在思科身份服务引擎配置指南的证书续订

目录

简介

本文描述最佳实践和积极的步骤更新在思科身份服务引擎(ISE)的证书。它也查看如何设置报警和通知，因此管理员被警告即将举行的活动例如证书到期。

> **注意**：本文没有打算是证书的一故障排除指南。

先决条件

要求

Cisco 建议您了解以下主题：

- X509证书
- 一个思科ISE的配置与证书的

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本1.2.0.899
- 设备或VMware

背景信息

作为ISE管理员，您最终将遇到事实ISE证书超时。如果您的ISE服务器有一个过期的证书，严重问题也许出现，除非用新替换过期的证书，有效证书。

> **注意**：如果使用可扩展的认证协议(EAP)的证书超时，所有认证也许发生故障，因为客户端不再委托ISE证书。如果HTTPS协议证书超时，风险是更加极大的：管理员也许不能再登陆到ISE，并且分布式部署也许停止作用和复制。

在本例中， ISE有从在一个月将超时的Certificate Authority (CA)服务器的一预装证书。在旧有证书超时前， ISE管理员应该安装新，在ISE的有效证书。此预防性的方法防止或最小化停机时间并且避免在您的最终用户的一影响。一旦预装证书的时间最近开始，您能启用在新证书的EAP和HTTPS协议。

您能配置ISE，以便生成报警并且通知管理员安装新建的证书，在旧有证书超时前。

> **注意**：本文以自签名证书使用HTTPS为了展示证书续订影响，但是此方法没有为一个实际系统推荐。使用CA证书EAP和HTTPS协议最好的。

配置

查看ISE自签名证书

当ISE安装时，生成自签名证书。自签名证书使用管理访问和在分布式部署(HTTPS)内的通信以及用户认证(EAP)。在一个实际系统中，请使用一个CA证书而不是自签名证书。

> **提示**：参考在思科思科身份服务引擎硬件安装指南的ISE部分的证书管理，版本1.2其他信息。

ISE证书的格式必须是增强加密邮件(PEM)或著名的编码规则(DER)。

为了查看最初的自签名证书，导航对**Administration > System>证书>本地证书**在ISE控制台：

如果通过证书签名请求(CSR)安装在ISE的一服务器证书并且更改HTTPS或EAP协议的证书，自己

签署的服务器证书存在，但是不再使用。

> **警告**：对于HTTPS协议更改， ISE服务的重新启动要求，创建几分钟停机时间。EAP协议更改不触发ISE服务的重新启动，并且不导致停机时间。

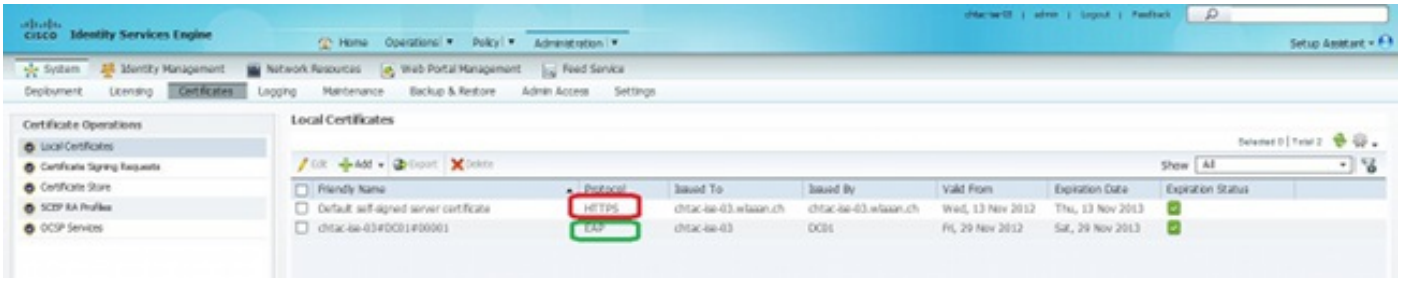
什么时候确定更改证书

假设，预装证书很快超时。让证书超时，在您更新它前最好的或在有效期前更改证书？您应该在有效期前更改证书，以便您有时间计划证书交换和管理交换造成的所有停机时间。

什么时候应该更改证书？获取与先于旧有证书的有效期的起始日期的一新证书。在那两个日期之间的时间是更改窗口。

> **警告**：如果启用HTTPS，导致在ISE服务器的服务重新启动，并且您体验几分钟停机时间。

此镜像在29十一月2013表示由CA发出的证书的信息并且超时：



生成证书签名请求

此步骤描述如何通过CSR更新证书：

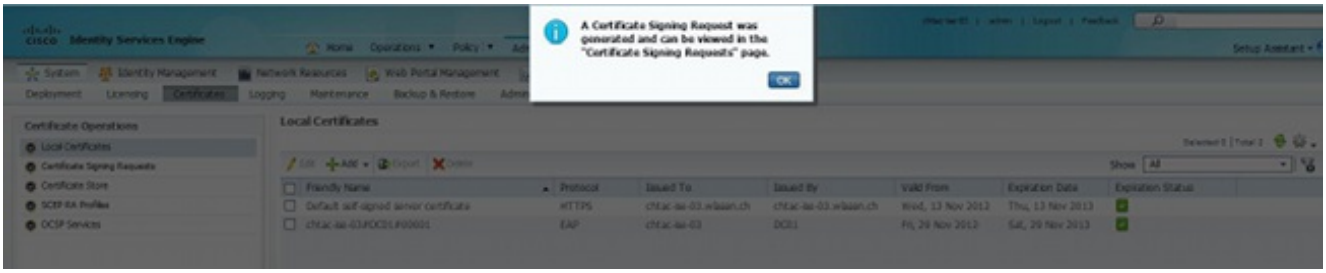
1. 在ISE控制台中，请导航添加**>生成证书签名请求**。

2. 您必须在**证书主题**文本字段输入的最低的信息是CN=ISEfqdn， *ISEfqdn*是ISE的完全合格的域名(FQDN)。添加另外的字段例如O (组织)， OU (组织单位)，或者C (国家)在与使用的证书主题逗号：

