Forcepoint TRITON AP-EMAIL Message Encryption

Email Encryption | TRITON AP-EMAIL | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

Forcepoint TRITON AP-EMAIL facilitates the secure transmission and delivery of email through connection and message encryption. Encryption functions are enabled in the TRITON Manager Email module console on the **Settings > Inbound/Outbound > Encryption** page.

This Forcepoint email protection solution supports the following types of message encryption:

- *Mandatory Transport Layer Security (TLS) connection encryption*
- *Advanced email encryption*
- *Third-party application message encryption*

The Forcepoint on-premises email protection solution also offers a Secure Messaging end-user portal in which your organization's customers and email recipients may view, send, and manage email that contains personally identifiable information. For example, you may wish to include sensitive personal health or financial information in a message to a client. The portal provides a secure location for the transmission of this data. See *Forcepoint Secure Messaging portal* for more information.

Mandatory Transport Layer Security (TLS) connection encryption

Email Encryption | TRITON AP-EMAIL | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

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

TRITON AP-EMAIL uses mandatory TLS as its default encryption method (enabled on the **Settings > Inbound/Outbound > Encryption** page.) Opportunistic TLS is used for other email protection functions.

This article offers some TLS basics, including how and where TLS is used in TRITON AP-EMAIL. It also covers TLS certificate handling, along with encryption key and certificate signing request (CSR) generation.

TLS Overview

TLS provides an extra layer of security for email transmissions. With this protocol, email communications can be encrypted to prevent devices such as non-trusted routers from allowing a third party to monitor or alter the communications between a server and client. TRITON AP-EMAIL can receive messages transferred over TLS and can also send messages via this protocol to particular domains. The email protection system uses a TLS encryption level of 128 bits.

Two levels of TLS are used in mail routing and email encryption functions. *Opportunistic TLS* can be enabled and used to protect email transfer communications during the message routing process and when using a third-party application for email encryption. *Mandatory TLS* is used for both the TLS and email hybrid service advanced email encryption options. You can also specify that connections to or from a specific IP or domain group use mandatory TLS via enforced TLS connection options (**Settings > Inbound/Outbound > Enforced TLS Connections**). Configure the security level and encryption strength for the connection on this page as well.

Opportunistic TLS

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.

Opportunistic TLS is used for message routing transfers. Create a new route that uses the TLS delivery option or edit an existing mail route to add the TLS option on the **Settings > Inbound/Outbound > Mail Routing > Add** (or **Edit**) **Route** page. At the bottom of the page, mark the **Use Transport Layer Security (TLS)** check box to use opportunistic TLS for message routing.

The third-party application message encryption feature also uses opportunistic TLS for data transfer security. Third-party application encryption options are configured on the **Settings > Inbound/Outbound > Encryption** page.

Mandatory TLS

As with opportunistic TLS, an encrypted data transfer occurs when the TLS handshake process is successful. Unlike opportunistic TLS, if the handshake fails during the connection attempt, the connection is terminated and no transfer occurs.

The message is placed in a delayed message queue for a later delivery attempt. The message delivery retry interval is configured in the **Settings > Inbound/Outbound > Non-Delivery Options** page.

Mandatory TLS is used for the following encryption options:

- Transport Layer Security (TLS) connection encryption
- Email hybrid service advanced email encryption

These features are enabled and configured on the **Settings > Inbound/Outbound > Encryption** page. If you want to use advanced email encryption, your product subscription must include both the Email Hybrid Module and the Email Encryption Module.

Backup encryption options may be selected if you use default TLS encryption. You can designate advanced email encryption, a third-party application, or secure messaging as a backup method, in case the TLS connection fails. Specifying a backup option allows you a second opportunity for encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

TLS Certificates

TRITON AP-EMAIL enables a default self-signed TLS certificate with product installation that is used for incoming connections. The email protection system presents this certificate during TLS communications.

You can view certificate information and generate a new self-signed certificate on the **Settings > Inbound/Outbound > TLS Certificate** page. You should note that generating a new certificate overwrites any certificate that already exists.

