S/MIME Security Services

This chapter contains the following sections:

Overview of S/MIME Security Services

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standards-based method for sending and receiving secure, verified email messages. S/MIME uses public/private key pair to encrypt or sign messages. This way,

- If the message is encrypted, only the message recipient can open the encrypted message.
- If the message is signed, the message recipient can validate the identity of the sender's domain and can be assured that the message has not been altered while in transit.

For more information about S/MIME, review the following RFCs:

- RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling
- RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Message Specification
- RFC 3369: Cryptographic Message Syntax

S/MIME Security Services in Email Gateway

Organizations may want to communicate securely using S/MIME without requiring that all end users possess their own certificates. For such organizations, the email gateway supports S/MIME security services (signing, encryption, verification, and decryption) at the gateway level using certificates that identify the organization rather than the individual user.

The email gateway provides the following S/MIME security services for Business-to-Business (B2B) and Business-to-Consumer (B2C) scenarios:

- Sign, encrypt, or sign and encrypt messages using S/MIME. See Signing, Encrypting, or Signing and Encrypting Outgoing Messages using S/MIME, on page 5.

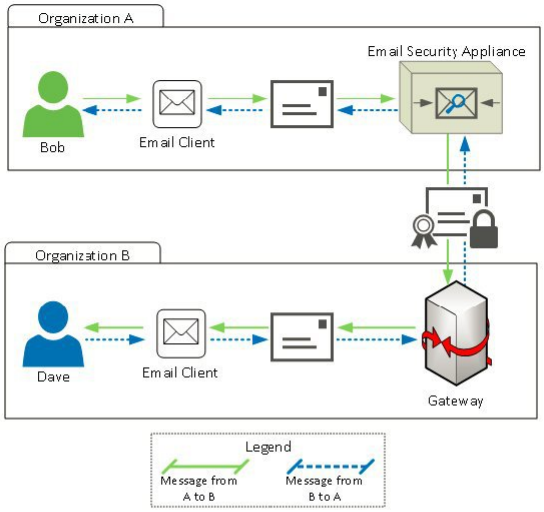
- Verify, decrypt, or decrypt and verify messages using S/MIME. See Verifying, Decrypting, or Decrypting and Verifying Incoming Messages using S/MIME, on page 15.

Related Topics

- Understanding How S/MIME Security Services Works, on page 2

Understanding How S/MIME Security Services Works

Scenario: Business-to-Business



Organizations A and B want all the messages communicated between them to be signed and encrypted using S/MIME. Organization A has configured Cisco Secure Email Gateway to perform S/MIME security services at the gateway level. Organization B has configured a third-party application to perform S/MIME security services at the gateway level.

Note The current example assumes that organization B is using a third-party application to perform S/MIME security services. In the real world, this can be any application or email gateway (including Cisco Secure Email Gateway) that can perform S/MIME security services at the gateway level.

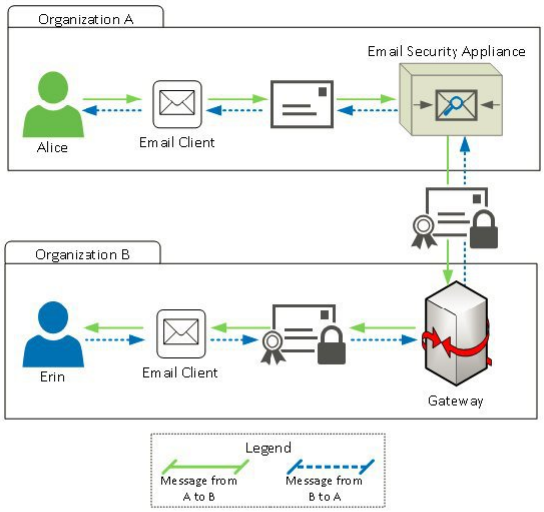
Organization A sending a message to Organization B:

1. Bob (Organization A) uses an email client to send an unsigned and unencrypted message to Dave (Organization B).
2. Cisco Secure Email Gateway in the Organization A signs and encrypts the messages and sends it to Organization B.
3. The third-party application at the gateway of Organization B decrypts and verifies the message.
4. Dave receives an unencrypted and signed message.