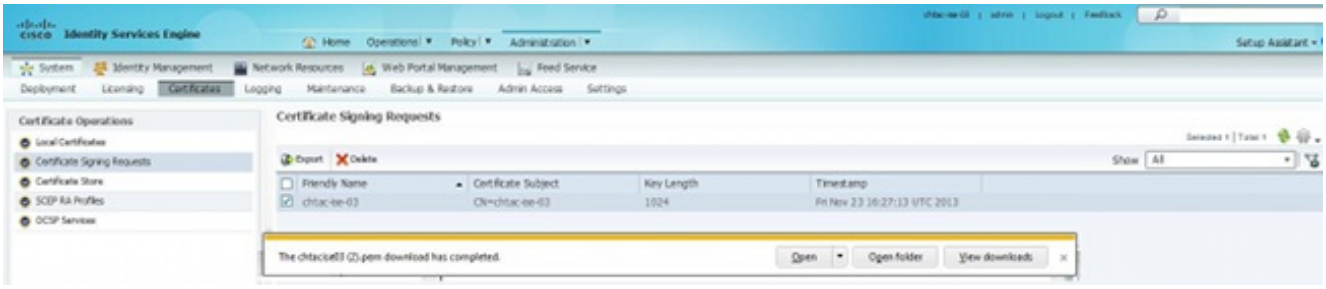
3. 其中一条**附属的替代方案名称(SAN)**文本字段线路必须重复ISE FQDN。如果要使用代替名称

