Websense Email Security Transition: Overview

Topic 70051 | TRITON AP-EMAIL | Version 8.0.x | Updated 03-Mar-2015

Part of the Websense® TRITON® APX security suite, Websense TRITON AP-EMAIL is an appliance-based email protection solution that combines on-premises email analysis with world-class Web analytics to provide maximum security against today's sophisticated blended threats. The Email Hybrid Module adds in-the-cloud prefiltering capabilities to the robust analysis capabilities of the on-premises solution. The Email Sandbox Module includes file and URL sandboxing capabilities to analyze and provide feedback regarding suspicious files and attachments.

This solution also offers Websense TRITON AP-DATA data loss protection (DLP) technology to accurately detect the transmission of sensitive data via email. Integration with Websense TRITON AP-WEB or Web Filter & Security allows the email protection system to use that module's master URL database to detect malicious embedded URLs in email.

This paper is for users of the Websense Email Security software solution who want information about making the transition to the TRITON AP-EMAIL on premises solution. It describes the key concepts inherent in the email protection system and its differences from Websense Email Security. It also contains some high-level suggestions and tips to ease the transition to TRITON AP-EMAIL.

For a description of sample policy configurations and a map of Websense Email Security functions and their associated on-premises TRITON AP-EMAIL functions, see Websense Email Security Transition: Policies and Settings.

Contents:

TRITON AP-EMAIL Key Concepts

Websense TRITON AP-EMAIL is functionally similar to Websense Email Security. However, some differences between these products should be considered and understood before you plan your transition project.

The following sections describe how TRITON AP-EMAIL functions parallel or differ from those in Websense Email Security:

- *Platform architecture*
- *Administration and administrator roles*
- *Email policy management*
- *Email and connection handling*
- *Message queue management*
- *Status, logging, and reporting*
- *Database management*
- *Data module integration*
- *Personal Email Manager*

Platform architecture

Part of the unified TRITON Manager, the Email module provides a single interface for all email protection management functions, including administration, policy, message, reporting, and system status controls. The TRITON console also includes management functions for Data module email DLP capabilities. Integration with the Web module provides additional protection from malicious embedded threats.

Unlike the Microsoft Windows-based Websense Email Security software product, the on-premises TRITON AP-EMAIL solution is hosted on 1 of the following Websense appliances:

- V-Series (V10000 or V5000)
- X-Series modular chassis blade server (X10G)
- Virtual appliance (VMware platform: ESXi v4.0 or later).

The V-Series appliance can be configured in one of two security modes:

- Email only (single mode)
- Email and Web (dual mode)

Both the X10G security blade and the virtual appliance may be deployed only in Email mode.

Personal Email Manager end-user functions in TRITON AP-EMAIL are hosted on an appliance and accessed through a Windows-based portal. The end-user tool is configured and managed in the Email module management interface.

The Email module is installed on a separate Windows machine. The Email Log Database requires an installation of Microsoft SQL Server.

See a complete list of TRITON AP-EMAIL system requirements in the Websense Technical Library Deployment and Installation Center.

Administration and administrator roles

Websense Email Security administrator settings are available in the Administrator Service section of the Server Configuration dialog box. Roles and permissions for remote administrators are defined, and certificate handling is managed here.

A TRITON AP-EMAIL Super Administrator is created in the TRITON console (**TRITON Settings > Administrators**). This administrator may in turn create other Email module-specific delegated administrators in the TRITON Settings page and manage them in the Email module **Settings > Administrators > Delegated Administrators** screen.

Like Websense Email Security administrators, these administrators may be given a wide range of roles and permissions to view or manage Email module functions. The Super Administrator has full access to all email protection system management functions. In addition to the Super Administrator, the following administrator roles are available in the Email module (**Settings > Administrators > Roles**):

Role	Description
Auditor	Configuration settings view-only permissions
Reporting Administrator	Edit, run, and schedule reports
Security Administrator	Has all Super Administrator permissions, except administrator creation and management
Policy Administrator	Create and manage email policies (rules) for specified users or groups; includes reporting and quarantine queue management for these users or groups
Quarantine Administrator	Manage specified blocked message queues
Group Reporting Administrator	Edit, run, and schedule reports only for users in specified groups

Email policy management

In Websense Email Security, you define and manage a set of rules in order to support your acceptable use policy for email. If an email message triggers a rule, Websense Email Security uses the actions specified in the rule to delay, drop, or isolate the email. The Rules Administrator is a graphical drag-and-drop tool that lets you create a rule to check mail. Content analysis can also be provided by the Websense Email Security Virtual Learning Agent and Dictionary Management functions.

