在思科身份服务引擎配置指南的认证续订

Contents

Introduction

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

> **Note**:本文没有打算是证书的一故障排除指南。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- X509证书
- Cisco ISE的配置与证书的

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE Release 1.2.0.899
- 工具或VMware

背景信息

作为ISE管理员，您最终将遇到事实ISE证书到期。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。

> **Note**:如果使用可扩展的认证协议(EAP)的认证到期，所有认证也许发生故障，因为客户端不再委托ISE认证。如果HTTPS协议认证到期，风险是更加极大的：管理员也许不能再登陆到ISE，并且被分配的配置也许停止作用和复制。

在本例中， ISE有从在一个月将到期的Certificate Authority (CA)服务器的一预装证书。在老认证到期前， ISE管理员应该在ISE上安装新，有效证书。此预防性的方法防止或使停工期减到最小并且避免对您的终端用户的影响。一旦预装证书的时间最近开始，您能enable (event)关于新证书的EAP和HTTPS协议。

您能配置ISE，以便生成警报并且通知管理员安装新的证书，在老证书到期前。

> **Note**:本文以自签证书使用HTTPS为了展示认证续订的影响，但是此方法为一个实际系统不是推荐的。使用CA证书EAP和HTTPS协议最好的。

Configure

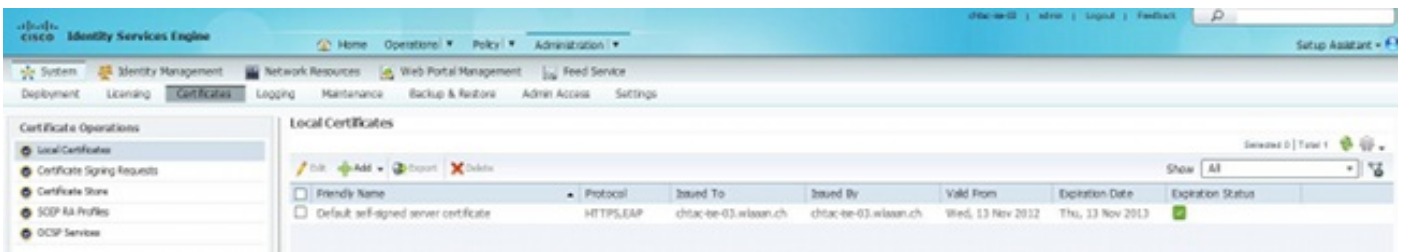
查看ISE自署名的认证

当安装时ISE，生成一自签证书。自签证书使用管理访问和在被分配的配置(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证书而不是自签证书。

> **提示**：请参见在Cisco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认证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证书，连接对**Administration > System>证书>**在ISE控制台的**本地证书**：