或通配符证书，您能添加秒钟SAN字段。

4. 弹出窗口指示CSR字段是否正确地完成：



5. 为了导出CSR，请点击**证书签名请求**在左面板中，选择您的CSR，并且点击**出口**：

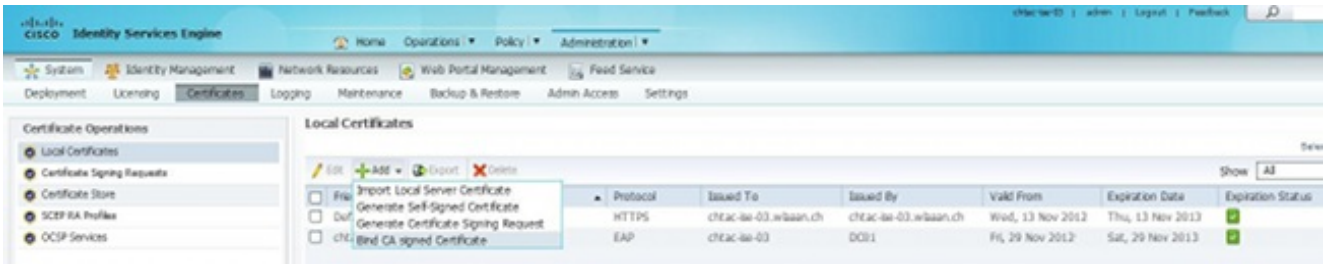


6. CSR在您的计算机保存。提交它对您的签名的CA。

安装证书

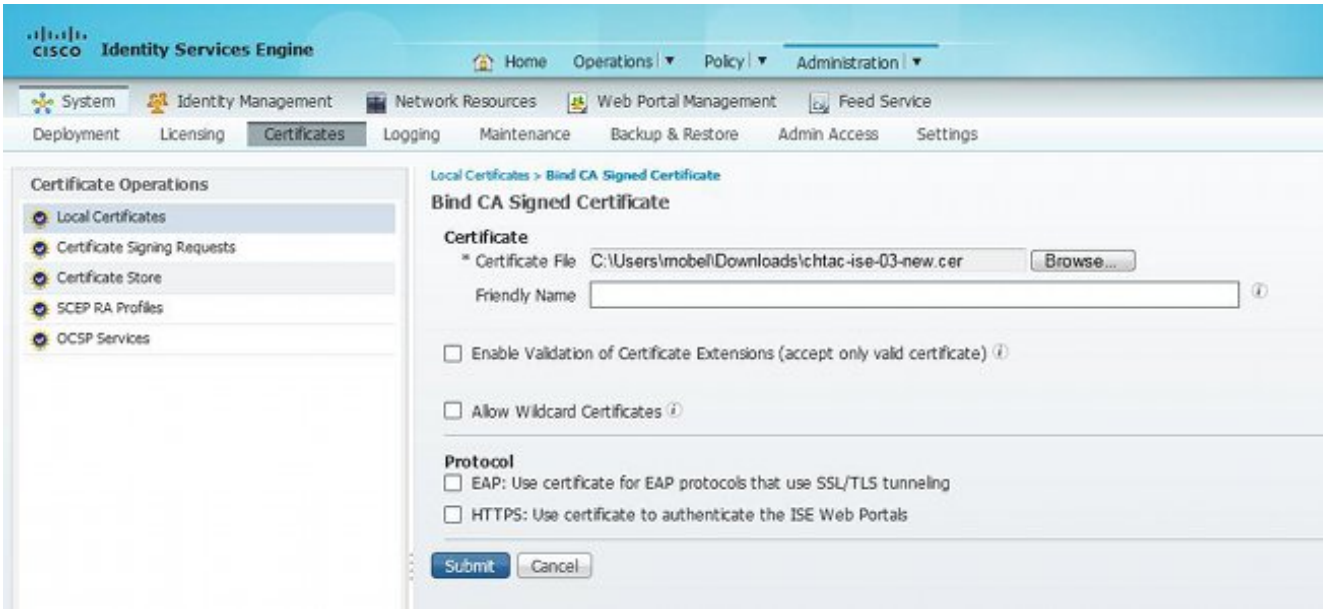
一旦接收从您的CA的最终证书，您必须添加证书到ISE ：

1. 在ISE控制台中，请点击**本地证书**在左面板中，然后单击**添加**并且**绑定CA签名证书**：

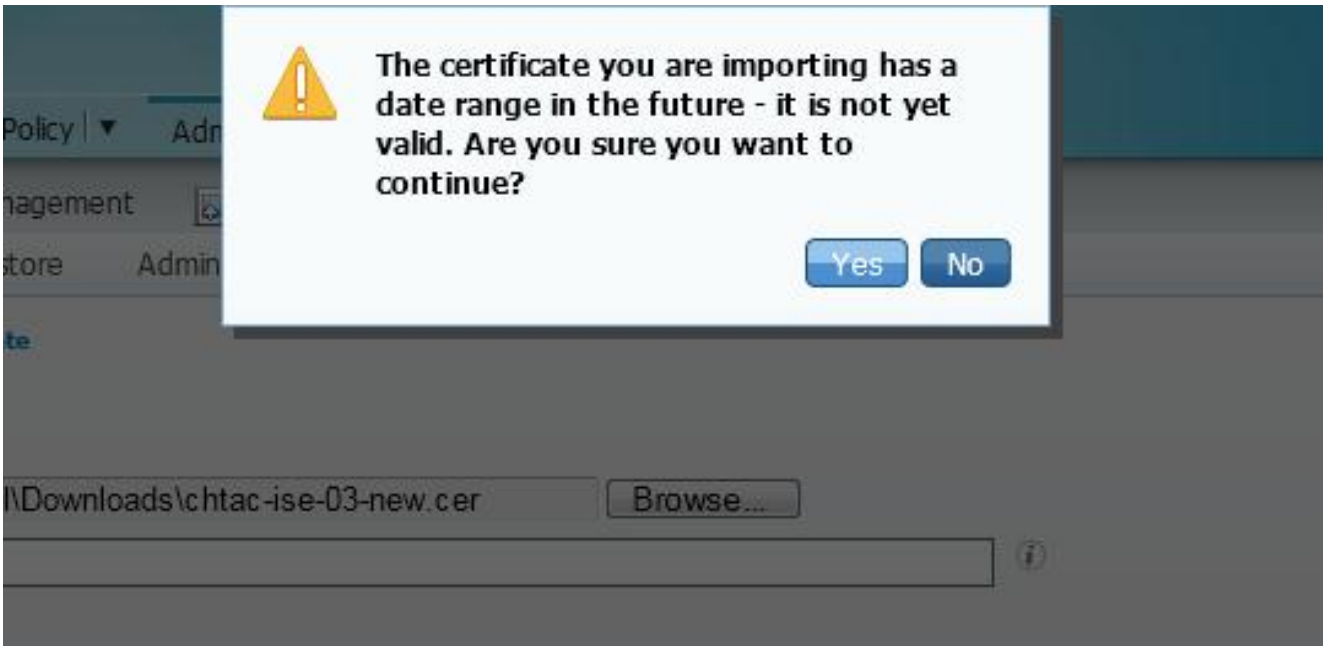


