数字证书

本章介绍如何配置数字证书。

- 关于数字证书，第 1 页
- 数字证书指南，第 8 页
- 配置数字证书，第 11 页
- 如何设置特定整数类型，第 30 页
- 设置证书到期警报（对于身份或 CA 证书），第 32 页
- 监控数字证书，第 33 页
- 证书管理历史记录，第 35 页

关于数字证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或IP地址。CA 负责管理证书请求和颁发数字证书。CA 是负责“签署”证书以验证证书真实性的可信机构，旨在确保设备或用户的身份真实有效。

数字证书还包括用户或设备的公钥副本。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。

如果使用数字证书进行身份验证，则 ASA 上必须存在至少一个身份证书及其颁发 CA 证书。此配置允许多个身份、根和证书层次结构。ASA 根据 CRL（也称为权限吊销列表）评估第三方证书，从身份证书一直到从属证书颁发机构链。

以下是几种不同类型的可用数字证书的说明：

- CA 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。
- CA 还会颁发身份证书，这是特定系统或主机的证书。
- 代码签名证书是用于创建数字签名以签署代码的特殊证书，经过签署的代码会透露证书源。

本地 CA 在 ASA 上集成独立的证书颁发机构功能，并且会部署证书，对已颁发的证书提供安全的吊销检查。本地 CA 凭借通过网站登录页面进行的用户注册提供安全、可配置的内部机构进行证书身份验证。

注释 CA 证书和身份证书适用于站点间 VPN 连接和远程访问 VPN 连接。本文档中的程序是指 ASDM GUI 中使用的远程访问 VPN。

提示 有关包括证书配置和负载均衡的情景示例，请参阅以下 URL：https://supportforums.cisco.com/docs/DOC-5964。

公钥加密

通过公钥加密实现的数字签名为设备和用户提供了一种身份验证方法。在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数 Web 浏览器都使用若干 CA 的根证书进行配置。对于 VPN，作为 IPsec 组件的 IKE 协议可使用数字签名在设置安全关联之前验证对等设备身份。

证书可扩展性

在没有数字证书的情况下，必须手动为每个与其通信的对等体配置各自的 IPSec 对等体；因此，每个添加到网络的新对等体都会要求对需要与其安全通信的每个对等体进行配置更改。

使用数字证书时，系统将向 CA 注册每个对等体。两个对等体试图进行通信时，它们将交换证书并以数字方式签署数据以进行相互身份验证。新对等体添加到网络时，会向 CA 注册该对等体，其他任何对等体都不需要修改。新对等体尝试进行 IPSec 连接时，证书将自动交换并且对等体可进行身份验证。

通过CA，对等体可将证书发送到远程对等体并执行一些公钥加密，从而自行向远程对等体进行身份验证。每个对等体发送由 CA 颁发的唯一证书。此过程之所以适用，是因为每个证书会封装关联对等体的公钥，每个证书由 CA 进行身份验证，且所有参与对等体都将 CA 视为身份验证机构。此过程称为带 RSA 签名的 IKE。

对等体可继续为多个 IPsec 会话发送其证书，并可向多个 IPSec 对等体发送证书，直到证书过期。证书过期后，对等体管理员必须从 CA 获取新的证书。

CA 还可以为不再参与 IPsec 的对等体吊销证书。已吊销的证书无法被其他对等体识别为有效证书。吊销的证书列在 CRL 中，在从其他对等体接收证书之前，每个对等体都可以对其进行检查。

某些 CA 在其实施过程中会使用 RA。RA 是一种用作 CA 的代理的服务器，以便 CA 功能可以在 CA 不可用时继续使用。

密钥对

密钥对包括 RSA 或椭圆曲线签名算法 (ECDSA) 密钥，具有以下特征：

- RSA 密钥可用于 SSH 或 SSL。
- SCEP 注册支持 RSA 密钥的认证。
- 最大 RSA 密钥大小为 4096，默认值为 2048。
- 最大 ECDSA 密钥长度为 521，默认值为 384。
- 您可以生成一个用于签名和加密的通用 RSA 密钥对，也可以为每种用途生成单独的 RSA 密钥对。单独的签名和加密密钥有助于减少密钥泄露，因为 SSL 使用密钥进行加密，但不签名。但是，IKE 使用密钥进行签名，但不加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

信任点

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

定义信任点之后，您可以在要求指定CA的命令中根据名称对其进行引用。您可以配置多个信任点。

注释 如果 ASA 有多个共享同一个 CA 的信任点，则只有其中一个共享该 CA 的信任点可用来验证用户证书。要控制使用哪个共享 CA 的信任点来验证该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 命令。

对于自动注册，信任点必须使用注册 URL 进行配置，并且信任点代表的 CA 必须在网络中可用且必须支持 SCEP。

您可以 PKCS12 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式对于在其他 ASA 上手动复制信任点配置来说非常有用。

证书注册

ASA 的每个信任点都需要一个 CA 证书，自身需要一个或两个证书，具体取决于信任点所用的密钥配置。如果信任点使用单独的 RSA 密钥进行签名和加密，则 ASA 需要两个证书，每个任务一个。在其他密钥配置中，只需要一个证书。

ASA 支持使用 SCEP 自动注册，也支持手动注册，后者可让您将 base-64 编码的证书直接复制到终端。对于站点间 VPN，您必须注册每个 ASA。对于远程访问 VPN，则必须注册每个 ASA 以及每个远程访问 VPN 客户端。

SCEP 请求的代理

ASA 可以代理 AnyConnect 客户端 和第三方 CA 之间的 SCEP 请求。如果 ASA 用作代理，则 CA 只需要允许它访问即可。为使 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用 AAA 支持的任何方法进行身份验证。您还可以使用主机扫描和动态访问策略执行注册资格规则。

ASA 仅对 AnyConnect 客户端 SSL 或 IKEv2 VPN 会话支持此功能。它支持所有符合 SCEP 的 CA，包括 Cisco IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。

无客户端（基于浏览器）访问不支持 SCEP 代理，但 WebLaunch（无客户端启动的 AnyConnect 客户端）则支持该代理。

ASA 不支持证书的轮询。

ASA 支持此功能的负载均衡。

撤销检查

颁发证书后，该证书在固定时期内有效。有时，CA 会在此时期到期前吊销证书，例如，因为安全问题、名称更改或关联。CA 会定期发布签署的已吊销证书列表。启用撤销检查会强制 ASA 检查每当它使用证书进行身份验证时，CA 都尚未撤销证书。

