在ISE上配置证书续订

目录

简介

本文档介绍在思科身份服务引擎 (ISE) 上更新证书的最佳做法和主动程序， 它还检查如何设置警报和通知，以便管理员收到即将发生的事件（如证书过期）的警告。

> **注意**：本文档不用作证书的诊断指南。

先决条件

要求

Cisco 建议您了解以下主题：

- X509 证书
- 配置带证书的 Cisco ISE

使用的组件

"本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响。”

- Cisco ISE 3.0.0.458 版本
- 设备或 VMware

背景信息

ISE 管理员终会面临 ISE 证书到期的事实。如果您的ISE服务器具有过期的证书，除非您使用新的有效证书替换过期的证书，否则可能出现严重问题。

> **注意**：如果用于可扩展身份验证协议(EAP)的证书到期，所有身份验证都会失败，因为客户端不再信任ISE证书。如果ISE管理员证书过期，风险更大：管理员将无法再登录ISE，并且分布式部署可以停止运行和复制。

ISE管理员必须在旧证书到期前在ISE上安装新的有效证书。这种主动做法可防止或最大程度减少停机时间，避免对最终用户造成影响。新安装证书的时段开始后，您可以在新证书上启用EAP/管理员或任何其他角色。

您可以配置 ISE，以生成警报并通知管理员在旧证书到期之前安装新证书。

> **注意**：本文档将ISE管理员证书用作自签名证书以演示证书续订的影响，但不建议将此方法用于生产系统。最好为EAP角色和Admin角色使用CA证书。

配置

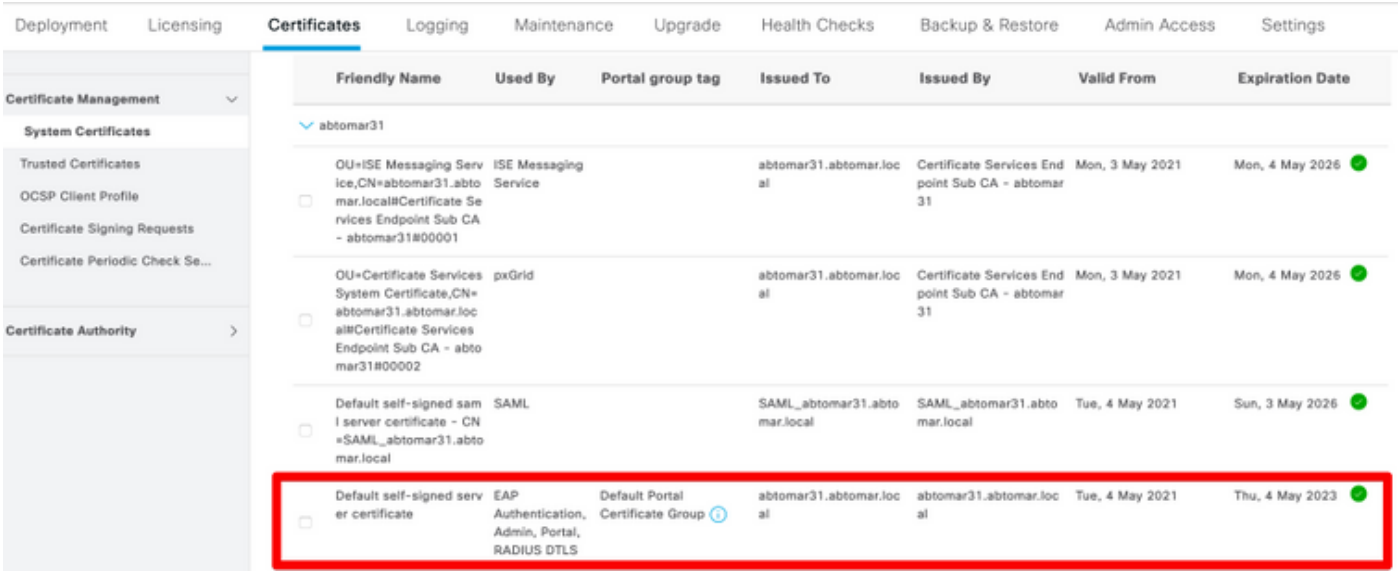
查看 ISE 自签名证书

安装 ISE 后，即可生成自签名证书。自签名证书用于管理访问、分布式部署中的通信 (HTTPS) 以及用户身份验证 (EAP)。 在实时系统中，请勿使用自签名证书，而是使用 CA 证书。

> **提示**：有关更多信息，请参阅《思科身份服务引擎硬件安装指南 3.0 版》的 Cisco ISE 证书管理部分。

ISE 证书必须为隐私增强邮件 (PEM) 格式或可辩别编码规则 (DER) 格式。

要查看初始自签名证书，请在 ISE GUI 中导航至**管理 > 系统 > 证书 > 系统证书**，如下图所示。



如果通过证书签名请求 (CSR) 在 ISE 上安装服务器证书，并更换管理员或 EAP 协议的证书，则自签名服务器证书仍然存在，但处于“未使用”状态。

> **警告**：更换管理员协议的证书时，需要重新启动 ISE 服务，这会导致停机数分钟。更换 EAP 协议的证书不会触发 ISE 服务重新启动，也不会导致停机。