You can also use a certificate from a third-party certificate authority (CA) for outgoing connections. TRITON AP-EMAIL uses CA-issued root and intermediate certificates (along with the default CA certificate bundle) to verify a server certificate presented by a third-party mail server during TLS communications. You need to generate encryption keys and a CSR to send to the CA and then import the purchased certificate files to the Email module.

Because the email hybrid service advanced email encryption option does not perform properly with the self-signed certificate, a trusted third-party certificate from a CA is required. (See *Trusted third-party certificates* for a list of trusted third-party certificates to use with advanced email encryption.)

The following sections provide details about generating encryption keys and a CSR and importing a third-party certificate to the Email module.

Generating encryption keys and a CSR

The process for generating encryption keys and a CSR involves the use of the **OpenSSL** tool, which is available with your installation of TRITON AP-EMAIL.

You can generate a CSR using the following steps:

1. Log on to the TRITON Manager Email module and open a command-line interface as administrator. Navigate to the installation path (by default, **C:\Program Files (x86)\Websense\EIP Infra\apache\bin\openssl**).
2. Execute the following command to create private encryption keys:

   ```
   openssl genrsa -des3 -out certificate.key 2048
   ```

   In this example command, the private keys are output to a file named **certificate.key**, and the key size is 2048 bits.
3. Set a password for the key file when prompted (maximum length is 100 characters).
4. Use the following command to generate the CSR, which contains the private encryption key file you just created:

   ```
   openssl req -new -config "C:\Program Files (x86)\Websense\EIP Infra\apache\conf\openssl.cnf" -key certificate.key -out certificate.csr
   ```

   In this example, **certificate.csr** is the name of the CSR file.
5. When prompted, enter the password you created in step 3.
6. Supply the following information when prompted:
   - Country Name (2-letter code), example: US
   - State or Province Name (full name), example: Texas
   - Locality Name (e.g., city), example: Austin
   - Organization Name (e.g., company), example: Forcepoint
   - Organizational Unit (e.g., section), example: Sales
   - Common Name (e.g., server hostname), example: email.forcepoint.com
   - Email Address, example: sales@forcepoint.com
   - Challenge password

   

   Important

   The value for Common Name must match the fully qualified domain name (FQDN) of the email protection management server. You may receive certificate errors if you do not specify the FQDN here.
7. Send your CSR to a CA for signing. Secure your private key file and passwords; you will need them in order to use your certificate.

Importing certificate files

The option to import a certificate from a CA is available in the TRITON Manager Email module console. Importing a third-party certificate overwrites an existing certificate.

Import a new certificate as follows:

1. Open a command prompt on the TRITON Manager server and run the following command to create a .pfx file that contains your certificate and key:

   ```
   C:\Program Files (x86)\Websense\EIP Infra\apache\bin>
   openssl pkcs12 -export -inkey certificate.key -in
   [certificate file] -out certificate.pfx
   ```

2. When prompted, enter your private key password and set a password for the .pfx file using only alphanumeric characters.
3. On the **Settings > Inbound/Outbound > TLS Certificate** page, click **Import**.
4. Click **Yes** in the confirmation dialog box. An Import Certificate area appears below the **Import** button.
5. Use **Browse** to navigate to your third-party certificate (.pfx) file. When you select the file, its filename appears in the **Certificate file** field.
6. Enter the password you specified in your CSR (maximum length is 100 characters).
7. Click **OK**.

Advanced email encryption

Email Encryption | TRITON AP-EMAIL | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

The email hybrid service can perform cloud-based message encryption on outbound messages if your subscription includes both the Email Hybrid Module and Email Encryption Module.

The email hybrid service must be registered and enabled in order to use advanced email encryption. See TRITON AP-EMAIL Administrator Help for details about hybrid service registration.

After you have successfully registered with the email hybrid service, you should contact Forcepoint Order Processing (op@websense.com) to ask that advanced email encryption capabilities be enabled for your account.

After advanced encryption is enabled, configure advanced email encryption by selecting the **Advanced Email Encryption** option in the **Encryption method** drop-down list (**Settings > Inbound/Outbound > Encryption**).

