages in their quarantine at once. To do so, they click **Quarantined**, then select an action to take from the drop-down list.



If, on the EUMR, the user clicks a link to a message that was accepted, only the message log entries are shown, because the message is no longer available to TRITON AP-EMAIL.

## Changing subscription details

Cloud TRITON Manager Help | Cloud Email Protection Solutions

If you have selected the **Allow end users to modify report content** option when setting up your EUMRs, end users can configure the system to send them message reports at any time interval. To define subscription details, they click the link **Change Subscription**.

 A screenshot of a web form titled "Change Subscription". The form is divided into two main sections: "Manage Accounts" and "Report Options". 
 The "Manage Accounts" section has a sub-header "Add or remove addresses to your end-user message report". It contains a checkbox for "joveas2@cust2.com" and an "Add Address" button. Below this is a note: "After you save changes, the owner is emailed and asked to approve the subscription request."
 The "Report Options" section contains several settings:
 - "Reporting period": 14 days (dropdown)
 - "Frequency sent": weekly (dropdown)
 - "Maximum length": 50 rows (dropdown)
 - "Email types to include": A list of checkboxes, all of which are checked: "Quarantined email received", "Quarantined email sent", "Non-quarantined email received", "Non-quarantined email sent", "Clean email received", and "Clean email sent".
 - "Sort by": Status (dropdown) in ascending (dropdown) order. A note below says "Applies to quarantined and non-quarantined messages only."
 - "Timezone": GMT +00:00 (dropdown)
 - "Language": English (British) (dropdown)
 At the bottom of the form are "Submit" and "Close" buttons.

On the **Change Subscription** screen, users can specify the following subscription:

- ◆ Manage Accounts

- Do they want to consolidate the end user message report (EUMR) data for multiple aliases or email accounts into one EUMR? (See [Consolidating end-user message report data](#), page 161.)
- ◆ Report Options
  - What time period do they want reported: the last 1, 2, 7, 14, or 30 days?
  - How often should the report be delivered: daily, weekdays, weekly, biweekly, or monthly?
  - How many rows do they want on each page in the report: 20, 50, 100, 200, or 500?
  - What sections do they want included in the report: quarantined suspicious messages received or sent, non-quarantined suspicious messages received or sent, clean messages received or sent?
  - In what order do they want the information about quarantined and non-quarantined messages to appear: status, date/time, subject, from, or to? Ascending or descending?

**Note**

Subscriptions to the message report lapse after 93 days. 62 days after subscribing, each time users receive a report, they are reminded that they should renew their subscription.

---

- What time zone should the report assume?
- In what language do they want the report delivered? The EUMR supports 14 languages:
  - Czech
  - Dutch
  - English (U.K. and U.S.)
  - French
  - German
  - Greek
  - Italian
  - Polish
  - Portuguese (Brazilian)
  - Romanian
  - Slovak
  - Spanish
  - Swedish

Regardless of the settings for the scheduled report, users can request a report by following the process outlined in [Requesting a message report](#), page 155.



## Consolidating end-user message report data

---

Cloud TRITON Manager Help | Cloud Email Protection Solutions

End users who are allowed to modify settings in their end-user message report (EUMR) can consolidate EUMR data from their other email accounts or aliases into one EUMR. They can also consolidate another person's email addresses, such as an assistant consolidating a manager's addresses into one report. Reviewing and managing one report versus several reports may help save time.

Note that if LDAP synchronization is enabled for the account, all aliases associated with an end user will be automatically listed on the Change Subscription screen under Manage subscription addresses. The end user can then add one or more of them into one consolidated report.

End users who want to consolidate addresses can do the following:

- ◆ From the EUMR, click **Change Subscription**.
- ◆ Under **Manage Accounts**, check the box for the email address or addresses to be added if a list is given, or enter the email address. The address must be from one of the domains owned by your company. For example, company xyz might have these domains: xyz.com, xyz.co.uk, or xyz.com.au.
- ◆ Click **Add Address**.
- ◆ To add a new email address, the end user must receive approval from the owner of that address. Clicking **Add Address** sends an email request for approval to the address owner. Until the owner approves the request, the email is marked "pending approval by owner." If the owner approves the request, the requestor is notified by email and the "pending" status is removed. The owner may choose to decline the request in which case the user may not add the email address to the EUMR report.
- ◆ To remove an address from the report, clear the check box next to the email address that they want to remove. Clearing the box reveals a "Remove" link. End users who click on this link are asked to confirm they want to remove the address.