启用撤销检查后，ASA 会在 PKI 证书验证过程中检查证书撤销状态，可以使用 CRL 和/或 OCSP 检查。仅当第一种方法返回错误时（例如，指示服务器不可用时），才会使用 OCSP。

通过 CRL 检查，ASA 将检索、分析和缓存 CRL，从而提供包含其证书序列号的撤销（以及未撤销）证书完整列表。ASA 根据 CRL（也称为授权撤销列表）评估证书，从身份证书一直到从属证书颁发机构链。

OCSP 提供了一种更具可扩展性的吊销状态检查方法，此方法通过验证机构对证书状态进行本地化，而验证机构会查询特定证书的状态。

支持的 CA 服务器

ASA 支持以下 CA 服务器：

思科 IOS CS、ASA 本地 CA 和符合 X.509 标准的第三方 CA 供应商，包括但不限于：

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape

- Microsoft 证书服务
- RSA Keon
- Thawte
- VeriSign

CRL

CRL 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 吊销。CRL 配置是信任点配置的一部分。

进行证书身份验证时，您可以使用 **revocation-check crl** 命令将 ASA 配置为强制进行 CRL 检查。您也可以使用 **revocation-check crl none** 命令将 CRL 检查设为可选检查，从而在 CA 无法提供更新后的 CRL 数据时，证书身份验证也会成功。

注释 恢复了在 9.13(1) 中删除的 **revocation-check crl none**。

ASA 可使用 HTTP、SCEP 或 LDAP 从 CA 检索 CRL。为每个信任点检索的 CRL 会在为每个信任点配置的时间内一直缓存。

注释 虽然 CRL 服务器使用 HTTP 标志“Connection：Keep-alive”进行响应以指示持久连接，但 ASA 不会请求支持持久连接。更改CRL服务器上的设置，以便在发送列表时以“Connection: Close”响应。

当ASA缓存CRL的时间超过配置的CRL缓存时间时，ASA会认为该CRL的版本过旧而不可靠（即“过时”）。下次证书身份验证要求检查过时 CRL 时，ASA 会尝试检索更新版本的 CRL。

如果超出 CRL 16MB 的大小限制，您可能收到针对用户连接/证书的 *revocation check* 故障。

ASA 缓存 CRL 的时间由以下两个因素确定：

- 使用 **cache-time** 命令指定的分钟数。默认值为 60 分钟。
- 检索到的 CRL 中的 NextUpdate 字段，CRL 中可能没有该字段。您可使用 **enforcenextupdate** 命令控制 ASA 是否需要和使用 NextUpdate 字段。

ASA 通过以下方式使用这两个因素：

- 如果不需要 NextUpdate 字段，则 会在经过由 **cache-time** 命令定义的时间长度后将 CRL 标记为过时。
- 如果需要 NextUpdate 字段，则 ASA 会在由 **cache-time** 命令和 NextUpdate 字段指定的两个时间中较早的那个时间将 CRL 标记为过时。例如，如果 **cache-time** 命令设置为 100 分钟，而 NextUpdate 字段指定下一次更新是在 70 分钟后，则 ASA 会将 CRL 标记为在 70 分钟内过时。

如果 ASA 的内存不足以存储为给定信任点缓存的所有 CRL，它将删除最近最少使用的 CRL 来为新检索的 CRL 腾出空间。大型 CRL 需要大量计算开销来进行解析。因此，为了获得更好的性能，请使用多个较小的 CRL，而不是几个大型 CRL，或者最好使用 OCSP。

请参阅以下缓存大小：

- 单情景模式 - 128MB
- 多情景模式 - 每个情景 16MB

OCSP

OCSP 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 吊销。OCSP 配置是信任点配置的一部分。

OCSP 在 ASA 查询特定证书状态的验证颁发机构（一台 OCSP 服务器，又称响应方）上本地化证书状态。相比 CRL 检查，此方法可提供更好的可扩展性和更新的吊销状态，并且可帮助组织进行大型 PKI 安装部署和扩展安全网络。

注释 ASA 会为 OCSP 响应留出 5 秒的时间偏差。

进行证书身份验证时，您可以使用 **revocation-check ocsp** 命令将 ASA 配置为强制进行 OCSP 检查。您也可以使用 **revocation-check ocsp none** 命令将 OCSP 检查设为可选检查，从而在验证机构无法提供更新后的 OCSP 数据时，证书身份验证也会成功。

注释 在 9.13(1) 中删除的 **revocation-check ocsp none** 已恢复。

OCSP 提供三种定义 OCSP 服务器 URL 的方法。ASA 按以下顺序使用这些服务器：

1. 使用 **match certificate** 命令在匹配证书覆盖规则中定义的 OCSP URL。
2. 使用 **ocsp url** 命令配置的 OCSP URL。
3. 客户端证书的 AIA 字段。

注释 要将信任点配置为验证自签名 OCSP 响应方证书，请将自签名响应方证书作为可信 CA 证书导入其自己的信任点。然后，在验证信任点的客户端证书中配置 **match certificate** 命令，以使用包括自签名 OCSP 响应方证书的信任点来验证响应器证书。使用同一程序配置客户端证书的验证路径外部配置验证响应方证书。

OCSP 服务器（响应方）证书通常会签署 OCSP 响应。收到响应后，ASA 会尝试验证响应方证书。CA 通常会将 OCSP 响应方证书的有效期设置为相对较短的时间以将受危害的可能性降至最低。CA 通常还会在响应方证书中包含 ocsp-no-check 扩展，表明此证书不需要进行吊销状态检查。但如此此扩展不存在，ASA 将尝试使用信任点中指定的相同方法检查吊销状态。如果响应方证书无法验证，则吊销检查失败。为了避免出现这种可能性，请使用 **revocation-check none** 命令来配置验证信任点的响应方证书，并使用 **revocation-check ocsp** 命令来配置客户端证书。

证书和用户登录凭证

下一节介绍使用证书和用户登录凭证（用户名和密码）进行身份验证和授权的不同方法。这些方法适用于 IPsec、 AnyConnect 客户端和无客户端 SSL VPN。

在所有情况下，LDAP 授权都不会使用密码作为凭证。RADIUS 授权对所有用户使用公用密码或使用用户名作为密码。

用户登录凭证

身份验证和授权的默认方法是使用用户登录凭证。

- 身份验证
  - 通过隧道组（也称为 ASDM 连接配置文件）中的身份验证服务器组设置进行启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过隧道组（也称为 ASDM 连接配置文件）中的授权服务器组设置进行启用
  - 使用用户名作为凭证

