数字证书

本章介绍如何配置数字证书。

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 Secure Client 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 Secure Client 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 Secure Client）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、 Secure Client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。

数字证书准则

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。

故障转移准则

- 在有状态的故障转移中不支持复制会话。
- 对于本地 CA，不支持故障转移。
- 如果配置状态故障转移，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。
- Secure Client 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 Secure Client可能不支持 EDDSA 证书。例如，您需要使用RSA证书进行远程访问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 Secure Client 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 访问 **Configuration > Remote Access VPN > Advanced > Reference Identity**。

将列出已配置的引用标识。可以 **Add** 新引用标识，选择并 **Edit** 现有引用标识，也可以选择并 **Delete** 现有引用标识。正在使用的引用标识不能删除。

步骤 2 通过选择 **Add** 或 **Edit** 创建或修改引用标识。

使用此 Add or Edit Reference Identity 对话框以选择并指定您的引用标识。

- 可向引用标识中添加多个任何类型的引用标识。
- 名称设置好后将无法修改，请删除并重新创建引用标识以更改名称。

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。

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

步骤 1 身份证书是证书在 ASA 上与对应的私钥一起配置的证书。它用于在 ASA 上启用 SSL 和 IPsec 服务时的带外加密或签名生成，并将通过信任点注册获得。要配置身份证书，请参考身份证书，第 13 页。

步骤 2 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 19 页。

步骤 3 如果您计划使用身份证书作为 webvpn java 代码签名功能的组成部分，请参考代码签名者证书，第 24 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记录。

身份证书

身份证书可用于通过 ASA 对 VPN 访问进行身份验证。

在 Identity Certificates Authentication 窗格中，可以执行以下任务：

- 添加或导入身份证书，第 13 页。
- 启用 CMPv2 注册作为来自 CA 的一个请求
- 显示身份证书的详细信息。
- 删除现有的身份证书。
- 导出身份证书，第 17 页。
- 设置证书到期警报。
- 向 Entrust 生成证书签名请求，第 17 页注册身份证书。

添加或导入身份证书

要添加或导入新的身份证书配置，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **远程访问 VPN** > **证书管理** > **身份证书**。

步骤 2 点击 **Add**。

系统将显示 **Add Identity Certificate** 对话框，其中选定信任点名称显示在顶部。

步骤 3 点击 **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** 单选按钮以从现有文件导入身份证书。

步骤 4 输入用于解密 PKCS12 文件的密码。

步骤 5 输入文件的路径名称，或点击 **Browse** 以显示 **Import ID Certificate File** 对话框。查找证书文件，然后点击 **Import ID Certificate File**。

步骤 6 点击 **Add a new identity certificate** 单选按钮以添加新的身份证书。

步骤 7 点击 **New** 以显示 **Add Key Pair** 对话框。

步骤 8 选择 **RSA**、**ECDSA** 或 **EdDSA** 密钥类型。

步骤 9 如果选择 **EdDSA**，系统会显示“**Edwards 曲线**”选项。点击 EdDSA1 单选按钮。

步骤 10 点击 **Use default keypair name** 单选按钮以使用默认密钥对名称。

步骤 11 点击 **Enter a new key pair name** 单选按钮，然后输入新名称。

步骤 12 从下拉列表中选择模数长度。如果选择的是**Edwards曲线**，请选择Ed25519。如果不确定模数长度，请咨询 Entrust。

对于 ASA 9.16(1) 及更高版本，请确保选择的 RSA 模数大小为 2048 或更大。当 RSA 密钥大小小于 2048 位时，CA 证书验证失败。要覆盖此限制，请启用允许弱加密选项。（请参阅 允许 CA 证书的弱加密，第 24 页）。

步骤 13 通过点击“**常规用途**”单选按钮（默认）或“**特殊**”单选按钮选择密钥对用法。选中**Special**单选按钮时，ASA 将生成两个密钥对，一个用于签名，一个用于加密。此选择表示对应的身份需要两个证书。

步骤 14 点击 **Generate Now** 以创建新密钥对，然后点击 **Show** 以显示 **Key Pair Details** 对话框，其中包含以下仅作显示用途的信息：