Note that after they have created a consolidated EUMR, end users who then order a message report, or are set up to automatically receive a report, receive the consolidated report. If the end user wishes to receive reports from more than one subscription (for example, an individual and a consolidated subscription), you, the administrator, must create these subscriptions in the Cloud TRITON Managerportal.



# 10

## Audit Trails

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The following audit trails are available:

- ◆ *Configuration audit trail* - Lets you examine the configuration audit database for your account. This gives you visibility into all of the configuration changes that have been made on the account. Access this by choosing **Account > Settings > Audit Trail**.
- ◆ *Quarantine audit trail* - Lets you examine the quarantine audit database for your account. This gives you visibility into the actions taken by administrators in the Message Center. Access this by choosing **Email > Messages > Quarantine Audit Trail**.

### Configuration audit trail

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The configuration audit trail provides visibility of all policy changes. You can access it by selecting **Account > Settings > Audit Trail**. Searches are by user and the change made within a defined date range.

Results indicate the changes that meet the search criteria, when they were made, and by whom.

Click **Export to CSV** to export the results of your audit trail search. This creates a file named `audit_trail.csv`; you can either open the file, save the file with the default name, or save the file with a new name.

### Quarantine audit trail

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

The quarantine audit trail provides visibility of actions performed by an administrator in the Message Center. To access it, choose **Email > Messages > Quarantine Audit**

**Trail.** You can base searches on message sender, recipient, subject, who performed the action, and the action itself, within a defined date range.

# 11

## Standard Email Configuration

Cloud TRITON Manager Help | Cloud Email Protection Solutions

The TRITON AP-EMAIL service provides a standard configuration for all email accounts. The settings for the standard configuration are described below, as well as the reasoning behind the settings. As an administrator, you can customize policy settings to suit your needs. Do this by clicking **Email**, then following the instructions in [Defining Email Policies](#), page 59.

Each table in this section represents a section in email configuration settings. Column 4 suggests various use cases for changing the standard setting.

1. Policy Management	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Policies</b>	One policy has been set up with the standard account configuration shown in this document.	(see individual settings below)	Additional policies should be added to support aliases, or to support a domain (or domains) that require differing configurations.

2. General tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Notifications</b>	Inbound: Recipient Outbound: Sender	Intended recipient needs visibility of blocking. Sender needs visibility of blocking.	Volume of notifications is too high, visibility is not required, or notifying sender is preferable.
<b>Annotations</b>	Inbound: on Outbound: on	Allows recipient to report spam easily and automatically. To give confidence to recipient that message is virus-free.	Transparency of TRITON AP-EMAIL service is important. Company-specific annotation is required.

3. Domains tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Domains</b>	Registered domain is shown.	At least one valid domain name must be provided.	Additional domains are to be analyzed.

3. Connections tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Inbound Mail Routing Rules</b>	No rules set up.	No inbound routing rules are provided at the time of registration.	Inbound mail is to be routed to different email servers depending on the recipients.
<b>Default Inbound and Outbound Routes</b>	Registered route information is shown.	At least one inbound and one outbound route must be provided.	More servers are to send email to or receive from the cloud service. An “A record” is needed if load balancing across servers is required.

4. Antivirus tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Active Content</b>	Inbound: HTML: medium Outbound: HTML: off Inbound: Macro analyzer: high Outbound: Macro analyzer: off	Protect user from non-obvious active elements. Active HTML content is from trusted source. Protect user from suspicious macros. Macros are from trusted source.	HTML mail is not rendered correctly. HTML mail should be filtered. Too many relevant files are blocked. Additional security is required.

4. Antivirus tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Encrypted messages</b>	Inbound: password-protected zips: on  Outbound: password-protected zips: off Inbound: Encrypted mail: on Outbound: Encrypted mail: off	Not possible to analyze content of password-protected zips. Files are from trusted source. Not possible to analyze encrypted mail. Messages are from trusted source.	Requirement to transmit password-protected zips  Additional security required  Requirement to exchange encrypted mail Additional security required
<b>Executables</b>	Inbound: Quarantine exe: on  Outbound: Quarantine exe: on	Most administrators do not allow users to receive executables. Most administrators do not allow users to send executables.	Most users need to transmit executables.  Most users need to transmit executables.