TRITON AP-EMAIL lets you define a policy that is applied to a specified set of email senders and recipients. When a message matches a policy's sender/recipient conditions, that policy is applied to the email. Other defined policies are not applied to that message.

You can create different policies for multiple sets of users in your organization and apply a different set of rules in each policy. Define your email policies in the **Main > Policy Management > Policies** page.

After you define a set of senders and recipients for a policy, you can add the policy rules (a combination of a filter and a filter action) to apply when the sender/recipient conditions of the email match the policy.

Acceptable use and email DLP policies are defined in the Data module.

Policies

In the Email module, you define policies that apply to specific sender/recipient groups. You then specify the rule (the filter and action pair) that determines how a message that matches a sender/recipient condition is analyzed and ultimately processed.

TRITON AP-EMAIL has three general types of policies, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domains (defined as all the domains that an organization owns and needs to protect, listed in **Settings > Users > Domain Groups > Protected Domain Group**):

- Inbound - The sender address is not in a protected domain, and the recipient address is in a protected domain.
- Outbound - The sender address is in a protected domain, and the recipient address is not in a protected domain.
- Internal - Both the sender and recipient addresses are in a protected domain.

The Email module has one default policy for each email direction, as well as a default email DLP policy for each direction. You can modify the email protection policies or define additional policies to suit your specific needs.

You can specify policy application order only for user-created policies. Default policies are always applied last, if the message has matched no other policy conditions.

Content analysis can be configured as part of an email DLP policy. For example, you can include language dictionaries to monitor acceptable use in organization email. See Data Security Manager Help for details about configuring email DLP policies.

An email content policy configured in the Data module may specify that a message should be encrypted for delivery. See *Encryption*, page 7, for information about email encryption options in TRITON AP-EMAIL.

Policy rules

Policy rules determine how a message that matches a policy's sender/recipient conditions is handled. Filters provide the basis for email analysis, and filter actions determine the final disposition of a message that triggers a particular filter. Together, a filter and its action constitute a policy rule.

The Email module includes the following filter types:

Filter	Description
Custom content	Analysis based on user-configured conditions set on message attributes like To and From field addresses, message header, or message subject
URL scanning	Analysis of embedded URLs and classification according to a Websense master database of known spam URLs
Antivirus	Content and attachment analysis to detect the presence of viruses and other threats
Antispam	Analysis to detect any characteristics of spam; uses digital fingerprinting, LexiRules, and heuristics analysis tools
Commercial bulk email	Analysis to determine whether the email sender is a third-party bulk email management company or a business
File sandbox	See *URL and file sandboxing*, page 7, for file sandboxing details.
Disclaimer	When enabled, adds defined text to the beginning or end of a message

These filters may be modified to fit your circumstances, or new filters may be created based on their properties. In general, a policy contains only 1 filter. Note, however, that a custom content filter may analyze a message for multiple message conditions.

Filter actions determine the disposition of a message that triggers a filter:

- Deliver message
- Resume processing
- Drop message

With the deliver or resume processing action, options for header modification, delayed delivery scheduling, blind copy delivery, and others may be configured. A dropped message may be forwarded to a specified address or saved to a message queue.

Email and connection handling

Websense Email Security message handling configuration is set primarily in the Server Configuration console. In this dialog box, the Send, Receive, and Rules services are maintained and connection management controls like protected domains, mail relays, message spoofing, and user authentication settings are specified.

Email protection system message handling is accomplished via a collection of configuration settings in the **Settings > Inbound/Outbound** pages. User validation and authentication options are configured in the **Settings > Users > User Authentication** screen.

