安全认证合规性

安全认证合规性

美国联邦政府机构有时需要仅使用符合由美国国防部和全球认证组织建立的安全标准的设备和软件。Firepower 4100/9300 机箱支持符合其中若干安全认证标准。

请参阅以下主题，了解支持符合这些标准的功能的启用步骤：

- 启用 FIPS 模式
- 启用通用标准模式
- 配置 IPSec 安全通道， 第 3 页
- 配置信任点静态 CRL， 第 9 页
- 关于证书撤销吊销列表检查， 第 10 页
- 配置 CRL 定期下载， 第 13 页
- 使用 NTP 设置日期和时间
- 设置 LDAP 密钥环证书， 第 15 页
- 配置 IP 访问列表
- 启用客户端证书身份验证， 第 16 页
- 配置最小密码长度检查

- 设置最大尝试登录次数

注释 请注意，这些主题只讨论在 Firepower 4100/9300 机箱上启用认证合规性。在 Firepower 4100/9300 机箱上启用认证合规性不会将合规性自动传播到它连接的任何逻辑设备。

生成 SSH 主机密钥

在 FXOS 版本 2.0.1 之前，设备初始设置期间创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥并生成新的主机密钥。有关详细信息，请参阅《启用 FIPS 模式》 或 《启用通用标准模式》 。

执行以下步骤，以销毁旧的 SSH 主机密钥并生成新的符合认证证书要求的主机密钥。

过程

步骤 1 从 FXOS CLI 进入服务模式：

scope system

scope services

步骤 2 删除 SSH 主机密钥：

delete ssh-server host-key

步骤 3 提交配置：

commit-buffer

步骤 4 将 SSH 主机密钥长度设置为 2048 位：

set ssh-server host-key rsa 2048

步骤 5 提交配置：

commit-buffer

步骤 6 创建新的 SSH 主机密钥：

create ssh-server host-key

commit-buffer

步骤 7 确认新的主机密钥长度：

show ssh-server host-key

主机密钥长度：2048

配置 IPSec 安全通道

IPSec 是由互联网工程任务组 (IETF) 开发的一个开放标准框架。它可以在 IP 网络上创建安全、经过身份验证和可靠的通信。IPsec 安全服务提供：

- 无连接完整性 - 确保接收的流量未被修改。
- 数据源身份验证 - 确保流量是由合法方发送的。
- 保密性（加密）- 确保用户的流量不被非授权方检查。
- 访问控制 - 防止未经授权使用资源。

注释 IPSec 连接只能从 FXOS 启动。FXOS 不接受传入的 IPSec 连接请求。

IPsec 隧道是 FXOS 在对等体之间建立的 SA 集合。SA 指定适用于敏感数据的协议和算法并指定对等体使用的密钥内容。IPSec SA 控制用户流量的实际传输。SA 是单向的，但是通常成对建立（入站和出站）。

机箱管理器上的 IPSec 有两种模式：

传输模式
IP 报头，IPSec 报头，TCP 报头，数据

隧道模式
新 IP 报头，IPSec 报头，原始 IP 报头，TCP 报头，数据

IPSec 的操作可分为五个主要步骤：

1. 流量选择 - 匹配 IPSec 策略的需要关注的流量会启动 IKE 进程。例如，可以使用 src/dst 主机 IP 或子网选择流量。或者，用户也可以通过 admin 命令来触发 IKE 进程。
2. IKE 第 1 阶段 - 对 IPSec 对等体进行身份验证，并设置安全通道以启用 IKE 交换
3. IKE 第 2 阶段 - 协商 SA 以设置 IPSec 隧道。SA 代表安全关联，它是 IPSec 终端之间的关系，描述了用于保护数据流量的安全服务。
4. 数据传输 - 使用 SA 中存储的参数和密钥将数据包加密并封装在 IPSec 报头中
5. IPSec 隧道终止 - IPSec SA 通过删除或超时终止。