- 要认证其公钥的密钥对的名称。
- 生成密钥对的时间和日期。
- RSA 密钥对的用法。
- 密钥对的模数长度（位）：512、768、1024、2048、3072、和 4096。默认值为 2048。
- 密钥数据，其中包含文本格式的特定密钥数据。

步骤 15 完成后点击 **OK**。

步骤 16 选择证书使用者 DN 以生成身份证书中的 DN，然后点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 17 从下拉列表中选择一个或多个要添加的 DN 属性，输入一个值，然后点击 **Add**。Certificate Subject DN 的可用 X.500 属性如下：

- **公用名 (CN)**
- **Department (OU)**
- **Company Name (O)**
- **国家/地区 (C)**
- **State/Province (ST)**
- **Location (L)**
- **邮件地址 (EA)**

步骤 18 完成后点击 **OK**。

步骤 19 选中 **Generate self-signed certificate** 复选框以创建自签名证书。

步骤 20 选中**作为本地证书颁发机构并向 TLS 代理颁发动态证书**复选框，以将身份证书作为本地 CA。

步骤 21 点击**高级**以建立其他身份证书设置。

系统将显示**Advanced Options**对话框，其中包含以下三个选项卡：**Certificate Parameters**、**Enrollment Mode** 和 **SCEP Challenge Password**。

注释　　注册模式设置和 SCEP 质询密码对于自签名证书不可用。

步骤 22　点击 **Certificate Parameters** 选项卡，然后输入以下信息：

- FQDN，一个明确的域名，用于指示 DNS 树状层次结构中的节点位置。
- 与身份证书关联的邮件地址。
- 网络中的 ASA IP 地址，采用由四部分组成的点分十进制表示法。
- 选中 **Include serial number of the device** 复选框以将 ASA 序列号添加到证书参数。

步骤 23　点击 **Enrollment Mode** 选项卡，然后输入以下信息：

- 通过点击 **Request by manual enrollment** 单选按钮或 **Request from a CA** 单选按钮选择注册方法。当选择 **Request from a CA** 以启用 CMPV2 注册时，请参阅启用 CMPv2 注册作为来自 CA 的一个请求 ，第 16 页。
- 选择注册协议 - scep、cmp 或 est。

  注释　　如果选择 EST 注册，则只能选择 RSA 和 ECDSA 密钥。不支持 EdDSA 密钥。

- 要通过 SCEP 自动安装的证书的注册 URL。
- 允许重试安装身份证书的最大分钟数。默认值为一分钟。
- 允许安装身份证书的最大重试次数。默认值为零，表示在重试期间重试次数无限制。

步骤 24　点击 **SCEP Challenge Password** 选项卡，然后输入以下信息：

- SCEP 密码
- SCEP 密码确认

步骤 25　完成后点击 **OK**。

步骤 26　如果需要此证书能够签署其他证书，请选中**启用基本约束扩展中的 CA 标志**。

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。将此选项保持选中状态不会产生任何危害。

步骤 27　点击 **Add Identity Certificate** 对话框中的 **Add Certificate**。

新身份证书将显示在 Identity Certificates 列表中。

步骤 28　点击 **Apply** 以保存新身份证书配置。

步骤 29　点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包含以下三个仅作显示用途的选项卡：

- **General** 选项卡显示类型、序列号、状态、用法、公钥类型、CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。
- **Issued to** 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。

- **Issued by** 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

步骤 30 要删除身份证书配置，请选择该配置，然后点击 **Delete**。

注释 删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

启用 CMPv2 注册作为来自 CA 的一个请求

为了定位为无线 LTE 网络中的安全网关设备，ASA 现在使用证书管理协议 (CMPv2) 支持某些证书管理功能。使用 CMPv2 注册 ASA 设备证书，您可以从启用 CMPv2 的 CA 执行第一和第二证书的手动注册，或执行手动证书更新，以替换先前颁发的使用相同密钥对的证书。收到的证书存储在常规配置外部，并用于启用证书的 Ipsec 配置中。