Inbound/outbound email options

The Email module **Settings > Inbound/Outbound** section lets you configure the following settings:

- Message controls, like message size and volume limits, invalid recipient settings, bounce address tag validation (BATV), and DomainKeys Identified Mail (DKIM) verification
- Connection options, like real-time blacklist, reverse DNS verification, Websense reputation service, SMTP greeting delay, and the SMTP VRFY command
- True source IP detection, for identifying the IP address of the first sender outside the network perimeter, to prevent IP spoofing and allow effective application of connection controls to sender information
- IP address groups, to define IP addresses that when detected, for example, are exempt from some connection controls (trusted IP addresses)
- Enforced TLS connections, to specify the connections to and from the email appliance that must use TLS and to determine the security level of those connections
- Directory harvest attack controls
- Relay control options, to control message relays in your network and help prevent open relays; also includes settings to check the Sender Policy Framework (SPF) of the sending domain
- Message exception settings, to specify how messages that cannot be processed or delivered for some reason should be handled
- Traffic shaping options, to determine the rate of traffic delivery for a specified source or destination group based on domain group or user directory settings. For example, these settings allow you to send large volumes of email at a rate that prevents possible blacklisting of the domain.
- Address rewriting capabilities, to redirect message delivery to a different recipient address or to mask sender address details from message recipients

Mail delivery routes

Websense Email Security protected domains are identified in the Server Configuration dialog box, in the Email Connection Management screen. Email routes are also defined in the Server Configuration dialog, in the Routing section.

In the Email module, you can configure delivery routes based on the recipient's domain. Configure the domain groups for which you want to define delivery routes in the **Settings > Users > Domain Groups > Add Domain Groups** page.

One of two delivery methods are available:

- Based on SMTP server address, so that messages sent to recipients in specified domains are delivered to a particular appliance. Configuring a delivery preference for each SMTP server facilitates message routing.
- Based on DNS rather than SMTP server address.

Delivery security options include the use of opportunistic TLS or requiring a user to present credentials.

A default domain-based route, which cannot be deleted, is used for routing all domains that are not protected.

URL and file sandboxing

The Websense Email Sandbox Module add-on comprises a set of URL and file sandboxing features that provide advanced security detection to guard against targeted attacks. Cloud-hosted file analysis inspects email attachment file types that commonly contain security threats (including .exe, .pdf, .xls, .xlsx, .doc, .docx, .ppt, .pptx, and archive files). URL sandboxing provides optimal protection via real-time analysis of uncategorized URLs that are embedded in inbound mail. The Email Hybrid module is required for the URL sandbox functionality.

When a user clicks an uncategorized URL, a landing page prompts the user to initiate URL analysis. If the analysis determines that the link is malicious, the site is blocked. If the link is not malicious, users receive notification that they may proceed to the site.

You can create a list of domains to which URL sandbox settings do not apply, along with recipient-specific settings based on domain or email addresses.

Encryption

Websense Email Security uses Smart Host routing to send outbound messages that require encryption to an encryption server. Encryption routing is configured in the Server Configuration dialog box, as part of the Send Service configuration settings. Websense Email Security uses Transport Layer Security (TLS) as its encryption method.

TRITON AP-EMAIL facilitates the secure transmission and delivery of email through encryption. A policy to trigger message encryption must be configured in the Data module. See Data Security Manager Help for information about configuring a policy with an “encrypt” action plan.

Encryption functions are configured on the **Settings > Inbound/Outbound > Encryption** page. The Email module supports the following encryption methods:

- TLS connection encryption
- Hybrid service message encryption, or Websense Advanced Email Encryption (requires the Email Hybrid Module and the Email Encryption Module add-ons)

  These add-on capabilities must be purchased separately.
- Third-party application message encryption

  The third-party application must support the use of x-headers for communication with the Email module.
- Secure messaging

  A secure portal in which an organization’s customers may view, send, and manage email that contains sensitive information.

For detailed information about email encryption, see the Websense TRITON AP-EMAIL Message Encryption paper.

Message queue management

The Monitor, Message Administrator, and QueueView components in Websense Email Security provide message queue viewing and message management capabilities. Real-time viewing is available via the Monitor, while the Message Administrator and QueueView provide blocked and delayed message control.

In TRITON AP-EMAIL, use the Real-Time Monitor (**Main > Status > Real-Time Monitor**) and the message queue options on the **Main > Message Management** pages to view and control email traffic in various default and user-configured message queues. Messages can be isolated (quarantined) so that administrators and end users can decide what to do with them, or those messages can be delivered or dropped.