Organization B sending a message to Organization A:

1. Dave (Organization B) uses an email client to send an unsigned and unencrypted message to Bob (Organization A).
2. The third-party application at the gateway of Organization B signs and encrypts the message and sends it to Organization A.
3. Cisco Secure Email Gateway in the Organization A decrypts and verifies the message.
4. Bob receives an unencrypted and signed message.

Scenario: Business-to-Consumer



Organizations A and B want all the messages communicated between them to be signed and encrypted using S/MIME. Organization A has configured Cisco Secure Email Gateway to perform S/MIME security services at the gateway level. Organization B has configured the email clients of all the users to perform S/MIME security services.

Organization A sending a message to Organization B:

1. Alice (Organization A) uses an email client to send an unsigned and unencrypted message to Erin (Organization B).
2. Secure Email Gateway in the Organization A signs and encrypts the messages and sends it to Organization B.
3. The email client in the Organization B decrypts and verifies the message and displays it to Erin.

Organization B sending a message to Organization A:

1. Erin (Organization B) uses the email client to sign and encrypt a message and sends it to Alice (Organization A).
2. Secure Email Gateway in the Organization A decrypts and verifies the message.
3. Alice receives an unencrypted and unsigned message.

Signing, Encrypting, or Signing and Encrypting Outgoing Messages using S/MIME

Note You can use the email gateway to sign, encrypt, and sign and encrypt outgoing and incoming messages.

S/MIME Signing and Encryption Workflow in Email Gateway

S/MIME Signing Workflow

The following process describes how the email gateway performs S/MIME signing.

1. Apply a hash algorithm to the message to create a message digest.
2. Encrypt the message digest using private key of the email gateway's S/MIME certificate.
3. Create a PKCS7 signature with the encrypted message digest and public key of the email gateway's S/MIME certificate.
4. Sign the message by attaching the PKCS7 signature to the message.
5. Send the signed message to the recipient.

S/MIME Encryption Workflow

The following process describes how the email gateway performs S/MIME encryption.

1. Create a pseudo-random session key.
2. Encrypt the message body using the session key.
3. Encrypt the session key using the public key of the recipient's (gateway or consumer) S/MIME certificate.
4. Attach the encrypted session key to the message.
5. Send the encrypted message to the recipient.

Note If PXE and S/MIME encryption is enabled on the email gateway, it encrypts messages using S/MIME first, and then using PXE.

How to Sign, Encrypt, or Sign and Encrypt Outgoing Messages using S/MIME

Steps	Do This	More Info
Step 1	Understand the S/MIME certificate requirements.	See S/MIME Certificate Requirements, on page 21.
Step 2	Depending on your requirements, do one of the following: • For S/MIME signing, set up an S/MIME signing certificate. • For S/MIME encryption, set up the public key of the recipient's S/MIME certificate. • For S/MIME signing and encryption, set up an S/MIME signing certificate and the public key of the recipient's S/MIME certificate, respectively.	See: • Setting Up Certificates for S/MIME Signing, on page 7 • Setting Up Public Keys for S/MIME Encryption, on page 9
Step 3	Create a profile for signing, encrypting, or signing and encrypting messages.	See Create an S/MIME Sending Profile for Signing, Encrypting, or Signing and Encrypting Messages, on page 12.
Step 4	Define the conditions that messages must meet in order for the email gateway to sign, encrypt, or sign and encrypt them.	See Determining Which Messages to Sign, Encrypt, or Sign and Encrypt, on page 13.
Step 5	Determine when in the email workflow to sign, encrypt, or sign and encrypt messages.	See: • Signing, Encrypting, or Signing and Encrypting and Immediately Delivering Messages using a Content Filter, on page 14 • Signing, Encrypting, or Signing and Encrypting a Message upon Delivery using a Content Filter, on page 14
Step 6	Define groups of users for whom you want to sign or encrypt messages.	Create a mail policy. See Mail Policies
Step 7	Associate the signing or encryption actions that you defined with the user groups you defined.	Associate the content filter with the mail policy. See Mail Policies

Note If you want to perform S/MIME signing, encryption, or signing and encryption using CLI, use the **`smimeconfig`** command. See *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.