注释 您将不会在 ASA 上拥有完整的 CMPv2 功能。

初始请求会建立与 CA 的信任并获得第一个证书。CA 证书必须在信任点中预先配置。当您确认正在安装的证书的指纹时，会发生身份验证。

点击 Advanced Options 窗口 Enrollment Mode 选项卡上的 **Request from a CA** 后，完成专门用于 CMPv2 注册的以下步骤：

开始之前

请执行添加或导入身份证书，第 13 页中的步骤。

过程

步骤 1 选择 CMP 作为注册协议，并在 http:// area 中输入 CMP URL。

步骤 2 要为所有 CMP 手动和自动注册自动生成新的密钥对，选择 **RSA** 或 **EDCSA**。

如果选择 RSA，从 Modulus 下拉菜单中选择一个值。如果选择 EDCSA，从 elliptic-curve 下拉菜单中选择一个值。

步骤 3 （可选）点击 **Regenerate the key pair** 以在更新证书时或建立注册请求前生成密钥对。

步骤 4 点击 **Shared Key** 并输入 CA 在带外提供的值。该值被 CA 和 ASA 用于确认它们所交换消息的真实性和完整性。

步骤 5 点击 **Signing Trustpoint** 并输入信任点（包含先前颁发的用于对 CMP 注册请求进行签名的设备证书）的名称。

仅当信任点注册协议设置为 CMP 时，这些选项才可用。当使用 CMP 信任点时，可指定共享密钥或签名证书，但不能同时指定两者。

步骤 6 点击 **Browse Certificate** 指定 CA 证书。

步骤 7 （可选）点击 **Auto Enroll** 复选框以触发 CMPv2 的自动注册。

步骤 8 在 Auto Enroll Lifetime 字段中，输入证书的绝对有效期百分比，在此时间之后将需要自动注册。

步骤 9 点击 **Auto Enroll Regenerate Key** 以在更新证书时生成新密钥。

导出身份证书

要导出身份证书，请执行以下步骤：

过程

步骤 1 点击 **Export** 以显示 **Export Certificate** 对话框。

步骤 2 输入要用于导出证书配置的PKCS12格式文件的名称。或者，点击**Browse**以显示**Export ID Certificate File** 对话框，以便查找要向其导出证书配置的文件。

步骤 3 通过点击 **PKCS12 Format** 单选按钮或 **PEM Format** 单选按钮选择证书格式。

步骤 4 输入用于加密要导出的 PKCS12 文件的密码。

步骤 5 确认加密密码。

步骤 6 点击 **Export Certificate** 以导出证书配置。

系统将显示一个信息对话框，通知您证书配置文件已成功导出到指定的位置。

生成证书签名请求

要生成将发送到 Entrust 的证书签名请求，请执行以下步骤：

过程

步骤 1 点击 **Enroll ASA SSL VPN with Entrust** 以显示 **Generate Certificate Signing Request** 对话框。

步骤 2 在 **Key Pair** 区域执行以下步骤：

a) 从下拉列表中选择其中一个配置的密钥对。

b) 点击**显示**以显示**密钥详细信息**对话框，其中提供有关选定密钥对的信息，包括生成日期和时间、用法（通用或特殊用法）、模数长度和密钥数据。

c) 完成后点击 **OK**。

d) 点击**新建**以显示**添加密钥对**对话框。在生成密钥对时，可将其发送到 ASA 或保存到文件中。

步骤 3 在 **Certificate Subject DN** 区域中输入以下信息：

a) ASA 的 FQDN 或 IP 地址。

b) 公司名称。

c) 两个字母的国家/地区代码。

步骤 4 在 **Optional Parameters** 区域执行以下步骤：

a) 点击 **Select** 以显示 **Additional DN Attributes** 对话框。
b) 从下拉列表中选择要添加的属性，然后输入值。
c) 点击 **Add** 以将每个属性添加到属性表中。
d) 点击 **Delete** 以从属性表中删除属性。
e) 完成后点击 **OK**。