证书

如果配置了数字证书，ASA 首先会验证该证书。但是，它不会使用证书的任何 DN 作为用户名进行身份验证。

如果启用了身份验证和授权，ASA 会使用用户登录凭证进行用户身份验证和授权。

- 身份验证
  - 通过身份验证服务器组设置进行启用
  - 使用用户名和密码作为凭证

- 授权
  - 通过授权服务器组设置进行启用
  - 使用用户名作为凭证

如果禁用身份验证，但启用授权，ASA 将使用主 DN 字段进行授权。

- 身份验证
  - 通过身份验证服务器组设置进行禁用（设置为 None）
  - 未使用凭证
- 授权
  - 通过授权服务器组设置进行启用
  - 使用证书主 DN 字段的用户名值作为凭证

注释 如果证书中不存在主 DN 字段，ASA 将使用辅助 DN 字段值作为授权请求的用户名。

以包含以下 Subject DN 字段和值的用户证书为例：

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

如果主 DN = EA（邮件地址），辅助 DN = CN（公共名称），则授权请求中使用的用户名将为 anyuser@example.com。

数字证书指南

本节介绍在配置数字证书之前应检查的准则和限制。

情景模式准则

- 对于第三方 CA，仅在单情景模式下受支持。

故障切换准则

- 在有状态的故障切换中不支持复制会话。
- 对于本地 CA，不支持故障切换。
- 如果配置状态故障切换，证书会自动复制到备用设备。如果发现证书缺失，请在主用设备上使用**write standby**命令。

IPv6 准则

不支持 IPv6。

本地 CA 证书

- 确保已正确配置 ASA 以支持证书。ASA 配置不正确可能会导致注册失败或请求的证书包括错误信息。
- 确保 ASA 的主机名和域名配置正确。要查看当前配置的主机名和域名，请输入 **show running-config** 命令。
- 在配置 CA 之前，确保 ASA 时钟设置正确。证书具有生效日期和时间以及到期日期和时间。当 ASA 注册到 CA 并获取证书时，ASA 会检查当前时间是否在证书的有效范围内。如果超出范围，则注册失败。
- 在本地 CA 证书到期前 30 天，系统会生成一个滚动更新替代证书，并且系统日志消息将通知管理员到时间进行本地 CA 滚动更新。新的本地 CA 证书必须在当前证书到期前导入到所有必要的设备上。如果管理员未通过将滚动更新证书安装为新的本地 CA 证书作出响应，则验证可能会失败。
- 本地 CA 证书将在到期后使用相同的密钥对自动滚动更新。滚动更新证书可使用 base 64 格式导出。

  以下示例显示 base 64 编码的本地 CA 证书：

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP 代理支持

- 确保 ASA 和思科 ISE 策略服务节点使用相同的 NTP 服务器进行同步。
- AnyConnect 客户端 终端上必须运行 3.0 或更高版本。
- 在组策略的连接配置文件中配置的身份验证方法必须设置为同时使用 AAA 身份验证和证书身份验证。
- 对于 IKEv2 VPN 连接，SSL 端口必须处于打开状态。
- CA 必须处于自动授予模式下。

其他准则

- 可以使用的证书类型受使用证书的应用支持的证书类型限制。使用证书的所有应用通常都支持RSA证书。但工作站操作系统，浏览器，ASDM 或 AnyConnect 客户端可能不支持 EDDSA 证书。例如，您需要使用RSA证书进行远程接入VPN身份和身份验证。对于ASA是使用证书的应用的站点间VPN，支持EDDSA。
- 对于配置为 CA 服务器或客户端的 ASA，证书的有效期限制为小于建议的结束日期：2038 年 1 月 19 日 03:14:08 UTC。本准则还适用于从第三方供应商导入的证书。
- 仅当满足以下任一认证条件时，ASA 才会建立 LDAP/SSL 连接：
  - LDAP 服务器证书受信任（存在于信任点或 ASA 信任池中）且有效。
  - 来自服务器颁发链的 CA 证书是受信任的（存在于信任点或 ASA 信任池）中，链中的所有从属 CA 证书都已完成且有效。
- 证书注册完成后，ASA 将存储包含用户的密钥对和证书链的 PKCS12 文件，该文件每次注册需要约 2 KB 的闪存或磁盘空间。实际的磁盘空间容量取决于已配置的 RSA 密钥长度和证书字段。在可用闪存容量有限的 ASA 上添加大量待处理的证书注册时，请记住此准则，因为这些 PKCS12 文件在配置的注册检索超时期间存储在闪存中。我们建议使用至少 2048 位的密钥长度。
- 应将 ASA 配置为使用身份证书来保护传至管理接口的 ASDM 流量和 HTTPS 流量。每次重新启动后都会重新生成使用 SCEP 自动生成的身份证书，因此请确保手动安装您自己的身份证书。有关仅应用于 SSL 的此操作步骤的示例，请参阅以下 URL：http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA 和 AnyConnect 客户端 只能验证其中 X520Serialnumber 字段（主题名称中的序列号）为 PrintableString 格式的证书。如果序列号格式使用编码（例如 UTF8），则证书授权将失败。
- 仅当在 ASA 上导入证书参数时，才对证书参数使用有效的字符和值。 在ASA中，对这些证书进行解码，以将其构建到内部数据结构中。具有空白字段的证书被解释为不符合解码标准，因此安装验证失败。但是，从版本9.16开始，可选字段的空白值不会影响解码和安装验证条件。
- 要使用通配符 (*) 符号，请确保在允许在字符串值中使用此字符的 CA 服务器上使用编码。虽然 RFC 5280 建议使用 UTF8String 或 PrintableString，但应使用 UTF8String，因为 PrintableString 无法将通配符识别为有效字符。如果在导入期间发现无效的字符或值，ASA 将拒绝导入的证书。例如：

