FIPS Management

This chapter contains the following sections:

FIPS Management Overview

The Federal Information Processing Standard (FIPS) 140 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by government agencies to protect sensitive but unclassified information. The Cisco Secure Email and Web Manager uses the CiscoSSL Cryptographic Toolkit to achieve FIPS 140-2 Level 1 compliance.

The CiscoSSL Cryptographic Toolkit is a GCT-approved cryptography suite that includes CiscoSSL, which is an enhanced version of OpenSSL's FIPS support, and the FIPS-compliant Cisco Common Cryptography Module. The Cisco Common Cryptography Module is a software library that Secure Email and Web Manager uses for FIPS-validated cryptographic algorithms for protocols such as SSH and TLS.

Note The Cisco Secure Email and Web Manager FIPS Certification only applies to email gateway integration and not to Secure Web Appliance integration.

Configuration Changes in FIPS Mode

The Secure Email and Web Manager uses Cisco SSL and FIPS-compliant certificates for communication when the appliance is in FIPS mode. See Switching the Appliance to FIPS Mode, on page 2 for more information.

To be FIPS Level 1 compliant, the Secure Email and Web Manager makes the following changes to your configuration:

- **SMTP receiving and delivery**: Incoming and outgoing SMTP conversations over TLS between a public listener on the Secure Email and Web Manager and a remote host use TLS version 1.1 or 1.2 and FIPS cipher suites. TLS v 1.1 and 1.2 are the version of TLS supported in FIPS mode.

- **Web interface**: HTTPS sessions to the Secure Email and Web Manager's web interface use TLS version 1.1 or 1.2 and FIPS cipher suites. This also includes HTTPS sessions to the Spam Quarantine and other IP interfaces.
- **LDAPS**: TLS transactions between the Secure Email and Web Manager and LDAP servers, including using an LDAP server for external authentication, use TLS version 1.1 or 1.2 and FIPS cipher suites. If the LDAP server uses MD5 hashes to store passwords, the SMTP authentication query will fail because MD5 is not FIPS-compliant.
- **Logs**: SSH2 is the only allowed protocol for pushing logs via SCP. For error messages related to FIPS management, read the FIPS Logs at the INFO level.
- **SSL Ciphers**: Only the FIPS compliant SSL ciphers are supported.

Switching the Appliance to FIPS Mode

Use the `fipsconfig` CLI command to switch the appliance over to FIPS mode.

Note Only administrators can use this command. A reboot is required after switching the appliance from non-FIPS mode to FIPS mode.

Before You Begin

Make sure that the appliance do not have any objects that are not FIPS compliant. To enable FIPS mode, you must modify all the non-FIPS-compliant objects to meet FIPS requirements. See Configuration Changes in FIPS Mode, on page 1. For instructions to check if your appliance contains non-FIPS-compliant objects, see Checking FIPS Mode Compliance, on page 3.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup

In FIPS mode, the RSA certificates must have 2048 bits or more key length, and the MD5
algorithm is deprecated.
It is not recommended to add WSA (in FIPS or non-FIPS mode) to an SMA in FIPS Mode.
It is not recommended to add ESA in non-FIPS mode to an SMA in FIPS Mode.
It is not recommended to move SMA to FIPS Mode when the connected ESA or WSA is in non-FIPS
 mode.

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to enable FIPS mode and reboot now ? [N]> y
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

Checking FIPS Mode Compliance

Use the `fipsconfig` command to check if your Secure Email and Web Manager contains any non-FIPS-compliant objects.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck
All objects in the current configuration are FIPS compliant.
FIPS mode is currently disabled.
```