您可以在 Firepower 4100/9300 机箱上配置 IPSec，对通过公用网络的数据包提供端到端数据加密和身份验证服务。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 1 页。

注释

- 如果您在 FIPS 模式下使用 IPSec 安全通道，则 IPSec 对等体必须支持 RFC 7427。
- 如果选择配置执行 IKE 和 SA 连接间加密密钥强度的匹配（在以下步骤中将 sa-strength-enforcement 设为 yes）：

启用 SA 执行后：	在 IKE 协商的密钥大小小于 ESP 协商的密钥大小时，连接失败。 IKE 协商的密钥大小大于或等于 ESP 协商的密钥大小时，SA 执行检查通过并且连接成功。
禁用 SA 执行后：	SA 执行检查通过且连接成功。

执行以下步骤，以配置 IPSec 安全通道。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 创建密钥环：

enter keyring ssp

! create certreq subject-name *subject-name* **ip** *ip*

步骤 3 输入关联的证书请求信息：

enter certreq

步骤 4 设置国家/地区：

set country *country*

步骤 5 设置 DNS：

set dns *dns*

步骤 6 设置邮件：

set e-mail 邮件

步骤 7 设置 IP 信息：

set ip *ip-address*

set ipv6 *ipv6*

步骤 8 设置位置：

set locality *locality*

步骤 9 设置组织名称：

set org-name *org-name*

步骤 10 设置组织单位名称：

set org-unit-name *org-unit-name*

步骤 11 设置密码：

! set password

步骤 12 设置状态：

set state *state*

步骤 13 设置 certreq 的主题名称：

set subject-name *subject-name*

步骤 14 退出：

exit

步骤 15 设置模数：

set modulus *modulus*

步骤 16 设置证书请求的重新生成：

set regenerate *{ yes | no }*

步骤 17 设置信任点：

set trustpoint interca

步骤 18 退出：

exit

步骤 19 输入新创建的信任点：

enter trustpoint interca

步骤 20 生成证书签名请求：

set certchain

示例：

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAsG
A1UECwwEU1RCVTELMAkGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWC3NzcEBzc3Au
bmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
```

```
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FlRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzYxVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRJW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
```

```
-----END CERTIFICATE-----
ENDOFBUF
```

步骤 21 显示证书签名请求：

show certreq

示例：

```
Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/lTKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPlX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