确定何时更换证书

如果已安装的证书即将到期，应该到期后更新证书，还是到期前更换证书？必须在到期之前更改证书，以便有时间规划证书交换并管理交换导致的任何停机时间。

何时必须更改证书？新证书的开始日期应早于旧证书的到期日期。这两个日期之间的时间段即为更换窗口期。

> **警告**：如果启用管理员协议，则会导致 ISE 服务器上的服务重新启动，并且会停机数分钟。

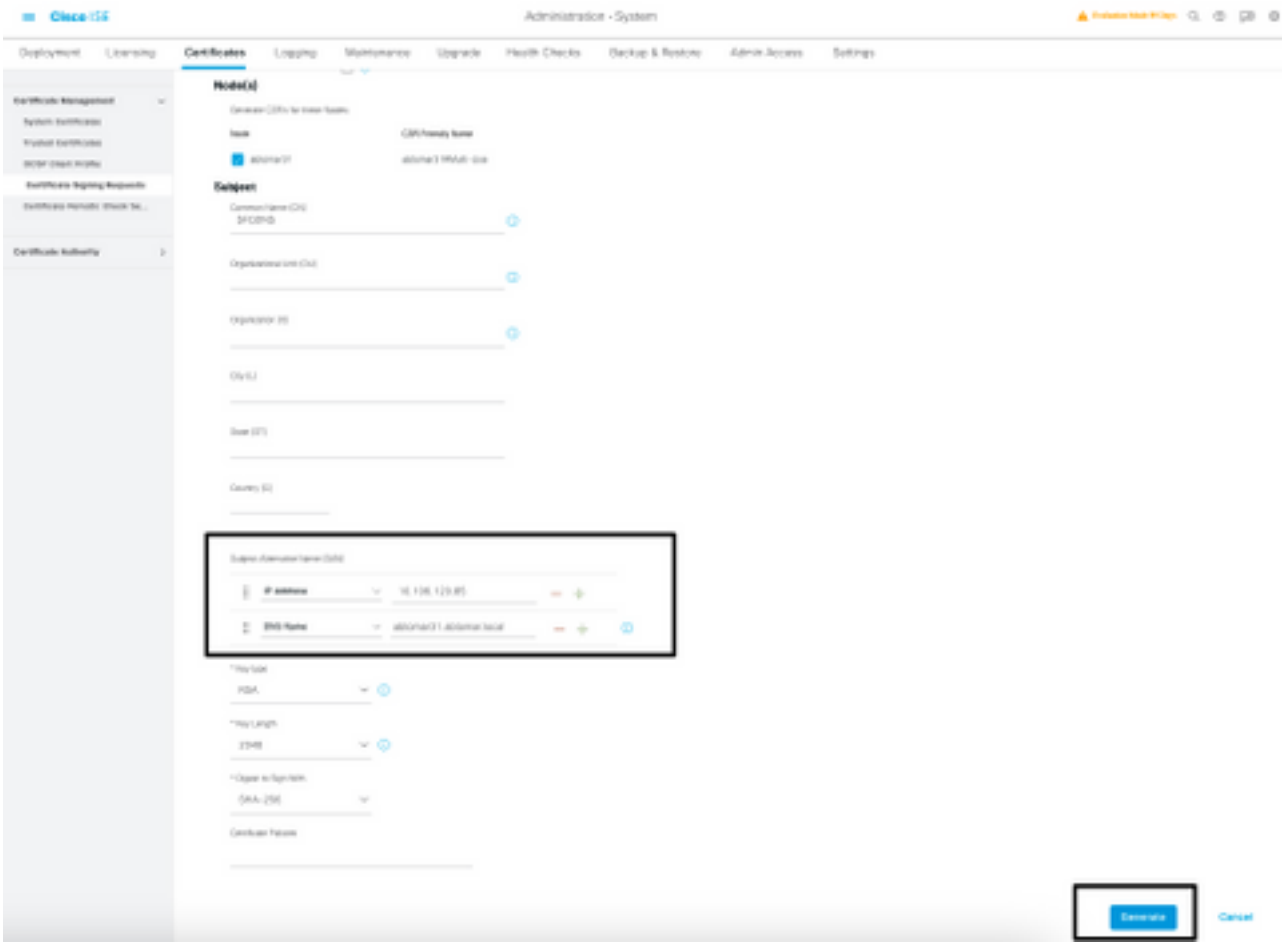
即将到期的证书信息如下图所示：

生成证书签名请求

通过 CSR 更新证书的流程如下：

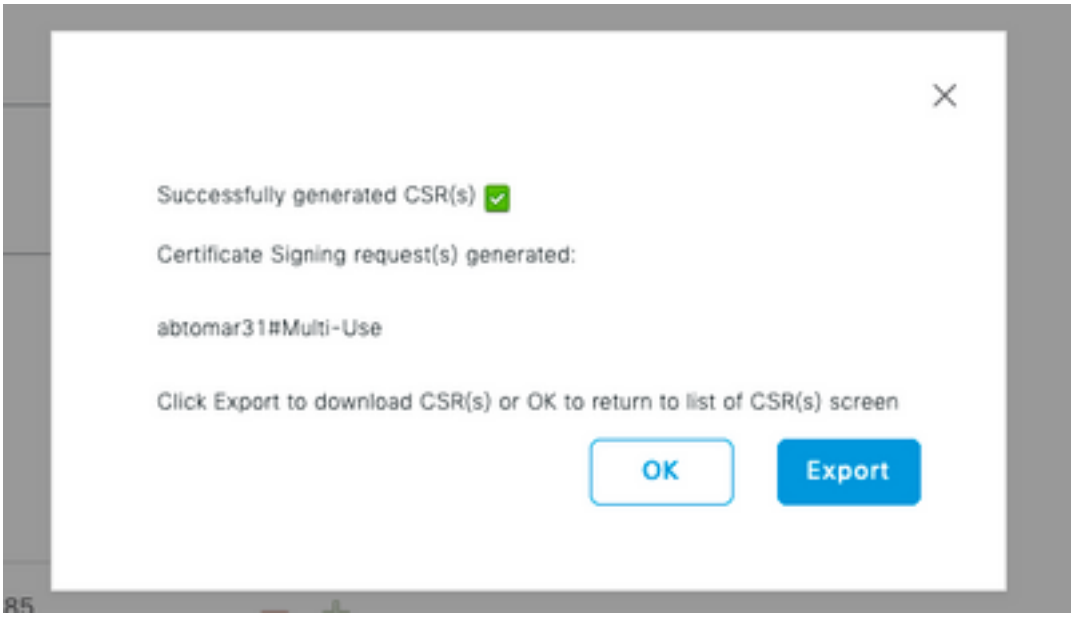
1. 在 ISE 控制台中，导航至**管理 > 系统 > 证书 > 证书签名请求**，然后点击**生成证书签名请求。**