5. Antispam tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Existing Rules</b>	Spam Score > 15.0 - discard	No false positives score as high as 15.0.	Discarding of spam not required or score needs to be higher or lower
	Spam Score > 6.0 - quarantine	System default spam threshold	Quarantining of spam not required or score needs to be higher or lower
<b>Exceptions</b>	Whitelist these addresses: off	No white list entries are provided at the time of registration.	Administrator may populate a white list for the account.
	Blacklist this address: off	No black list entries are provided at the time of registration.	Administrator may populate a black list for the account.
<b>End Users</b>	Allow users to populate their own white lists and black lists: on	Allow users some control over incoming senders for their own address	No control or visibility is desired for end users.
	Allow users to obtain a copy of an email that has been quarantined as spam: on	Allow users safe control over spam email sent to their own address	No control or visibility is desired for end users.
<b>Keep Messages</b>	Keep a copy of clean messages so they can be learnt from if later reported as spam: on	Cloud service keeps a private copy of the message for a short time to aid in spam-tuning when the 'Report this email as Spam' link is clicked.	No retention of clean messages for spam tuning is desired.



6. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Attachments</b>	Inbound: Mask attachments with .eml extension	Unable to analyze .eml files	.eml files are not a concern or if more file extensions are to be added
	Outbound: Do not mask any attachments	Files are from trusted source.	Different file types are to be considered suspicious.
	Inbound: Quarantine messages containing nominated file types: off	Allow admin to populate list before applying it	Blocking of certain file types is required.
	Outbound: Quarantine messages containing nominated file types: off	Allow admin to populate list before applying it	Blocking of certain file types is required.
	Inbound: Quarantine messages containing files of unknown type: off	Cloud service can identify majority of file types	There is a need for quarantining unknown attachments.
	Outbound: Quarantine messages containing files of unknown type: off	Files are from trusted source	Outgoing attachments are to be considered suspicious.
	Inbound: Quarantine messages containing inappropriate images: off	Requires license for image analysis	There is a need to analyze images.
	Outbound: Quarantine messages containing inappropriate images: off	Requires license for image analysis	Outgoing images are to be considered suspicious.
	Inbound: Quarantine messages with images that could not be scanned: off	This setting can only be enabled when image quarantine is on.	There is a need to check large images.
	Outbound: Quarantine messages with images that could not be analyzed: off	Files are from trusted source	There is a need to quarantine and check large images.
	Inbound: Park attachments meeting nominated criteria: off	Most large attachments can be delivered successfully	There is a need to conserve users' mailbox size.
	Outbound: Park attachments meeting nominated criteria: off	Files are from trusted source	There is a need to conserve recipients' mailbox size.

6. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
<b>Message Size</b>	Inbound: Non-deliver > 50MB: on Outbound: Non-deliver > 50MB: on Inbound: Quarantine > 10MB: off  Outbound: Quarantine > 10MB: off  Inbound: Defer delivery: off  Outbound: Defer delivery: off	Contractual maximum message size Contractual maximum message size Max message size usually acceptable  Max message size usually acceptable  Requires your policy to be applied  Requires your policy to be applied	Lower limit is required.  Lower limit is required.  Lower the limit below the maximum size to conserve your bandwidth. Lower the limit below the maximum size to conserve recipient organization's bandwidth.  There is a need to conserve your bandwidth during certain time periods. There is a need to assist with conserving recipient organization's bandwidth during certain time periods.
<b>Content Filtering</b>	Inbound: Filter using these lexical rules: on  Outbound: Filter using these lexical rules: on  Inbound: Quarantine messages if content analysis does not complete: off  Outbound: Quarantine messages if content analysis does not complete: off	Allow new rule to be implemented immediately. Allow new rule to be implemented immediately. Cloud service rarely fails to complete lexical analysis.  Cloud service rarely fails to complete lexical analysis.	Suspension of lexical filtering  Suspension of lexical filtering  There is a large number of lexical rules and regular expressions, which could mean analysis does not complete. There is a large number of lexical rules and regular expressions, which could mean analysis does not complete.

# A

## Checklists for Setting up LDAP in Various Use Cases

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

Whether you are a new or existing customer, you should plan your approach before performing your first synchronization. This section provides checklists for setting up directory synchronization in various use cases. Find yours to determine the best course of action.

- ◆ [New Web and/or email customers](#)
- ◆ [New and existing email customers](#)
- ◆ [Existing Web and/or email customers](#)
- ◆ [Considerations for existing customers](#)

### New Web and/or email customers

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

For new web and/or email customers, see the following:

- ◆ [Synchronizing users/groups with a single Web policy and exceptions, page 171](#)
- ◆ [Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory, page 172](#)

### Synchronizing users/groups with a single Web policy and exceptions

- ❑ Plan the cloud data structure: users and groups (See [Groups, page 19](#)), policies (See [Defining Web Policies, page 213](#)) and exceptions. (See [Exceptions, page 239](#).)
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
- ❑ Download the client and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.)

---

Review the results and modify the search as necessary to ensure it returns expected results.

- ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication](#), page 34.) This will be the username/ logon used for the Directory Synchronization Client to log onto the portal.
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
- ❑ Now you are ready! In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization](#), page 31.)
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- ❑ Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 36.)
- ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
- ❑ If you are planning to set up exceptions based on group membership, do this now in the cloud manager. (See [Exceptions](#), page 239.)
- ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
- ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

## Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory

- ❑ Plan the cloud data structure: users and groups (See [Groups](#), page 19), policies (See [Defining Web Policies](#), page 213) and exceptions. (See [Exceptions](#), page 239.) Create an extra policy or policies as required.
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
- ❑ Download the client and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Review the results and modify the search as necessary to ensure it returns expected results.

- 
- ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication](#), page 34.) This will be the username/logon used for the Directory Synchronization Client logs into the cloud manager.
  - ❑ Decide whether email will be sent after new users are synchronized from LDAP.
  - ❑ Now you are ready! In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization](#), page 31.)
  - ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
  - ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
  - ❑ Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 36.)
  - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
  - ❑ Go to each policy in turn, and set up the group/policy assignments. This moves users to the appropriate policies.
  - ❑ Go to the Directory Synchronization configuration page and check that the default policy setting is correct.
  - ❑ Return to the **Account > End Users** page and check that users are in the correct policies.
  - ❑ If you are planning to set up exceptions based on group membership, do this now in the cloud manager. (See [Exceptions](#), page 239.)
  - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
  - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

## New and existing email customers

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

For TRITON AP-EMAIL customers, see the following:

- ◆ [Synchronizing email addresses to provide a “white list” of valid email addresses](#)
- ◆ [Synchronizing users/groups to provide per-user/per-group exceptions to email policies](#)

---

## Synchronizing email addresses to provide a “white list” of valid email addresses

- ❑ Review the existing LDAP/Active Directory data structure and decide how to search for all relevant email addresses.
- ❑ Download the client and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract email addresses to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Review the results and modify the search as necessary to ensure it returns expected results.
- ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication](#), page 34.) This will be the username/logon used for the Directory Synchronization Client logs onto the cloud manager.
- ❑ In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization](#), page 31.) Make sure “Reject mail for unknown users” is *not* enabled. (Turn this on only when you are *sure* the mail list is synchronized and correct)
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of email address additions. This is visible in the Synchronization page and also from the notification email messages.
- ❑ Go to the cloud manager, Configure Directory Synchronization page and download a CSV file of email addresses. (See [Configure directory synchronization](#), page 31.) Check if these are correct, perhaps by comparing them against a known list from Active Directory.
- ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
- ❑ If everything appears to be working, go to the Configure Directory Synchronization page again and select **Reject mail for unknown users**. Email address filtering is now live.
- ❑ Set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool. If there is a problem with the first scheduled synchronization, you can restore the directory to its previous version. (See [Restore directories](#), page 37.)

## Synchronizing users/groups to provide per-user/per-group exceptions to email policies

- ❑ Plan the cloud data structure: users and groups ([Groups](#), page 19), policies ([Defining Email Policies](#), page 59) and exceptions.

- 
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
  - ❑ Download the client and install it on the target client machine.
  - ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Review the results and modify the search as necessary to ensure it returns expected results.
  - ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication](#), page 34.) This will be the username/ logon used for the Directory Synchronization Client to log onto the cloud manager.
  - ❑ Decide whether email will be sent after new users are synchronized from LDAP.
  - ❑ Now you are ready! In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization](#), page 31.)
  - ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
  - ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
  - ❑ Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 36.)
  - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
  - ❑ If you are planning to set up per-user/per-group configurations for Antispam, Antivirus or Content Filter in email policies then do it now. Use the **per-user** link on each of these tabs to configure custom rules for each user or group. (You can enter user or group names into the per-user dialogs.) Refer to [Configuring Email Settings](#), page 41 for more information on per-user configuration options.
  - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
  - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

## Existing Web and/or email customers

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

For existing cloud web and/or email customers, see the following:



- 
- ◆ [Wanting to manage users/groups from an LDAP directory, page 176](#)
  - ◆ [Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal, page 177](#)