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

配置数字证书

以下主题介绍如何配置数字证书。

配置密钥对

要创建或删除密钥对，请执行以下步骤：

过程

步骤 1 生成一个默认、通用 RSA 密钥对。

crypto key generate rsa modulus 2048

示例：

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

默认密钥模块大小为2048，但是您应明确指定模块大小以确保要求。该密钥命名为Default-RSA-Key。

对于 RSA 密钥，模块大小可以是以下其中之一（位数）：2048或 4096。

如果还想要椭圆曲线签名算法 (ECDSA) 密钥，您可以生成 Default-ECDSA-Key。默认长度为 384，但您也可以使用 256 或 521。

crypto key generate ecdsa elliptic-curve 384

如果还想要椭圆曲线签名算法 (Edwards) 密钥，您可以生成 Default-ECDSA-Key。默认长度为 256 位。

注释 不支持使用类型为 EdDSA (Ed25519) 的密钥对的 ASA 上的 EST 注册。EST 注册只能使用 RSA 或 ECDSA 密钥。

crypto key generate eddsa edward-curve Ed25519

步骤 2 （可选）创建具有唯一名称的其他密钥。

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

示例：

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

该标签由使用密钥对的信任点引用。

步骤 3 验证已生成的密钥对。

show crypto key mypubkey {**rsa** | **ecdsa**}

示例：

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

步骤 4 保存已生成的密钥对。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 5 如有必要，请删除现有密钥对，以便可以生成新的密钥对。

crypto key zeroize {**rsa** | **ecdsa**}

示例：

```
ciscoasa(config)# crypto key zeroize rsa
```

步骤 6 （可选）存档本地 CA 服务器证书和密钥对。

copy

示例：

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

此命令使用 FTP 或 TFTP 从 ASA 复制本地 CA 服务器证书和密钥对及所有文件。

注释 确保尽可能经常备份所有本地 CA 文件。

示例

以下示例显示如何删除密钥对：

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

配置信任点

要配置信任点，请执行以下步骤：

过程

步骤 1 创建与 ASA 需要从中接收证书的 CA 相对应的信任点。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

您可以进入 crypto ca trustpoint 配置模式，该模式控制可从步骤 3 开始配置的 CA 特定信任点参数。

步骤 2 选择以下选项之一：

- 请求使用 SCEP 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol scep *url*

  示例：

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- 请求使用 CMP 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol cmp *url*

  示例

  ```
  ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- 通过将从 CA 收到的证书粘贴到终端，请求使用指定信任点手动注册。

  enrollment terminal

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

- 请求自签名证书。

  enrollment self

- 请求使用 EST 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol est *url*

  示例

  ```
  asa(config-ca-trustpoint)# enrollment protocol est ?

  crypto-ca-trustpoint mode commands/options:
    url CA server enrollment URL
  asa(config-ca-trustpoint)# enrollment protocol est url ?
   crypto-ca-trustpoint mode commands/options:
    LINE < 477 char  URL
  asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
  ```

步骤 3 如果信任点在以上步骤中被配置为使用CMP，可以选择性地启用自动请求证书的功能。这种自动功能集于可配置的触发器来控制是否使用CMPv2自动更新、触发时间以及是否生成新密钥对。输入需要自动注册前允许的绝对有效期百分比，并指定在更新证书时是否要生成新密钥。

```
[no] auto-enroll [<percent>] [regenerate]
```

步骤 4 指定可用的 CRL 配置选项。

revocation-check crl none

注释　　恢复了在 9.13(1) 中删除的 **revocation-check crl none**。

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

注释　　要启用必需或可选的 CRL 检查，请确保在获得证书后为 CRL 管理配置信任点。

步骤 5 启用或禁用基本约束扩展和 CA 标志。

[**no**] **ca-check**

基本约束扩展标识证书主体是否为证书颁发机构 (CA)，这种情况下证书可用于签署其他证书。CA 标志是此扩展的一部分。证书中存在这些项目表明证书的公钥可用于验证证书签名。

ca-check 命令默认已启用，因此仅当您想要禁用基本约束和 CA 标志时，才需要输入此命令。

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

步骤 6 在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的邮件地址。

email *address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

步骤 7 （可选）指定重试周期（以分钟为单位），且仅应用于 SCEP 注册。

enrollment retry period

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

步骤 8 （可选）指定允许的最大重试次数，且仅应用于 SCEP 注册。

enrollment retry count

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

步骤 9 在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的完全限定域名。

fqdn *fqdn*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

步骤 10 在注册期间，要求 CA 在证书中包括 ASA 的 IP 地址。

ip-address *ip-address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

步骤 11 指定要认证其公钥的密钥对。

keypair 名称

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

步骤 12 当已为CMP配置信任点时，才能确定是否要为任何CMP手动和自动注册生成EDCSA密钥、EDCSA密钥，还是 RSA 密钥。

```
no keypair name | [rsa modulus 2048|4096] | [edcsa elliptic-curve 256|384|521] | [ eddsa
edwards-curve Ed25519 ]
```

注释 不支持使用类型为 EDDSA (Ed25519) 的密钥对的 ASA 上的 EST 注册。EST 注册只能使用 RSA 和 ECDSA 密钥。

注释 使用 ECDHE_ECDSA 密码组时，请使用包含支持 ECDSA 的密钥的证书配置信任点。具有 RSA 密钥的证书与 ECDSA 密码不兼容。

步骤 13 配置 OCSP URL 覆盖和信任点以用于验证 OCSP 响应方证书。

match certificate map-name override ocsp

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

步骤 14 配置 ASA 连接 OCSP 的源接口：

interface *nameif*

示例：

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
```

步骤 15 在 OCSP 请求上禁用随机数扩展。随机数扩展以加密方式将请求与响应绑定以避免重放攻击。

ocsp disable-nonce

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

步骤 16 为 ASA 配置 OCSP 服务器，以用于检查与信任点（而不是客户端证书的 AIA 扩展中指定的服务器）关联的所有证书。

ocsp url

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

步骤 17 指定在注册过程中向 CA 注册的质询短语。CA 通常使用此短语对随后的吊销请求进行身份验证。

password 字符串

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

步骤 18 设置一种或多种吊销检查方法：CRL、OCSP 和随机数。

注释 分配 OCSP URL 以进行吊销检查时，可以指定可从其访问 OCSP 的接口（包括管理接口）。此接口值确定路由决策。

revocation check

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

步骤 19 在注册过程中，要求 CA 在证书中包含指定的使用者 DN。如果 DN 字符串包含逗号，可用双引号将值字符串引起来（例如，O=”Company, Inc.”）。

subject-name *X.500* 名称

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

步骤 20 在注册期间，要求 CA 在证书中包括 ASA 序列号。

serial-number

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

步骤 21 保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为信任点配置 CRL

要在证书身份验证过程中使用强制或可选CRL检查，您必须为每个信任点配置CRL。要为信任点配置 CRL，请执行以下步骤：

过程

步骤 1 针对要修改其 CRL 配置的信任点进入 crypto ca trustpoint 配置模式。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa (config)# crypto ca trustpoint Main
```

注释　　确保在输入此命令之前已启用 CRL。此外，CRL 必须可用才能成功进行身份验证。

步骤 2 针对当前信任点进入 crl 配置模式。

crl configure

示例：