如果在ISE上安装一个服务器证明通过认证署名请求(CSR)并且更改HTTPS或EAP协议的认证，自已签署的服务器证明存在，但是不再使用。

> **警告：**对于HTTPS协议更改， ISE服务的重新启动需要，创建几分钟停工期。EAP协议更改不触发ISE服务的重新启动，并且不导致停工期。

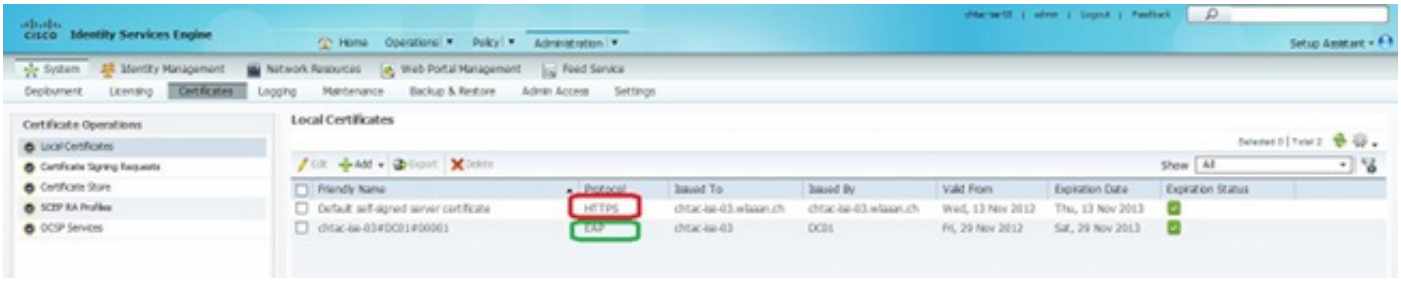
什么时候确定更改认证

假设，预装证书很快到期。让认证到期，在您更新它前最好的或在到期前更改认证？您应该在到期前更改认证，以便您有时间计划认证交换和管理交换造成的所有停工期。

什么时候应该更改认证？获得与先于老认证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enable (event) HTTPS，它导致在ISE服务器的服务重新启动和您请体验几分钟停工期。

此镜像表示CA发行的认证信息并且到期2013年11月29日：



生成认证署名请求

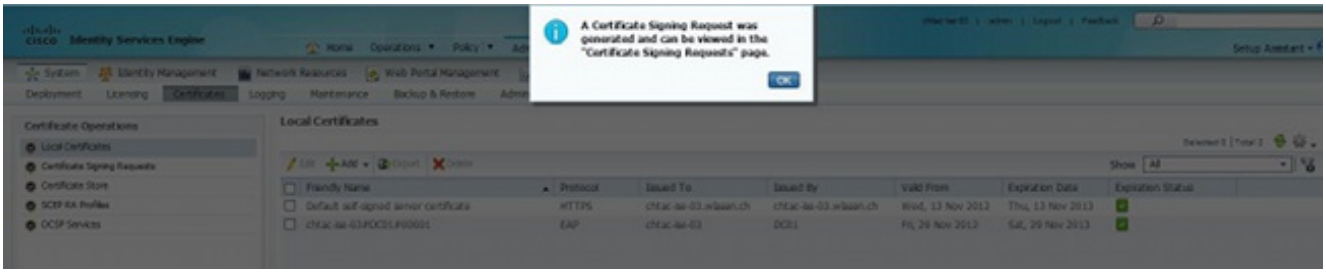
此程序描述如何通过CSR更新认证：

1. 在ISE控制台中，请连接对**Add>生成认证署名请求**。

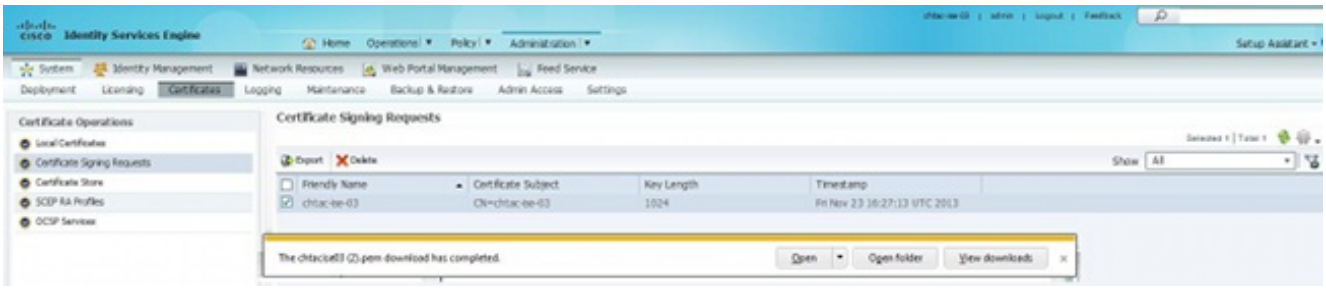
2. 您必须在**证书主题**文本字段输入的最低的信息是CN=ISEfqdn， *ISEfqdn*是ISE的完全合格的域名(FQDN)。添加另外的字段例如O (组织)， OU (组织单位)，或者C (国家)在与使用的证书主题逗号：