Messages can be stored in either local or remote queue storage.

Message queues list

The **Main > Message Management > Message Queues** page contains a list of all default and user-created message queues, providing centralized queue management. You can view existing queues, or create and configure new message queues on the Message Queues page. You can also modify queue properties for the following default queues if desired:

- virus
- spam
- exception
- encryption-fail
- decryption-fail
- archive
- secure-encryption
- data-security

The list on the Message Queues page contains the following information about each queue: the queue name, usage status, current message volume, current size, and storage location.

View a message queue by clicking its name. Configure a time range to view a particular set of message records, or perform a search for specific messages, sorting by keyword, sender, recipient, subject, or policy.

Blocked messages queue

The **Main > Message Management > Blocked Messages** queue lists the blocked messages across all appliances together in a single table. A table column entry indicates the name of the queue in which each message is stored. This queue provides centralized search and management capabilities for all the blocked messages in your system. Messages in the archive and Delayed Messages queues are not included on this page.

View a message queue by configuring a time range to see a particular set of message records, or perform a search for specific messages, sorting by keyword, sender, recipient, subject, policy, queue, or appliance name.

Information displayed in the blocked messages list includes the following items:

- Sender email address
- Recipient email address
- Message subject. View detailed message information and message contents by clicking the Subject column link.
- Message size
- Date/time of message receipt
- The policy and rule applied to the message. If an email DLP policy is applied to a message, a View Incident link opens DLP incident information in the Data module, where processing of this message occurs.
- Queue name
- Message type (for example, spam, virus, exception, commercial bulk, encryption error, or decryption error)
- The name of the appliance that processed the message
- The reason why a message has been quarantined

Apply any one of several operations or actions to a selected message in the queue (for example, deliver, delete, forward, resume processing, or not spam).

Delayed messages queue

Email that is temporarily undeliverable due to connection issues is sent to the delayed messages queue (**Main > Message Management > Delayed Messages**). Delayed messages may be automatically resent by the system. Set the retry interval and configure a notification message on the Email module **Settings > Inbound/Outbound > Non-Delivery Options** screen.

Delayed message delivery may also be scheduled using a custom content filter action in a policy, configured on the **Main > Policy Management > Actions > Add** (or **Edit**) **Action** page.

View message queue contents by setting a time range to see a particular set of message records, or perform a search for specific messages, sorting by keyword, sender, recipient, subject, or appliance name.

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. View detailed message information and message contents by clicking the Subject column link.
- Message size
- Date/time of message receipt
- The policy and rule applied to the message. If an email DLP policy is applied to a message, a View Incident link opens DLP incident information in the Data module, where processing of this message occurs.
- Date of the next scheduled message delivery attempt
- The reason a message is delayed. Entries in this column may be one of the following:
  - Exception delay *n*. A temporary delay due to connection issues; *n* is the number of retry attempts remaining for the message.
  - Scheduled delay. An intentional delay that is scheduled via a custom content filter action
  - File sandbox delay. A temporary delay due to in-progress file sandbox analysis
- The name of the appliance that processed the message

Apply any one of several options to a selected message in the queue (for example, release, delete, forward, or download).

Status, logging, and reporting

Websense Email Security system status appears in the Dashboard component, which includes panels for viewing filtering statistics, system alerts and status, connection and filtering activity, and number of messages in each quarantine queue.

In an event-driven environment like Websense Email Security, separate logs are created for each message state. A message with multiple recipients has multiple message log entries. Separate message logs are maintained in Websense Email Security based on message direction: receive log and send log. A connection log records inbound connection attempts, and an audit log maintains a history of actions performed on messages. A system log collects all system activities.

Reports for Websense Email Security are generated in a separate Report Central tool, which copies the Websense Email Security log database and uses that copy to generate its reports.

TRITON AP-EMAIL also has a dashboard for displaying system and message traffic health and status. A collection of logs display data for various email traffic and system activities (**Main > Status > Logs**). Presentation reports are generated within the Email module, in the **Main > Status > Presentation Reports** page.

Dashboard

The TRITON AP-EMAIL dashboard appears when you first log on to the Email module (**Main > Status > Dashboard)**.

