# 思科中的证书管理 ISE-PIC

证书是标识个人、服务器、公司或其他实体并将实体与公钥关联的电子文档。公钥基础结构 (PKI) 是一种加密技术，用于实现安全通信和验证使用数字签名的用户的身份。证书用于在网络中提供安全访问。证书可以自签名，也可以由外部证书颁发机构 (CA) 进行数字签名。自签证书由证书创建者签名。CA 签名的数字证书符合行业标准且更安全。ISE-PIC 可以作为 pxGrid 的外部 CA，为 pxGrid 用户数字签名 pxGrid 证书。

思科 ISE-PIC 使用证书进行节点间通信（每个节点将其证书提供给另一节点以相互通信）以及与 pxGrid 的通信（ISE-PIC 和 pxGrid 相互提供证书）。对于其中每个用途，每个节点可以生成一个证书。证书会向 pxGrid 标识思科 ISE 节点身份，并确保 pxGrid 与思科 ISE 节点之间的安全通信。

安装时，ISE-PIC 将为每个 ISE-PIC 节点自动生成自签证书（在安装期间，系统将提示管理员接受从主节点自动为辅助节点创建的证书），并为 pxGrid 服务自动生成由主 ISE-PIC 节点数字签名的证书。此后，您可以生成 pxGrid 用户的证书，以便保证 pxGrid 和用户之间的相互信任，从而最终使用户身份能够从 ISE-PIC 传递到用户。ISE-PIC 中提供**证书 (Certificate)** 菜单，从中可查看证书、生成其他 ISE-PIC 证书并执行某些高级任务。

**注释** 管理员能够使用企业证书，ISE-PIC 在默认情况下设计为使用内部颁发机构为用户颁发 pxGrid 证书。



# 思科 ISE-PIC 中的证书匹配

设置部署中的思科 ISE-PIC 节点后，这两个节点将互相通信。系统将检查每个 ISE-PIC 节点的 FQDN，以确保其匹配（例如 ise1.cisco.com 和 ise2.cisco.com，如果使用通配符证书，则为 *.cisco.com）。此

外，当外部机器向 ISE-PIC 服务器提供证书时，将根据 ISE-PIC 服务器中的证书对提供用于身份验证的外部证书进行检查（或匹配）。如果两个证书匹配，则身份验证成功。

思科 ISE-PIC 按以下方式检查匹配的主题名称：

1. 思科 ISE-PIC 查看证书的主题别名 (SAN) 扩展。如果 SAN 包含一个或多个 DNS 名称，则其中必须有一个 DNS 名称与思科 ISE 节点的 FQDN 相匹配。如果使用通配符证书，则通配符域名必须与思科 ISE 节点的 FQDN 中的域匹配。
2. 如果 SAN 中不包含 DNS 名称、或 SAN 完全缺失，则证书主题字段中的通用名称或通配符域必须与节点的 FQDN 匹配。
3. 如果未找到匹配项，则会拒绝该证书。

# 通配符证书

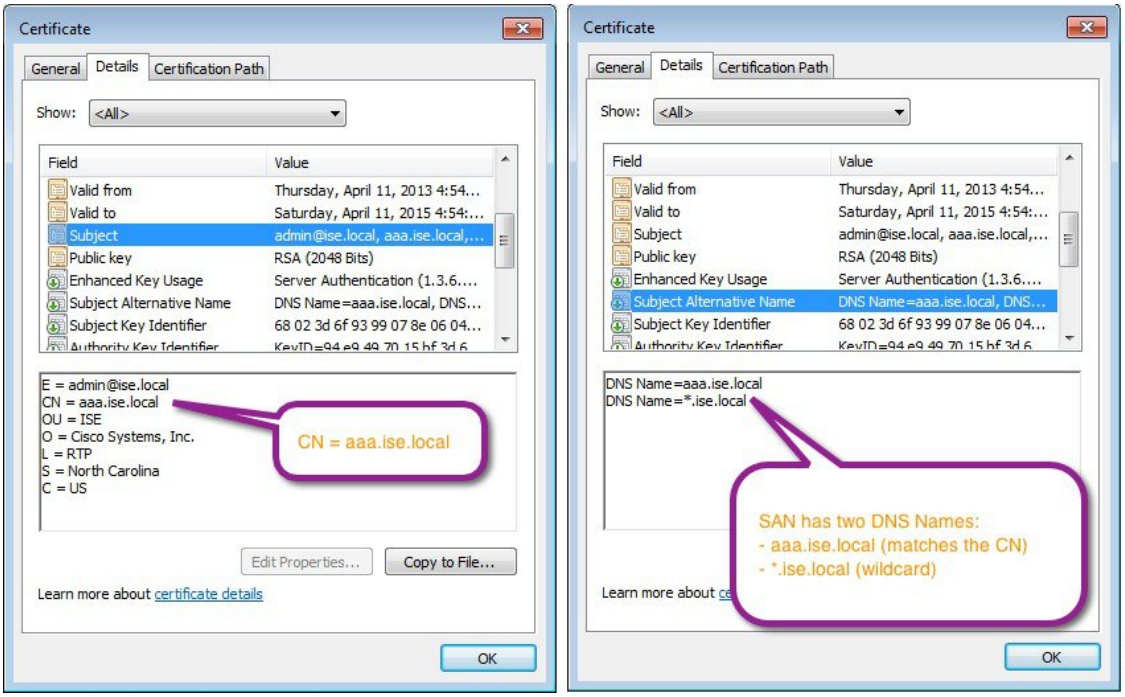
通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。例如，Certificate Subject 中的 CN 值可以是一些通用主机名（例如 aaa.ise.local），SAN 字段会包含相同的通用主机名和通配符表示法（例如 DNS.1=aaa.ise.local 和 DNS.2=*.ise.local）。

如果将某个通配符证书配置为使用 *.ise.local，可以使用同一证书来保护 DNS 名称以“.ise.local”结尾的任何其他主机，例如：psn.ise.local。

通配符证书用与普通证书一样的方式保护通信安全，并且使用相同的验证方法处理请求。

下图显示用于保护 Web 站点的一个通配符证书的示例。

**图 *1:* 通配符证书示例**



通过在 SAN 字段中使用星号 (*)，可以在两个节点上共享单个证书（如果已安装两个节点），并有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个思科 ISE 节点分配唯一服务器证书的安全性低。

注释 FQDN 的一些示例取自完整的 ISE 安装，因此可能不同于与 ISE-PIC 安装相关的地址。

# 使用通配符证书的优势

- 节约成本。由第三方证书颁发机构签名的证书都很昂贵，尤其是当服务器数量增加的时候。在思科 ISE 部署中，可以在多个节点上使用通配符证书。
- 提高运营效率。通配符证书允许所有策略服务节点 (PSN) EAP 和 Web 服务共享同一证书。除了能显著节约成本之外，由于可以只创建证书一次，然后就可以将其应用于所有 PSN，所以还能简化证书管理。
- 降低身份验证错误。通配符证书可以解决 Apple iOS 设备常见的证书问题，即客户端将受信任证书存储于配置文件中，而不遵循信任签名 root 的 iOS Keychain。当 iOS 客户端首次与 PSN 通信时，它不会明确信任 PSN 证书，即使受信任证书颁发机构已为该证书签名。使用通配符证书，所有 PSN 上证书都将一样，所以用户只须接受一次该证书，接下来对不同 PSN 的身份验证就会继续进行，而不会报错或出现提示。
- 简化请求方配置。例如，启用 PEAP-MSCHAPv2 和服务器证书信任的 Microsoft Windows 请求方要求您指定要信任的各个服务器证书，否则当客户端使用不同的 PSN 进行连接时，系统会提示用户是否信任各个 PSN 证书。使用通配符证书，可以信任一个统一的服务器证书，而不需从每个 PSN 逐一信任各个证书。
- 通配符证书可以减少提示，增强无缝连接，从而提高用户体验。