Setting Up Certificates for S/MIME Signing

You must set up an S/MIME certificate for signing messages. The email gateway allows you to set up S/MIME signing certificates using one of the following methods:

- Create a self-signed S/MIME certificate using the email gateway. See Creating a Self-Signed S/MIME Certificate, on page 7.
- Import an existing S/MIME certificate to the email gateway. See Importing an S/MIME Signing Certificate, on page 8.

Note Cisco recommends that you use self-signed S/MIME certificates for sending signed messages to the users within your organization or in a testing environment. For sending signed messages to external users or in a production environment, use a valid S/MIME certificate obtained from a trusted CA.

For understanding the certificate requirements for S/MIME, see S/MIME Certificate Requirements, on page 21.

Creating a Self-Signed S/MIME Certificate

You can generate self-signed S/MIME certificates that are compliant to RFC 5750 (Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling) using the web interface or CLI.

Note Cisco recommends that you use self-signed S/MIME certificates for sending signed messages to the users within your organization or in a testing environment.

Procedure

Step 1 Click **Network** > **Certificates**.

Step 2 Click **Add Certificate**.

Step 3 Choose **Create Self-Signed S/MIME Certificate**.

Step 4 Enter the following information for the self-signed certificate:

Common Name	**The fully qualified domain name.**
Organization	The exact legal name of the organization.
Organizational Unit	Section of the organization.
City (Locality)	The city where the organization is legally located.

Common Name	The fully qualified domain name.
State (Province)	The state, county, or region where the organization is legally located.
Country	The two letter ISO abbreviation of the country where the organization is legally located.
Duration before expiration	The number of days before the certificate expires.
Subject Alternative Name(Domains)	If you configure this field, any user from the specified domain can send signed messages. Name of the domain from which you plan to send signed messages. Examples include domain.com and *.domain.net . For multiple entries, use a comma-separated list.
Subject Alternative Name(Email)	If you configure this field, only the specified users can send signed messages. Email address of the user who is planning to send signed messages, for example, user@somedomain.com . For multiple entries, use a comma-separated list.
Private Key Size	Size of the private key to generate the certificate signing request (CSR).

Note An S/MIME signing certificate can contain both Subject Alternative Name (Domains) and Subject Alternative Name (Email).

Step 5 Click **Next** to view the certificate and signature information.

Step 6 Depending on your requirements, do the following:

- Select the **FQDN Validation** check box to allow the email gateway to check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the certificate, are in the FQDN format.
- Enter a name for the certificate.
- If you want to submit a CSR for the self-signed certificate to a certificate authority, click **Download Certificate Signing Request** to save the CSR in PEM format to a local or network machine.

Step 7 Submit and commit your changes.

What to do next

Note Use the `certconfig` command to generate self-signed S/MIME certificates using CLI.

Importing an S/MIME Signing Certificate

If you already have an S/MIME certificate for signing messages, you can add it to the email gateway by importing it.

Before You Begin

Make sure that the S/MIME certificate that you plan to import meets the requirements described in S/MIME Certificate Requirements, on page 21.

Procedure

Step 1 Click **Network** > **Certificates**.

Step 2 Click **Add Certificate**.

Step 3 Choose **Import Certificate**.

Step 4 Enter the path to the certificate file on your network or local machine.

Step 5 Enter the passphrase for the file.

Step 6 Click **Next** to view the certificate's information.

Step 7 [Optional] Select the **FQDN Validation** check box to allow the email gateway to check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the certificate, are in the FQDN format.

Step 8 Enter a name for the certificate.

Step 9 Submit and commit your changes.

What to do next

Note Use the `certconfig` command to import S/MIME certificates using CLI.

Setting Up Public Keys for S/MIME Encryption

You must add the public key of the recipient's S/MIME certificate to the email gateway for encrypting messages. Depending on your organizational policies and processes, you can use one of the following methods to add the public key to the email gateway:

- Request the recipient to send the public key using an electronic channel, for example, email. You can then add the public key using the web interface or CLI.

  For instructions to add the public key, see Adding a Public Key for S/MIME Encryption, on page 9.

- Enable public key harvesting using the web interface or CLI and request the recipient to send a signed message. The Email Security email gateway can harvest the public key from the signed message.

  For instructions to harvest public key from an incoming signed message, see Harvesting Public Keys, on page 10.

Adding a Public Key for S/MIME Encryption

Before You Begin

- Make sure that the public key meets the requirements described in S/MIME Certificate Requirements, on page 21.
- Make sure that the public key is in PEM format.