2. 至少必须在**证书主题**文本字段中输入 CN = *ISEfqdn*，其中 *ISEfqdn* 是 ISE 的完全限定域名 (FQDN)。在“证书主题”中添加其他字段时请使用逗号隔开，例如“O（组织），OU（组织单位）或 C（国家/地区）”。

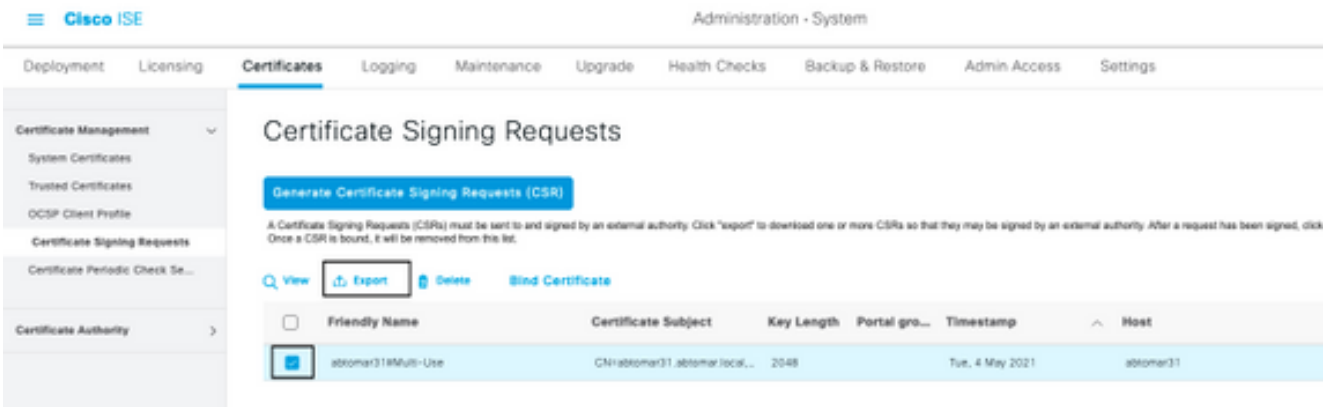


3. **主题备用名称 (SAN)** 文本字段中的一行必须重复 ISE FQDN。如果要使用备用名称或通配符证书，可以添加第二个 SAN 字段。

4. 点击**生成**，随即显示弹出窗口，指示 CSR 字段是否正确填写：



5. 要导出 CSR，请点击左侧面板中的**证书签名请求**，选择 CSR，然后点击**导出**。

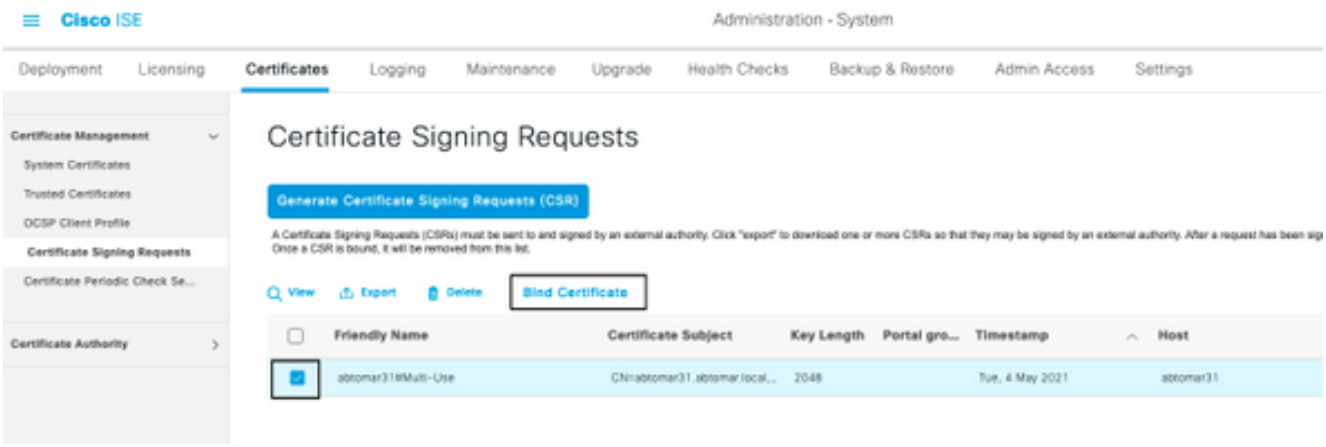


6. CSR存储在您的计算机上。请将其提交 CA 进行签名。

安装证书

从 CA 收到最终证书后，必须将其添加到 ISE：

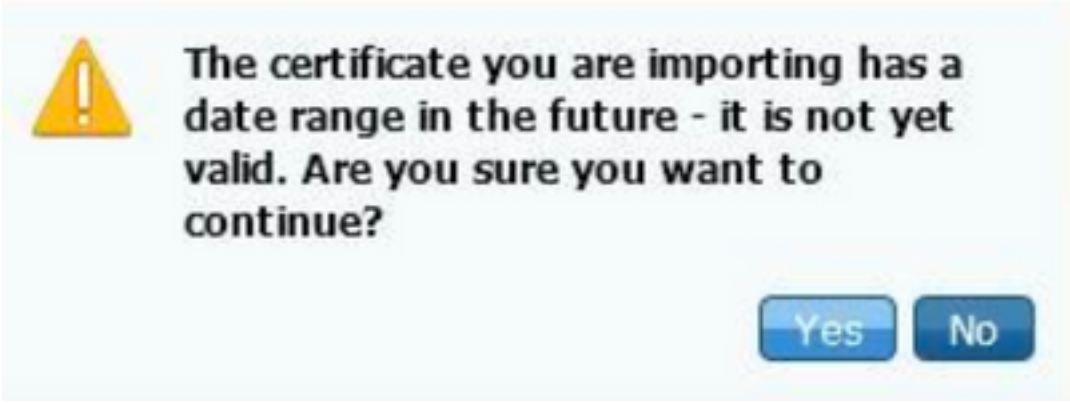
1. 在 ISE 控制台中，导航至**管理 > 系统 > 证书 > 证书签名请求**，然后选中 CSR 复选框并点击**绑定证书**。



