Overview

The Cisco Secure Email Encryption Service (Encryption Service) is a hosted service that provides support for Cisco Encryption technology. Encryption Service works in conjunction with Cisco Secure Email Gateways and Cisco Encryption appliances, which provide on-premises content scanning, policy enforcement, and encryption. Encryption Service stores per-message encryption keys for encrypted messages. Recipients of encrypted messages authenticate themselves with the service to receive decryption keys.

Note The latest version of this guide and other Encryption Service documentation is available on this https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html.

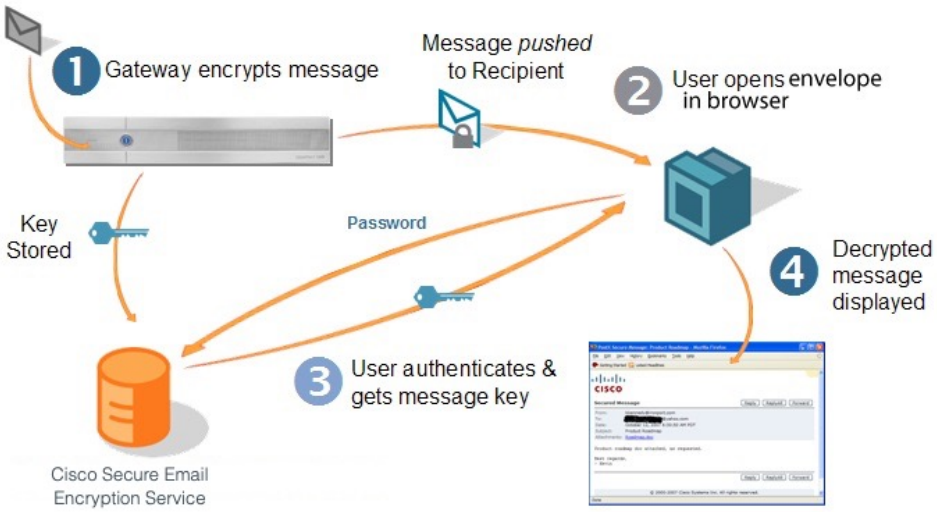
- Role of Cisco Secure Email Encryption Service in Encryption, on page 1
- Corporate Account Administration, on page 2

Role of Cisco Secure Email Encryption Service in Encryption

The service manages the following elements of encryption:

- **Recipient Enrollment—** Recipients of a Secure Message (an encrypted message) must enroll with the service the first time they open an envelope, unless the message is sent with low security. Enrollment is free of charge.
- **Authentication—** Enrolled users use Single Sign-On (SSO) or provide a password to open Secure Messages and read encrypted messages.
- **Encryption Keys—** An encryption key is created for each encrypted message. When enrolled recipient enter their password in the Secure Message, the service sends the decryption key that opens the envelope.
- **Message Expiration and Locking—** Enrolled users can set the expiration date and control message locking for the encrypted messages that they send. Corporate account administrators can control expiration dates and message locking for all encrypted messages sent using the corporate account.
- **Secure Forward and Secure Reply Messages—**Depending on the corporate account configuration, recipients may be able to forward and reply to encrypted messages using encryption. Encryption Service handles the encryption for Secure Forward and Secure Reply messages.

The following figure shows how Encryption Service works in conjunction with a Cisco Secure Email Gateway. The service supplies the decryption key to the registered recipient of a encrypted message.



The above figure explains the following process:

Procedure

Step 1 The Cisco Secure Email Gateway uses encryption to encrypt a message and deliver it.

Step 2 The recipient enters the Encryption Service password in the Secure Message.

Note If the message is configured for low security, then the recipient need not enter a password to open the secure envelope.

Step 3 Encryption Service supplies the decryption key that opens the envelope.

Step 4 The recipient's web browser displays the decrypted message.

Corporate Account Administration

Encryption Service provides administrative functionality for corporate accounts of organizations. The initial Encryption Service administration role is assigned to the Registered Technical Contact. An administrator for a corporate account performs the following tasks:

- Customize the logo displayed on Secure Message
- Manage messages sent through the service
- Generate account usage reports
- Manage users (such as lock accounts and reset passwords)
- Configure TLS settings for encrypted secure reply without requiring a secure message