## Wanting to manage users/groups from an LDAP directory

- ❑ Review the existing cloud data structure, specifically the structure of users, groups, and policies. Go to **Account > End Users** and **Account > Groups** to view groups and users. (See [Groups, page 19](#)). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure. Review the exceptions in the policy. (See [Defining Web Policies, page 213](#)) and exceptions. (See [Exceptions, page 239](#).)
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the cloud data more closely.
- ❑ Modify cloud and/or LDAP data to match each other as closely as possible. You might do this by creating new LDAP groups with the same name and members as the cloud groups
- ❑ Download the client and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the cloud data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.
- ❑ Decide whether to allow overwriting of groups of the same names. In the cloud manager, set **Overwrite groups** as necessary. (See [Configure directory synchronization](#) for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the cloud, then change any group-based notification in the cloud manager to the new LDAP names as required.
- ❑ If you have more than one Web policy, go to each policy and assign groups to it
- ❑ Then on the Configure Directory Synchronization screen, assign users to a default policy and for **User policy assignment**, select **Follow group membership**. With this setting, as users are moved to a different LDAP group, their policy assignment changes in step.
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
- ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication, page 34](#).) This will be the username/logon used for the Directory Synchronization Client logs into the cloud manager.
- ❑ Now you are ready! In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization, page 31](#).)
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)



- 
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
  - ❑ Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 36.)
  - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
  - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use **Restore** to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
  - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

## Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal

- ❑ Review the existing cloud data structure, specifically the structure of users, groups, and policies. Go to **Account > End Users** and **Account > Groups** to view groups and users. (See [Groups](#), page 19). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure.
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the cloud data more closely.
- ❑ Modify cloud and/or LDAP data to match each other as closely as possible.
- ❑ Download the client and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups, users, and email addresses to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the cloud data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.
- ❑ Decide whether to allow overwriting of groups of the same names. In the cloud manager, set **Overwrite groups** as necessary. (See [Configure directory synchronization](#) for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the portal, then change any group-based notification on the portal to the new LDAP names as required.
- ❑ If you have more than one web policy, go to each policy and assign groups to it.
- ❑ Then on the Configure Directory Synchronization screen, assign users to a default policy and for **User policy assignment**, select **Fixed**. With this setting, new web users are assigned to the web policy when first synchronized into the service. After that you must manage all movement of users between policies in the cloud manager using the Manage Users page. (Group membership is ignored.)
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.

- 
- ❑ In the cloud manager, set up a contact with Directory Synchronization permissions. (See [Set up authentication](#), page 34.) This will be the username/ logon used for the Directory Synchronization Client logs into the cloud manager.
  - ❑ Now you are ready! In the cloud manager, enable Directory Synchronization. (See [Configure directory synchronization](#), page 31.)
  - ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
  - ❑ During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
  - ❑ Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 36.)
  - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 37.)
  - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
  - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

## Considerations for existing customers

---

Cloud TRITON Manager Help | Cloud Web and Email Protection Solutions

If you have already set up users, groups, passwords, policies, and exceptions in the cloud manager and you want to switch to LDAP synchronization, consider the following:

- ◆ You can minimize the impact by carefully matching your LDAP group names and membership to the existing setup. Matching LDAP group names and membership to those already in the cloud service allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.
- ◆ You are responsible for avoiding ambiguous configurations, for example, users belonging to multiple groups which are assigned to different policies. It is up to you to set up groups in the LDAP directories in such a way that ambiguities don't occur. (When there are ambiguities, the service selects the closest group-to-policy assignment for each individual user, taking the first group in alphabetical order where there are multiple assignments at the same hierarchical level.)
- ◆ Existing users can retain their passwords and whether you manage users through the portal, LDAP synchronization, or both is completely transparent to them.

# B

## Standard Regular Expression Strings

Cloud TRITON Manager Help | Cloud Email Protection Solutions

Regular expressions (RegEx) are a powerful way of matching a sequence of simple characters. You can use regular expressions in TRITON AP-EMAIL to create dictionary entries for lexical rules (see [Filtering using lexical rules](#), page 96).

You can enclose a range of characters in square brackets to match against all of those characters. For example:

Expression	Description
[ ]	may also be used on a range of characters separated by a – character.
[0-9]	matches any digit.
[a-z]	matches any alpha character
[a-z0-9]	matches any alphanumeric character
^	is the “not” character, so [^0-9] matches against any character that is not a digit.

Although you can use ranges to specify a group of characters, you can also use the following shortcuts:

Expression	Description
.	matches against any character
\d	matches against a digit [0-9]
\D	matches against a non-digit [^0-9]
\s	matches against a whitespace character (such as a tab, space, or line feed character)
\S	matches against a non-whitespace character
\w	matches against an alphanumeric character [a-zA-Z_0-9]
\W	matches against a non-alphanumeric character
\xhh	matches against a control character (for the hexadecimal character hh)
\uhhhh	matches against a Unicode character (for the hexadecimal character hhhh)



### Note

As the backslash character is used to denote a specific search expression, if you want to match against this character, you must enter a double backslash (\\).

To match against occurrences of a character or expression, you can use the following.