添加的属性显示在 **Additional DN Attributes** 字段中。

步骤 5 如果 CA 需要，请输入其他完全限定域名信息。

步骤 6 点击**生成请求**以生成证书签名请求，之后可将其发送到 Entrust，或保存到文件中稍后发送。

系统将显示 **Enroll with Entrust** 对话框，其中显示了 CSR。

步骤 7 通过点击 **request a certificate from Entrust** 链接完成注册过程。然后，复制并粘贴所提供的 CSR 且通过 http://www.entrust.net/cisco/ 上提供的 Entrust Web 表单将其提交。或者，如果要稍后注册，请将生成的 CSR 保存到文件中，然后点击 **Identity Certificates** 窗格上的 **enroll with Entrust** 链接。

步骤 8 Entrust 将在验证请求的真实性后颁发证书，这可能需要几天时间。然后，您需要通过在 **Identity Certificate** 窗格中选择待处理的请求并点击 **Install** 来安装证书。

步骤 9 点击 **Close** 以关闭 **Enroll with Entrust** 对话框。

安装身份证书

要安装新的身份证书，请执行以下步骤：

过程

步骤 1 在 **Identity Certificates** 窗格中，点击 **Add** 以显示 **Add Identity Certificate** 对话框。

步骤 2 点击 **Add a new identity certificate** 单选按钮。

步骤 3 更改密钥对或创建新的密钥对。密钥对是必需的。

步骤 4 输入证书使用者 DN 信息，然后点击 **Select** 以显示 **Certificate Subject DN** 对话框。

步骤 5 指定相关 CA 所需的所有使用者 DN 属性，然后点击 **OK** 以关闭 **Certificate Subject DN** 对话框。

步骤 6 在 **Add Identity Certificate** 对话框中，点击 **Advanced** 以显示 **Advanced Options** 对话框。

步骤 7 要继续，请参阅添加或导入身份证书，第 13 页中的步骤 17 至 23。

步骤 8 在 **Add Identity Certificate** 对话框中，点击 **Add Certificate**。

系统将显示 **Identity Certificate Request** 对话框。

步骤 9 输入 CSR 文本文件的文件名，例如 c:\verisign-csr.txt，然后点击 **OK**。

步骤 10 将 CSR 文本文件发送到 CA。或者，您也可以将该文本文件粘贴到 CA 网站上的 CSR 注册页面中。

步骤 11 当 CA 将身份证书返回给您时，请转至 **Identity Certificates** 窗格，选择待处理的证书条目，然后点击 **Install**。

系统将显示 **Install Identity Certificate** 对话框。

步骤 12 通过点击适用的单选按钮，选择以下其中一个选项：

- **Install from a file**。

  或者，点击 **Browse** 以搜索文件。

- **Paste the certificate data in base-64 format**。

  将复制的证书数据粘贴到提供的区域中。

步骤 13 点击 **Install Certificate**。

步骤 14 点击 **Apply** 以将新安装的证书保存到 ASA 配置中。

步骤 15 要显示有关所选身份证书的详细信息，请点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包括以下仅显示选项卡：

General 选项卡显示类型、序列号、状态、用法、公钥类型、CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。

Issued to 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。

Issued by 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

步骤 16 要删除代码签名者证书配置，请选择该配置，然后点击 **Delete**。

注释 删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Import** 以重新输入所有证书配置信息。

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。

添加或安装 CA 证书

要添加或安装 CA 证书，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **远程访问 VPN** > **证书管理** > **CA 证书**。

步骤 2 点击 **Add**。

系统将显示 **Install Certificate** 对话框。

步骤 3 点击 **Install from a file** 单选按钮以从现有文件添加证书配置（这是默认设置）。

步骤 4 输入路径和文件名，或点击 **Browse** 以搜索文件。然后，点击 **Install Certificate**。

步骤 5 系统将显示 **Certificate Installation** 对话框，其中包含一条指示证书已安装成功的消息。点击 **OK** 以关闭此对话框。

步骤 6 点击 **Paste certificate in PEM format** 单选按钮以手动注册。

步骤 7 将 PEM 格式（base64 或十六进制）证书复制并粘贴到提供的区域中，然后点击 **Install Certificate**。

步骤 8 系统将显示 **Certificate Installation** 对话框，其中包含一条指示证书已安装成功的消息。点击 **OK** 以关闭此对话框。