2. 在**友好名称**文本字段中输入证书说明，请确保简单明了，然后点击“提交”。

   注意：此时请勿启用 EAP 或管理员协议。
3. 您会在“系统证书”下发现一个未使用的新证书，如下所示：

4. 由于新证书安装日期早于旧证书到期日期，因此您会看到一条报错消息，指出日期范围是在将来：



5. 单击 **Yes 继续操作。**证书现已安装，但未使用，以绿色突出显示。

注意：如果在分布式部署中使用自签名证书，则必须将主自签名证书安装到辅助 ISE 服务器的受信任证书库中。 同样，必须将辅助自签名证书安装到主 ISE 服务器的受信任证书库中。此操作允许 ISE 服务器相互进行身份验证。 没有此功能，部署可能会中断。如果通过第三方 CA 更新证书，请验证根证书链是否已发生变化，并相应地更新 ISE 中的受信任证书库。在这两种情况下，请确保ISE节点、终端控制系统和请求方能够验证根证书链。

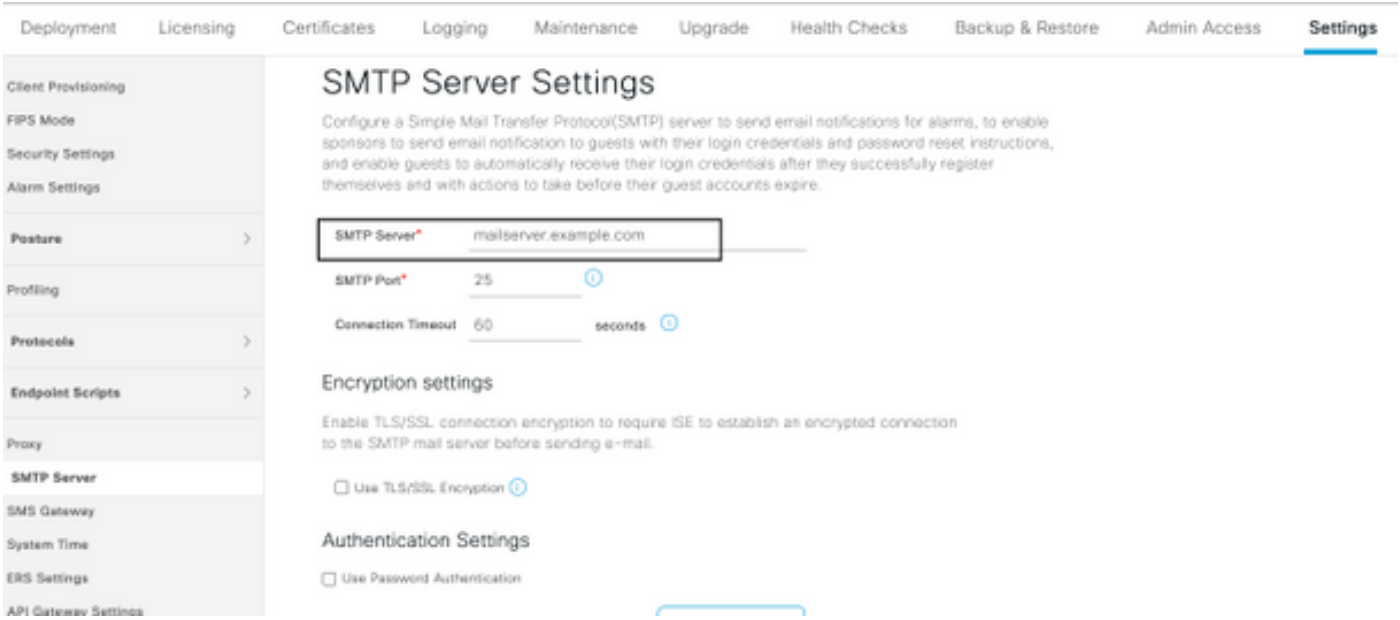
配置警报系统

距离本地证书到期日还有 90 天时，Cisco ISE 会向您发出通知。借助这类事先通知，您可有效避免证书到期情况，为更换证书制定计划，防止或最大程度减少停机时间。