步骤 22 进入 IPSec 模式：

scope ipsec

步骤 23 设置日志冗长级别：

set log-level *log_level*

步骤 24 创建并输入一个 IPSec 连接：

enter connection *connection_name*

步骤 25 将 IPSec 模式设置为隧道或传输：

set mode *tunnel_or_transport*

步骤 26 设置本地 IP 地址：

set local-addr *ip_address*

步骤 27 设置远程 IP 地址：

set remote-addr *ip_address*

步骤 28 如果使用隧道模式，则设置远程子网：

set remote-subnet *ip/mask*

步骤 29 （可选）设置远程身份：

set remote-ike-ident *remote_identity_name*

步骤 30 设置密钥环名称：

set keyring-name *name*

步骤 31 （可选）设置密钥环密码：

set keyring-passwd *passphrase*

步骤 32 （可选）设置 IKE-SA 生命周期（分钟）：

set ike-rekey-time *minutes*

minutes 值可以是 60-1440（包含在内）之间的任何整数。

步骤 33 （可选）设置子 SA 生命周期（分钟）(30-480)：

set esp-rekey-time 分钟

minutes 值可以是 30-480（包含在内）之间的任何整数。

步骤 34 （可选）设置初次连接期间重新传输序列的执行次数：

set keyringtries *retry_number*

retry_number 值可以是 1-5（包含在内）之间的任何整数。

步骤 35 （可选）启用或禁用证书吊销列表检查：

set revoke-policy *{ relaxed | strict }*

步骤 36 启用连接：

set admin-state enable

步骤 37 重新加载连接：

reload-conns

系统会停止所有连接，然后重新加载它们。系统将尝试重新建立所有连接。

步骤 38 （可选）将现有信任点名称添加至 IPsec：

create authority *trustpoint_name*

步骤 39 配置执行 IKE 和 SA 连接间加密密钥强度的匹配：

set sa-strength-enforcement *yes_or_no*

配置信任点静态 CRL

已吊销证书保留在证书吊销列表 (CRL) 中。客户端应用使用 CRL 检查服务器的身份验证。服务器应用利用 CRL 授予或拒绝来自不再受信任的客户端应用的访问请求。

您可配置 Firepower 4100/9300 机箱以使用证书吊销列表 (CRL) 信息验证对等证书。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 1 页。

执行这些步骤以使用 CRL 信息验证对等证书。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 进入信任点模式：

scope trustpoint *trustname*

步骤 3 进入吊销模式：

scope revoke

步骤 4 下载 CRL 文件：

import crl *protocol*://*user_id@CA_or_CRL_issuer_IP*/tmp/*DoDCA1CRL1.crl*

注释 FXOS 中不支持 DER 格式静态 CRL。必须使用以下命令将 DER 格式 CRL 文件转换为 PEM 格式：

```
openssl crl -in filename.crl -inform DER -outform PEM -out crl.pem
```

步骤 5 （可选）显示 CRL 信息的导入过程状态：

show import-task detail

步骤 6 将证书撤销方法设置为仅限于 CRL：

set certrevokemethod {crl}

关于证书撤销吊销列表检查

您可以在IPSec、HTTPS和安全LDAP连接中将证书吊销列表(CRL)检查模式配置为“严格”或“宽松”。

FXOS 从 X.509 证书的 CDP 信息中获取动态（非静态）CRL 信息，该信息指示动态 CRL 信息。系统管理人员会手动下载指示 FXOS 系统中的本地 CRL 信息的静态 CRL 信息。FXOS 根据证书链中当前正在处理的证书处理动态 CRL 信息。静态 CRL 信息则应用于整个对等证书链。

有关启用或禁用对安全IPSec、LDAP和HTTPS连接的证书吊销检查的具体步骤，请参阅配置 IPSec 安全通道、创建 LDAP 提供程序和配置 HTTPS。

注释

- 如果“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”，则仅当对等证书链具有级别 1 或更高级别时，静态 CRL 才适用。（例如，当对等证书链仅包含根 CA 证书和根 CA 签名的对等证书时。）
- 为 IPSec 配置静态 CRL 时，导入的 CRL 文件中必须具有“授权密钥标识符 (authkey) (Authority Key Identifier [authkey])”字段。否则，IPSec 会将其视为无效。
- 静态CRL优先于来自同一颁发者的动态CRL。当FXOS验证对等证书时，如果存在同一颁发者的有效（已确定）静态 CRL，FXOS 会忽略对等证书中的 CDP。
- 默认在以下场景中启用严格 CRL 检查：
  - 新创建的安全 LDAP 提供程序连接、IPSec 连接或客户端证书条目
  - 新部署的 FXOS 机箱管理器（使用 FXOS 2.3.1.x 或更高版本的初始启动版本部署）

下表说明了连接结果，具体取决于证书吊销列表检查设置和证书验证。

表 *1:* 无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	需要完整的证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链	需要完整的证书链
针对对等证书链的根CA证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
对等证书链中缺少一个 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接失败，系统显示系统日志消息
无法下载对等证书链中的任何 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，但 CDP 服务器已关闭	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，服务器已启动且 CRL 在 CDP 上具有 CRL，但 CRL 具有无效签名	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息

表 *2:* 具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个 CDP（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功

具有本地静态 CRL	LDAP 连接	IPSec 连接
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有CDP，连接会失败并生成系统日志消息