Expression	Description
*	matches against zero or more occurrences of the previous character or expression
+	matches against one or more occurrences of the previous character or expression
?	matches zero or one occurrences of the previous character or expression
{n}	matches n occurrences of the previous character or expression
{n,m}	matches from n to m occurrences of the previous character or expression
{n,}	matches at least n occurrences of the previous character or expression

You can provide text to replace all or part of your search string. To do this, you need to group together matches by enclosing them in parentheses so they can be referenced in the replacement. To reference a matched parameter, use \$n where n is the parameter starting from 1.

## Regular expression examples

### Example 1: IP address

The following regular expression matches against any IP address:

```
\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b
```

You can test this regex with any phrase including a standard IP address, for example 192.23.44.1.

### Example 2: Dates

The following regular expression matches against dates in the format DD-MMM-YYYY:

```
\b\d\d?-[a-zA-Z]{3}-\d\d\d\d\b
```

To test this regex, enter a sentence similar to “The project completes on 14-Feb-2009”.

---

### **Example 3: Social Security Numbers**

The following regular expression matches against Social Security numbers in UK format:

```
\b\w{2}\d{6}\w\b
```

You can test this regex with any Social Security number in the format XY123456Z.





# Supported File Types

Cloud TRITON Manager Help | Cloud Email Protection Solutions

This appendix provides a list of all the file formats and types supported for attachment blocking and parking in TRITON AP-EMAIL.

File format	File type
Compressed and Encoded Formats	Serialized Object Format (SOF)
	Disk Doubler
	ZIP Archive
	PAK/ARC Archive
	cpio archive (CRC Header)
	cpio archive (CHR Header)
	SUN PEX Binary Archive
	UU encoded
	Stuftt (MAC)
	WANG Office GDL Header
	OLE Compound Document
	SHAR
	Unix Compress
	GZ Compress
	TAR
	BinHex
	SMTP
	MIME
	Compactor / Compact Pro
	PGP Secret Keyring
	PGP Public Keyring
	PGP Encrypted Data
	PGP Signed Data
	PGP Signed and Encrypted Data

File format	File type
	PGP Signature Certificate
	PGP Compressed Data
	ASCII-armored PGP Public Keyring
	ASCII-armored PGP encoded
	MacBinary
	Apple Single
	Apple Double
	Microsoft Outlook
	Microsoft Outlook PST
	RAR
	IBM Lotus Notes Database NSF/NTF
	OpenPGP Message Format (with new packet format)
	LHA Archive
	IBM Lotus representation of Domino design elements in XML format
	Legato Extender Native Message ONM
	Transport Neutral Encapsulation Format (TNEF)
	Legato EMailXtender Archives Format (EMX)
	7 Zip Format (7z)
	Microsoft Cabinet File (CAB)
	Group Wise File Surf email (GWFS)
	Archive by Robert Jung (ARJ)
	Microsoft Outlook Restricted Permission Message (RPMSG)
	Microsoft Outlook for Macintosh (OLM)
	Web ARChive (WARC)
Database Formats	MORE Database MAC
	Filemaker MAC
	SmartWare II (DB)
	Microsoft Works for MAC
	Microsoft Works for DOS
	Microsoft Works for Windows
	Reflex
	Paradox
	dBase



File format	File type
	Ability DB
	Microsoft Access
	Microsoft Access 95
	Microsoft Access 97
	Microsoft Access 2000
Desktop Publishing Formats	PageMaker for Macintosh
	PageMaker for Windows
	FrameMaker
	Maker Markup Language
	Quark Xpress MAC
	Microsoft Publisher
Executable Formats	MS-DOS Batch File
	SDOS/Windows Program
	DOS/Windows Object Library
	Unix Executable (PDP-11/pre-System V VAX)
	Unix Executable (Basic-16)
	Unix Executable (x86)
	Unix Executable (iAPX 286)
	Unix Executable (MC680x0)
	Unix Executable (3B20)
	Unix Executable (WE32000)
	Unix Executable (VAX)
	Unix Executable (Bell 5.0)
	Unix Object Module (VAX Demand)
	Unix Object Module (old MS 8086)
	Unix Object Module (Z8000)
	DOS/Windows Object Module
	PC (.COM)
	MSDOS Device Driver
	ELF Relocatable
	ELF Executable
	ELF Dynamic Library
	Java Class format (CLASS)
High-End Graphics	Corel Draw
	Computer Graphics Metafile (CGM)