The dashboard format provides flexibility for administrators to display message data and system information on the dashboard. The dashboard can display up to 7 dashboard tabs, each of which can accommodate up to 12 charts. You can populate your dashboard tabs with any of the more than 40 customizable charts.

Logging

In the Email module, the log and reporting systems are message-driven rather than event-driven. The scanned results of messages (clean or not), and delivery status (delivered, delayed, or dropped) are written to a single message log rather than to separate logs. A message with multiple recipients has only one log entry, which contains the analysis result and delivery status of each recipient. Other logs in the Email module include:

- Connection log, to record incoming connection attempts and status
- Audit log, to provide an audit trail of Email module administrator actions
- Personal Email Manager log, to record end-user email management activities performed in Personal Email Manager
- System log, to show the current system status, including errors or warnings generated
- Console log, to provide a history of administrator activities in the TRITON console
- Hybrid service log, to record the messages blocked by the email hybrid service (only with the Email Hybrid Module)

To access these logs, go to the **Main > Status > Logs** page and select the appropriate tab. These logs are searchable by predefined time periods, or you can customize the time period you want to search. Some logs also allow you to refine your search for messages, using search conditions like email address, scanning result, or message status.

Real-Time Monitor

Available on the **Main > Status > Real-Time Monitor** page, the Real-Time Monitor lets you view and search for log information for email traffic in real time. View various status details, along with message analysis determination.

Specify any of the following types of log information for display:

- Message status
- Connection status
- Message delivery status
- Message analysis result

Use the search filter to find individual log entries, or use advanced search functions to filter the log entries by subject, IP address, or email address.

Reporting

The Email Log Database receives system health and message traffic data, which it uses to generate reports. The dashboard displays this information in system and email status and activity charts, providing a graphical representation of email protection system value.

The **Main > Status > Presentation Reports** page enables you to generate various reports of system and email activity from predefined report templates. Some templates can be customized to suit specific needs. For example, message data may be sorted by hour, day, week, or month. Run a report immediately or schedule it to be automatically generated and delivered at specified intervals.

If email archiving is a compliance requirement, you may need to maintain your legacy Websense Email Security system and have it available for generating archived email reports. Websense Email Security, the database, and the Report Central report generator should all be running. The recommended length of time to maintain the legacy system should be equal to the length of time defined in your organization's email retention policy.

Database management

Websense Email Security requires an instance of Microsoft SQL Server, either on the same server where Websense Email Security is installed, or on a separate, dedicated server. All database maintenance and download scheduling tasks are configured in one place, the Websense Email Security Scheduler component.

TRITON AP-EMAIL collects data about email traffic and system activity to generate presentation reports and dashboard charts and statistics. Data is sent to a SQL Server Log Database on a Windows Server for storage, where it is accessed to generate a variety of reports and charts. You can configure the main database to create partitions, which can provide flexibility and performance advantages.

In TRITON AP-EMAIL, you configure database maintenance and database downloads in separate locations.

- Database download scheduling is maintained on the **Settings > General > Database Downloads** page.
- Database maintenance tasks are configured on the **Settings > Reporting > Log Database** page.

Data module integration

Integration with the Data module provides an email content analysis capability to prevent sensitive data from leaving the organization. It filters all content outside of antispam and antivirus analysis.

With Websense Email Security, a data security component (an agent) must be manually installed and registered on the SMTP server.

The Email module is tightly integrated with the Data module. It does not require a separate subscription, and leverages email DLP rules, dictionary, fingerprinting, and filter technology.

Registration with the Data module is automatic if you add an appliance to the TRITON console from the Email module interface. Otherwise you need to manually register with the Data module through **Settings > General > Data Loss Protection**. For more information about Data module registration, see Registering the Email DLP Module.

Acceptable use and email DLP policies are defined in the Data module. You can configure custom policies or rules, or apply granular controls to users and groups. Messages in violation of the email DLP policy are quarantined on the Data module management server instead of the email appliance.

For more information on how to configure an email DLP policy, see the Data Security Help topic titled Configuring the Email Data Loss Prevention Policy or the Email DLP Quick Start document.

Personal Email Manager

A Personal Email Manager end-user tool is available for both Websense Email Security and TRITON AP-EMAIL. This facility enables users to review personal lists of quarantined email messages and decide whether to delete the messages or treat them as legitimate email and deliver them.