Procedure

Step 1 Click **Mail Policies** > **Public Keys**.
Step 2 Click **Add Public Key**.
Step 3 Enter the name of the public key.
Step 4 Enter the public key.
Step 5 Submit and commit your changes.

What to do next

Note Use the `smimeconfig` command to add public keys using CLI.

S/MIME Harvested Public Keys

You can configure the email gateway to retrieve (harvest) public keys from the incoming S/MIME signed messages and use the harvested keys to send encrypted messages to the owners (business or consumer) of the harvested keys.

Public key harvesting can be enabled on the Mail Flow Policies. All the harvested public keys are listed on the S/MIME Harvested Public Keys page.

Related Topic

- Harvesting Public Keys, on page 10

Harvesting Public Keys

You can configure the email gateway to retrieve (harvest) public key from the incoming S/MIME signed messages and use it to send encrypted messages to the owner (business or consumer) of the harvested key.

Note By default, public keys from expired or self-signed S/MIME certificates are not harvested.

Before You Begin

Make sure that the public key of the sender's S/MIME certificate meets the requirements described in S/MIME Certificate Requirements, on page 21.

Procedure

Step 1 Click **Mail Policies** > **Mail Flow Policies**.
Step 2 Create a new Mail Flow Policy or modify an existing one.
Step 3 Scroll down to the **Security Features** section.
Step 4 Under S/MIME Public Key Harvesting, do the following:

- Enable S/MIME public key harvesting.
- (Optional) Choose whether to harvest public keys if the verification of the incoming signed messages fail.
- (Optional) Choose whether to harvest updated public keys.

Note If an email gateway receives more than one updated public key from the same domain or message within 48 hours, it sends out a warning alert.

Step 5 Submit and commit your changes.

What to do next

Note The size of the harvested public key repository on the email gateway is 512 MB. If repository is full,the email gateway will automatically remove unused public keys.

Use the **`listenerconfig`** command to enable key harvesting using CLI.

Next Step

Request the recipient to send a signed message to the email gateway administrator. The email gateway will harvest the public key from the signed message and displays it on the Mail Policies > Harvested Public Keys page.

Related Topics

- S/MIME Harvested Public Keys, on page 10

Managing S/MIME Sending Profiles

An S/MIME sending profile allows you define parameters such as:

- S/MIME mode to use, for example, sign, encrypt, and so on.
- S/MIME certificate for signing
- S/MIME signing mode to use, for example, opaque or detached.
- Action to take if the public key of the recipient's S/MIME certificate is not available on the email gateway.

For example, one organization requires all the messages sent to them be signed and another one requires all the messages sent to them be signed and encrypted. In this scenario, you must create two sending profiles, one for signing alone and one for signing and encryption.

You to can create, edit, delete, import, export, and search S/MIME sending profiles using the web interface or CLI.

Related Topics

- Create an S/MIME Sending Profile for Signing, Encrypting, or Signing and Encrypting Messages, on page 12
- Edit an S/MIME Sending Profile, on page 13

Create an S/MIME Sending Profile for Signing, Encrypting, or Signing and Encrypting Messages

Procedure

Step 1 Click **Mail Policies** > **Sending Profiles**.

Step 2 Click **Add Profile**.

Step 3 Configure the following fields:

S/MIME Profile Name	Enter the name of the sending profile.
S/MIME Mode	Choose the S/MIME mode. Possible values are: • **Sign** • **Encrypt** • **Sign/Encrypt**. Sign and then encrypt • **Triple**. Sign, encrypt, and then sign again **Note** If you are using one of the following S/MIME modes: **Sign**, **Sign/Encrypt**, or **Triple**, messages will be bounced to the sender if the signing fails.
Signing Certificate	Choose the signing certificate to use. **Note** You need to set this field only if you choose one of the following S/MIME modes: **Sign**, **Sign/Encrypt**, or **Triple**.
S/MIME Sign Mode	Choose the mode of S/MIME signing. Possible values are: • **Opaque.** An opaque-signed message contains the message and signature combined in a single part and can be read only by verifying the signature. • **Detached.** The signature information is separate from the text being signed. The MIME type for this is multipart/signed with the second part having a MIME subtype of application/(x-)pkcs7-signature. **Note** You need to set this field only if you choose one of the following S/MIME modes: **Sign**, **Sign/Encrypt**, or **Triple**.