```
ciscoasa(config-ca-trustpoint)# crl configure
```

提示　　要将所有 CRL 配置参数设置为默认值，请使用 **default** 命令。在 CRL 配置过程中，可以随时重新输入此命令来重新启动该程序。

步骤 3　选择下列其中一项来配置检索策略：

- CRL 仅从已通过身份验证的证书中指定的 CRL 分发点 (CDP) URL 进行检索。

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  注释　　证书中指定的分发点不支持 SCEP 检索。

- CRL 仅从您配置的认证映射匹配规则 中进行检索。

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- CRL 仅从已通过身份验证的证书中指定的 CRL 分发点和您配置的认证映射匹配规则 中进行检索。

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

步骤 4　如果您在配置 CRL 策略时使用关键字 **static** 或 **both**，则必须为 CRL 检索配置认证映射匹配规则 。您现在可以将多个静态 CDP 配置到单个映射。

enrollment terminal

要删除特定实例，请在命令的**否定**形式中包含序列号或 URL。确保指定的值与配置的值匹配。要删除映射的所有条目，只需使用**否定**命令。

示例：

```
ciscoasa(crypto ca trustpoint)#enrollment terminal

ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  10 url http://192.0.2.10
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  20 url http://192.0.2.12
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  30 url http://192.0.2.13
```

步骤 5　指定 HTTP、LDAP 或 SCEP 作为 CRL 检索方法。

protocol http | **ldap** | **scep**

示例：

```
ciscoasa(config-ca-crl)# protocol http
```

步骤 6 配置 ASA 为当前信任点缓存 CRL 的时长。*refresh-time* 参数是 ASA 在认为 CRL 过时之前等待的时间（以分钟为单位）。

cache-time *refresh-time*

示例：

```
ciscoasa(config-ca-crl)# cache-time 420
```

步骤 7 选择以下其中一个选项：

- 要求 CRL 中有 NextUpdate 字段。这是默认设置。

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- 允许 CRL 中没有 NextUpdate 字段。

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

步骤 8 如果 LDAP 被指定为检索协议，则向ASA 标识 LDAP 服务器。您可以按 DNS 主机名或按 IP 地址指定服务器。如果服务器侦听端口上的 LDAP 查询，则您还可以提供端口号，而不是使用默认端口号 389。

ldap-defaults *server*

示例：

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

注释　　如果使用主机名而非 IP 地址来指定 LDAP 服务器，请确保已将 ASA 配置为使用 DNS。

步骤 9 如果 LDAP 服务器需要凭证，则允许 CRL 检索。

ldap-dn *admin-DN password*

示例：

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

步骤 10 从指定信任点所代表的 CA 检索当前 CRL，并测试当前信任点的 CRL 配置。

crypto ca crl request 信任点

示例：

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

步骤 11 保存运行配置。

write memory

示例：

```
ciscoasa (config)# write memory
```

导出或导入信任点配置

要导出和导入信任点配置，请执行以下步骤：

过程

步骤 1 以 PKCS12 格式导出带有所有关联密钥和证书的信任点配置。

crypto ca export 信任点

示例：

```
ciscoasa(config)# crypto ca export Main
```

ASA 将在终端显示 PKCS12 数据。您可以复制该数据。信任点数据受密码保护；但是，如果将信任点数据保存在文件中，请确保该文件处于安全位置。

步骤 2 导入与信任点配置关联的密钥对和已颁发证书。

crypto ca import 信任点 **pkcs12**

示例：