For Websense Email Security, Personal Email Manager is an optional facility for end users and must be launched separately. The tool includes a My Junk Email page for managing blocked messages. It also lets end users maintain personal Always Allowed and Always Deleted lists.

In TRITON AP-EMAIL, personal email management is integrated and the interface is hosted on am appliance. By default, Personal Email Manager is enabled, but notification message contents and end user authorization for maintaining block and permit lists must be set by the administrator in the **Settings > Personal Email** pages.

Making the Move

Making the transition from Websense Email Security to on-premises TRITON AP-EMAIL requires careful planning. This section outlines some specific issues for your consideration and research to enable a smooth transition to TRITON AP-EMAIL. Topics address issues in the following areas:

- *Before you begin*
- *Install TRITON AP-EMAIL*
- *Get started with TRITON AP-EMAIL*

Before you begin

Before you make the transition to on-premises TRITON AP-EMAIL, you should perform the activities described in the following sections.

Review email protection system requirements

Ensure that your system meets the minimum hardware and operating system requirements. An appliance-based solution, the TRITON AP-EMAIL system should also include Windows servers for the management console and the Email Log Database.

See the online Deployment and Installation Center for complete details on the system resources required to support your deployment.

See the email protection system Deployment Guide for information about deployment options.

Back up your existing system

As a precaution, you should back up your existing Websense Email Security system to save all current configuration settings. You will want to run Websense Email Security in production while you deploy and test the new email protection system.

Use the following steps to back up the system settings in Websense Email Security:

1. From the Database Tools menu, select **Configuration Database Management**. The Configuration Database wizard opens.
2. Select **Backup database to a file**. The SQL/MSDE Server details screen displays.
3. Specify the location of the server that contains the database to be backed up.
   - To connect to the server through a trusted connection, select the **Use trusted connection** check box.
   - To connect to the server using the username and password you specify, clear the **Use trusted connection** check box and enter the username and password.
4. Click **Next**. The Configuration Database Backup Details dialog box displays.
5. Select the database from the drop-down list (default is STEMConfig).

6. Enter or browse to the location of the file where the database is to be saved. Default is:

   Program files\Websense Email Security\Database\STEMConfig_<date>.bak
7. Click **Next**. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
8. A confirmation screen appears when the backup is complete. Click **Finish**.

Archive Log Database

In order to retain Log Database records from your Websense Email Security system, you should archive your existing email logs. You will not be able to access these records directly from the new Email module after the transition is complete.

Use the following steps to archive the Websense Email Security Log Database to a file:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.
2. Select **Archive the log database to a file** and click **Next**. The MSDE/SQL Server Details screen displays.
3. From the **Server** drop-down list, select the server that contains the Log Database.
4. Connect to the server using either:
   - A trusted connection
   - A username and password you supply
5. Click **Next**.
6. Select the Log Database to archive.
7. Browse to the location where you want the archive file to be stored and click **Next**. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
8. A confirmation screen appears when the Log Database has been successfully archived. Click **Finish**.

Print Websense Email Security configuration settings

TRITON AP-EMAIL configuration settings must be entered manually when you make the transition from Websense Email Security, including mail relays, block lists, routes, and SMTP properties. To simplify this manual process, Websense recommends that you print your existing settings, so they are readily available when you configure your new email protection system.

Use the following steps to print your Websense Email Security system configuration settings:

1. Open the Monitor and select **File > Server Configuration**. The Server Configuration Console opens.
2. Click the **Administration Settings** function and click **Print Configuration**. A text file displays all of the Server Configuration settings.

   By default, the name of the file is STEFCFG_date_time (for example, STEFCFG_27_Jun_2014). You can save the file as any name in any location.

Install TRITON AP-EMAIL

On-premises TRITON AP-EMAIL is an appliance-based solution that requires the Email module and an instance of Microsoft SQL Server to be installed on separate Windows Server machines.

Appliance installation instructions for a Websense V-Series appliance are described in the V-Series appliance Getting Started Guide.

The appliance components may also be deployed on a virtual appliance, available from the MyWebsense Downloads page. See the quick start guide for instructions on setting up a virtual appliance. The same Windows component requirements apply to a system that includes a virtual appliance.