3. 其中一条**附属的代替命名(SAN)**文本字段线路必须重复ISE FQDN。如果要使用代替名字或通配符认证，您能添加秒钟SAN字段。

4. 一个弹出窗口指示CSR字段是否正确地被填入：



5. 为了导出CSR，请点击在左面板的**认证署名请求**，选择您的CSR，并且点击**导出**：

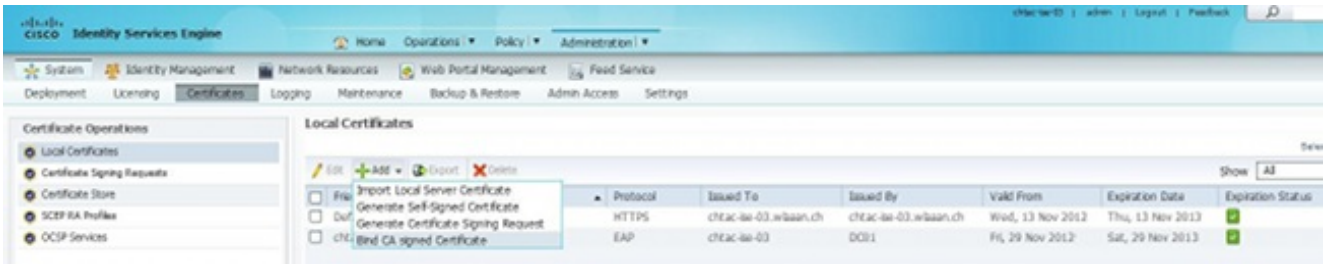


6. CSR在您的计算机被保存。提交它给您的CA为签名。

安装证书

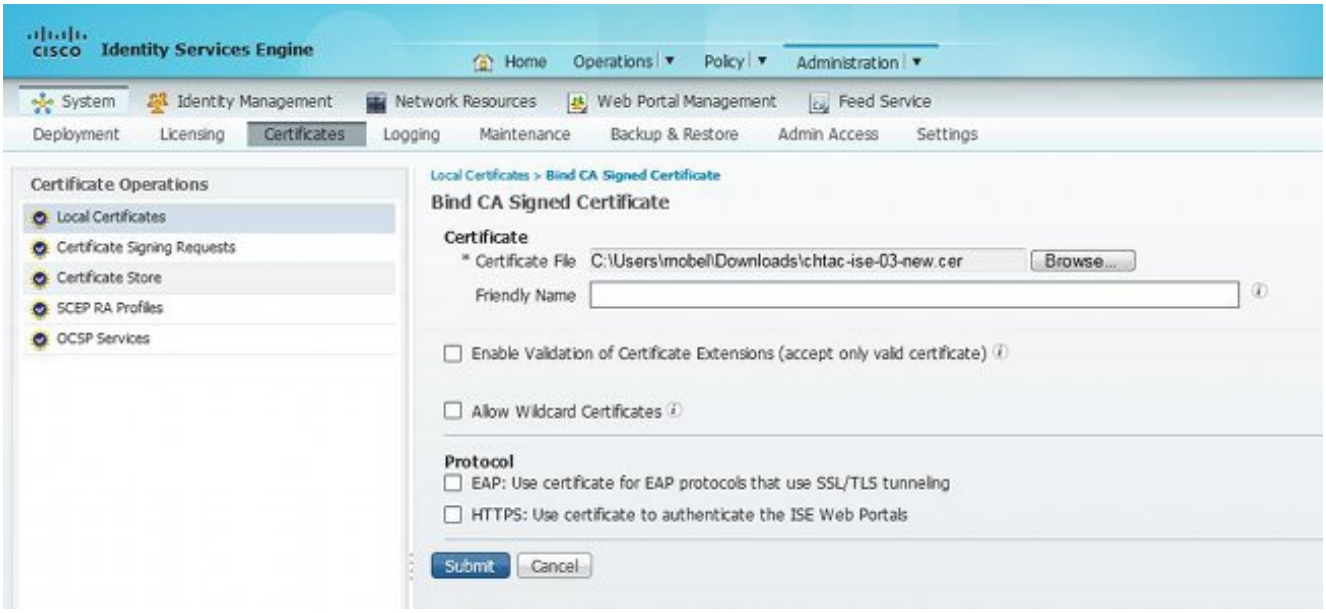
一旦从您的CA接受最终认证，您必须添加认证到ISE ：

1. 在ISE控制台中，请点击在左面板的**本地证书**，然后点击**添加**并且**捆绑CA签名的证书**：

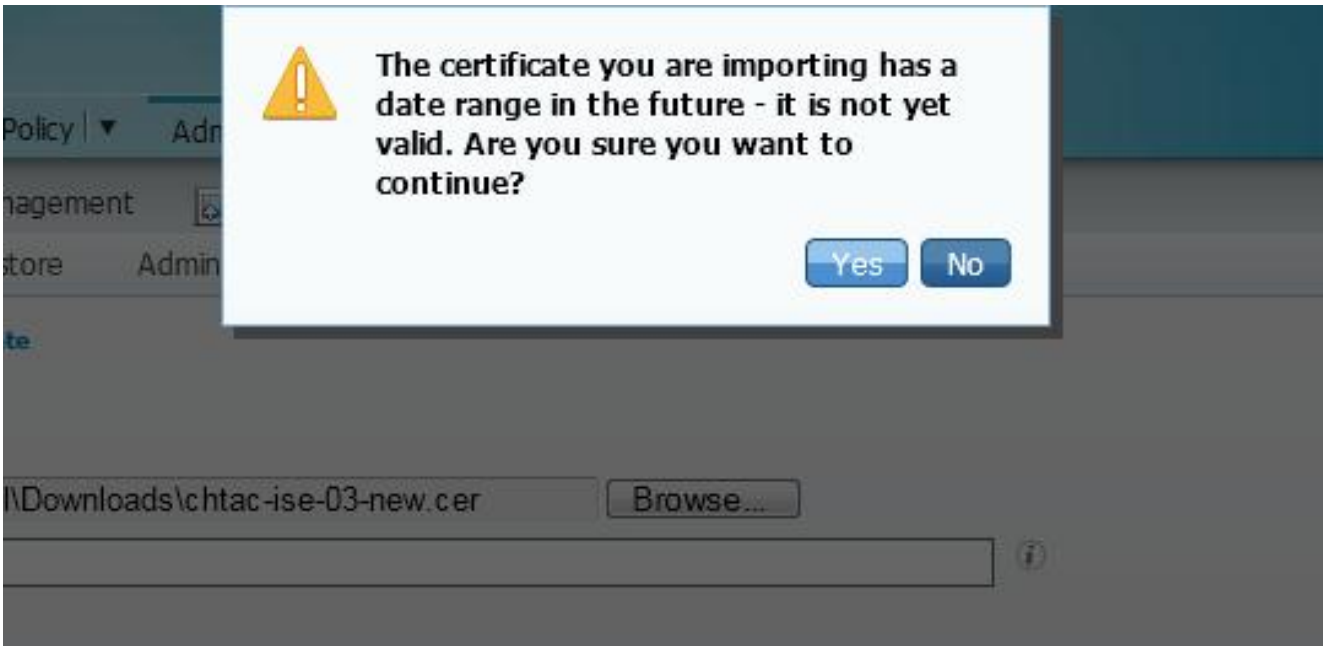


2. 在**友好名称**文本字段输入认证的一个简单，清楚的说明：