2. 在**友好名称**文本字段输入证书的一简单，清楚说明：

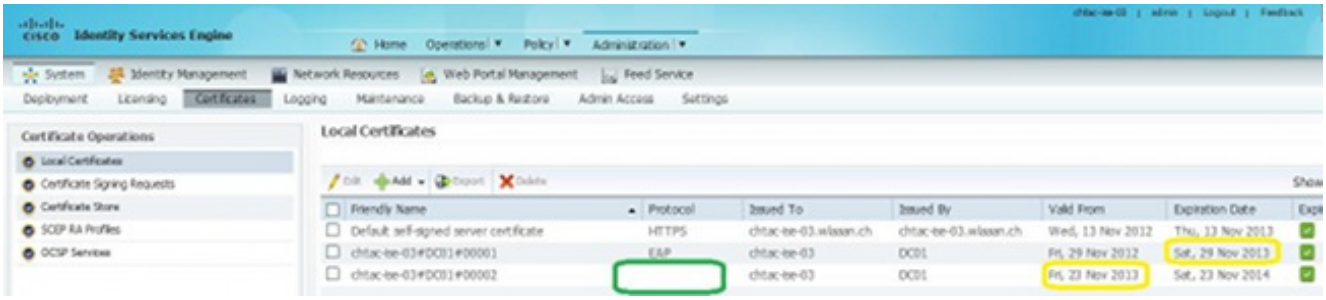
注意：请勿此时启用EAP或HTTPS协议。



3. 由于您安装新证书，在旧有一个超时前，您看到在将来报告日期范围的错误(在本例中的23十一月2013)。



4. 单击 **Yes** 继续操作。证书当前安装，但是不在使用中，如突出显示以绿色。在有效期和有效日期之间的重叠用黄色表示：



注意：如果在一分布式部署使用自签名证书，必须安装主要的自签名证书到附属ISE服务器的信任证书存储。 同样，必须安装附属自签名证书到主要的ISE服务器的信任证书存储。这允许