# 使用通配符证书的缺点

以下是与通配符证书相关的一些安全问题：

- 失去可审核性和不可否认性
- 提高了私钥的泄露风险
- 不常见或管理员不了解

通常认为通配符证书没有每个 ISE 节点均拥有的唯一的服务器证书那么安全。但是，成本和运营因素比安全风险更重要。

ASA 等安全设备也支持通配符证书。

部署通配符证书时，一定要谨慎。例如，如果您使用 *.company.local 创建一个证书，而某个攻击者能够发现其私钥，则该攻击者就可以监听 company.local 域中的任意服务器。因此，最好给域空间分区以避免这类威胁。

要解决可能出现的这个问题和限制使用范围，也可以使用通配符证书保护您的组织的具体子域。在您想要指定通配符的通用名称子域部分添加一个星号 (*)。

例如，如果您为 *.ise.company.local 配置通配符证书，则可以将该证书用于保护 DNS 名称以“.ise.company.local”结尾的任意主机，例如：

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

# 通配符证书兼容性

通常在创建通配符证书时，会将通配符列为证书使用者的公用名 (CN)。思科 ISE 支持这种类型的结构。但并不是所有的终端请求方都支持在证书使用者中使用通配符字符。

通过测试的所有 Microsoft 本机请求方（包括 Windows Mobile）不支持在证书使用者中使用通配符字符。

您可以使用另一个请求方，例如 Cisco AnyConnect 网络访问管理器 (NAM)，它可能允许在 Subject 字段中使用通配符字符。

您还可以使用特殊通配符证书（例如设计为与不兼容设备配合使用的 DigiCert 的 Wildcard Plus），方法是在证书的 Subject Alternative Name 中包含特定子域。

尽管 Microsoft 请求方限制似乎禁止使用通配符证书，但仍有其他方法创建通配符证书，允许它与通过测试的所有设备配合使用，从而实现安全访问，包括 Microsoft 本机请求方。

为此，您必须在 Subject Alterative Name (SAN) 字段中使用通配符字符，而不是在 Subject 中使用通配符字符。SAN 字段保留专为检查域名而设计的扩展名（DNS 名称）。有关详细信息，请参阅 RFC 6125 和 2128。

# 证书层次结构ISE-PIC

在ISE-PIC中，您可以查看所有证书的证书层次结构或证书信任链。证书层级包括证书、所有中间证书颁发机构 (CA) 证书和根证书。例如，当选择从ISE-PIC查看系统证书时，默认情况下会显示相应系统证书的详细消息。证书层级显示在该证书的顶部。点击层次结构中的任何证书可查看其详细信息。自签名证书没有任何层次结构或信任链。

在证书列表页面的“状态”(Status) 列中，您将会看到以下图标之一：

- 绿色图标 - 表示有效证书（有效信任链）
- 红色图标 - 表示存在错误（例如，信任证书缺失或过期）
- 黄色图标 - 警告证书即将到期并提示续订

# 系统证书

思科 ISE-PIC 系统证书是向部署中的其他节点和客户端应用标识思科 ISE-PIC 节点身份的服务器证书。要访问系统证书，请依次选择**证书 (Certificates)** > **系统证书 (System Certificates)**。系统证书的用途如下：

- 用于思科 ISE-PIC 部署中的节点间通信。在 Usage 字段中为这些证书选择 Admin 选项。
- 用于与 pxGrid 控制器通信。在 Usage 字段中为这些证书选择 pxGrid 选项。

必须在思科 ISE-PIC 部署中的每个节点上安装有效的系统证书。默认情况下，在安装期间，将在思科 ISE-PIC 节点上创建两个自签证书和一个由内部思科 ISE CA 签名的证书：

- 指定用于 用于管理员和 pxGrid 的自签名服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 SAML IdP 之间安全通信的自签名 SAML 服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 pxGrid 客户端之间安全通信的内部思科 ISE CA 签名的服务器证书（密钥长度为 4096，有效期为一年）。

设置部署并注册辅助节点时，指定用于 pxGrid 控制器的证书将自动替换为由主要节点的 CA 签名的证书。因此，所有 pxGrid 证书将属于同一 PKI 信任层次结构。

**注释** 要确定对应于您的版本的支持密钥和密码信息，请查找适当版本的《思科身份识别服务引擎网络组件兼容性》指南。

为了提高安全性，建议您使用 CA 签名的证书替换自签证书。要获取 CA 签名的证书，您必须：

1. 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 15 页
2. 将根证书导入受信任证书库，第 13 页
3. 将 CA 签名的证书与 CSR 绑定，第 16 页

# 查看系统证书

“系统证书”(System Certificate) 页面列出添加至思科 ISE-PIC 的所有系统证书。

**步骤 1** 依次选择 **证书 (Certificates)** > **系统证书 (System Certificates)** 。

系统显示 System Certificates 页面，提供关于本地证书的以下信息：

- Friendly Name - 证书的名称。
- Used By - 使用此证书的服务。

- “门户组标记”(Group Tag) - 仅适用于指定用于门户用途的证书。指定必须将哪个证书用于门户。
- Issued To - 证书使用者的通用名称。
- Issued By - 证书颁发者的通用名称。
- Valid From - 创建证书的日期，也称为开始时间证书属性。
- Expiration Date - 证书的到期日期，也称为截止时间证书属性。指示证书何时过期。到期日期有五个类别，每个类别有一个如下所述的关联图标：
  - 距到期还有 90 天以上（绿色图标）
  - 距到期还有 90 天或不足 90 天（蓝色图标）
  - 距到期还有 60 天或不足 60 天（黄色图标）
  - 距到期还有 30 天或不足 30 天（橙色图标）
  - 已到期（红色图标）

**步骤 2** 选择证书并选择 **View** 以显示证书详细信息。

# 导入系统证书

可以从管理员门户为任意思科 ISE-PIC 节点导入系统证书。

**注释** 更改主 PAN 上管理员角色证书的证书会重新启动所有其他节点上的服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

### 开始之前

- 确保您在运行客户端浏览器的系统上拥有系统证书和私钥文件。
- 如果您导入的系统证书由外部 CA 签名，则将相关根 CA 或中间 CA 证书导入受信任证书存储区（**证书 (Certificates) > 受信任的证书 (Trusted Certificates)**）。
- 如果导入的系统证书中包含 CA 标志设置为 true 的基本约束扩展，请确保有密钥用法扩展并且设置了 keyEncipherment 位或 keyAgreement 位。