File format	File type
	Lotus PIC
	PostScript
	Windows Metafile (no header)
	Freehand MAC
	HP Graphics Language
	AutoCAD DXF
	OS/2 PM Metafile
	Lasergraphics Language
	AutoShade Rendering
	GEM VDI
	HP Printer Control Language
	VRML
	QuickDraw 3D Metafile
	Corel CMX
	AutoDesk Drawing (DWG)
	AutoDesk WHIP
	Micrografx Designer
	Simple Vector Format (SVF)
	Enhanced Metafile
	Microsoft Office Drawing
	DeVice Independent file (DVI)
	Harvard Graphics Chart
	Harvard Graphics Symbol File
	Harvard Graphics Configuration File
	Harvard Graphics Palette
	Intergraph Standard File Format (ISFF) V7 DGN (non-OLE)
	MicroStation V8 DGN (OLE)
	CADAM Drawing
	CADAM Drawing Overlay
	NURSTOR Drawing
	HP Graphics Language (Plotter)
	CATIA Formats (CAT*)
	ODF Drawing
Other Formats	SmartWare II (Other)

---

File format	File type
	Microsoft Works for MAC
	Framework
	Framework II
	WordPerfect auxiliary file
	Windows Help File
	Ability Other
	NeWS bitmap font
	SUN vfont Definition
	Windows Group
	TrueType Font
	Program Information File (PIF)
	Windows C++ Object Storage
	FTP Session Data
	Netscape Bookmark File
	Office 2007 document
	Unknown binary
	Advanced Systems Format (ASF)
	Yahoo! Messenger chat log (YCHAT)
	MATLAB file format (MAT, FIG)
	SEG-Y Seismic Data format (SGY, SEGY)
	Microsoft Windows NT Event Log (EVT)
	Microsoft Windows Vista Event Log (EVTX)
Presentations	PowerPoint PC
	PowerPoint MAC
	PowerPoint 95
	PowerPoint 97
	Persuasion
	Applix Graphics
	Lotus Freelance for DOS
	Lotus Freelance for Windows
	Lotus Freelance for OS/2
	Lotus Freelance 96
	Lotus Freelance 97
	Corel Presentations
	Harvard Graphics

File format	File type
	Microsoft PowerPoint 2000
	Microsoft Visio
	Microsoft PPT 2007 XML
	Microsoft PPT Macro 2007 XML
	ODF Presentation
	Apple iWork Keynote format
Scheduling/Planning	Microsoft Project
	PlanPerfect
	Microsoft Project 4
	Microsoft Project 4.1
	Microsoft Project 98
	Microsoft Project 2000
Sound	Microsoft Wave
	MIDI
	NeXT/Sun Audio Data
	RIFF MIDI
	Audio Interchange File Format (AIFF)
	Amiga MOD
	Amiga IFF (8SVX) Sound
	Creative Voice (VOC)
	MPEG Audio
	Real Audio
	Window Media Audio Format (WMA)
Spreadsheets	Multiplan (PC)
	Multiplan (Mac)
	SYLK
	Symphony
	Uniplex Ucalc
	Data Interchange Format (DIF)
	Enable Spreadsheet
	Supercalc
	UltraCalc
	SmartWare II (Spreadsheet)
	Microsoft Works for MAC
	Microsoft Works for Windows

File format	File type
	Quattro Pro for DOS
	Quattro Pro for Windows
	Ability Spreadsheet
	CSV (Comma Separated Values)
	PeachCalc
	Lotus 1-2-3
	Lotus 1-2-3 Formatting
	Lotus 1-2-3 97
	Microsoft Excel
	Microsoft Excel 95
	Microsoft Excel 97
	Lotus 1-2-3 Release 9
	Applix Spreadsheets
	Microsoft Excel 2000
	Microsoft Excel 2007 XML
	Microsoft Excel Macro 2007 XML
	ODF Spreadsheet
	Microsoft Excel Binary 2007
	Quattro Pro 9+ for Windows
	Apple iWork Numbers format
Standard Graphics	Windows Bitmap
	Encapsulated PostScript
	CCITT G3 1D
	Graphics Interchange Format (GIF87a)
	Graphics Interchange Format (GIF89a)
	GEM Bit Image
	Sun Raster
	MacPaint
	PC Paintbrush Graphics (PCX)
	QuickDraw Picture
	Lotus Ami Pro Draw
	Targa
	TIFF
	Windows Metafile
	WordPerfect Graphics