S/MIME Profile Name	Enter the name of the sending profile.
S/MIME Action	Choose the action that the email gateway must take if the recipient's public key is not available. Possible values are: • **Bounce**. The message is bounced to the sender if any one of the recipient's public key is not available. • **Drop**. The message is dropped if any one of the recipient's public key is not available. • **Split**. The message is split. The message to the recipients whose public keys are not available are delivered without encryption and the message to the recipients whose public keys are available are encrypted and delivered. **Example**: Assume that you are sending a message to bob@example1.com and dave@example2.com and the public key of dave@example2.com is not available. In this scenario, if you have selected **Split**, the email gateway will: • Deliver the message to bob@example1.com after encrypting it. • Deliver the message to dave@example2.com without encrypting it. **Note** You need to set this field only if you choose one of the following S/MIME modes: **Encrypt**, **Sign/Encrypt**, or **Triple**.

Step 4 Submit and commit your changes.

What to do next

Note Use the `smimeconfig` command to create sending profiles using CLI.

Edit an S/MIME Sending Profile

Procedure

Step 1 Click **Mail Policies** > **Sending Profiles**.

Step 2 Click on the sending profile that you want to modify.

Step 3 Edit the fields as described in Create an S/MIME Sending Profile for Signing, Encrypting, or Signing and Encrypting Messages, on page 12.

Step 4 Submit and commit your changes.

Determining Which Messages to Sign, Encrypt, or Sign and Encrypt

After you create a sending profile, you need to create an outgoing content filter that determines which email messages should be signed, encrypted, or signed and encrypted. The content filter scans outgoing email and

determines if the message matches the conditions specified. Once the content filter determines a message matches the condition, the email gateway signs, encrypts, or signs or encrypts the message.

Related Topics

- How to Filter Messages Based on Content

Signing, Encrypting, or Signing and Encrypting and Immediately Delivering Messages using a Content Filter

Before You Begin

Understand the concept of building conditions for content filters. See How Content Filters Work.

Procedure

Step 1 Go to **Mail Policies > Outgoing Content Filters**.

Step 2 In the Filters section, click **Add Filter**.

Step 3 In the Conditions section, click **Add Condition.**

Step 4 Add a condition to filter the messages that you want to sign, encrypt, or sign and encrypt. For example, to encrypt sensitive material, you might add a condition that identifies messages containing particular words or phrases, such as “Confidential,” in the subject or body.

Step 5 Click **OK**.

Step 6 In the Actions section, click **Add Action**.

Step 7 Select **S/MIME Sign/Encrypt (Final Action)** from the **Add Action** list.

Step 8 Select the sending profile to associate with the content filter.

Step 9 Click **OK**.

Step 10 Submit and commit your changes.

What to do next

After you add the content filter, you need to add the filter to an outgoing mail policy. You may want to enable the content filter on the default policy, or you may choose to apply the filter to a specific mail policy, depending on your organization’s needs. For information about working with mail policies, see Overview of Mail Policies.

Signing, Encrypting, or Signing and Encrypting a Message upon Delivery using a Content Filter

Create a content filter to sign, encrypt, or sign and encrypt a message on delivery, which means that the message continues to the next stage of processing, and when all processing is complete, the message is signed, encrypted, or signed and encrypted, and delivered.

Before You Begin

- Understand the concept of building conditions for content filters. See Overview of Content Filters.

Procedure

Step 1 Go to **Mail Policies > Outgoing Content Filters**.

Step 2 In the Filters section, click **Add Filter**.

Step 3 In the Conditions section, click **Add Condition.**

Step 4 Add a condition to filter the messages that you want to sign, encrypt, or sign and encrypt. For example, to encrypt sensitive material, you might add a condition that identifies messages containing particular words or phrases, such as “Confidential,” in the subject or body.

Step 5 Click **OK**.

Step 6 In the Actions section, click **Add Action**.

Step 7 Select **S/MIME Sign/Encrypt on Delivery** from the **Add Action** list.

Step 8 Select the sending profile to associate with the content filter.

Step 9 Click **OK**.

Step 10 Submit and commit your changes.