**步骤 1**

**步骤 2** 单击**导入**。
此时将打开“导入服务器证书”(Import Server Certificate) 屏幕。

**步骤 3** 输入您要导入的证书的值。

**步骤 4** 点击**提交 (Submit)**。

# 生成自签证书

通过生成自签证书添加新的本地证书。思科建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署思科ISE-PIC，务必尽可能使用CA签名证书，确保生产网络中更统一地接受。

**注释** 如果使用自签证书并且必须更改思科 ISE-PIC 节点的主机名，则必须登录思科 ISE-PIC 节点的，删除采用旧主机名的自签证书，生成新的自签证书。否则，思科 ISE-PIC 将继续使用采用旧主机名的自签证书。

# 编辑系统证书

可以使用此页面编辑系统证书，续订自签证书。当编辑通配符证书时，更改将被复制到部署中的所有节点上。当删除通配符证书时，此通配符证书将从部署中的所有节点删除。

**步骤 1** 依次选择 **证书 (Certificates)** > **系统证书 (System Certificates)** 。

**步骤 2** 选中要编辑的证书旁边的复选框，然后点击 **Edit**。

**步骤 3** 要续订自签证书，请选中**续签期限 (Renewal Period)** 复选框，然后输入以天、周、月或年为单位的到期 TTL。

**步骤 4** 点击 **Save** 保存更改。

如果选中**管理 (Admin)** 复选框，系统将重新启动思科 ISE-PIC 节点上的应用服务器。

注释 使用 Chrome 65 及更高版本启动 ISE 可能会导致 BYOD 门户或访客门户无法在浏览器中启动，即使 URL 已成功重定向也是如此。这是因 Google 引入的新安全功能所致，此功能要求所有证书具有“主题备用名称”(Subject Alternative Name) 字段。对于版本 ISE 2.4 及更高版本，必须填充“主题备用名称”(Subject Alternative Name) 字段。

要使用 Chrome 65 及更高版本启动，请执行以下步骤：

1. 通过填充“主题备用名称”(Subject Alternative Name) 字段，从 ISE GUI 生成新的自签证书。必须填充 DNS 和 IP 地址。

2. ISE 服务现在将重新启动。

3. 在 Chrome 浏览器中重定向门户。

4. 在浏览器中，“查看证书”(View Certificate) > “详细信息”(Details) > 通过选择 base-64 编码来复制证书。

5. 将证书安装到受信任路径。

6. 关闭 Chrome 浏览器，然后尝试重定向门户。

注释 在为操作系统 Win RS4 或 RS5 中的浏览器 Firefox 64 及更高版本配置无线 BYOD 设置时，可能无法添加证书例外。如果是全新安装 Firefox 64 及更高版本，此行为是预计行为，如果是从先前版本升级到 Firefox 64 及更高版本，则不会出现此行为。通过以下步骤，可以在此情况下添加证书例外：

1. 针对 BYOD 流程单/双 PEAP 或 TLS 进行配置。

2. 通过 Windows ALL 选项配置 CP 策略。

3. 在最终客户端 Windows RS4/RS5 中连接 Dot1.x/MAB SSID。

4. 在 FF64 浏览器中键入 1.1.1.1 以重定向至访客/BYOD 门户。

5. 点击**添加例外 (Add Exception)** > **无法添加证书 (Unable to add certificate)**，然后继续进行流程。

解决方法是，必须导航至**选项 (Options)** > **隐私和设置 (Privacy & Settings)** > **查看证书 (View Certificates)** > **服务器 (Servers)** > **添加例外 (Add Exception)**，手动为 Firefox 64 添加证书。

# 删除系统证书

您可以删除不再使用的系统证书。

可以一次从系统证书存储区中删除多个证书，但必须至少具有一个可用于管理员 身份验证的证书。此外，无法删除用于管理员或 pxGrid 控制器的任何证书。但是，在禁用服务时可以删除 pxGrid 证书。

如果您选择删除通配符证书，则系统会从部署中的所有节点删除该证书。

**步骤 1** 依次选择 **证书 (Certificates)** > **系统证书 (System Certificates)** 。

**步骤 2** 选中想要删除的证书旁边的复选框，然后点击**删除 (Delete)**。

系统将显示一条警告消息。

**步骤 3** 点击 **Yes**，删除证书。

# 导出系统证书

您可以导出所选择的系统证书或某个证书及其关联的私钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

**步骤 1** 依次选择 **证书 (Certificates)** > **系统证书 (System Certificates)**。。

**步骤 2** 选中您要导出的证书旁边的复选框，然后点击**导出 (Export)**。

**步骤 3** 选择是仅导出证书，还是导出证书及其关联的私钥。

**提示** 由于可能会暴露私钥值，我们不建议导出与证书关联的私钥。如果您必须导出私钥（例如，导出要导入其他节点以用于节点间通信的通配符系统证书时），请指定私钥加密密码。将此证书导入另一思科ISE-PIC节点时，需要指定此密码以解密私钥。

**步骤 4** 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

**步骤 5** 点击 **Export** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以隐私强化邮件的格式进行存储。如果同时导出证书和私钥，则证书会导出为 .zip 文件，其中包含隐私强化邮件格式的证书和已加密的私钥文件。

# 受信任证书库

受信任证书库包括用于信任和简单证书注册协议 (SCEP) 的 X.509 证书。

X.509 证书仅从特定日期开始有效。当系统证书到期时，取决于证书的思科 ISE 功能会受到影响。当距离到期日还有 90 天时，思科 ISE 会通知您系统证书即将到期。系统以多种方式显示此通知：

- 彩色到期状态图标显示在 System Certificates 页面。
- 到期消息显示在思科 ISE 系统诊断报告中。
- 在距离到期日 90 天和 60 天时生成到期警报，在最后 30 天内，每天生成一次警报。

如果即将到期的证书为自签证书，您可以编辑证书，延长到期日。对于 CA 签名的证书，必须留出足够的时间，从 CA 获取替换证书。

思科 ISE 将受信任证书用于以下用途：

- 验证由终端和访问ISE-PIC门户的思科 ISE 管理员（使用基于证书的管理员身份验证）用于身份验证的客户端证书。
- 确保部署中思科 ISE-PIC 节点之间的安全通信。受信任证书库必须包含与部署中每个节点上的系统证书建立信任所需的 CA 证书链。
  - 如果将自签证书用于系统证书，则各个节点的自签证书必须放在 PAN 的受信任证书库中。
  - 如果将自签证书用于系统证书，则 CA root 证书以及信任链中的任何中间证书都必须放在 PAN 的受信任证书库中。

注释

- 导入到思科 ISE 的 X.509 证书的格式必须为隐私增强邮件 (PEM) 或卓越编码规则 (DER) 格式。可以根据特定限制，导入包含证书链的文件，也就是系统证书以及签名的受信任证书的序列。
- 将公共通配符证书分配给访客门户并使用根 CA 证书导入从属 CA 后，在 ISE 服务重新启动之前不会发送证书链