步骤 9 点击 **Use SCEP** 单选按钮以自动注册。ASA 将使用 SCEP 联系 CA，获取证书并将它们安装到设备上。要使用 SCEP，您必须向支持 SCEP 的 CA 注册，并且必须通过互联网注册。使用 SCEP 自动注册要求提供以下信息：

- 要自动安装的证书的路径和文件名。
- 重试证书安装的最大分钟数。默认值为一分钟。
- 安装证书的重试次数。默认值为零，表示在重试期间重试次数无限制。

步骤 10 点击 **More Options** 以显示新证书和现有证书的其他配置选项。

系统将显示 **Configuration Options for CA Certificates** 窗格。

步骤 11 要更改现有的 CA 证书配置，请选择该配置，然后点击 **Edit**。

步骤 12 要删除 CA 证书配置，请选择该配置，然后点击 **Delete**。

注释 删除证书配置后，无法将其恢复。要重新创建已删除的证书，请点击 **Add** 以重新输入所有证书配置信息。

步骤 13 点击 **Show Details** 以显示 **Certificate Details** 对话框，其中包含以下三个仅作显示用途的选项卡：

- **General** 选项卡显示类型、序列号、状态、用法、公钥类型、CRL 分发点、证书有效期和关联信任点等值。这些值同时适用于可用和暂停状态。
- **Issued to** 选项卡显示使用者 DN 或证书所有者的 X.500 字段及其值。这些值仅适用于可用状态。
- **Issued by** 选项卡显示授予证书的实体的 X.500 字段。这些值仅适用于可用状态。

配置要撤销的 CA 证书

要配置 CA 证书吊销检查，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **站点间 VPN** > **证书管理** > **CA 证书** > **添加**以显示**安装证书**对话框。然后，点击 **More Options**。

步骤 2 点击 **Revocation Check** 选项卡。

步骤 3 点击 **Do not check certificates for revocation** 单选按钮以禁用证书的吊销检查。

步骤 4 点击 **Check certificates for revocation** 单选按钮以选择一个或多个吊销检查方法（CRL 或 OCSP）。

步骤 5 点击 **Add** 可将某个吊销方法移至右侧，将其变为可用。点击 **Move Up** 或 **Move Down** 可更改方法顺序。

您选择的方法按照其添加顺序进行执行。如果某个方法返回错误，则会激活下一个吊销检查方法。

步骤 6 选中 **Consider certificate valid if revocation checking returns errors无法检索信息**。

步骤 7 点击 **OK** 以关闭 **Revocation Check** 选项卡。

配置 CRL 检索策略

要配置 CRL 检索策略，请执行以下步骤：

开始之前

- 要分配静态 URL，

过程

步骤 1 依次选择**配置** > **站点间 VPN** > **证书管理** > **CA 证书** > **添加**以显示**安装证书**对话框。然后，点击 **More Options**。

步骤 2 选中 **Use CRL Distribution Point from the certificate** 复选框以将吊销检查从正在检查的证书定向至 CRL 分发点。

步骤 3 选中 **Use Static URLs configured below** 复选框以列出要用于 CRL 检索的特定 URL。您选择的 URL 按照其添加顺序进行实施。如果指定的 URL 发生错误，则顺序采用下一个 URL。

步骤 4 点击**静态配置 (Static Configuration)** 区域中的**添加 (Add)**。

系统将显示 **Add Static URL** 对话框。

步骤 5 输入用于分发 CRL 的静态 URL，然后点击 **OK**。

输入的 URL 将显示在 **Static URLs** 列表中。

步骤 6 点击 **OK** 以关闭此对话框。

配置 CRL 检索方法

要配置 CRL 检索方法，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **站点间 VPN** > **证书管理** > **CA 证书** > **添加**以显示**安装证书**对话框。然后，点击 **More Options**。

步骤 2 点击 **Configuration Options for CA Certificates** 窗格中的 **CRL Retrieval Methods** 选项卡。