```
ciscoasa(config)# crypto ca import Main pkcs12
```

ASA 会提示您将文本以 base-64 格式粘贴到终端。系统将向与信任点一起导入的密钥对分配与所创建的信任点名称相匹配的标签。

注释 如果 ASA 的信任点共享同一个 Ca，您只能使用共享 CA 的其中一个信任点来验证用户证书。要控制使用哪个共享 CA 的信任点来验证该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 关键字。

示例

以下示例显示使用密码 Wh0zits 导出信任点 Main 的 PKCS12 数据：

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

以下示例使用密码 Wh0zits 将 PKCS12 数据手动导入信任点 Main：

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

以下示例手动导入信任点 Main 的证书：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

配置 CA 证书映射规则

您可以根据证书的 Issuer 和 Subject 字段配置规则。使用您创建的规则，可以通过 **tunnel-group-map** 命令将 IPsec 对等体证书映射到隧道组。

要配置 CA 证书映射规则，请执行以下步骤：

过程

步骤 1 输入您要配置的规则的 CA 证书映射配置模式，并指定规则序列号。

crypto ca certificate map [*map_name*]*sequence-number*

示例：

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

如果不指定映射名称，该规则将添加到默认映射：DefaultCertificateMap。对于每个规则编号，您可以指定一个或多个要匹配的字段。

步骤 2 指定发布者名称或主题名称：

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

示例：

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

您可以匹配整个值，也可以指定要匹配的属性。以下为有效属性

- c - 国家/地区
- cn - 公用名
- dc - 域组件
- dnq - DN 限定符
- emailAddress - 邮件地址
- genq - 世代限定符
- gn - 名
- i - 首字母
- ip - IP 地址
- i - 位置
- n - 名称
- o - 组织名称
- ou - 组织单位
- ser - 序列号
- sn - 姓
- sp - 州/省
- t - 职务
- uid - 用户 ID
- uname - 非结构化名称

以下是有效的运算符：

- eq - 字段或属性必须与给定的值相同。

- ne - 字段或属性不能与给定的值相同。
- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段或属性的任何部分都不能与给定的值相匹配。

步骤 3 指定备用主题名称：

alt-subject-name *operator string*

示例：

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

以下是有效的运算符：

- eq - 字段必须与给定的值相同。
- ne - 字段不能与给定的值相同。
- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段的任何部分都不能与给定的值相匹配。

步骤 4 指定扩展密钥的用法：

extended-key-usage *operator OID_string*

示例：

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

以下是有效的运算符：

- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段的任何部分都不能与给定的值相匹配。

以下是有效的 OID 字符串：

- *string* - 用户定义的字符串。
- clientauth - 客户端身份验证 (1.3.6.1.5.5.7.3.2)
- codesigning - 代码签名 (1.3.6.1.5.5.7.3.3)
- emailprotection - 安全邮件保护 (1.3.6.1.5.5.7.3.4)
- ocspsigning - OCSP 签名 (1.3.6.1.5.5.7.3.9)
- serverauth - 服务器身份验证 (1.3.6.1.5.5.7.3.1)
- timestamping - 时间戳 (1.3.6.1.5.5.7.3.8)

配置引用标识

当 ASA 用作 TLS 客户端时，它将支持用于验证应用服务器标识是否符合 RFC 6125 中的定义的规则。此 RFC 将指定用于表示引用标识（在 ASA 上配置）并根据提供的标识（从应用服务器发送）验证它们的程序。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接，并将记录错误。

服务器通过将一个或多个标识符包括在建立连接时提供给ASA的服务器证书中，来提供其标识。引用标识将在ASA上进行配置，以便在建立连接期间与服务器证书中提供的标识进行比较。这些标识符是 RFC 6125 中指定的四种标识符类型的特定实例。四种标识符类型包括：

- CN_ID：证书主题字段中的一个相对可分辨名称(RDN)，它仅包含一个公用名称(CN)类型的属性类型和值对，其中值与域名的整体形式相匹配。CN值不能是自由文本。CN-ID引用标识符不会标识应用服务。
- DNS-ID：dNSName 类型的 subjectAltName 条目。这是一个 DNS 域名。DNS-ID 引用标识符不会标识应用服务。
- SRV-ID：otherName 类型的 subjectAltName 条目，根据 RFC 4985 中的定义，其名称形式为 SRVName。SRV-ID 标识符可以同时包含域名和应用服务类型。例如，SRV-ID“_imaps.example.net”可以拆分为 DNS 域名部分“example.net”和应用服务类型部分“imaps”。
- URI-ID：uniformResourceIdentifier类型的subjectAltName条目，其值同时包括(i)“scheme”和(ii)与RFC 3986中指定的“reg-name”规则相匹配的“host”组成部分（或其等效部分）。URI-ID标识符必须包含 DNS 域名，而非 IP 地址，并且不仅是主机名。例如，URI-ID“sip:voice.example.edu”可以拆分为 DNS 域名部分“voice.example.edu”和应用服务类型“sip”。

在使用以前未使用的名称配置引用标识时，将创建一个引用标识。在创建引用标识后，可向或从引用标识中添加或删除四种类型的标识符及其相关联的值。引用标识符可以包含标识应用服务的信息，并且必须包含标识 DNS 域名的信息。

开始之前

- 当仅连接到系统日志服务器和智能许可服务器时，将使用引用标识。其他 ASA SSL 客户端模式连接目前都不支持配置或使用引用标识。
- ASA 将实施用于匹配 RFC 6125 中所述标识符的所有规则（除交互式客户端的已固定证书和回退以外）。
- 不会实施固定证书的功能。因此，不会出现 `No Match Found`、`Pinned Certificate`。此外，如果由于我们的实施并非交互式客户端而未找到匹配，则不会向用户提供固定证书的机会。

过程

步骤 1 在全局配置模式下输入 **[no] crypto ca reference-identity** 命令，以将 ASA 置于 ca-reference-identity 模式下。

[no] crypto ca reference-identity *reference-identity-name*

如果未找到包含此 *reference-identity-name* 的引用标识，将创建一个新引用标识。如果为仍在使用中的引用标识发布了该命令的 **no** 形式，则将显示一条警告，并且不会删除引用标识。

步骤 2 在处于 ca-reference-identity 模式下时输入引用标识。可向引用标识中添加多个任何类型的引用标识。

- **[no] cn-id** 值
- **[no] dns-id** 值
- **[no] srv-id** 值
- **[no] uri-id** 值

要删除引用标识，请使用该命令的 no 形式。

示例

为系统服务器的 RFC 6125 服务器证书验证配置引用标识：

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

下一步做什么

在配置系统日志和 Smart Call Home 服务器连接时，请使用引用标识。

手动获取证书

要手动获取证书，请执行以下步骤：

开始之前

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

过程

步骤 1 导入已配置的信任点的 CA 证书。

crypto ca authenticate 信任点

示例：

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
```

```
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

信任点是否要求手动获取证书由配置信任点时是否使用 **enrollment terminal** 命令而定。

步骤 2 使用信任点注册 ASA。

crypto ca enroll 信任点

示例：

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
```

此命令生成用于签署数据和根据已配置的密钥类型加密数据的证书。如果对签署和加密使用不同的 RSA 密钥，则 **crypto ca enroll** 命令显示两个证书请求，每个密钥各一个。如果对签名和加密使用通用 RSA 密钥，则 **crypto ca enroll** 命令显示一个证书请求。

要完成注册，请从适用信任点所代表的CA 获取由 **crypto ca enroll** 命令生成的所有证书请求的证书。确保证书采用 base-64 格式。

步骤 3 在为 CMP 配置信任点时，可以指定共享密钥值 (ir)，或者指定包含将要签署请求的 (cr) 证书的信任点的名称，但不能同时指定两者。通过 CA提供带外值（用于确认与 ASA 交换的消息的真实性和完整性），或者提供包含过去颁发的设备证书的信任点的名称（用于签署CMP注册请求）。仅在将信任点注册协议设置为 CMP 时，共享密钥或签名证书关键字才可用。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

步骤 4 确定是否应在建立注册请求之前生成新密钥对。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

步骤 5 导入从 CA 收到的每个证书并确保以 base-64 格式将证书粘贴到终端。

crypto ca import 信任点 **certificate**

示例：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

步骤 6 通过显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。

show crypto ca certificate

示例：

```
ciscoasa(config)# show crypto ca  certificate Main
```

步骤 7 保存运行配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 8 对于为手动注册配置的每个信任点重复上述步骤。

使用 SCEP 自动获取证书

本节介绍如何使用 SCEP 自动获取证书。

开始之前

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

过程

步骤 1 获取已配置的信任点的 CA 证书。

crypto ca authenticate 信任点

示例：

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

配置信任点时，使用 **enrollment url** 命令确定是否必须通过 SCEP 自动获取证书。

步骤 2 使用信任点注册 ASA。此命令检索用于签署数据和根据已配置的密钥类型加密数据的证书。在输入此命令前，请与 CA 管理员联系，其可能需要在 CA 授予证书之前手动对注册请求进行身份验证。

crypto ca enroll 信任点

示例：

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

如果 ASA 未在发送证书请求后一分钟（默认值）内从 CA 收到证书，则会重新发送证书请求。ASA 会继续每分钟发送一次证书请求，直到收到证书。

如果为信任点配置的完全限定域名与ASA的完全限定域名（包括字符的大小写）不同，则系统将显示警告。要解决此问题，请退出注册过程，进行任何必要的更正，然后重新输入 **crypto ca enroll** 命令。