安装时，受信任证书存储区将填充自动生成的受信任证书。根证书（思科根 CA）给生产（思科 CA 生产）证书签名。

# 受信任证书命名限制

CTL 中的受信任证书可以包含名称限制扩展。此扩展为证书链中后续证书的所有主题名称和主题替代名称的值定义命名空间。思科 ISE 不检查根证书中指定的限制。

思科 ISE 支持以下名称限制：

- 目录名称

  目录名称限制应该是主题/SAN 中目录名称的前缀。例如，

  - 正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：O=Cisco,CN=Salomon

  - 不正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：CN=Salomon,O=Cisco

- DNS
- 邮件
- URI（URI 限制必须以一个 URI 前缀开头，例如 http://、https://、ftp:// 或 ldap://）。

思科 ISE 不支持以下名称限制：

- IP 地址
- 其他名称

当受信任证书包含不支持的限制并且验证的证书不包含相应字段时，系统会拒绝此证书，因为思科 ISE 无法验证不支持的限制。

以下是受信任证书中名称限制的一个示例：

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

以下是与以上定义匹配的一个可接受客户端证书主题：

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

# 查看受信任证书库证书

“受信任证书”(Trusted Certificates) 页面列出所有已添加到思科 ISE-PIC 的受信任证书。

要查看所有证书，请依次选择**证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。系统将显示受信任证书页面，其中列出了所有受信任的证书。

# 更改受信任证书库中的证书状态

必须启用证书状态，思科 ISE-PIC 才能使用此证书建立信任。将证书导入受信任证书库时，将自动启用此证书。

# 在受信任的证书库中添加证书

可以通过“证书存储区”(Certificate Store) 页面向思科 ISE-PIC 添加 CA 证书。

开始之前

- 确保证书库证书位于运行您的浏览器的计算机文件系统上。证书必须是 PEM 或 DER 格式。
- 如果您计划将证书用于管理员或 EAP 身份验证，请确保在证书中定义基本限制并且确保 CA 标志设置为 true。

# 编辑受信任证书

在将证书添加到受信任证书库之后，可以通过使用编辑设置进行进一步编辑。

**步骤 1** 依次选择 **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。。

**步骤 2** 选中要编辑的证书旁边的复选框，然后点击 **Edit**。

**步骤 3** 根据需要修改可编辑字段。

**步骤 4** 点击 **Save** 以保存对证书库所做的更改。

# 删除受信任证书

可以删除不再需要的受信任证书。不过，请确保不会删除 ISE-PIC 内部 CA（证书颁发机构）证书。ISE-PIC 内部 CA 证书只能在替换整个部署的 ISE-PIC 根证书链时删除。

**步骤 1** 依次选择 **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。

**步骤 2** 选中想要删除的证书旁边的复选框，然后点击 **Delete**。

系统将显示一条警告消息。如果已选择删除 ISE-PIC 内部 CA 证书，则点击：

- **删除 (Delete)** - 删除 ISE-PIC 内部 CA 证书。ISE-PIC 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。要允许终端再次接入网络，请将相同的 ISE-PIC 内部 CA 证书导入受信任证书存储区。
- **删除并撤销 (Delete & Revoke)** - 删除并撤销 ISE-PIC 内部 CA 证书。ISE-PIC 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。此操作无法撤销。必须替换整个部署的 ISE-PIC 根证书链。

**步骤 3** 点击 **Yes**，删除证书。

# 从受信任证书库导出证书

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

注释 如果从内部CA导出证书，并计划使用该导出从备份恢复，则必须使用CLI命令 `application configure ise`。有关详细信息，请参阅导出思科 ISE CA 证书和密钥，第 27 页。

**步骤 1** 依次选择**证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。。

**步骤 2**

**步骤 3** 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

**步骤 4** 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

# 将根证书导入受信任证书库

导入根 CA 和中间 CA 证书时，您可以指定要为其使用受信任 CA 证书的服务。

### 开始之前

您必须具有来自已对 CSR 进行签名并返回数字签名 CA 证书的证书颁发机构的根证书和其他中间证书。

**步骤 1** 依次选择**证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。

**步骤 2**

**步骤 3** 单击**导入**。

**步骤 4** 在显示的**将新证书导入证书存储区 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)** 以选择您的 CA 签名和返回的根 CA 证书。

**步骤 5** 在 **Friendly Name** 中输入友好的名称。

如果没有输入**友好名称**，思科 ISE-PIC 将使用 *common-name#issuer#nnnnn* 格式的名称填充此字段， 其中 *nnnnn* 是唯一编号。可以再次编辑证书来更改**友好名称**。

**步骤 6** 选中要为其使用此受信任证书的服务旁边的复选框。

**步骤 7** （可选）在**说明 (Description)** 字段中，输入此证书的说明。

**步骤 8** 点击**提交 (Submit)**。

### 下一步做什么

将中间 CA 证书导入到受信任证书库（如果适用）。

# 证书链导入

您可以从单个文件导入多个证书，这个文件中包含从证书库接收的证书链。文件中的所有证书都必须为隐私增强邮件 (PEM) 格式，并且这些证书必须按照以下顺序排列：

- 文件中的最后一个证书必须是 CA 颁发的客户端证书或服务器证书。
- 前面的所有证书必须是根 CA 证书和所颁发证书的签名链中的所有中间 CA 证书。

导入证书链的过程分为两个步骤：

1. 在 Admin 门户中将证书链文件导入受信任证书库。此操作会将除最后一个证书之外的所有证书导入受信任证书库。
2. 使用绑定CA签名的证书操作导入证书链文件。此操作会将文件中的最后一个证书导入作为本地证书。

# 受信任证书导入设置

表 *1:* 受信任证书导入设置

| 字段名称 | 说明 |
|---|---|
| **Certificate File** | 点击**浏览 (Browse)** 从运行浏览器的计算机选择证书文件。 |
| **Friendly Name** | 输入证书的友好名称。如果您不指定名称，思科 ISE-PIC 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。 |
| **Trust for authentication within ISE** | 如果您希望将此证书用于验证服务器证书（从其他 ISE-PIC 节点或 LDAP 服务器），请选中此复选框。 |
| **Trust for client authentication and Syslog** | （仅在选中了“信任 ISE-PIC 中的身份验证”(Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框：<br>• 对使用 EAP 协议连接至 ISE-PIC 的终端进行身份验证<br>• 信任系统日志服务器 |
| **Trust for authentication of Cisco Services** | 如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。 |

| 字段名称 | 说明 |
| --- | --- |
| 验证证书扩展名 | （仅适用于同时选中 Trust for client authentication 选项和 Enable Validation of Certificate Extensions 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。 |
| 说明 **(Description)** | 输入可选的说明。 |

**相关主题**

受信任证书库，第 9 页
证书链导入，第 14 页
将根证书导入受信任证书库，第 13 页

# 证书签名请求

对于证书颁发机构 (CA)，要签发签名证书，您必须创建证书签名请求 (CSR) 并将其提交给 CA。

Certificate Signing Requests 页面会提供您已创建的证书签名请求 (CSR) 的列表。要从证书颁发机构 (CA) 获得签名，您必须导出 CSR，然后将证书发送至 CA。CA 给证书签名，然后返回证书。