ISE服务器相互互相验证。 没有此，部署也许中断。如果更新从第三方CA的证书，请验证根证明一系列是否更改并且相应地更新ISE的信任证书存储。在两种情况下，请保证ISE节点、终端操作系统和恳求者能验证根证明一系列。

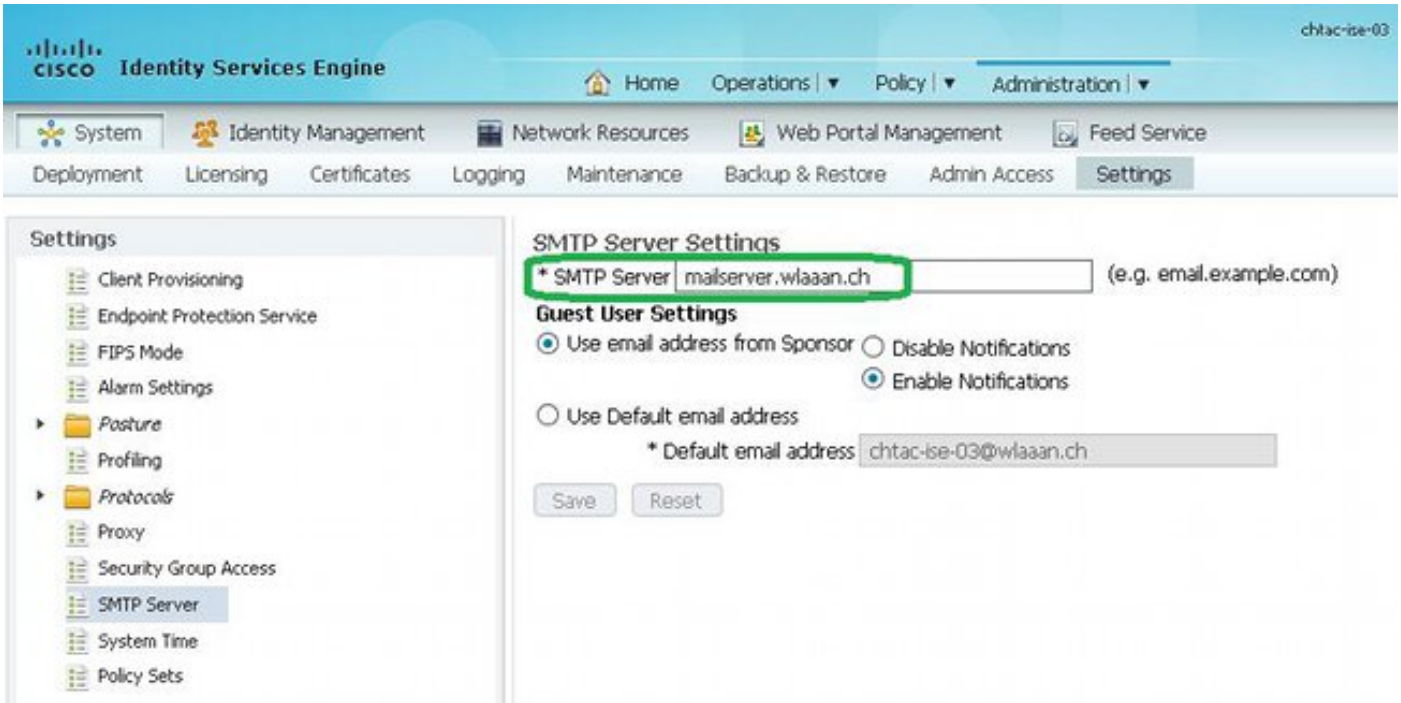
配置警报系统

当一本地证书的有效期是在90天内时，思科ISE通知您。这样预先通知帮助您避免过期的证书，计划证书更改和防止或者最小化停机时间。

通知出现用几个方式：

- 颜色有效期状态图标在本地证书页出现。
- 到期通知在思科ISE系统诊断报告出现。
- 有效期报警生成在90天和60天，然后日报在有效期前的最终30天。

配置有效期报警电子邮件通知的ISE。在ISE控制台中，请导航到**管理>System >设置> SMTP服务器**，识别简单邮件传输协议(SMTP)服务器，并且定义其他服务器设置，以便电子邮件通知为报警发送：