系统以多种方式显示通知：

- “本地证书”页面会以彩色图标显示到期状态。
- Cisco ISE 系统诊断报告中会显示到期消息。
- 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。

请配置 ISE，以接收到期警报的电子邮件通知。在 ISE 控制台中，导航至**管理 > 系统 > 设置 > SMTP 服务器**，确定简单邮件传输协议 (SMTP) 服务器，并定义其他服务器设置，以针对警报发送电子邮件通知。

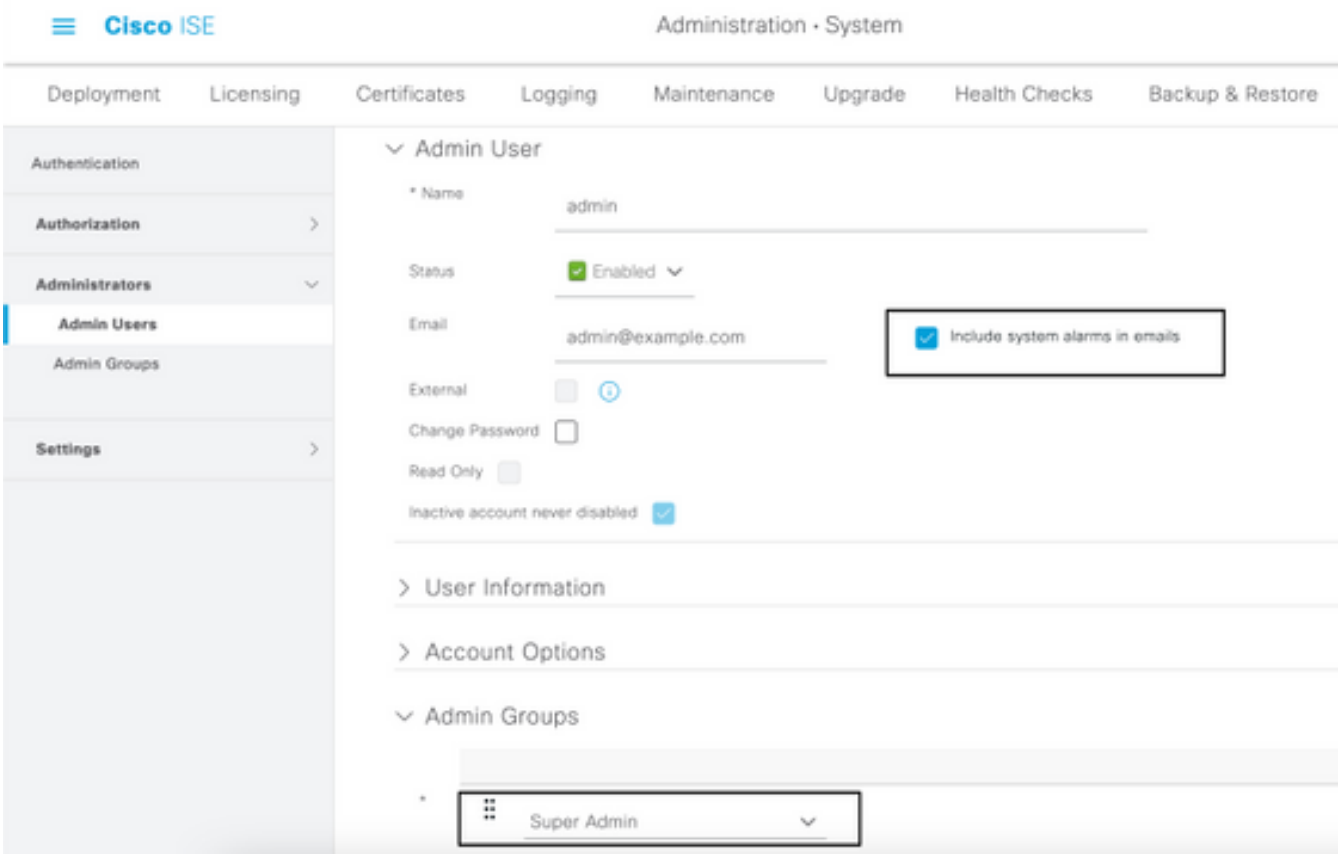


可以通过两种方式设置通知：

- 通知管理员时，使用“管理员访问权限”：

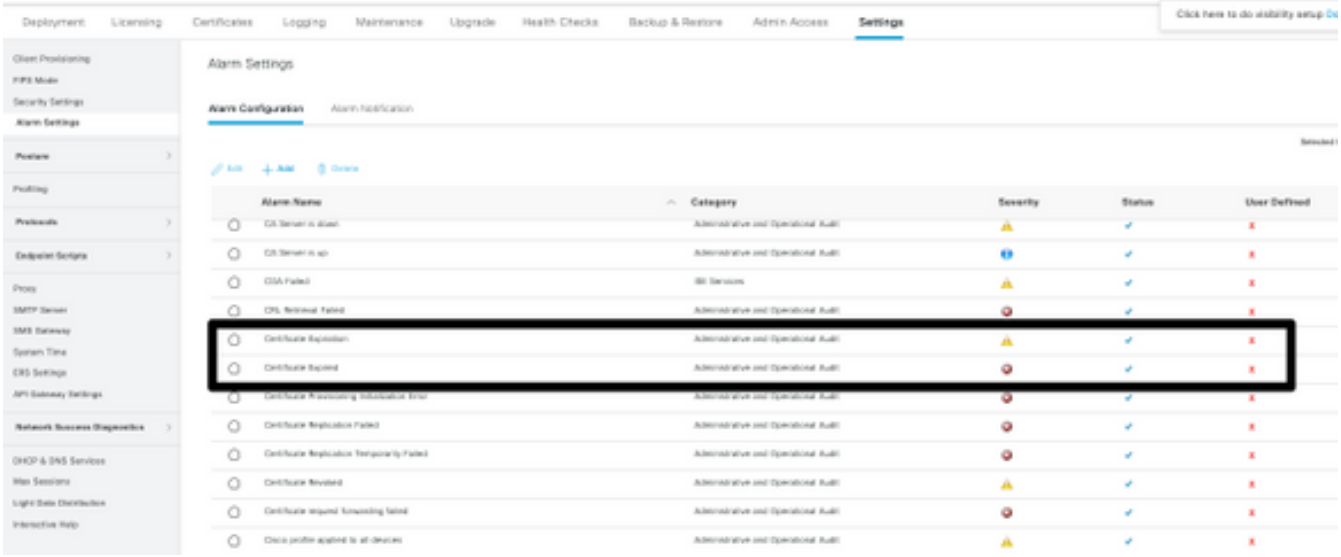