您可以从 Admin 门户集中管理证书。您可以为您的部署中的所有节点创建 CSR 并导出这些 CSR。然后，您应该将这些 CSR 提交给 CA，从 CA 获取 CA 签名的证书，将 CA 返回的 root 和中间 CA 证书导入受信任证书库，并且将 CA 签名的证书与 CSR 绑定。

## 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构

可以生成证书签名请求 (CSR)，为部署中的节点获取 CA 签名的证书。可以为部署中的选定节点或所有节点生成 CSR。

**步骤 1** 依次选择 **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 输入用于生成 CSR 的值。有关其中每个字段的信息，请参阅证书签名请求设置。

**步骤 3** 点击 **Generate** 以生成 CSR。

系统将生成 CSR。

**步骤 4** 点击 **Export** 以在 Notepad 中打开 CSR。

**步骤 5** 复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的所有文本。

**步骤 6** 将 CSR 的内容粘贴到选定 CA 的证书请求中。

**步骤 7** 下载签名证书。

某些CA可能会将签名的证书通过邮件发送给您。签名的证书采用ZIP文件形式，其中包含必须添加到思科ISE-PIC受信任证书存储区的CA新颁发证书和公共签名证书。将数字签名的CA证书、根CA证书和其他中间CA证书（如果适用）下载到运行客户端浏览器的本地系统中。

# 将 CA 签名的证书与 CSR 绑定

在具有由AC返回的数字签名证书之后，您必须将其绑定到证书签名请求(CSR)。您可以从管理员门户为部署中的所有节点执行绑定操作。

### 开始之前

- 您必须具有数字签名的证书，以及由 CA 返回的相关根和中间 CA 证书。
- 将相关的根和中间 CA 证书导入受信任证书存储区（**证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。）。

**步骤 1** 依次选择 **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)** 。

选择您正为其绑定 CSR 与 CA 签名的证书的节点旁边的复选框。

**步骤 2** 点击 **Bind**。

**步骤 3** 点击 **Browse** 选择 CA 签名的证书。

**步骤 4** 为证书指定 Friendly Name。

**步骤 5** 如果您希望思科 ISE-PIC 验证证书扩展，请选中**验证证书扩展 (Validate Certificate Extensions)** 复选框。

如果您启用**验证证书扩展 (Validate Certificate Extensions)** 选项，且您正在导入的证书包含 CA 标志设置为 ture 的基本约束扩展，则请确保存在密钥用法扩展，且已设置 keyEncipherment 位和/或 akeyAgreement 位。

**注释** ISE 要求 EAP-TLS 客户端证书具有数字签名密钥使用扩展。

**步骤 6** 选中要为其将此证书用于 Usage 区域的服务。

如果您在生成CSR时已启用Usage选项，则此信息会自动填充。 如果您不想在绑定证书时指定用法，请取消选中Usage选项。您可以稍后编辑证书并指定用法。

**注释** 更改主 PAN 上管理员角色证书的证书会重新启动所有其他节点上的服务

更改主 PAN 上管理员角色证书的证书会重新启动所有其他节点上的服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

**步骤 7** 点击 **Submit** 以绑定 CA 签名的证书。

如果您已选择将此证书用于思科 ISE-PIC 节点间通信，则思科 ISE-PIC 节点上的应用服务器会重新启动。

要在其他节点上绑定 CSR 与 CA 签名的证书，请重复此流程。

下一步做什么

将根证书导入受信任证书库，第 13 页

# 导出证书签名请求

您可以使用此页面导出证书签名请求。

**步骤 1** 依次选择 **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)** 。

**步骤 2** 选中想要导出的证书旁边的复选框，点击 **Export**。

**步骤 3** 点击 **OK**，将文件保存到正在运行客户端浏览器的文件系统中。

# 证书签名请求设置

通过思科 ISE-PIC，只需一个请求即可从管理员门户为部署中的节点生成 CSR。此外，还可以选择为部署中的单个节点或节点生成 CSR。如果选择为单个节点生成 CSR，则 ISE 会自动在证书使用者的 CN= 字段中替换特定节点的完全限定域名 (FQDN)。如果选择在证书的“主体可选名称”(SAN) (Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE-PIC 节点的 FQDN。如果选择为部署中的两个节点生成 CSR，请选中“允许通配符证书”(Allow Wildcard Certificates) 复选框，然后在 SAN 字段（“DNS 名称”(DNS name)）中输入通配符 FQDN 符号，例如，*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个思科 ISE-PIC 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个思科 ISE-PIC 节点分配唯一服务器证书的安全性低。

表 *2:* 证书签名请求设置

| 字段 | 使用指南 |
| --- | --- |
| **Certificate(s) will be used for** | |

| 字段 | 使用指南 |
| --- | --- |
| | 选择即将对其使用证书的服务：<br>**思科 ISE 身份证书**<br>• **多用途 (Multi-Use)**：用于多种服务（管理员、EAP-TLS 身份验证、pxGrid）。多用途证书同时使用客户端和服务器密钥用法。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性：<br>  • **Key Usage (密钥使用)**：数字签名（签名）<br>  • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2)<br>• **管理 (Admin)**：用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE-PIC 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性：<br>  • **Key Usage (密钥使用)**：数字签名（签名）<br>  • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1)<br>• **pxGrid**：同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性：<br>  • **Key Usage (密钥使用)**：数字签名（签名）<br>  • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2)<br>• **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。<br>  • **Key Usage (密钥使用)**：数字签名（签名）<br>  • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1)<br>**注释** 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息：<br>`source=local type=fatal message="unsupported certificate"`<br>思科 **ISE** 证书颁发机构证书 |

| 字段 | 使用指南 |
| --- | --- |
| | • **ISE 根 CA (ISE Root CA)**：（仅适用于内部 CA 服务）用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。<br>• **ISE 中间 CA (ISE Intermediate CA)**：（仅适用于当 ISE-PIC 用作外部 PKI 的中间 CA 时的内部 CA 服务）用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成辅助 CA 证书。签名 CA 的证书模板通常称为辅助证书颁发机构。此模板具有以下属性：<br>  • **基本约束 (Basic Constraints)**：关键、是证书颁发机构<br>  • **密钥使用 (Key Usage)**：证书签名、数字签名<br>  • **扩展密钥使用 (Extended Key Usage)**：OCSP 签名 (1.3.6.1.5.5.7.3.9)<br>• **更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)**：（仅适用于内部 CA 服务）用于更新整个部署的 ISE-PIC OCSP 响应方证书（不是证书签名请求）。出于安全原因，建议您每六个月更新一次 ISE-PIC OCSP 响应方证书。 |
| **Allow Wildcard Certificates** | 选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。 |
| **Generate CSRs for these Nodes** | 选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成CSR，必须取消 Allow Wildcard Certificates 选项。 |
| **Common Name (CN)** | 默认情况下，公用名是您正为其生成CSR的ISE-PIC节点的FQDN。$FQDN$ 表示 ISE-PIC 节点的 FQDN。当为部署中的多个节点生成 CSR 时，CSR 中的 Common Name 字段会替换为各个 ISE 节点的 FQDN。 |
| **Organizational Unit (OU)** | 组织单位名称。例如，Engineering。 |
| **Organization (O)** | 组织名称。例如，Cisco。 |
| **City (L)** | （请勿缩写）城市名称。例如，圣何塞。 |
| **State (ST)** | （请勿缩写）省/自治区/直辖市名称。例如，加州。 |
| **Country (C)** | 国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。 |