注释　如果 ASA 在您发出 **crypto ca enroll** 命令后但在收到证书前重新启动，请重新输入 **crypto ca enroll** 命令并通知 CA 管理员。

步骤 3 通过显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。

show crypto ca certificate

示例：

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

步骤 4 保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为 SCEP 请求配置代理支持

要使用第三方 CA 配置 ASA 以对远程访问终端进行身份验证，请执行以下步骤：

过程

步骤 1 进入 tunnel-group ipsec-attributes 配置模式。

tunnel-group 名称 **ipsec-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

步骤 2 启用客户端服务。

crypto ikev2 enable outside client-services port 端口号

示例：

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

默认端口号为 443。

注释 仅当支持 IKEv2 时，才需要此命令。

步骤 3 进入 tunnel-group general-attributes 配置模式。

tunnel-group 名称 **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

步骤 4 为隧道组启用 SCEP 注册。

scep-enrollment enable

示例：

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

步骤 5 进入 group-policy attributes 配置模式。

group-policy 名称 **attributes**

示例：

```
ciscoasa(config)# group-policy FirstGroup attributes
```

步骤 6 为组策略注册 SCEP CA。为每个组策略输入一次此命令，以支持第三方数字证书。

scep-forwarding-url value *URL*

示例：

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL 是 CA 上的 SCEP URL。

步骤 7 当证书不适用于 SCEP 代理的 WebLaunch 支持时，请提供通用辅助密码。

secondary-pre-fill-username clientless hide use-common-password 密码

示例：

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

您必须使用 **hide** 关键字支持 SCEP 代理。

例如，证书对于请求该证书的终端不可用。终端获得证书后，AnyConnect 客户端 断开连接，然后重新连接到 ASA 以对提供内部网络资源访问权限的 DAP 策略进行限定。

步骤 8 隐藏 AnyConnect 客户端 VPN 会话的辅助预填写用户名。

secondary-pre-fill-username ssl-client hide use-common-password 密码

示例：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password secret
```

尽管从更早版本继承了 **ssl-client** 关键字，但此命令用于支持使用 IKEv2 或 SSL 的 AnyConnect 客户端 会话。

您必须使用 **hide** 关键字支持 SCEP 代理。

步骤 9 当证书不可用时，请提供用户名。

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

示例：

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback
 cisco-secure-desktop machine-unique-id
```

如何设置特定整数类型

在您建立可信证书后，您就可以开始其他基础任务，如建立身份证书或更高级的配置，如建立本地 CA 或代码签名证书。

开始之前

阅读关于数字证书的信息，并建立可信证书。不含私钥的 CA 证书将供所有 VPN 协议和 webvpn 使用，并在信任点中配置，以验证传入客户端证书。同样，信任池是webvpn功能使用的可信证书的列表，该功能将使用这些证书验证通向 https 服务器的代理连接，以及验证 smart-call-home 证书。

过程

本地 CA 允许 VPN 客户端直接从 ASA 注册证书。这项高级配置会将 ASA 转换为 CA。要配置 CA，请参考CA 证书，第 31 页。

下一步做什么

设置证书到期警报或监控数字证书和证书管理历史。

CA 证书

在此页面中，可管理 CA 证书。以下主题介绍您可以执行的操作。

CA 服务器管理

管理用户证书

要更改证书状态，请执行以下步骤：

过程

步骤 1 在 **Manage User Certificates** 窗格中按用户名或按证书序列号选择特定证书。

步骤 2 选择以下其中一个选项：

- 如果用户证书有效期到期，请点击 **Revoke** 以删除用户访问。本地 CA 还会在证书数据库中将证书标记为已吊销，自动更新信息并重新发出 CRL。
- 选择已吊销证书并点击 **Unrevoke** 以恢复访问。本地 CA 还会在证书数据库中将证书标记为未吊销，自动更新证书信息并重新发出已更新的 CRL。

步骤 3 完成后点击 **Apply** 以保存更改。

配置信任池证书的自动导入

智能许可使用 Smart Call Home 基础设施。ASA 在后台配置 Smart Call Home 匿名报告时，ASA 会自动创建一个包含颁发 Call Home 服务器证书的 CA 的证书的信任点。现在，如果服务器的颁发层次结构发生变化，ASA 支持对证书进行验证，而无需客户来调整证书层次结构变化。您可以按照定期的间隔自动执行信任池捆绑包的更新，以便在 CA 服务器的自签名证书发生变化时 Smart Call Home 可以保持活动状态。此功能在多情景部署环境下不受支持。

信任池证书捆绑包的自动导入需要您指定 ASA 下载和导入捆绑包所用的 URL。使用以下命令，以便每天可以按照固定的间隔使用默认的思科 URL 和 22 小时的默认时间进行导入：

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

您还可以使用以下命令以自定义 URL 启用 自动导入：

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

为了能让您在非高峰时段或其他便利时间灵活地设置下载，请输入以下命令，以使用自定义时间启用导入：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

使用自定义 URL 和自定义时间 设置自动导入需要使用以下 命令：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

显示信任池策略的状态

使用以下命令查看 trustpool 策略的当前状态：

```
show crypto ca trustpool policy
```

此命令返回 如下信息：

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

清除 *CA* 信任池

要将 trustpool 策略重置为默认状态，请使用以下命令：

```
clear configure crypto ca trustpool
```

由于默认情况下会禁用 自动导入 trustpoint 证书，因此使用此命令 会禁用该功能。

设置证书到期警报（对于身份或 CA 证书）

ASA 每隔 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。

系统提供 CLI 来配置提醒和循环间隔。默认情况下，在到期前 60 天开始提醒并且每 7 天循环提醒一次。您可以通过使用以下命令配置提醒发送间隔和发送第一个提醒时的到期前天数：

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

不考虑警报配置， 在到期的最后一周内每天发送提醒。此外，还新增了 **show** 和 **clear** 命令，具体如下：

```
clear conf crypto ca alerts
show run crypto ca alerts
```

除了续签提醒之外，如果系统在配置中找到已到期证书，则每天会生成一次系统日志，以通过续签证书或删除已到期证书来调整配置。

例如，假设到期提醒配置为在到期前 60 天开始，此后每 6 天重复提醒一次。如果 ASA 在到期前 40 天重新启动，则系统当日会发送提醒，并在第 36 天发送下一个提醒。