Because advanced email encryption does not function properly with the self-signed certificate provided with TRITON AP-EMAIL, a trusted third-party certificate from a CA is required. See *Trusted third-party certificates* for a list of trusted certificates to use with the advanced email encryption function. See *Generating encryption keys and a CSR* for information regarding CSR generation.

Message encryption process

A content policy that specifies the conditions under which an outbound message should be encrypted is configured in the TRITON Manager Data module. See Data Security Manager Help for details about configuring an outbound email data loss prevention (DLP) policy with an encryption action plan. See *Creating an email DLP policy for encryption* for a high-level procedure for email DLP policy configuration.

> **Important**
>
> The outbound DLP policy mode set in the Email module console must be set to **Enforce** in order for advanced email encryption to work properly (**Main > Policy Management > Policies > Outbound > Data Loss Prevention**).

When an email DLP policy identifies an outbound message for encryption, the message is sent to the email hybrid service via a TLS connection. If a secure TLS connection is not made, the message is placed in a delayed message queue for a later delivery attempt.

The email hybrid service analyzes a message for threats in email routed for encryption. If threats are detected, the email hybrid service sends a non-delivery receipt (NDR) to the Email module.

If the analyses determine that a message contains no email-borne threats, the hybrid service encrypts the email, which is then sent as an HTML message attachment to the email recipient. Encrypted content is not stored in the cloud during this process. After the email hybrid service encrypts a message, it is forwarded directly to its recipient.

> **Important**
>
> The email hybrid service checks the email appliance FQDN for a valid public "A" record. This record should contain the FQDN IP address.
>
> The email hybrid service also checks the public IP address for an associated PTR, or reverse DNS lookup record. This record must point to the FQDN referenced in the certificate subject and set in the Email module **Settings > General > System Settings** Fully Qualified Domain Name field.

When opened in a browser, the message attachment displays a button that allows the recipient to access a secure encryption network via HTTPS. The email recipient must register an email address and password with the encryption network on first access. This password is used to open all subsequent encrypted messages to this email address.

Encryption is not performed on inbound or internal email messages, although the email protection system can forward inbound email to an encryption gateway for decryption. The DLP policy must designate only outbound messages for encryption

when advanced email encryption is used. See the Data Security Manager Help for details.

When decryption is enabled (**Settings > Inbound/Outbound > Encryption**), the email hybrid service attempts to decrypt inbound encrypted mail, and adds an x-header to the message to indicate whether the decryption operation succeeded. Message analysis is performed regardless of whether message decryption is successful.

Trusted third-party certificates

Advanced email encryption requires a certificate from a third-party CA that is trusted by the email hybrid service. See *Generating encryption keys and a CSR* for information about obtaining a certificate. After you have generated a CSR, follow the third-party CA acquisition procedures for the certificate you want to purchase.

Use a certificate from one of the following trusted CAs for advanced email encryption:

- AddTrust Class 1 CA Root
- AddTrust External CA Root
- AddTrust Public CA Root
- AddTrust Qualified CA Root
- America Online Root Certification Authority 1
- America Online Root Certification Authority 2
- AOL Time Warner Root Certification Authority 1
- AOL Time Warner Root Certification Authority 2
- AS Sertifitseerimiskeskus Juur-SK
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- Baltimore CyberTrust Root
- Bratislava CA Disig
- Buypass Class 2 CA 1
- Buypass Class 3 CA 1
- Certplus Class 2 Primary CA
- certSIGN ROOT CA
- Chambers of Commerce Root
- CNNIC ROOT
- Comodo CA Limited AAA Certificate Services
- Comodo CA Limited Secure Certificate Services
- Comodo CA Limited Trusted Certificate Services
- COMODO Certification Authority
- COMODO ECC Certification Authority