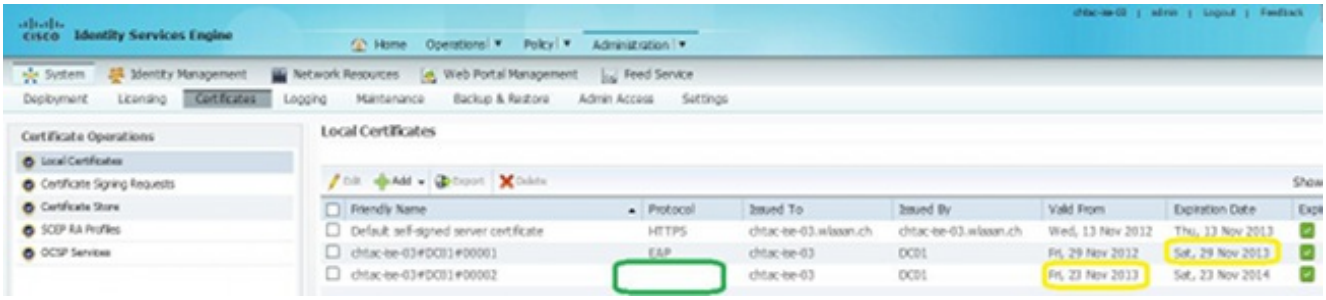
   Note:不此时enable (event) EAP或HTTPS协议。



3. 由于您安装新证书，在老一个到期前，您看到在将来报告日期范围的错误(2013年11月23日在本例中)。



4. **是**点击为了继续。认证当前安装，但是不在使用中，如突出显示在绿色上。在有效期和有效日期之间的重叠用黄色表示：



Note:如果在被分配的配置使用自署名的认证，必须安装主要的自签证书到附属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，配置也许中断。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了并且相应地更新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。