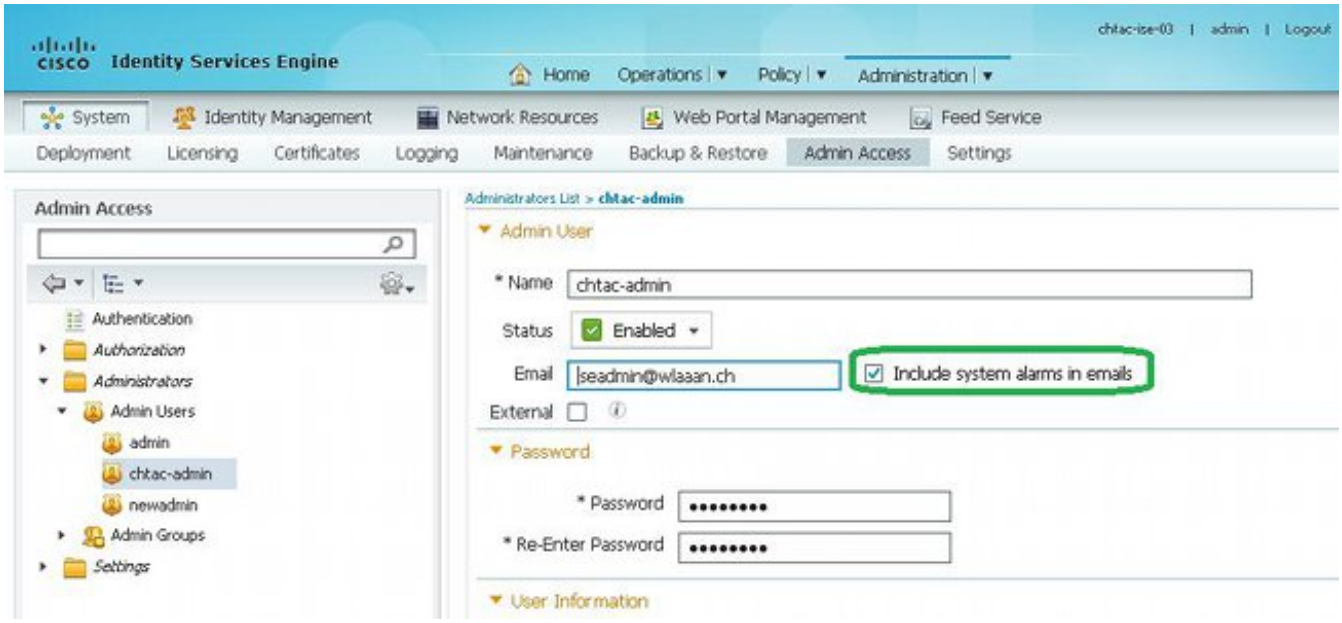


有两种方式您能设置通知：

- 请使用Admin访问为了通知管理员：

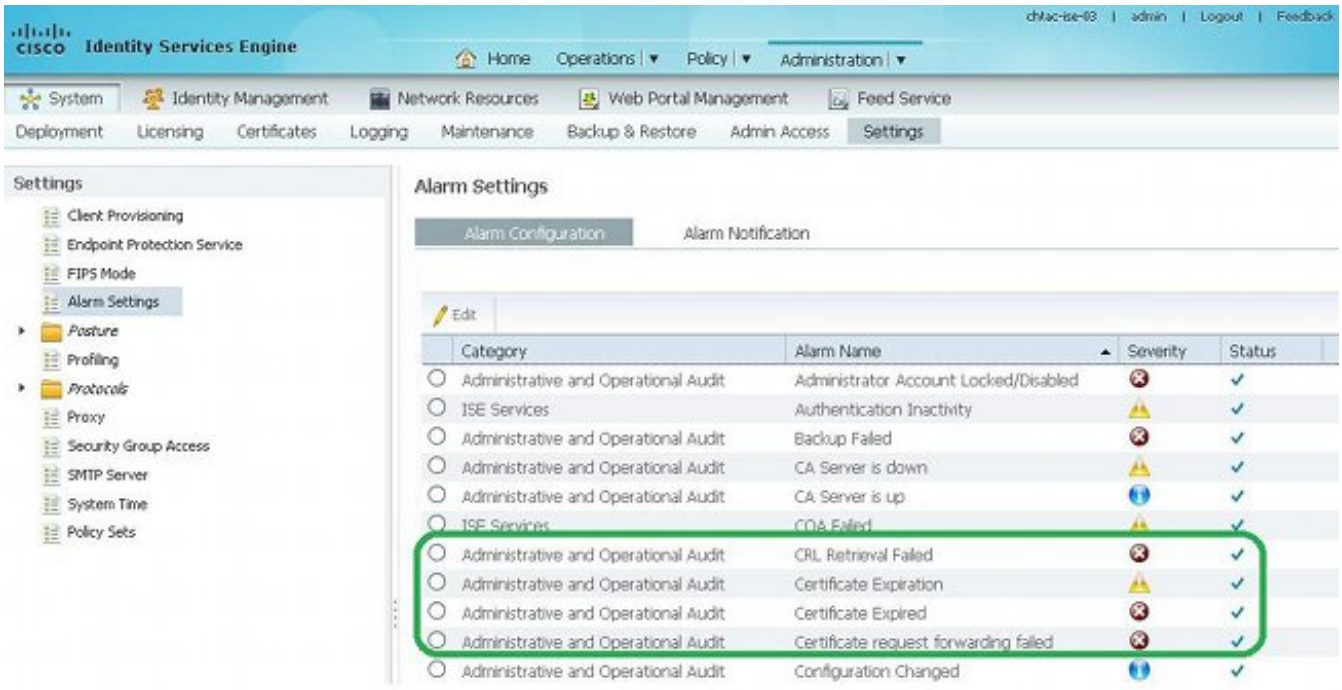
  导航给**管理>System > Admin访问>管理员>管理员用户**。

  检查**在电子邮件**复选框的**包括系统警报**需要接收告警通知的管理员用户。告警通知的发送方的电子邮件地址硬编码作为ise @*主机名*。

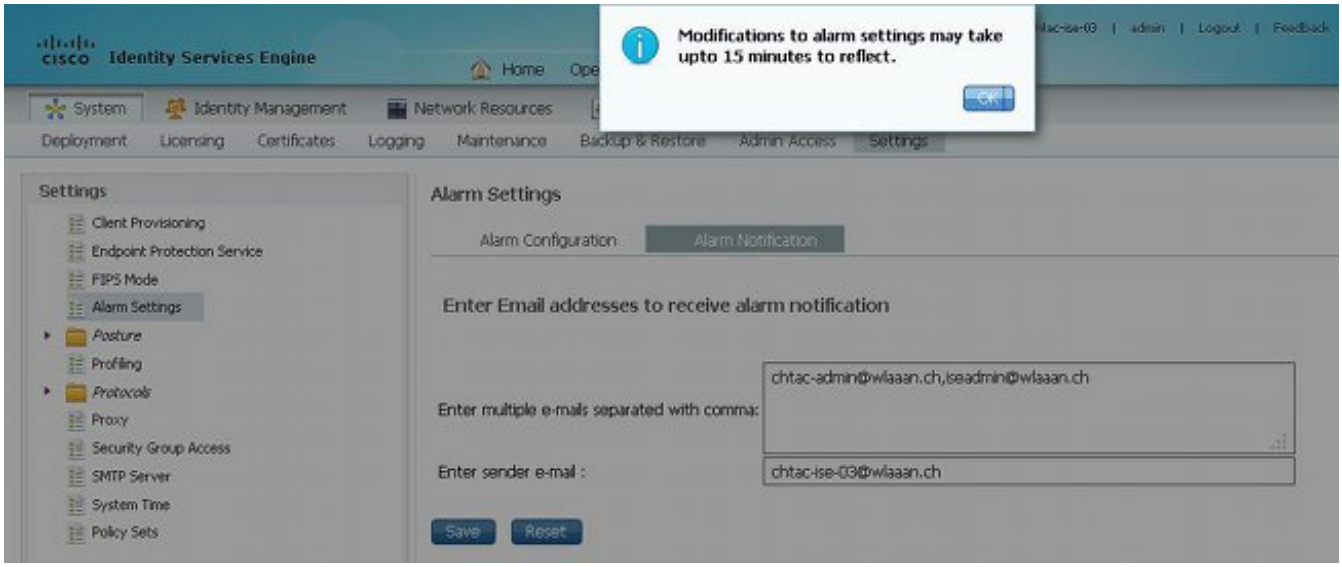


- 配置ISE告警设置为了通知用户：

导航对**管理>System >设置>告警设置>报警配置**：



注意：如果希望防止报警该类别，请禁用类别的状态。点击**告警通知**，输入用户的电子邮件地址将通知，并且保存配置更改。15分钟，在他们是活跃的前，更改也许占去对。