| 字段 | 使用指南 |
| --- | --- |
| **Subject Alternative Name (SAN)** | “IP 地址”(IP address)、“DNS 名称”(DNS name)、“统一资源标识符”(Uniform Resource Identifier, URI) 或与证书关联的“目录名称”(Directory Name)。<br>• **DNS 名称 (DNS name)**：如果选择“DNS 名称”(DNS name)，请输入 ISE-PIC 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项，请指定通配符符号（域名前的星号和句号）。例如：*.amer.example.com。<br>• **IP 地址 (IP address)**：将与证书关联的 ISE-PIC 节点的 IP 地址。<br>• **统一资源标识符 (Uniform Resource Identifier)**：您希望与证书关联的 URI。<br>• **目录名称 (Directory Name)**：根据 RFC 2253 定义的可区分名称 (DN) 的字符串表示。使用逗号 (,) 隔开多个 DN。对于“dnQualifier”RDN，避免使用逗号而是使用反斜杠“\”作为分隔符。例如，CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL |
| 密钥类型 | 指定要用于创建公共密钥的算法：RSA 或 ECDSA。 |
| 密钥长度 | 指定公共密钥的位大小。<br>以下选项可用于 RSA：<br>• 512<br>• 1024<br>• 2048<br>• 4096<br>以下选项可用于 ECDSA：<br>• 256<br>• 384<br>注释 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。<br>如果计划获取公共的 CA 签名证书，请选择 2048 或更大长度。 |
| **Digest to Sign With** | 选择下列散列算法之一：SHA-1 或 SHA-256。 |
| 证书策略 | 输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。 |

# 思科 ISE CA 服务

证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。ISE-PIC 可用作 pxGrid 的外部证书颁发机构 (CA)，对 pxGrid 证书进行数字签名。CA 签名的数字证书被视为行业标准而且更安全。ISE-PIC CA 提供以下功能：

- 颁发证书：为连接您的网络的终端验证和签发证书签名请求 (CSR)。
- 密钥管理：在 上生成并安全地存储密钥和证书。
- 存储证书：存储向用户和设备颁发的证书。
- 支持在线证书状态协议 (OCSP)：提供 OCSP 响应器以检查证书的有效性。

当 CA 服务在主管理节点上禁用时，CA 服务仍被视为在辅助管理节点的 CLI 上运行。理想情况下，CA 服务应被视为禁用。此为已知的思科 ISE 问题。

## 省略曲线加密证书支持

思科 ISE-PIC CA 服务支持基于忽略曲线加密 (ECC) 算法的证书。与其他加密算法相比，ECC 提供的安全性和性能更高，即使使用更小的密钥大小也是如此。

下表比较了 ECC 和 RSA 的密钥大小以及安全强度。

| **ECC 密钥大小（位）** | **RSA 密钥大小（位）** |
|---|---|
| 160 | 1024 |
| 224 | 2048 |
| 256 | 3072 |
| 384 | 7680 |
| 521 | 15360 |

由于密钥大小较小，加密速度更快。

思科 ISE-PIC 支持以下 ECC 曲线类型。曲线类型越高，密钥规模越大，安全性就越强。

- P-192
- P-256
- P-384
- P-521

ISE-PIC 不支持证书中 EC 部分的显式参数。如果尝试导入具有显式参数的证书，将显示以下错误：“证书验证失败: 仅支持命名的 EC 参数”(Validation of certificate failed: Only named ECParameters supported)。

可以从证书调配门户生成 ECC 证书。

# 思科 ISE-PIC 证书颁发机构证书

“证书颁发机构 (CA) 证书”(Certificate Authority (CA) Certificates) 页面列出了与内部思科 ISE-PIC CA 相关的所有证书。此页面按节点列出这些证书。可以展开某个节点以查看该特定节点的所有 ISE-PIC CA 证书。主要和辅助管理节点具有根 CA、节点 CA、从属 CA 和 OCSP 响应器证书。部署中的其他节点具有终端从属 CA 和 OCSP 证书。

启用思科 ISE-PIC CA 服务时，将在所有节点上自动生成和安装这些证书。此外，在替换整个 ISE-PIC 根 CA 链时，将在所有节点上自动重新生成和安装这些证书。不需要手动干预。

思科 ISE-PIC CA 证书遵循以下命名约定：**证书服务 <终端从属 *CA*/节点 *CA*/根 *CA*/*OCSP* 响应器>-<**节点主机名>#证书编号。

在“CA 证书”(CA Certificates) 页面中，可以编辑、导入、导出、删除和查看思科 ISE-PIC CA 证书。

## 编辑思科 ISE-PIC CA 证书

在添加证书到思科 ISE-PIC CA 证书存储区之后，可以采用编辑设置对其进行进一步编辑。

**步骤 1** 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。。

**步骤 2** 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

**步骤 3** 选中要编辑的证书旁边的复选框，然后点击 **Edit**。

**步骤 4** 根据需要修改可编辑字段。有关这些字段的说明，请参阅编辑证书设置。

**步骤 5** 点击 **Save** 以保存对证书库所做的更改。

## 导出思科 ISE CA 证书

要导出思科 ISE 根 CA 和节点 CA 证书：

### 开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

**步骤 1** 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。

**步骤 2** 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

**步骤 3** 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

**步骤 4** 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

# 导入思科 ISE-PIC CA 证书

如果客户端尝试使用来自其他部署的思科 ISE-PIC 颁发的证书对您的网络进行身份验证，您必须将来自该部署的思科 ISE-PIC 根 CA 证书、节点 CA 证书和终端从属 CA 证书导入到思科 ISE-PIC 受信任证书存储区。

### 开始之前

- 将 ISE-PIC 根 CA 证书、节点 CA 证书和终端从属 CA 证书从终端证书签名的部署中导出，并将其存储在浏览器运行所在的计算机的文件系统。

**步骤 1** 依次选择 **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。

**步骤 2**

**步骤 3** 点击**导入 (Import)**。

**步骤 4** 如有必要，配置这些字段值。有关详细信息，请参阅受信任证书导入设置。

如果启用基于证书的客户端身份验证，则思科 ISE-PIC 将重新启动您的部署中每个节点上的应用服务器，从 PAN 。

# 编辑证书设置

下表介绍了“证书存储区编辑证书”(Certificate Store Edit Certificate) 窗口上的字段，可以使用此窗口编辑证书颁发机构 (CA) 证书属性。此页面的导航路径为**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **证书 (Certificate)** > **编辑 (Edit)**。