表 *3:* 无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	完整的证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链	完整的证书链
针对对等证书链的根CA证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个 CDP	连接成功	连接成功	连接失败，系统显示系统日志消息
某个CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接成功
无法下载对等证书链中的任何 CDP	连接成功	连接成功	连接成功
证书具有CDP，但CDP服务器已关闭	连接成功	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但CRL 具有无效签名	连接成功	连接成功	连接成功

表 *4:* 具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个CDP（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有CDP，连接会失败并生成系统日志消息

配置 CRL 定期下载

您可将系统配置为定期下载 (CRL)，以便每隔 1 至 24 小时使用新的 CRL 验证证书。

您可将以下协议和接口用于该功能：

- FTP
- SCP
- SFTP

- TFTP
- USB

注释
- 不支持 SCEP 和 OCSP。
- 每个 CRL 仅可配置一个定期下载。
- 每个信任点支持一个 CRL。

注释 您仅可以一小时为间隔配置周期。您只能以一小时为间隔配置周期。

执行以下步骤，以配置 CRL 定期下载。

开始之前

确保您已配置 Firepower 4100/9300 机箱以使用 (CRL) 信息验证对等证书。有关详细信息，请参阅配置信任点静态 CRL ， 第 9 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 进入信任点模式：

scope trustpoint

步骤 3 进入吊销模式：

scope revoke

步骤 4 编辑吊销配置：

sh config

步骤 5 设置首选配置：

示例：

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
```

```
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

步骤 6 退出配置文件：

exit

步骤 7 （可选）通过下载新 CRL 测试新配置：

示例：

```
Firepower-chassis /security/trustpoint/revoke # sh import-task

Import task:
File Name Protocol Server          Port      Userid        State
--------- -------- --------------- ---------- -------------- -----
rootCA.crl Scp     182.23.33.113   0         myname        Downloading
```

设置 LDAP 密钥环证书

您可配置安全的 LDAP 客户端密钥环证书，以便在支持 Firepower 4100/9300 机箱上的支持 TLS 连接。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 1 页。

注释 如果启用“通用标准 (Common Criteria)”模式，则必须启用 SSL，且必须使用服务器 DNS 信息创建密钥环证书。

如果为 LDAP 服务器条目启用 SSL，则系统会在建立连接时引用和检查密钥环信息。

LDAP 服务器信息必须是 CC 模式下用于安全 LDAP 连接（启用 SSL）的 DNS 信息。

执行以下步骤，以配置安全的 LDAP 客户端密钥环证书：

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 进入 LDAP 模式：

scope ldap

步骤 3 进入 LDAP 服务器模式：

enter server *{server_ip|server_dns}*

步骤 4 设置 LDAP 密钥环：

set keyring *keyring_name*

步骤 5 提交配置：

commit-buffer

启用客户端证书身份验证

您可使系统将客户端证书与LDAP结合使用，对HTTPS访问用户进行身份验证。Firepower 4100/9300机箱上的默认身份验证配置基于凭据。

注释 启用证书身份验证后，这是允许用于 HTTPS 的唯一一种身份验证形式。

客户端证书身份验证功能的 FXOS 2.1.1 版本不支持证书吊销检查。

客户端证书必须满足以下要求，才能使用此功能：

- 用户名必须包含在 X509 属性“证书持有者备用名称 - 邮件 (Subject Alternative Name - Email)”中。
- 客户端证书必须由已将其证书导入到管理引擎上的信任点的根 CA 进行签名。客户端证书必须由已将其证书导入到管理引擎上的信任点的根 CA 签名。

过程

步骤 1 从 FXOS CLI 进入服务模式：

scope system

scope services

步骤 2 （可选）查看 HTTPS 身份验证选项：

set https auth-type

示例：

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

步骤 3 将 HTTPS 身份验证设为基于客户端：

set https auth-type cert-auth

步骤 4 提交配置：

commit-buffer