File format	File type
	JPEG Interchange Format
	Windows Icon Format
	Windows Cursor
	Ability Image
	Curses Screen Image
	DCX FAX Format (PCX images
	Lotus Notes Bitmap
	Portable Network Graphics (PNG)
	Windows Animated Cursor
	Windows Palette
	RIFF Device Independent Bitmap
	OLE DIB object
	SGI Image
	MS Windows Device Independent Bitmap
	Portable Bitmap Utilities ASCII Format
	Portable Bitmap Utilities Binary Format
	Portable Greymap Utilities ASCII Format
	Portable Greymap Utilities Binary Format
	Portable Pixmap Utilities ASCII Format
	Portable Pixmap Utilities Binary Format
	X Bitmap Format
	X Pixmap Format
	FPX Format
	PCD Format
	Microsoft Document Imaging Format
	PaperPort image file (MAX)
Text	EBCDIC Text
	HTML
	Text
Vector Graphics	Windows Draw (Micrografx)
Videos	Video for Windows (AVI)
	RIFF Multimedia Movie
	MPEG Movie
	QuickTime Movie
	AutoDesk Animator FLIC

---

File format	File type
	AutoDesk Animator Pro FLIC
	Lotus ScreenCam
	Macromedia Director
	Window Media Video Format (WMV)
	MPEG-PS container with CDXA stream (MPG)
Word Processing	Multiplus (AES)
	APPLIX ASTERIX
	Convergent Technologies DEF Comm. Format
	Word Connection
	COMET TOP
	CEOwrite
	DSA101 (Honeywell Bull)
	DCA-RFT (IBM Revisable Form)
	CDA / DDIF
	DG Common Data Stream (CDS)
	Vistaword
	DECdx
	Enable Word Processing
	HP Word PC
	IBM 1403 Line Printer
	DCF Script
	DCA-FFT (IBM Final Form)
	Interleaf
	Display Write
	Lotus Ami Pro
	Lotus Ami Pro Style Sheet
	Lyrix Word Processing
	MASS-11
	Microsoft Word for Macintosh
	Microsoft Word for Windows
	MultiMate
	MultiMate Footnote File
	MultiMate Advantage
	MultiMate Advantage Footnote File
	MultiMate Advantage II

---

File format	File type
	MultiMate Advantage II Footnote File
	Rich Text Format (RTF)
	Microsoft Word for PC
	Microsoft Word for PC Style Sheet
	Microsoft Word for PC Glossary
	Microsoft Word for PC Driver
	Microsoft Word for PC Miscellaneous File
	NBI Async Archive Format
	Navy DIF
	NBI Net Archive Format
	NIOS TOP
	OLIDIF (Olivetti)
	Office Writer
	CPT
	Philips Script
	PRIMEWORD
	Q-One V1.93J
	Q-One V2.0
	SAMNA Word
	SmartWare II (WP)
	Targon Word
	Uniplex
	Microsoft Word UNIX
	WANG PC
	WordERA
	WANG WPS
	WordPerfect MAC
	WordPerfect
	WordPerfect VAX
	WordPerfect Macro
	WordPerfect Spelling Dictionary
	WordPerfect Thesaurus
	WordPerfect Resource File
	WordPerfect Driver
	WordPerfect Configuration File



---

File format	File type
	WordPerfect Hyphenation Dictionary
	WordPerfect Miscellaneous File
	WordMARC
	WordStar
	WANG WITA
	Xerox 860
	Xerox Writer
	Microsoft Works for MAC
	Microsoft Works for DOS
	Microsoft Works for Windows
	MacWrite
	MacWrite II
	Maker Interchange Format (MIF)
	Windows Write
	Volkswriter
	Ability WP
	XYWrite / Nota Bene
	IBM Writing Assistant
	WordStar 2000
	WriteNow MAC
	Q & A for DOS
	Q & A for Windows
	WPS-PLUS
	DCS
	Lotus Notes CDF
	ODA / ODIF
	ALIS
	Envoy
	Portable Document Format
	USENET
	SGML
	ACT
	Applix Words
	XML
	Unicode

---

File format	File type
	Lotus Word Pro 96
	Lotus Word Pro 97
	Microsoft Word 95
	Microsoft Word 97
	Microsoft Pocket Word
	Microsoft Word 2000
	Folio Flat File
	HWP(Arae-Ah Hangul)
	ICHITARO V4-10
	Verity XML
	Oasys format
	Microsoft Word 2003 XML
	Microsoft Excel 2003 XML
	Microsoft Visio 2003 XML
	StarOffice Text XML
	StarOffice Spreadsheet XML
	StarOffice Presentation XML
	XHTML
	SWF
	Microsoft Word 2007 XML
	Microsoft Word Macro 2007 XML
	Microsoft XML Paper Specification(XPS)
	ODF Text
	Yahoo! Instant Messenger History
	Founder Chinese E-paper Basic (ceb)
	MHT format
	Microsoft Office Groove Format
	Apple iWork Pages format
	Windows Journal format (JNT)