**表 *3:* 证书库编辑设置**

| 字段名称 | 使用指南 |
|---|---|
| Certificate Issuer | |
| **Friendly Name** | 输入证书的友好名称。 |
| 状态 | 选择 Enabled 或 Disabled。如果选择 Disabled，ISE 将不使用此证书建立信任。 |
| 说明 | 输入可选的说明。 |
| Usage | |
| **Trust for authentication within ISE** | 如果您想要使用此证书验证服务器证书（从其他 ISE 节点或 LADP 服务器），请选中此复选框。 |

| 字段名称 | 使用指南 |
| --- | --- |
| **Trust for client authentication and Syslog** | （仅适用于选中 Trust for authentication within ISE 复选框的情况）如果您想将此证书用于以下用途，请选中此复选框：<br>• 对使用 EAP 协议连接至 ISE 的终端进行身份验证<br>• 信任系统日志服务器 |
| **Trust for authentication of Cisco Services** | 如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。 |
| **Certificate Status Validation** | ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至 ISE 的证书吊销列表 (CRL) 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。 |
| **Validate Against OCSP Service** | 选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。 |
| **Reject the request if OCSP returns UNKNOWN status** | 如果 OCSP 无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致 ISE 拒绝当前评估的客户端或服务器证书。 |
| **OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)** | 选中此复选框供 ISE 在 OCSP 响应器无法访问时拒绝请求。 |
| **Download CRL** | 选中此复选框以使思科 ISE 下载 CRL。 |
| **CRL Distribution URL** | 输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了 URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。 |
| **Retrieve CRL** | 可以自动或定期下载 CRL。请配置下载时间间隔。 |
| **If download failed, wait** | 配置在思科 ISE 再次尝试下载 CRL 之前等待的时间间隔。 |

| 字段名称 | 使用指南 |
| --- | --- |
| **Bypass CRL Verification if CRL is not Received** | 选中此复选框，以使系统在收到CRL之前接受客户端请求。如果取消选中此复选框，思科 ISE 会拒绝使用选定CA签名的证书的所有客户端请求，直到收到 CRL 文件为止。 |
| **Ignore that CRL is not yet valid or expired** | 如果您希望思科 ISE 忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝EAP-TLS身份验证，请选中此复选框。<br>如果您希望思科 ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查 CRL 文件，请取消选中此复选框。如果 CRL 尚未激活或已到期，思科 ISE 会拒绝使用此 CA 签名的证书的所有身份验证。 |

相关主题

受信任证书库，第 9 页
编辑受信任证书，第 12 页

# 思科 ISE-PIC CA 证书和密钥的备份与恢复

必须安全地备份思科 ISE-PIC CA 证书和密钥，以在出现 PAN 故障以及您要将辅助管理节点升级作为外部 PKI 的根 CA 或中间 CA 的情况下在辅助管理节点上恢复这些证书和密钥。思科 ISE-PIC 配置备份不包括 CA 证书和密钥。您应使用命令行界面 (CLI) 将 CA 证书和密钥导出至存储库，然后再导入。**application configure ise** 命令现在包含导出和导入选项，用于备份和恢复 CA 证书和密钥。

来自受信任证书库的以下证书存储于辅助管理节点上：

- 思科 ISE Root CA 证书
- 思科 ISE 子 CA 证书
- 思科 ISE 终端 RA 证书
- 思科 ISE OCSP 响应器证书

在以下情况下，您必须备份和恢复思科 ISE CA 证书和密钥：

- 部署中有辅助管理节点
- 替换整个思科 ISE-PIC CA 根链
- 配置思科 ISE-PIC 根 CA 作为外部 PKI 的从属 CA
- 从配置备份恢复数据。在这种情况下，必须首先重新生成思科 ISE-PIC CA 根链，然后备份和恢复 ISE CA 证书和密钥。

注释 每次在部署中更换思科 ISE 内部 CA 后，还必须同时刷新 ISE 消息服务，以检索完整的证书链。

## 导出思科 ISE CA 证书和密钥

您必须从 PAN 导出 CA 证书和密钥，才能将其导入到辅助管理节点。通过此选项，辅助管理节点可以在 PAN 关闭和您将辅助管理节点升级到 PAN 时为终端颁发和管理证书。

### 开始之前

确保您已经创建了用于存储 CA 证书和密钥的存储库。

**步骤 1** 在思科 ISE CLI 上输入 **application configure ise** 命令。

**步骤 2** 输入 7 以导出证书和密钥。

**步骤 3** 输入存储库名称。

**步骤 4** 输入加密密钥。

系统将显示成功消息和已导出的证书列表，以及主题、颁发机构和序列号。

**示例：**

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

## 导入思科 ISE-PIC CA 证书和密钥

在注册辅助管理节点之后，您必须从 PAN 导出 CA 证书和密钥并将它们导入到辅助管理节点。

**步骤 1** 在思科 ISE-PIC CLI 上输入 **application configure ise** 命令。

**步骤 2** 输入 8 以导入 CA 证书和密钥。

**步骤 3** 输入存储库名称。

**步骤 4** 输入要导入的文件的名称。文件名应采用以下格式 **ise_ca_key_pairs_of_<vm hostname>**。

**步骤 5** 输入加密密钥以解密文件。

系统将显示一条成功消息。

**示例：**

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

# 生成根 CA 和从属 CA

设置部署时，思科 ISE-PIC 会在节点。但是，当更改 节点 的域名或主机名时，必须分别在主 PAN 上重新生成根 CA，在 PSN 上重新生成从属 CA。

**步骤 1** 依次选择 **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 点击**生成证书签名请求 (Generate Certificate Signing Requests)**。

**步骤 3** 从 **Certificate(s) will be used for** 下拉列表中选择 ISE 根 CA。

**步骤 4** 点击 **Replace ISE Root CA Certificate chain**。

系统会为部署中的所有节点生成根 CA 和从属 CA 证书。

### 下一步做什么

如果部署中具有辅助 PAN，请从主 PAN 获取思科 ISE-PIC CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助 PAN 可以在主 PAN 故障时用作根 CA，您可将辅助 PAN 升级为主 PAN。

# 将思科 ISE-PIC 根 CA 配置为外部 PKI 的辅助 CA

如果您希望主 PAN 上的根 CA 作为外部 PKI 的从属 CA，则生成 ISE-PIC 中间 CA 证书签名请求，将其发送到外部 CA，获取根 CA 证书和 CA 签名的证书，将根 CA 证书导入受信任证书存储区，将 CA 签名的证书绑定到 CSR。在这种情况下，外部 CA 为根 CA，节点 为外部 CA 的从属 CA，PSN 为 节点 的从属 CA。

**步骤 1** 依次选择 **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)** 。

**步骤 2** 点击 **Generate Certificate Signing Requests (CSR)**。

**步骤 3** 从 **Certificate(s) will be used for** 下拉列表选择 ISE 中级 CA。

**步骤 4** 点击 **Generate**。

**步骤 5** 导出 CSR，将其发送到外部 CA，获取 CA 签名的证书。

**步骤 6** 将根 CA 证书从外部 CA 导入受信任证书库。

**步骤 7** 将 CA 签名证书与 CSR 绑定。

# OCSP 服务

在线证书状态协议 (OCSP) 是一种用于检查 x.509 数字证书状态的协议。此协议替代证书吊销列表 (CRL) 并解决导致处理 CRL 的问题。

思科 ISE 能够通过 HTTP 与 OCSP 服务器进行通信，以在身份验证中验证证书的状态。OCSP 配置在可从思科 ISE 中配置的任何证书颁发机构 (CA) 证书引用的可重用配置对象中进行配置。