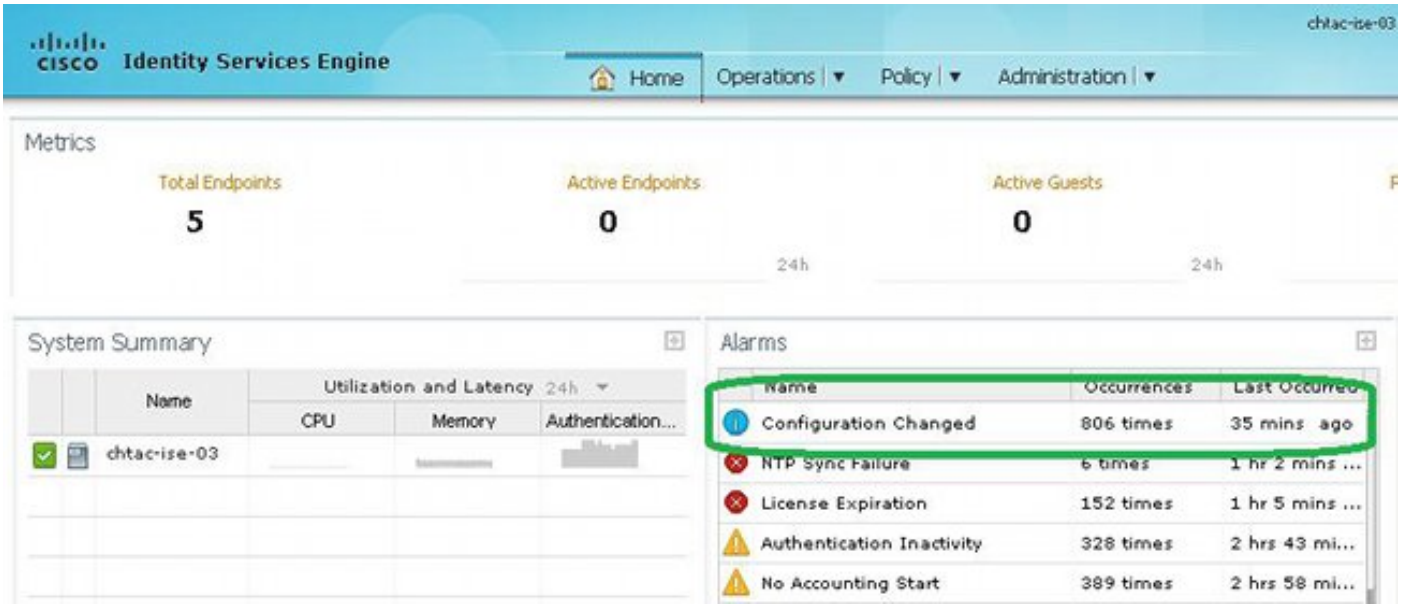


验证

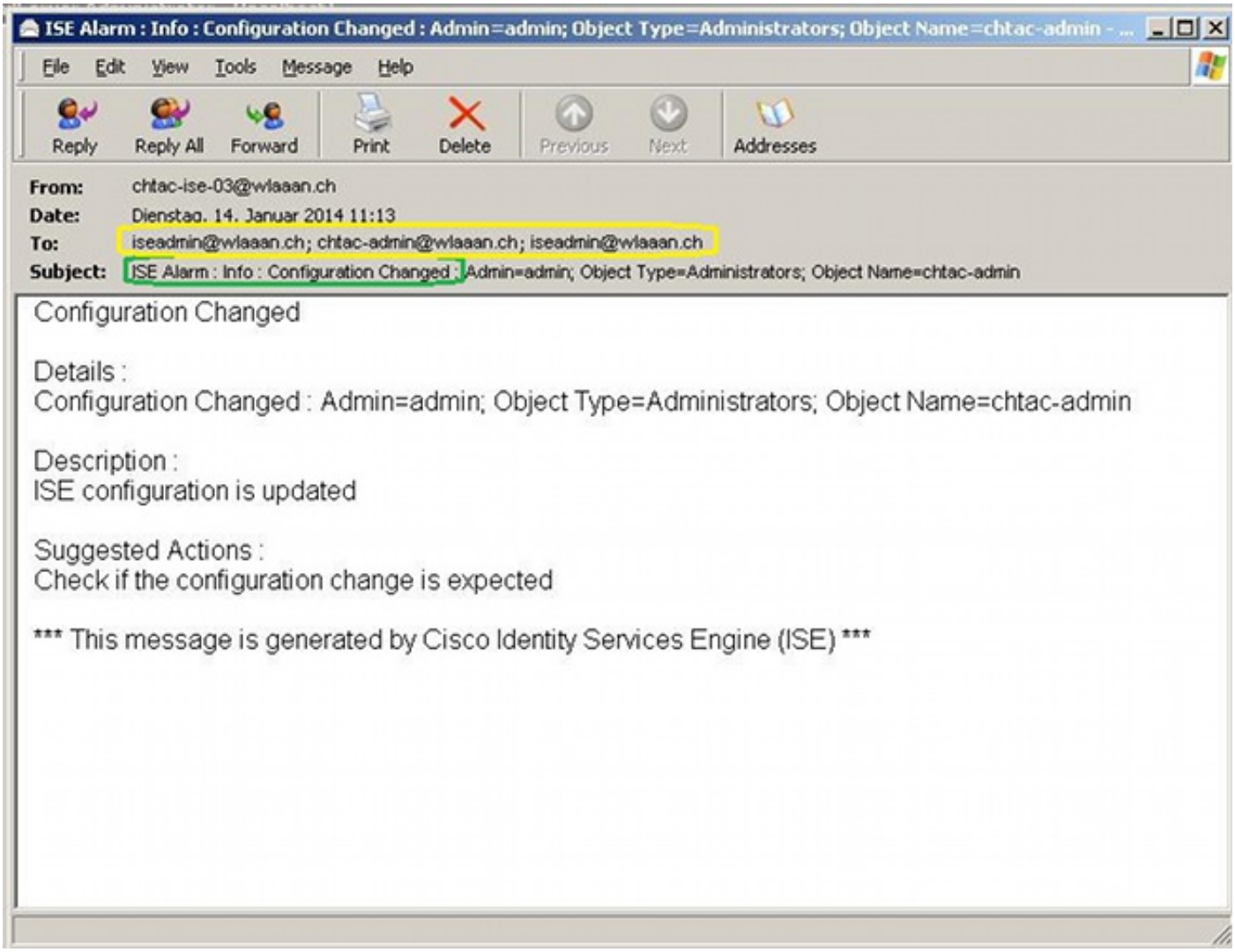
使用本部分可确认配置能否正常运行。

验证警报系统

验证警报系统正确地运转。在本例中，配置更改生成与严重级别的一警报信息。(信息报警是最低的严重性，而证书到期生成高严重程度级亚里桑。)