  导航至**管理 > 系统 >** 管理员访问权限 > 管理员 > 管理员用户。

  针对需要接收警报通知的管理员用户，选中**在电子邮件中添加系统警报**复选框。警报通知发件人的电子邮件地址硬编码为 ise@*hostname*。

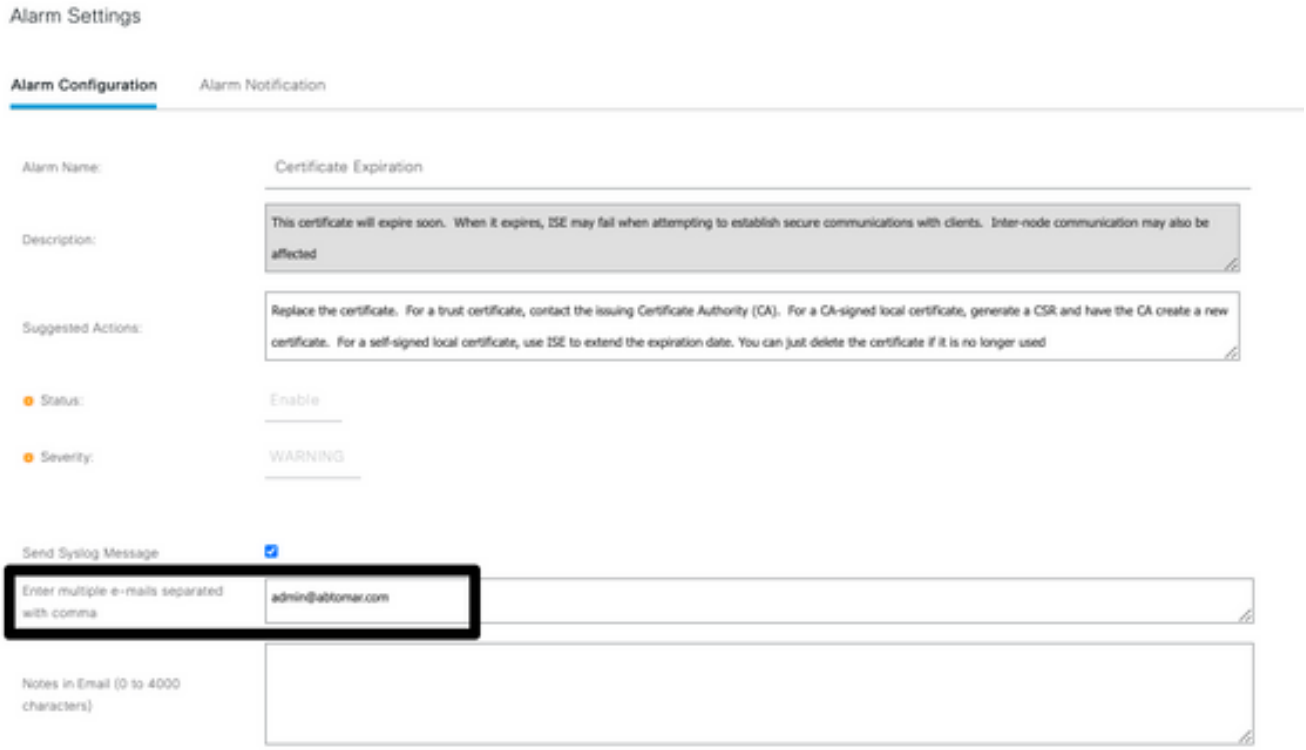


- 通知用户时，配置 ISE 警报设置：

  导航至**管理 > 系统 > 设置 > 警报设置 > 警报配置**，如下图所示。



注意：如果希望阻止某个类别的警报，请禁用该类别的状态。选择“证书到期”，然后点击**警报通知**，输入要向其发送通知的用户的电子邮件地址，并保存配置更改。更改最多可能需要15分钟才能生效。