In addition, TRITON AP-EMAIL can be deployed on a Websense X-Series modular chassis blade server. See the following resources for information about X-Series appliance deployment:

- X-Series Appliance Command Line Interface Guide
- X-Series Appliance Getting Started Guide

Procedures for installing on-premises TRITON AP-EMAIL and SQL Server can be found in the online Technical Library Deployment and Installation Center:

- Creating TRITON management server
- Obtaining SQL Server

Get started with TRITON AP-EMAIL

This section contains information about the types of settings and activities you need to consider as you start working with on-premises TRITON AP-EMAIL. You should configure and test your email protection system thoroughly before you make it your production environment. Details about some configuration settings appear in a TRITON AP-EMAIL Configuration Information technical paper.

Configure some initial email protection system settings

After you have installed all email protection system product components, you should log on to the Email module user interface and configure some basic settings. The

First-Time Configuration Wizard can guide you through some of these initial system settings, including the following:

- Appliance fully qualified domain name (FQDN)
- Domain-based mail route
- Trusted IP addresses for inbound mail
- Email Log Server information
- System notification email address

The Configuration Wizard is available only once, the first time you log on to the Email module.

Migrate existing Websense Email Security settings

You should have already printed your current Websense Email Security system settings. It is important to know how your existing system is configured so you can successfully replicate it in TRITON AP-EMAIL.

After completing the first-time configuration wizard, you should examine the following areas in the Email module carefully for possible settings modifications, comparing their default settings to your Websense Email Security configuration:

- Message and connection controls (**Settings > Inbound/Outbound**)
- Mail relay controls (**Settings > Inbound/Outbound**)
- Mail routing (**Settings > Inbound/Outbound**)
- User directories (**Settings > Users**)
- User validation/authentication (**Settings > Users**)
- Personal Email Manager end-user options (**Settings > Personal Email**)
- Queue management (**Main > Message Management**)

Integrate the Email Hybrid Module

This section applies only to users who want to deploy the Email Hybrid Module to implement the email hybrid service.

The email hybrid service lets you integrate Websense in-the-cloud email analysis with on-premises TRITON AP-EMAIL. Email hybrid service detects and drops infected email traffic before it reaches the on-premises infrastructure, thereby helping to reduce the traffic load to the on-premises system.

The email hybrid service is available only when your subscription includes the Email Hybrid Module. To enable the email hybrid service, you need to register for the service and then activate it.

See the email Administrator Help topic titled Registering the Email Hybrid Module for detailed instructions on how to configure the email hybrid service.

Review or modify email protection system default policies

As mentioned previously, on-premises TRITON AP-EMAIL has three types of policies, depending on mail traffic direction—inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domains. A predefined default policy exists for each email direction, along with a default email DLP policy.

The default policies apply to all senders and recipients. You can modify the default policies to suit your requirements.

All predefined email policies are enabled by default. You cannot change the order of, or delete, default policies (which are always applied last if a message has not triggered any other policy).

Important

Email DLP policies can only be enabled or disabled in the Email module. To use an email DLP policy, you need to configure it in the Data module. See the Data Security Manager Help topic titled Configuring the Email Data Loss Prevention Policy.

Create email custom policies

On-premises TRITON AP-EMAIL lets you define policies that are applied to specific sets of email senders and recipients. After you define a set of senders and recipients in a policy, you can add the policy rules (a combination of filter and filter action) to apply when the senders and recipients of a message meet policy conditions.

Note

Custom policies developed in Websense Email Security cannot be migrated directly into TRITON AP-EMAIL. You must recreate these policies in the Email module.

You can use TRITON AP-EMAIL custom content filter attributes or the custom properties in the email DLP policy to reproduce your Websense Email Security policies.

For more information on managing policies in the Data module, refer to the Data Security Manager Help topic titled Policies Overview.

Create a custom inbound, outbound, or internal email protection policy in the **Main > Policy Management > Policies > Add Policy** page. Name and describe your new policy and specify the order in which you want this policy applied. Define your sender/recipient conditions, and then determine which policy rules are applied in association with this policy.

See email Administrator Help for detailed information about custom policy configuration.