这是由ISE发送电子邮件报警的示例：



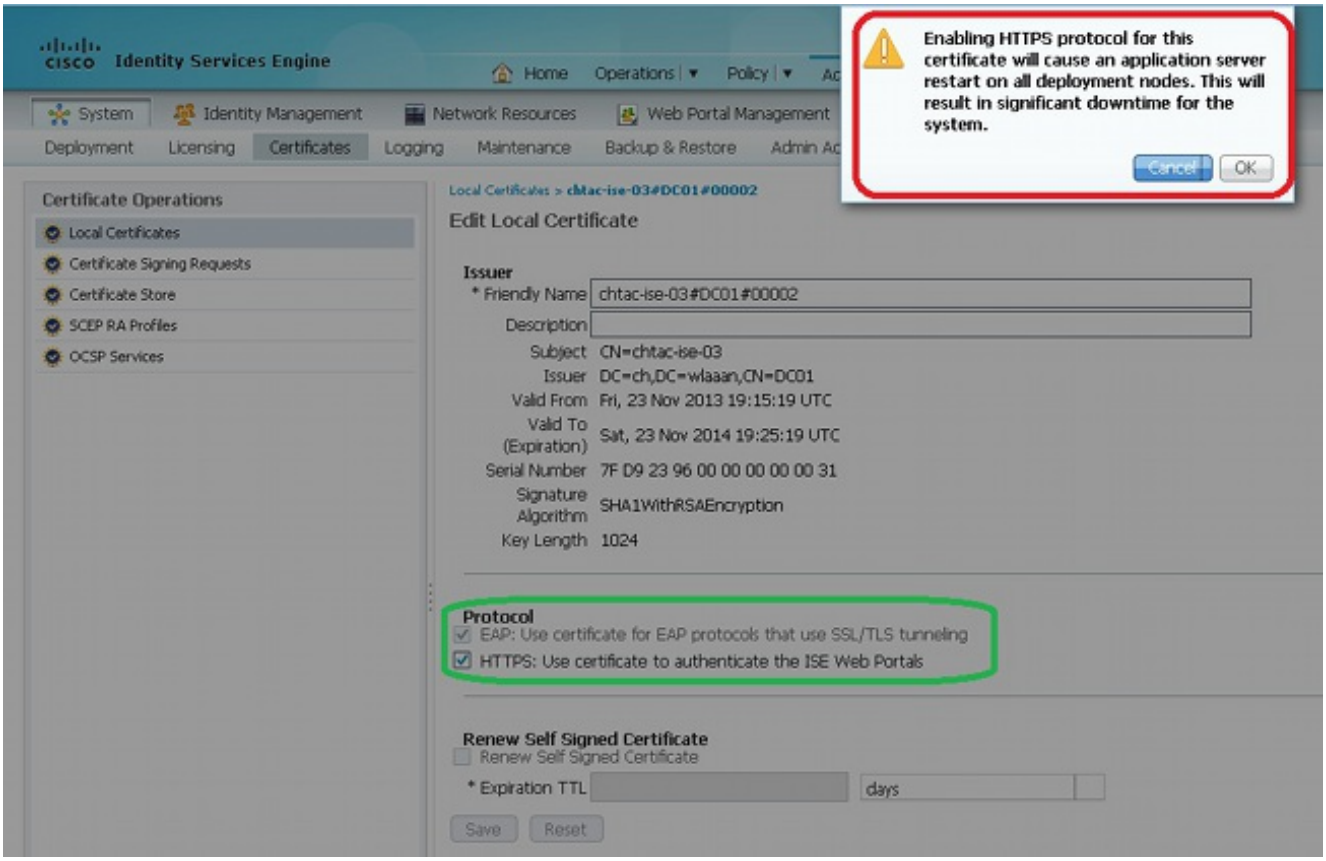
注意：在本例中， ISE两次传送电子邮件警报信息对iseadmin@wlaaan.ch，如用黄色表示。此电子邮件地址用解释的两个方法设置接收通知配置警报系统。

验证证书崔凡吉莱

此步骤描述如何验证证书正确地安装和如何更改EAP和HTTPS的协议：

1. 在ISE控制台上，请导航对**Administration >证书>本地证书**，并且选择新证书为了查看详细信息。

   警告：如果启用HTTPS协议， ISE服务重新启动，导致服务器停机时间。



在本例中，假设， HTTPS重新启动ISE服务。

2. 为了验证在ISE服务器的证书状态，请输入此命令到CLI ：

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

3. 一旦所有服务是活跃的，请尝试登陆作为管理员。

4. 对于一个分布式部署方案，请导航对在ISE控制台的**管理>System >部署> Status节点**，并且验证Status节点。

5. 检查最终用户验证是成功的。在ISE控制台上，请导航对**操作>认证**，并且查看Protected Extensible Authentication Protocol (PEAP) /EAP传输层安全(TLS)验证的证书。

验证证书

如果要检查证书外部，您能使用嵌入式Microsoft Windows工具或Openssl工具套件。

Openssl是安全套接字协议层(SSL)协议的开放原始码的软体实施。如果证书使用您自己的私有CA，您在本地设备必须放置您的根CA证书和使用Openssl选项- *CApath*。如果有中间CA，您必须放置它到同一个目录。

为了得到关于证书的一般信息和验证它，使用：

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

转换与Openssl工具套件的证书也许也是有用的：

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

故障排除

目前没有针对此配置的故障排除信息。

结论

由于您能安装在ISE的一新证书，在是活跃的前，思科建议您安装新证书，在旧有证书超时前。在旧有证书到期到期日和新证书起始日期之间的此重叠期限提供您时刻更新证书和计划他们的安装用很少或不停机时间。一旦新证书输入其有效日期范围，请启用EAP和HTTPS协议。切记，如果启用HTTPS，有服务重新启动。