步骤 3 选择以下三种检索方法的其中一种：

- 要启用 LDAP 进行 CRL 检索，请选中 **Enable Lightweight Directory Access Protocol (LDAP)** 复选框。通过 LDAP，CRL 检索通过连接到使用密码进行访问的已命名 LDAP 服务器来启动 LDAP 会话。默认情况下，连接位于 TCP 端口 389 上。输入以下必需参数：
  - 名称
  - 密码
  - 确认密码
  - **Default Server**（服务器名称）
  - **Default Port** (389)
- 要启用 HTTP 以进行 CRL 检索，请选中 **Enable HTTP** 复选框。

步骤 4 点击 **OK** 以关闭此选项卡。

配置 OCSP 规则

要配置 OCSP 规则以获取 X.509 数字证书的吊销状态，请执行以下步骤。

开始之前

确保您已在尝试添加OCSP规则之前配置证书映射。如果尚未配置证书映射，系统将显示错误消息。

过程

步骤 1 依次选择**配置** > **站点间 VPN** > **证书管理** > **CA 证书** > **添加**以显示**安装证书**对话框。然后，点击 **More Options**。

步骤 2 点击 **Configuration Options for CA Certificates** 窗格中的 **OCSP Rules** 选项卡。

步骤 3 选择要匹配此 OCSP 规则的证书映射。证书映射会将用户权限与证书中的特定字段进行匹配。ASA 用于验证响应方证书的 CA 的名称显示在 **Certificate** 字段中。规则的优先级编号显示在 **Index** 字段中。此证书的 OCSP 服务器的 URL 显示在 **URL** 字段中。

步骤 4 点击 **Add**。

系统将显示 **Add OCSP Rule** 对话框。

步骤 5 从下拉列表中选择要使用的证书映射。

步骤 6 从下拉列表中选择要使用的证书。

步骤 7 输入规则的优先级编号。

步骤 8 输入此证书的 OCSP 服务器的 URL。

步骤 9 完成后，点击 **OK** 以关闭此对话框。

新添加的 OCSP 规则将显示在列表中。

步骤 10 点击 **OK** 以关闭此选项卡。

配置高级 CRL 和 OCSP 设置

要配置其他 CRL 和 OCSP 设置，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **站点间 VPN** > **证书管理** > **CA 证书** > **添加**以显示**安装证书**对话框。然后，点击 **More Options**。

步骤 2 点击 **Configuration Options for CA Certificates** 窗格中的 **Advanced** 选项卡。

步骤 3 在 **CRL Options** 区域中输入缓存刷新之间的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为了避免必须从 CA 重复检索同一 CRL，ASA 可以将检索的 CRL 存储在本地，我们称之为 CRL 缓存。CRL缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的CRL会超出其存储限制，则 ASA 会删除最近最不常用的 CRL，直到更多空间可用为止。

步骤 4 选中 **Enforce next CRL update** 复选框可要求有效的 CRL 具有未到期的 Next Update 值。取消选中 **Enforce next CRL update** 复选框可允许有效的 CRL 没有 Next Update 值或具有已到期的 Next Update 值。

步骤 5 在 **OCSP Options** 区域中输入 OCSP 服务器的 URL。ASA 按以下顺序使用 OCSP 服务器：

a) 匹配证书覆盖规则中的 OCSP URL
b) 选定 OCSP Options 属性中配置的 OCSP URL
c) 用户证书的 AIA 字段

步骤 6 默认情况下，**Disable nonce extension** 复选框处于选中状态，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的OCSP服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

步骤 7 在 **Other Options** 域中，选择以下其中一个选项：

- 选中 **Accept certificates issued by this CA** 复选框，以指示 ASA 应从指定的 CA 接收证书。
- 选中 **Accept certificates issued by the subordinate CAs of this CA** 复选框，以指示 ASA 应从附属 CA 接收证书。

步骤 8 点击 **OK** 以关闭此选项卡，然后点击 **Apply** 以保存配置更改。

CA 服务器管理

允许 CA 证书的弱加密

当存在以下属性时，CA证书验证操作会失败：

- 使用具有RSA加密算法的SHA-1签名的证书。
- RSA密钥大小小于2048位的证书。

但是，您可以通过配置permit弱加密选项覆盖这些限制。启用后，ASA允许在验证证书时使用上述属性。我们不建议允许使用弱加密密钥，因为此类密钥不如具有更大密钥大小的密钥安全。