Create email custom filters

Email protection system filters specify the type of analysis performed on a message that matches a policy's sender/recipient conditions. You can create custom filters that are based on one of the following predefined default filter types:

- Antivirus
- Antispam
- URL scanning (with Web module integration)
- File sandboxing
- Commercial bulk email
- Disclaimer

You can also create a custom content filter to allow analysis based on message attributes like message header or subject. Configure a custom filter on the **Main > Policy Management > Filters > Add Filter** page. For more information on how to create custom filters, see the email Administrator Help topic titled Working with Filters and Policies.

> **Note**
>
> Custom filters and rules developed in Websense Email Security cannot be migrated directly into TRITON AP-EMAIL You must recreate these policies in the Email module.
>
> You can use email custom content filter attributes or custom properties in the email DLP policy.

Generate a report

Reports provide a graphical representation of statistical data captured by the email protection system. Use reports to measure the effectiveness of your email policy implementation, and to view information about email traffic activities and system health.

Verify that your system is collecting the data you need by viewing dashboard charts or running a presentation report. You can use templates from the Report Catalog to generate graphical or tabular reports based on the current database records.

> **Note**
> At some point, you may need to generate a report from a Websense Email Security database. In this case, you must continue to run Websense Email Security in parallel with on-premises TRITON AP-EMAIL. For information, see *Reporting*, page 12.

Generate a report in the Email module on the **Main > Status > Presentation Reports** page. Select the report you want to create in the Report Catalog, and then click **Run**. Configure your date range, select the output format, and then run the report.

For additional instructions on working with reports, see the email Administrator Help topic titled Working with presentation reports.

Test your email protection system

After successfully configuring on-premises TRITON AP-EMAIL, you should test the functionality of the system outside of production to ensure that mail is properly routed, policies are applied correctly, and the system provides adequate security and protection for your network from malicious threats.

The following sections describe some activities that can help you verify that your email system is functioning properly.

Create a staging environment

The staging environment should be a mirror of the actual environment, so that you have a temporary location in which to test your email protection system.

Choose one of the following options for your staging environment:

- **Create a new internal domain**

  You can create a new internal domain that lives within your company or your lab (with its own DNS servers, Exchange Server, and Active Directory). When you create an internal domain, ensure that the email appliance is properly located to manage the email messages for that domain.

- **Register a new domain**

  If you register a new domain, ensure it includes MX records.

Specify the server on which you want to test the email system

You can choose to test the email system on a separate Exchange Server, or on the existing company server.

Create new user accounts

For best practice, set up additional accounts in the existing email client that point to the test server.

Alternatively, you can create new user accounts in the new domain.

Configure delegated administrators

Set up multiple users with different roles and permission levels to verify that administrator privileges in your email protection system work as expected.

Define always block and always permit lists

Provide entries for the lists of addresses that you want always blocked or always permitted. Compose email specifically to test these entries, to ensure that the system performs as expected.

This data cannot be directly imported from Websense Email Security. It must be entered manually in the **Main > Policy Management > Always Block/Permit** page.

Test that the policies, rules, and alerts work as expected

If you have correctly configured the system, on-premises TRITON AP-EMAIL should properly detect and block infected messages based on policy conditions (both for email policies and email DLP policies).

- **Send messages that breach policy**

  Send messages that intentionally breach policy to an email address in your company domain. For example, you could include content that contains spam or sensitive data.
- **Send malicious attachments**

  Send email messages with attachments that include spam or virus content through your email system.
- **Confirm that email traffic is flowing in the right direction**

  Check the transaction volume in TRITON AP-EMAIL.
- **Check the logs regularly**

  View the current state of the email system in the dashboard (**Main > Status**). This page should correctly reflect email traffic activities that have occurred within the past 24 hours.
- **Set up SNMP monitoring and alerting**

  Use the **Settings > Alerts > Enable Alerts** page to enter SNMP settings.
- **Set up a script**

  Write a script to send email messages at predefined time intervals.
- **Check message analysis functions**

  If policies are configured correctly, the email protection system should properly detect and handle messages based on policy conditions.

- **Confirm proper message delivery**

  Check your inbox to see if legitimate email messages are being delivered.
- **Verify appropriate message blocking**

  View the Blocked Messages queue (**Main > Message Management > Blocked Messages**) to see if email messages are being blocked as intended.