- ComSign Secured CA
- Cybertrust Global Root
- Deutsche Telekom Root CA 2
- Dhimyotis Certigna
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- Digital Signature Trust CA X3
- Digital Signature Trust CA X6
- Digital Signature Trust DSTCA E1
- Digital Signature Trust DSTCA E2
- EDICOM ACEDICOM Root CA
- Entrust Root Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure eBusiness CA-2
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA 2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority - G2
- GeoTrust Primary Certification Authority - G3
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- Global Chambersign Root
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Go Daddy Class 2 CA
- GTE CyberTrust Global Root
- Hongkong Post Root CA 1
- Japanese Government Application CA
- Microsec e-Szigno Root CA
- NetLock Arany (Class Gold) F\xC5\x91tan\xC3\xBAs\xC3\xADtv\xC3\xA1ny
- NetLock Expressz (Class C) Tanusitvanykiado
- NetLock Kozjegyzoi (Class A) Tanusitvanykiado
- NetLock Uzleti (Class B) Tanusitvanykiado

- Network Solutions Certificate Authority
- OISTE WISeKey Global Root GA CA
- PKI Root Certification Authority
- PM/SGDN IGC
- QuoVadis Root CA 2
- QuoVadis Root CA 3
- QuoVadis Root Certification Authority
- RSA Security 1024 V3
- RSA Security 2048 V3
- Secure Global CA
- SecureSign RootCA11
- SecureTrust CA
- Security Communication EV RootCA1
- Security Communication RootCA1
- Sociedad Cameral de Certificaci\xC3\xB3n Digital AC Ra\xC3\xADz Certic\xC3\xA1mara S.A.
- Sonera Class2 CA
- Staat der Nederlanden Root CA
- Staat der Nederlanden Root CA - G2
- Starfield Class 2 Certification Authority
- StartCom Certification Authority
- Swisscom Root CA 1
- SwissSign Gold CA - G2
- SwissSign Silver CA - G2
- Taiwan Government Root Certification Authority
- TC TrustCenter Class 2 CA
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA
- TC TrustCenter Class 3 CA II
- TC TrustCenter Universal CA I
- TDC Internet Root CA
- TDC OCES CA
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- Thawte Timestamping CA

- The USERTRUST Network - DATACorp SGC
- The USERTRUST Network USERFirst-Hardware
- Trustis EVS Root CA
- Trustis FPS Root CA
- Unizeto Certum CA
- ValiCert Class 1 Policy Validation Authority
- ValiCert Class 2 Policy Validation Authority
- ValiCert Class 3 Policy Validation Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- Visa eCommerce Root
- Wells Fargo Root Certificate Authority
- WellsSecure Public Root Certificate Authority
- XRamp Global Certification Authority

Third-party application message encryption

Applies To:	TRITON AP-EMAIL v8.3

TRITON AP-EMAIL supports the use of third-party software for message encryption. Enable this encryption method by selecting the **Third-party application** option in the **Encryption method** drop-down list (**Settings > Inbound/Outbound > Encryption**).

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

TRITON AP-EMAIL can be configured to add an x-header to a message that triggers an encryption policy. Other x-headers can indicate encryption success or failure. These x-headers facilitate communication between the email protection system and the third-party encryption software. You must ensure that the x-header settings made in the Email module Encryption page match the corresponding settings in the third-party software configuration. See TRITON AP-EMAIL Administrator Help for information about configuring the Email module for a third-party encryption application.

You also need to configure an outbound email DLP policy in the Data module. See Data Security Manager Help for details about configuring an email DLP policy with an encryption action plan. See *Creating an email DLP policy for encryption* for a sample email DLP policy configuration.

Preparations for using third-party application encryption also involve the following tasks:

- *Setting the encryption gateway IP address*
- *Setting the encryption gateway options*

Setting the encryption gateway IP address

Perform the following steps in the TRITON Manager Email module to configure the encryption gateway IP address:

1. In the **Settings > Inbound/Outbound > IP Groups** page, click **Encryption Gateway** in the IP Address Group List.
2. In the IP Address Group box, enter the IP address of your encryption gateway machine in the **IP address** field.
3. Click the arrow button to add the address to the Added IP Addresses list.
4. Click **OK**.