过程

步骤 1 浏览到配置设备管理证书管理身份证书，或配置远程访问VPN证书管理身份证书，或配置远程访问VPN证书管理代码签名者。 > > > > > > > > >

步骤 2 要允许小于2048位的密钥大小和SHA-1签名算法，请在弱加密配置下，点击允许弱密钥大小和散列算法复选框。

代码签名者证书

导入代码签名者证书

要导入代码签名者证书，请执行以下步骤：

过程

步骤 1 在 **Code Signer** 窗格中，点击 **Import** 以显示 **Import Certificate** 对话框。

步骤 2 输入用于解密 PKCS12 格式文件的密码。

步骤 3 输入要导入的文件的名称，或点击 **Browse** 以显示 **Import ID Certificate File** 对话框并搜索文件。

步骤 4 选择要导入的文件并点击 **Import ID Certificate File**。

选定证书文件将显示在 **Import Certificate** 对话框中。

步骤 5 点击 **Import Certificate**。

导入的证书将显示在 **Code Signer** 窗格中。

步骤 6 点击 **Apply** 以保存新导入的代码签名者证书配置。

导出代码签名者证书

要导出代码签名者证书，请执行以下步骤：

过程

步骤 1 在**代码签名者 (Code Signer)** 窗格中，点击**导出 (Export)** 以显示 **导出证书 (Export Certificate)** 对话框。

步骤 2 输入要用于导出证书配置的 PKCS12 格式文件的名称。

步骤 3 在**证书格式 (Certificate Format)** 区域中，要使用公钥加密标准（可以是 base64 编码或十六进制格式），请点击**PKCS12 格式 (PKCS12 format)** 单选按钮。否则，请点击 **PEM 格式 (PEM format)** 单选按钮。

步骤 4 点击**浏览 (Browse)** 以显示**导出 ID 证书文件 (Export ID Certificate File)** 对话框，以便查找要向其导出证书配置的文件。

步骤 5 选择文件并点击**导出 ID 证书文件 (Export ID Certificate File)**。

选定证书文件将显示在 **Export Certificate** 对话框中。

步骤 6 输入用于解密要导出的 PKCS12 格式文件的密码。

步骤 7 确认解密密码。

步骤 8 点击**导出证书 (Export Certificate)** 以导出证书配置。

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。

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。

过程

步骤 1 依次浏览到**配置** > **设备管理** > **证书管理** > **身份证书/CA 证书**。

步骤 2 选中**启用证书到期提醒**复选框。

步骤 3 填写所需的天数：

- Send the first alert before - 配置将发出第一个提醒时的到期前天数（1 至 90）。
- Repeat the alert for - 配置未续签证书时的提醒频率（1 至 14 天）。默认情况下，在到期前 60 天发送第一个提醒，此后每周发送一次提醒，直至续签并删除证书。此外，系统会在到期当日发送提醒，此后每天发送一次提醒，并且无论提醒如何配置，都会在到期前的最后一周内每天发送提醒。

监控数字证书

请参阅以下命令来监控数字证书状态。

- **Monitoring > Properties > CRL**

  此窗格显示 CRL 详细信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

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。 引入了以下屏幕： Configuration > Remote Access VPN > Certificate Management Configuration > Site-to-Site VPN > Certificate Management。 引入或修改了以下屏幕： Configuration > Firewall > Advanced > Certificate Management > CA Certificates Configuration > Device Management > Certificate Management > CA Certificates。
证书管理	7.2(1)	

功能名称	平台版本	说明
证书管理	8.0(2)	
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。 修改了以下屏幕：Configuration > Remote Access VPN > Advanced Configuration > Device Management > Logging > Syslog Servers > Add/Edit Configuration > Device Management > Smart Call Home
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。 新建/修改菜单项：**配置** > **设备管理** > **证书管理** > **CA 证书**
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。

功能名称	平台版本	说明
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。
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。