FIPS 管理

本章包含以下部分：

FIPS 管理概述

联邦信息处理标准 (FIPS) 140 是美国和加拿大联邦政府共同开发且公开发布的标准，其中规定了政府机构用于保护敏感但非保密性信息的密码模块的要求。思科安全邮件和 Web 管理器使用思科 SSL 密码工具条件来实现 FIPS 140-2 1 级合规。

Cisco SSL 密码工具包是一个 GGSG 批准的加密套件，其中包括 作为 OpenSSL FIPS 支持增强版的 Cisco SSL 以及符合 FIPS 标准的思科通用加密模块。思科通用加密模块是一个软件库，供思科安全邮件和 Web 管理器用于对 SSH 等协议的 FIPS 验证密码算法。

Note 思科安全邮件和 Web 管理器 FIPS 认证仅适用于邮件网关集成，而不适用于安全 Web 设备集成。

FIPS 模式下的配置更改

当设备处于 FIPS 模式时，思科安全邮件和 Web 管理器使用 Cisco SSL 和符合 FIPS 标准的证书进行通信。有关详细信息，请参阅将设备切换到 FIPS 模式, on page 2。

为了符合 FIPS 级别 1 标准，思科安全邮件和 Web 管理器会对配置进行以下更改：

- **SMTP 接收和传送**：在思科邮件安全和 Web 管理器设备上的公共侦听程序与远程主机之间通过 TLS 进行的传入和传出 SMTP 会话使用 TLS 第 1.1 版或 1.2 版及 FIPS 密码套件。TLS v 1.1 和 1.2 是在 FIPS 模式下支持的唯一版本的。
- **Web 界面**：与思科邮件安全和 Web 管理器的 Web 界面进行的 HTTPS 会话使用 TLS 第 1.1 版或 1.2 版和 FIPS 密码套件。这还包括与垃圾邮件隔离区和其他 IP 接口的 HTTPS 会话。

- **LDAPS**：思科安全邮件和 Web 管理器与 LDAP 服务器之间的 TLS 事务（包括使用 LDAP 服务器进行外部身份验证）使用 TLS 第 1.1 版或 1.2 版和 FIPS 加密套件。如果 LDAP 服务器使用 MD5 散列存储密码，则由于 MD5 不符合 FIPS 标准，因此 SMTP 身份验证查询会失败。
- **日志**：SSH2 是允许通过 SCP 推动日志的唯一协议。对于与 FIPS 管理相关的错误消息，请阅读信息级别的 FIPS 日志。
- **SSL 密码**：仅支持符合 FIPS 的 SSL 密码。

将设备切换到 FIPS 模式

使用 `fipsconfig` CLI 命令将设备切换到 FIPS 模式。

Note 只有管理员可以使用此命令。将设备从非 FIPS 模式切换到 FIPS 模式后，需要重新启动。

准备工作

确保设备没有任何不符合 FIPS 的对象。要启用 FIPS 模式，必须修改所有不符合 FIPS 标准的对象以符合 FIPS 要求。请参阅FIPS 模式下的配置更改, on page 1。有关检查设备是否包含不符合 FIPS 标准的对象的说明，请参阅检查 FIPS 模式合规性, on page 2。

程序

```
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...
```

检查 FIPS 模式合规性

使用 `fipsconfig` 命令检查思科安全邮件和 Web 管理器是否包含任何不符合 FIPS 标准的对象。

程序

```
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.
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。