Setting the encryption gateway options

Perform the following steps in the Email module to configure the encryption gateway options:

1. In the **Settings > Inbound/Outbound > Encryption** page, select **Third-party application** from the **Encryption method** drop-down list.
2. In the Add Encryption Server area, enter the IP address (or hostname) and port of your encryption gateway server.
3. Mark the **Enable MX lookup** check box to enable the MX lookup function.

Important

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

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

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

4. Click the arrow button to add this information to the Encryption Server List.
5. Ensure that **Encryption Gateway** is displayed in the **Encrypted IP address group** drop-down list. This selection helps to prevent the creation of an email routing loop.
6. If you want users to present credentials to view encrypted mail, mark the **Require authentication** check box and supply the desired user name and password in the appropriate fields. Authentication must be supported and configured on your encryption server to use this function.
7. In the **Encryption X-header** field, enter the header name and value that you created in your third-party application using the following format:

   ```
   header name: value
   ```
8. In the **Encryption success X-header** field, enter the header name and value that you created in your third-party application for the encryption success header using the format shown in the previous step.
9. In the **Encryption failure X-header** field, enter the header name and value that you created in your third-party application for the encryption failure header using the format shown in step 7.
10. Click **OK**.

Creating an email DLP policy for encryption

Email Encryption | TRITON AP-EMAIL | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

See Data Security Manager Help for information about creating an email DLP policy for encryption. The following steps describe how to create a simple email DLP policy with an encryption action plan:

1. In the **Main > Policy Management > DLP Policies > Manage Policies** page, click **Add > Custom Policy**.
2. In the General tab, enter a policy name and description in the **Policy name** and **Description** fields, respectively.
3. Click **Edit** to add the policy owners who can view and edit the policy and receive policy notifications.
4. Click **OK**.
5. Select **Use the policy name for the rule name**, unless you want the rule associated with this policy to have a custom name and description.
6. Click **Next**.
7. In the Condition tab, configure the conditions under which the rule is triggered. Rule conditions include options for patterns and phrases, file properties, and number of email attachments, among others.
8. Click **Next**.
9. In the Severity & Action tab, click the **Add a new action plan** icon.

10. Enter an action plan name and description in the pop-up box.
11. In the **Email** action drop-down list, select **Encrypt**.
12. Click **OK**.
13. Select your new policy action name in the action plan drop-down list in the Severity & Action tab.
14. Click **Next**.
15. In the Source tab, indicate the users and computers to which this rule is applied.
16. Click **Next**.
17. In the Destination tab, ensure that **Outbound** is selected for email traffic direction.
18. Click **Finish**.
19. Deploy your new policy by clicking **Yes** in the Deployment Needed dialog box. You must deploy the policy in the TRITON Manager Data module for your changes to take effect.

Forcepoint Secure Messaging portal

Email Encryption | TRITON AP-EMAIL | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

Forcepoint Secure Messaging provides a secure end-user portal for the transmission and viewing of personally identifiable data in email. You configure the secure portal and the permission levels for your customers and other email recipients on the TRITON Manager Email module **Settings > Inbound/Outbound > Encryption** page.

Select **Secure Message Delivery** from the **Encryption method** drop-down list to display secure messaging options, including a template for the notification that customers receive to alert them to a secure email delivery.

Select the secure email management activities you want to allow your customers to perform from among the following options:

- Reply all
- Forward
- Compose
- Attach file

For each action, you can specify whether your customers can send mail only to your internal domain email addresses, or to external domain email addresses. At least one internal email address is required for the latter option.

An email recipient is prompted to create a portal account on receipt of the first secure message delivery notification. After an account is created, a recipient may be able to

perform some or all of the following activities in the secure messaging portal, depending on the permissions you have configured:

- View a received secure message
- Reply to a received secure message
- Forward a received secure message
- Compose a new secure message
- Include an attachment in a composed secure message
- View secure messages that have been sent
- Send a secure message to Trash
- Perform a keyword search of secure messages

See the topic titled Handling encrypted messages in the Administrator Help for TRITON AP-EMAIL for portal and notification message configuration details. See the Forcepoint Secure Messaging User Help for end-user portal information.