What to do next

After you add the content filter, you need to add the filter to an outgoing mail policy. You may want to enable the content filter on the default policy, or you may choose to apply the filter to a specific mail policy, depending on your organization’s needs. For information about working with mail policies, see Overview of Mail Policies.

Verifying, Decrypting, or Decrypting and Verifying Incoming Messages using S/MIME

Note You can use the email gateway S/MIME security services to verify, decrypt, or decrypt and verify outgoing and incoming messages.

S/MIME Verification and Decryption Workflow in Email Gateway

S/MIME Verification Workflow

The following process describes how the email gateway performs S/MIME verification.

1. Apply a hash algorithm to the signed message to create a message digest.
2. Decrypt the PKCS7 signature attached to the signed message using the public key of the sender's S/MIME certificate, and get the message digest.
3. Compare the generated message digest with the message digest retrieved from the signed message. If the message digests match, the message is verified.
4. Validate the S/MIME certificate of the sender domain with the Certificate Authority.

S/MIME Decryption Workflow

The following process describes how the email gateway performs S/MIME decryption.

1. Decrypt the session key using the private key of the email gateway's S/MIME certificate
2. Decrypt the message body using the session key.

How to Verify, Decrypt, or Decrypt and Verify Incoming Messages Using S/MIME

Steps	Do This	More Info
Step 1	Understand the S/MIME certificate requirements.	See S/MIME Certificate Requirements, on page 21.

Step 2	Depending on your requirements, do one of the following:
	• For S/MIME decryption, add your organization's S/MIME certificate (that contains the private key required to perform decryption) to the email gateway.
	• For S/MIME verification, add the public key of the sender's S/MIME certificate required to perform verification to the email gateway.
	• For S/MIME decryption and verification, add the following to the email gateway:
	  • Your organization's S/MIME certificate (that contains the private key required to perform decryption) to the email gateway.
	  • Certificate Authority of the sender domain.
	  • Public key of the sender's S/MIME certificate required to perform verification.
		See
		• Setting Up Certificates for Decrypting Messages, on page 17
		• Setting Up Public Keys for Verifying Signed Messages, on page 18
		• Importing a Custom Certificate Authority List

Step 3	Configure your mail flow policies to verify, decrypt, or decrypt and verify incoming messages using S/MIME.	See Enabling S/MIME Decryption and Verification, on page 20.

Steps	Do This	More Info
Step 4	(Optional) Define the action that the email gateway takes on decrypted or verified messages.	See Configuring an Action for S/MIME Decrypted or Verified Message, on page 20.

Note If you want to perform S/MIME verification, decryption, or decryption and verification using CLI, use the `listenerconfig > hostaccess` command. See the CLI inline help for more details.

Setting Up Certificates for Decrypting Messages

You must add your organization's S/MIME certificate (that contains the private key required to perform decryption) to the email gateway.

Before You Begin

- Share the public key of the email gateway's S/MIME certificate with the sender (business or consumer) in one of the following ways:
  - Send the public key using an electronic channels, for example, email.
  - Request the sender to the retrieve the public key using key harvesting.

  The sender can use this public key to send encrypted messages to your email gateway.

Note In a B2C scenario, if your organization's S/MIME certificate is a domain certificate, some email clients (for example, Microsoft Outlook) may not be able to send encrypted messages using the public key of your organization's S/MIME certificate. This is because these email clients do not support encryption using public keys of domain certificates.

- Make sure that the S/MIME certificate that you plan to import meets the requirements described in S/MIME Certificate Requirements, on page 21.

Procedure

Step 1 Click **Network** > **Certificates**.
Step 2 Click **Add Certificate**.
Step 3 Choose **Import Certificate**.
Step 4 Enter the path to the certificate file on your network or local machine.
Step 5 Enter the passphrase for the file.
Step 6 Click **Next** to view the certificate's information.
Step 7 Enter a name for the certificate.
Step 8 Submit and commit your changes.

What to do next

Note Use the **certconfig** command to add the S/MIME certificates using CLI.

Setting Up Public Keys for Verifying Signed Messages

You must add the public key of the sender's S/MIME certificate to the email gateway for verifying signed messages. Depending on your organizational policies and processes, you can use one of the following methods to add the public key to the email gateway:

- Request the sender to send their public key using an electronic channels, for example, email. You can then add the public key using the web interface or CLI.