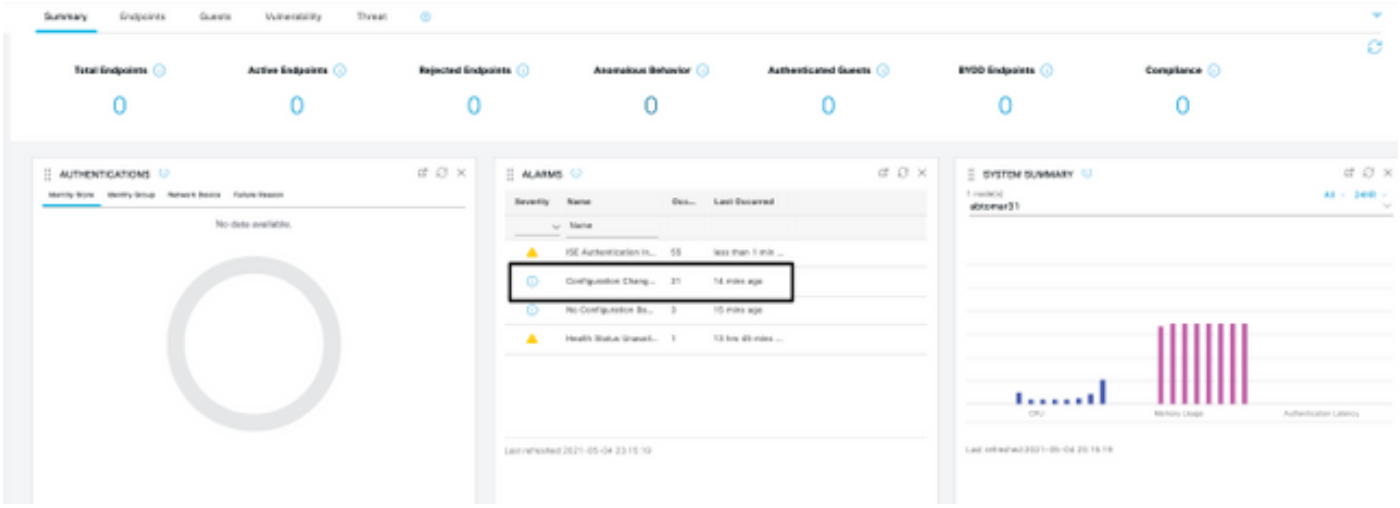


验证

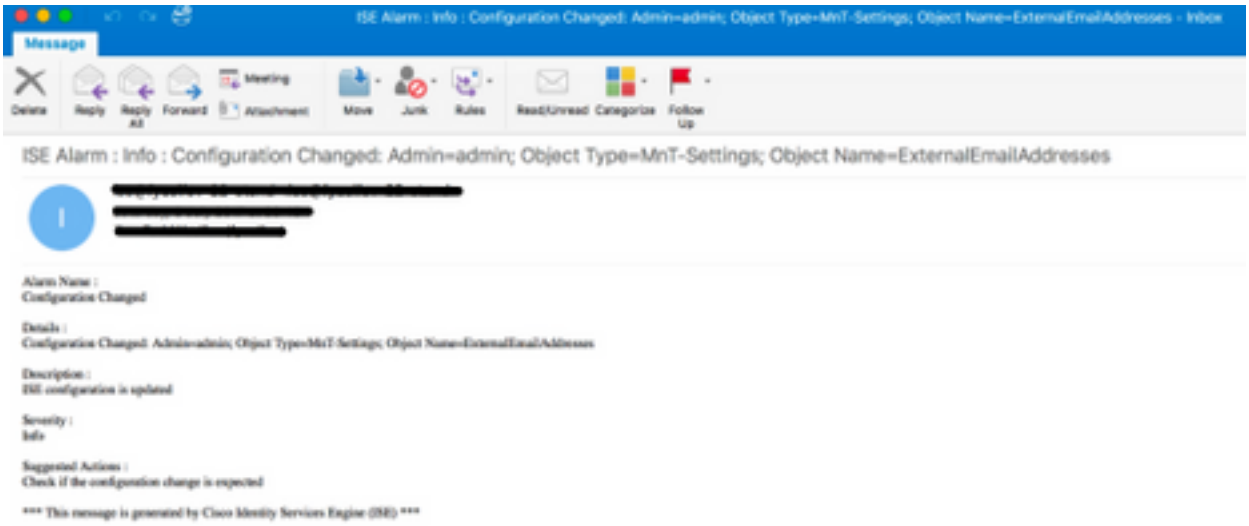
使用本部分可确认配置能否正常运行。

验证警报系统

验证警报系统是否正常工作。在本例中，更改配置会生成严重性级别为“信息”的警报（“信息”警报严重性级别最低，而证书到期会生成“警告”警报，其严重性级别更高）。



ISE 会发送如下所示的电子邮件警报：

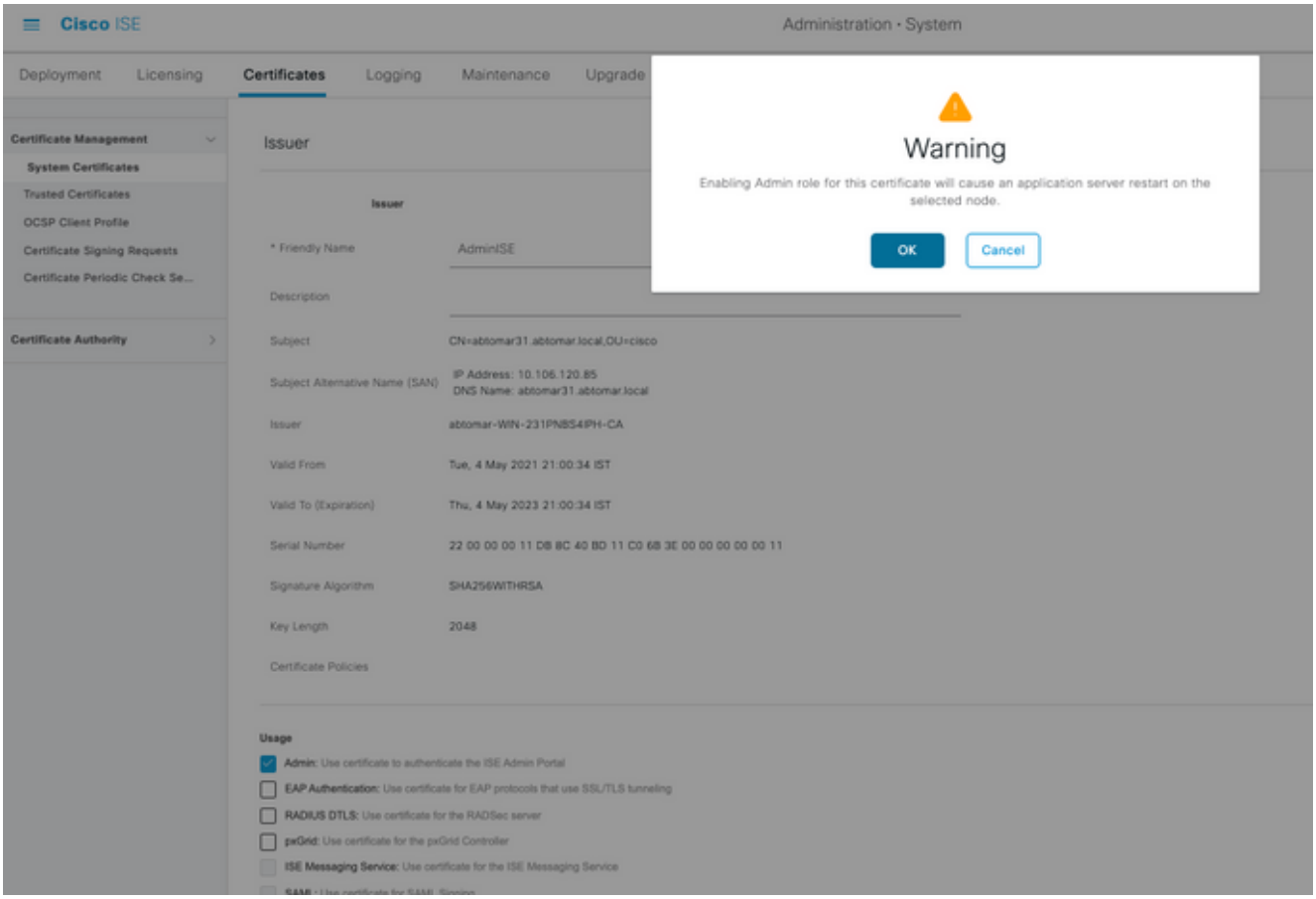


验证证书更换

此过程介绍如何验证证书是否正确安装，以及如何更改EAP和/或管理员角色：

1. 在 ISE 控制台中，导航至**管理 > 证书 > 系统证书**，然后选择新证书以查看详细信息。

   警告：如果启用“管理员使用情况”，则 ISE 服务会重新启动，这会导致服务器停机。



2. 要验证 ISE 服务器上的证书状态，请在 CLI 中输入以下命令：

```
CLI:> show application status ise
```

3. 所有服务都处于活动状态后，即可尝试以管理员身份登录。

4. 对于分布式部署方案，请导航到**管理>系统>部署。**验证节点是否显示绿色图标。将光标置于图标上以验证图例显示“已连接”。

5. 检查最终用户身份验证是否成功。为此，请导航到**操作> RADIUS >实时日志。** 您可以找到特定的身份验证尝试，并验证这些尝试是否已成功进行身份验证。

验证证书

如果要通过外部方式检查证书，可以使用嵌入式 Microsoft Windows 工具或 OpenSSL 工具包。

OpenSSL 是安全套接字层 (SSL) 协议的开源实现。如果证书使用您自己的专用 CA，则必须将根 CA 证书放在本地计算机上，并使用 OpenSSL 选项 *-CApath*。如果有中间 CA，必须将其置于同一目录中。

要获取证书的一般信息并对其进行验证，请使用：

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

使用OpenSSL工具包转换证书也非常有用：

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

故障排除

当前没有可用于此配置的特定诊断信息。

结论

由于可以在激活 ISE 之前在其上安装新证书，因此思科建议您在旧证书到期之前安装新证书。您可以利用旧证书到期日期与新证书开始日期之间的这段重叠时间，更新证书并针对新证书的安装制定计划，以尽量减少或完全避免停机时间。新证书生效后，请启用 EAP 和/或管理员协议。请注意，如果启用“管理员使用情况”，则服务会重新启动。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。