注释 对于信任池证书不会执行到期检查。本地 CA 信任点会被视为也需要进行到期检查的普通信任点。

监控数字证书

请参阅以下命令来监控数字证书状态。

- **show crypto ca server**

  此命令显示本地 CA 配置和状态。

- **show crypto ca server cert-db**

  此命令显示由本地 CA 颁发的用户证书。

- **show crypto ca server certificate**

  此命令以 base 64 格式显示控制台上的本地 CA 证书以及滚动更新证书（可用时），包括用于在新证书导入到其他设备时对其进行验证的滚动更新证书指纹。

- **show crypto ca server crl**

  此命令显示 CRL。

- **show crypto ca server user-db**

  此命令显示用户及其状态，可与以下限定符配合使用来减少显示的记录数：

  - allowed。仅显示当前允许注册的用户。
  - enrolled。仅显示已注册并持有有效证书的用户。
  - expired。仅显示持有已到期证书的用户。
  - on-hold。仅列出无证书且当前不允许注册的用户。

- **show crypto ca server user-db allowed**

  此命令显示符合注册条件的用户。

- **show crypto ca server user-db enrolled**

  此命令显示具有有效证书的已注册用户。

- **show crypto ca server user-db expired**

  此命令显示具有过期证书的用户。

- **show crypto ca server user-db on-hold**

  此命令显示无证书且不允许注册的用户。

- **show crypto key** *name of key*

  此命令显示您已生成的密钥对。

- **show running-config**

  此命令显示本地 CA 证书映射规则。

示例

以下示例显示 RSA 通用密钥：

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

以下示例显示本地 CA CRL：

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
```

```
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

以下示例显示一个暂停用户：

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

以下示例显示 **show running-config** 命令的输出，其中会显示本地 CA 证书映射规则：

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

证书管理历史记录

表 *1:* 证书管理历史记录

功能名称	平台版本	说明
证书管理	7.0(1)	数字证书（包括 CA 证书、身份证书和代码签名者证书）是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。
证书管理	7.2(1)	引入了以下命令： **issuer-name** *DN-string*、**revocation-check crl none**、**revocation-check crl**、**revocation-check none**。 废弃了以下命令：**crl** {**required** | **optional** | **nocheck**}。

功能名称	平台版本	说明
证书管理	8.0(2)	引入了以下命令： **cdp-url**、**crypto ca server**、**crypto ca server crl issue**、**crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、**crypto ca server user-db remove** *username*、**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、**crypto ca server user-db write**、[**no**] **database path** *mount-name directory-path*、**debug crypto ca server** [*level*]、**lifetime** {**ca-certificate** | **certificate** | **crl**} *time*、**no shutdown**、**otp expiration** *timeout*、**renewal-reminder** *time*, **show crypto ca server**、**show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]、**show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**]、**show crypto key** *name of key*、**show running-config**、**shutdown**。
SCEP 代理	8.4(1)	引入了此功能，可从第三方CA对设备证书进行安全部署。 引入了以下命令： **crypto ikev2 enable outside client-services port** *portnumber*、**scep-enrollment enable**, **scep-forwarding-url value** *URL*、**secondary-pre-fill-username clientless hide use-common-password** *password*、**secondary-pre-fill-username ssl-client hide use-common-password** *password*、**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。
引用标识	9.6(2)	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。身份验证将在PKI验证期间仅针对与系统日志服务器和智能许可服务器的TLS连接执行。如果所显示的身份无法与配置的参考身份匹配，则不会建立连接。 添加或修改了以下命令：**crypto ca reference-identity**、**logging host** 和 **call home profile destination address**。

功能名称	平台版本	说明
本地 CA 服务器	9.12(1)	要使注册 URL 的 FQDN 可配置，而不是使用 ASA 的已配置 FQDN，引入新的 CLI 选项。此新选项已添加到 crypto ca server 的 smpt 模式。 我们启用了本地CA服务器，并将在后续版本中删除—当 ASA 配置为本地 CA 服务器时，系统会启用该服务器以颁发数字证书、发布证书吊销列表 (CRL)，并安全地撤销已颁发的证书。此功能已过时，因此弃用加密 CA 服务器命令。
本地 CA 服务器	9.13(1)	删除了本地 CA 服务器支持。因此，将会删除 **crypto ca server** 命令及其子命令。 删除了以下命令：**crypto ca server** 及其所有子命令。
对 CRL 分发点命令的修改	9.13(1)	静态 CDP URL 配置命令将被删除并移至匹配证书命令。 新增/修改的命令：**crypto-ca-trustpoint crl**、**crl url** 与其他相关逻辑一起删除。**match-certificate override-cdp** 引入了。
增加了 CRL 缓存大小	9.13(1)	为防止大型 CRL 下载失败，增加了缓存大小，并且删除了单个 CRL 中的条目数限制。 • 在多情景模式下，将每个情景的 CRL 缓存总大小增加到 16 MB。 • 在单一情景模式下，将 CRL 缓存总大小增加到 128 MB。
恢复绕行证书有效性检查选项	9.15(1)	恢复了由于在 9.13(1) 中删除的 CRL 或 OCSP 服务器的连接问题而绕过吊销检查的选项已恢复。 新增/修改的命令：恢复了 **revocation-check crl none**、**revocation-check ocsp none**、**revocation-check crl ocsp none** 和 **revocation-check ocsp crl none** 。
修改匹配证书命令以支持静态CRL分发点URL	9.15(1)	静态 CDP URL 配置命令允许将静态 CDP 唯一映射到正在验证的链中的每个证书。但是，每个证书仅支持一个此类映射。此次修改后，系统允许将静态配置的 CDP 映射到证书链以进行身份验证。 新增/修改的命令：**match certificate** *map* **override cdp** *seq* **url** *url* and **no match certificate** *map* **override cdp** *seq* **url** *url*

功能名称	平台版本	说明
对信任点密钥对和加密密钥生成命令的修改	9.16（1）	不再支持密钥大小小于 2048 的证书。任何使用 512、768 或 1024 位选项的配置都将过渡到 2048，并发出通知。 不再支持使用 SHA1 散列算法进行认证。 注释 引入了 **crypto ca permit-weak-crypto** 命令以覆盖这些限制。 新的密钥选项 - EDDSA 已添加到现有 RSA 和 ECDSA 选项中。

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。