  For instructions to add the public key, see Adding a Public Key for S/MIME Encryption, on page 9.

- Retrieve the public key using key harvesting. See Harvesting Public Keys, on page 10.

Adding a Public Key for S/MIME Verification

Before You Begin

- Make sure that the public key meets the requirements described in S/MIME Certificate Requirements, on page 21.
- Make sure that the public key is in PEM format.

Procedure

Step 1 Click **Mail Policies** > **Public Keys**.

Step 2 Click **Add Public Key**.

Step 3 Enter the name of the public key.

Step 4 Enter the public key.

Step 5 Submit and commit your changes.

What to do next

Note Use the **smimeconfig** command to add public keys using CLI.

Harvesting Public Keys for S/MIME Verification

You can configure the email gateway to retrieve (harvest) public key from the incoming S/MIME signed messages and use it to verify signed messages from the owner (business or consumer) of the harvested key.

Note By default, public keys from expired or self-signed S/MIME certificates are not harvested.

1. Enable public key harvesting using the web interface or CLI. See Enabling Public Key Harvesting, on page 19.
2. Request the sender to send a signed message.
3. After the harvesting is complete, add the harvested public key to the email gateway. See Adding a Harvested Public Key for S/MIME Verification, on page 19.

This step is to ensure that the message is verified at the gateway level.

Enabling Public Key Harvesting

Procedure

Step 1 Click **Mail Policies** > **Mail Flow Policies**.

Step 2 Create a new Mail Flow Policy or modify an existing one.

Step 3 Scroll down to the **Security Features** section.

Step 4 Under S/MIME Public Key Harvesting, do the following:

- Enable S/MIME public key harvesting.
- (Optional) Choose whether to harvest public keys if the verification of the incoming signed messages fail.
- (Optional) Choose whether to harvest updated public keys.

Note If an email gateway receives more than one updated public key from the same domain or message within 48 hours, it sends out a warning alert.

Step 5 Submit and commit your changes.

What to do next

Note The size of the harvested public key repository on the email gateway is 512 MB. If the repository is full used, the email gateway automatically removes unused public keys.

Use the `listenerconfig` command to enable key harvesting using CLI.

Adding a Harvested Public Key for S/MIME Verification

Procedure

Step 1 Click **Mail Policies** > **Harvested Public Keys**.

Step 2 Click on the intended harvested public key and copy the public key.

Step 3 Add the public key to the email gateway. See Adding a Public Key for S/MIME Verification, on page 18.

Step 4 Submit and commit your changes.

Enabling S/MIME Decryption and Verification

Procedure

Step 1 Click **Mail Policies** > **Mail Flow Policies**.

Step 2 Create a new Mail Flow Policy or modify an existing one.

Step 3 Scroll down to the **Security Features** section.

Step 4 Under S/MIME Decryption/Verification, do the following:

- Enable S/MIME decryption and verification.
- Choose whether to retain or remove the digital signature from the messages after S/MIME verification. If you do not want your end users to know about S/MIME gateway verification, select **Remove**.

For triple wrapped messages, only the inner signature is retained or removed.

Step 5 Submit and commit your changes.

What to do next

Tip If S/MIME Decryption and Verification is enabled in the Mail Flow Policies, all the S/MIME messages are delivered irrespective of the status of the decryption and verification. If you want to configure an action for handling S/MIME Decrypted or Verified Messages, you can use the message filter rules—smime-gateway-verified and smime-gateway . For more information, see Configuring an Action for S/MIME Decrypted or Verified Message, on page 20.

Configuring an Action for S/MIME Decrypted or Verified Message

After the email gateway performs S/MIME decryption, verification, or both, you may want to take different actions depending on the results. You can use the message filter rules— smime-gateway-verified and smime-gateway to perform actions on the messages based on the result of decryption, verification, or both. For more information, see Using Message Filters to Enforce Email Policies

Note You can also use the content filter conditions—**S/MIME Gateway Message** and **S/MIME Gateway Verified** to perform actions on the messages based on the result of decryption, verification, or both. For more information, see Content Filters

Example: Quarantine S/MIME Messages that failed Verification, Decryption, or Both

The following message filter checks if the message is an S/MIME message and quarantines it if the verification or decryption using S/MIME fails.