您可以根据 CA 配置 CRL 和/或 OCSP 验证。如果同时选择两者，则思科 ISE 会先通过 OCSP 执行验证。如果检测到主 OCSP 服务器和辅助 OCSP 服务器均有通信问题，或者如果针对给定证书返回未知状态，则思科 ISE 会切换至检查 CRL。

## 思科 ISE CA 服务在线证书状态协议响应器

思科 ISE CA OCSP 响应器是与 OCSP 客户端进行通信的服务器。思科 ISE CA 的 OCSP 客户端包括内部思科 ISE OCSP 客户端和自适应安全设备 (ASA) 上的 OCSP 客户端。OCSP 客户端应使用 RFC 2560 和 5019 中定义的 OCSP 请求/响应结构与 OCSP 响应器进行通信。

ISE CA 向 OCSP 响应器颁发证书。OCSP 响应器在端口 2560 上侦听任何传入请求。此端口配置为仅允许 OCSP 流量。

OCSP 响应器接受遵循 RFC 2560 和 5019 中定义的结构的请求。OCSP 请求中支持随机数扩展。OCSP 响应器获取证书的状态，然后创建 OCSP 响应并对其进行签名。OCSP 响应不会缓存到 OCSP 响应器上，但您可以将 OCSP 响应缓存到客户端上，最长期限为 24 小时。OCSP 客户端应验证 OCSP 响应中的签名。

PAN 上的自签名 CA 证书（如果 ISE 用作外部 CA 的中间 CA，则是中间 CA 证书）颁发 OCSP 响应器证书。PAN 上的此 CA 证书颁发 PAN 和 PSN 上的 OCSP 证书。此自签名 CA 证书也是整个部署

的根证书。整个部署中的所有 OCSP 证书都放在 ISE 的受信任证书库中，以验证任何使用这些证书签名的响应。

# OCSP 证书状态值

OCSP 服务面向给定的证书请求返回以下值：

- Good - 表示对状态查询的肯定回答。它意味着仅在下次时间间隔（存活时间）值之前证书未被吊销并且状态良好。
- Revoked - 证书被吊销。
- Unknown - 证书状态未知。如果证书不是由此 OCSP 响应者的 CA 颁发，则 OCSP 服务会返回此值。
- Error - 没有收到 OCSP 请求的任何响应。

# OCSP 高可用性

思科 ISE 能够为每个 CA 配置最多两台 OCSP 服务器，我们将其称为主 OCSP 服务器和辅助 OCSP 服务器。每个 OCSP 服务器配置均包含以下参数：

- URL - OCSP 服务器 URL。
- Nonce - 请求中发送的随机数。此选项可确保重放攻击无法利用旧通信数据。
- Validate response - 思科 ISE 验证从 OCSP 服务器接收到的响应签名。

在超时（5 秒钟）情况下，当思科 ISE 与主要 OCSP 服务器进行通信时，它会切换为辅助 OCSP 服务器。

思科 ISE 在尝试再次使用主要服务器之前，会在可配置的时间内使用辅助 OCSP 服务器。

# OCSP 故障

以下是三个一般 OCSP 故障情况：

- OCSP 缓存或 OCSP 客户端（思科 ISE）故障。
- OCSP 响应器故障情况，例如：

  第一个主要 OCSP 响应器无响应，辅助 OCSP 响应器响应思科 ISE OCSP 请求。

  无法从思科 ISE OCSP 请求接收错误或响应。

  OCSP 响应器可能不向思科 ISE OCSP 请求提供响应或可能返回一个不成功的 OCSP Response Status 值。可能的 OCSP Response Status 值如下所示：

  - tryLater
  - signRequired

- unauthorized
- internalError
- malformedRequest

  OCSP 请求中有很多日期时间检查、签名验证检查等。有关详细信息，请参阅 *RFC 2560 X.509* 互联网公钥基础结构在线证书状态协议 - *OCSP*，其中描述了所有可能的状态，包括错误状态。

- OCSP 报告故障

# 添加 OCSP 客户端配置文件

您可以使用 OCSP Client Profile 页面，将新 OCSP 客户端配置文件添加到思科 ISE。

### 开始之前

如果 Certificate Authority (CA) 正在非标准端口（不是 80 或 443）上运行 OCSP 服务，则必须在交换机上配置 ACL，允许在思科 ISE 和 CA 之间通过此端口进行通信。例如：

**permit tcp** <*source ip*> <*destination ip*> **eq** <*OCSP* 端口号>

**步骤 1** 依次选择 **证书 (Certificates)** > **OCSP 客户端配置文件 (OCSP Client Profile)** 。

**步骤 2** 输入值，添加 OCSP 客户端配置文件。

**步骤 3** 点击**提交 (Submit)**。

# OCSP 统计计数器

思科 ISE 使用 OCSP 计数器记录并监控 OCSP 服务器的数据和运行状况。日志记录每五分钟记录进行一次。思科 ISE 将系统日志消息发送到监控节点，并在本地库中进行保存。本地库包含之前五分钟的数据。思科ISE发送系统日志消息后，计数器会重新开始计算下一个间隔。这表示在五分钟后，新的五分钟时间间隔将会启动。

以下表格列出 OCSP 系统日志消息及其说明。

**表 *4: OCSP* 系统日志消息**

| 消息 | 说明 |
|---|---|
| OCSPPrimaryNotResponsiveCount | 无响应的主请求数量 |
| OCSPSecondaryNotResponsiveCount | 无响应的辅助请求数量 |
| OCSPPrimaryCertsGoodCount | 对于使用 OCSP 主服务器的给定 CA 所返回的“good”证书数量 |

| 消息 | 说明 |
| --- | --- |
| OCSPSecondaryCertsGoodCount | 对于使用 OCSP 主服务器的给定 CA 所返回的“good”状态数量 |
| OCSPPrimaryCertsRevokedCount | 对于使用 OCSP 主服务器的给定 CA 所返回的“revoked”状态数量 |
| OCSPSecondaryCertsRevokedCount | 对于使用 OCSP 辅助服务器的给定 CA 所返回的“revoked”状态数量 |
| OCSPPrimaryCertsUnknownCount | 对于使用 OCSP 主服务器的给定 CA 所返回的“Unknown”状态数量 |
| OCSPSecondaryCertsUnknownCount | 对于使用 OCSP 辅助服务器的给定 CA 所返回的“Unknown”状态数量 |
| OCSPPrimaryCertsFoundCount | 主源缓存中查找到的证书数量 |
| OCSPSecondaryCertsFoundCount | 辅助源缓存中查找到的证书数量 |
| ClearCacheInvokedCount | 经过间隔时间后触发缓存清理的次数 |
| OCSPCertsCleanedUpCount | 经过间隔时间后清除的已缓存条目的数量 |
| NumOfCertsFoundInCache | 缓存中已执行的请求数量 |
| OCSPCacheCertsCount | 在 OCSP 缓存中查找到的证书数量 |