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified)
{ quarantine("Policy"); }
```

S/MIME Certificate Requirements

Certificate Requirements for Signing

The S/MIME certificate for signing must contain the following information:

Common Name	**The fully qualified domain name.**
Organization	The exact legal name of the organization.
Organizational Unit	Section of the organization.
City (Locality)	The city where the organization is legally located.
State (Province)	The state, county, or region where the organization is legally located.
Country	The two letter ISO abbreviation of the country where the organization is legally located.
Duration before expiration	The number of days before the certificate expires.
Subject Alternative Name(Domains)	Name of the domain from which you plan to send signed messages. Examples include domain.com and *.domain.net . For multiple entries, use a comma-separated list.
Subject Alternative Name(Email)	Email address of the user who is planning to send signed messages, for example, user@somedomain.com . For multiple entries, use a comma-separated list.
Private Key Size	Size of the private key to generate for the CSR.
Key Usage	Key usage is a restriction method that determines what a certificate can be used for. If the key usage extension is specified, the following bits: digitalSignature and nonRepudiation must be set. If the key usage extension is not specified, receiving clients must presume that the digitalSignature and nonRepudiation bits are set.

For detailed information about S/MIME certificates, see RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling.

Certificate Requirements for Encryption

The S/MIME certificate for encryption must contain the following information:

Common Name	The fully qualified domain name.
Organization	The exact legal name of the organization.
Organizational Unit	Section of the organization.
City (Locality)	The city where the organization is legally located.
State (Province)	The state, county, or region where the organization is legally located.
Country	The two letter ISO abbreviation of the country where the organization is legally located.
Duration before expiration	The number of days before the certificate expires.
Subject Alternative Name(Domains)	Name of the domain to which you plan to send encrypted messages. Examples include domain.com and *.domain.net . For multiple entries, use a comma-separated list. If you plan to send encrypted messages to all the users in a domain, the public key should include a SAN Domain.
Subject Alternative Name(Email)	Email address of the user to whom you plan to send encrypted messages, for example, user@somedomain.com . For multiple entries, use a comma-separated list.
Private Key Size	Size of the private key to generate for the CSR.
Key Usage	Key usage is a restriction method that determines what a certificate can be used for. The key usage extension must be specified and the following bit must be set: keyEncipherment .

For detailed information about S/MIME certificates, see RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling.

Managing Public Keys

the email gateway requires:

- The public key of the recipient's S/MIME encryption certificate for encrypting the outgoing messages.
- The public key of the sender's S/MIME signing certificate for verifying incoming signed messages.

You can add public keys to your email gateway in one of the following ways:

- If you have the intended public key in PEM format, you can add it using the web interface or CLI. See Adding a Public Key, on page 23.
- If you have an export file that contains the intended public keys, you can copy the export file to the /configuration directory and import it using the web interface or CLI. See Importing Public Keys from an Existing Export File, on page 23.

The email gateway also supports key harvesting (automatically retrieving public keys from incoming signed messages). For more information, see S/MIME Harvested Public Keys, on page 10.

Adding a Public Key

Before You Begin

- Make sure that the public key meets the requirements described in S/MIME Certificate Requirements, on page 21.
- Make sure that the public key is in PEM format.

Procedure

Step 1 Click **Mail Policies** > **Public Keys**.

Step 2 Click **Add Public Key**.

Step 3 Enter the name of the public key.

Step 4 Enter the public key.

Step 5 Submit and commit your changes.

What to do next

Note Use the `smimeconfig` command to add public keys using CLI.

Importing Public Keys from an Existing Export File

Before You Begin

Copy the export file to the /configuration directory of the email gateway. For instructions to create an export file, see Exporting Public Keys, on page 24.

Procedure

Step 1 Click **Mail Policies** > **Public Keys**.

Step 2 Click **Import Public Keys**.

Step 3 Select the export file and click **Submit**.

Note The import process may take longer if you are importing a file with large number of public keys. Make sure that you adjust the web interface or CLI inactivity timeout accordingly.

Step 4 Commit your changes.

Exporting Public Keys

All public keys on the email gateway are exported together in a single text file and stored in the /configuration directory.

Procedure

Step 1 Choose **Mail Policies > Public Keys**.

Step 2 Click **Export Public Keys**.

Step 3 Enter a name for the file and click **Submit**.