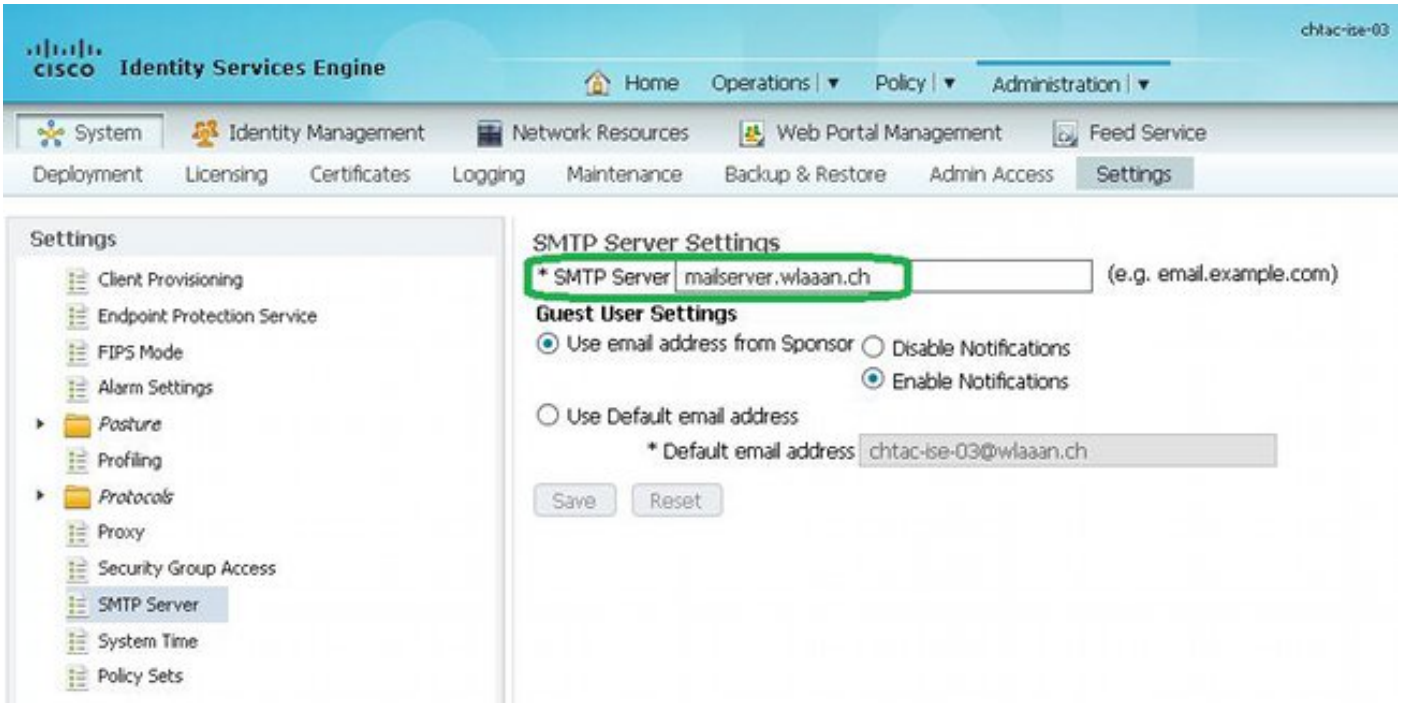
配置警报系统

当一个本地认证的有效期是在90天内时， Cisco ISE通知您。这样预先通知帮助您避免过期的证书，计划认证更改和防止或者使停工期减到最小。

通知出现用几个方式：

- 颜色到期状态图标出现于本地证书页。
- 到期通知出现于Cisco ISE系统诊断报告。
- 到期警报每日生成在90天和60天，然后在到期前的最终30天。

配置到期警报的电子邮件通知的ISE。在ISE控制台中，请连接到**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警报被发送：

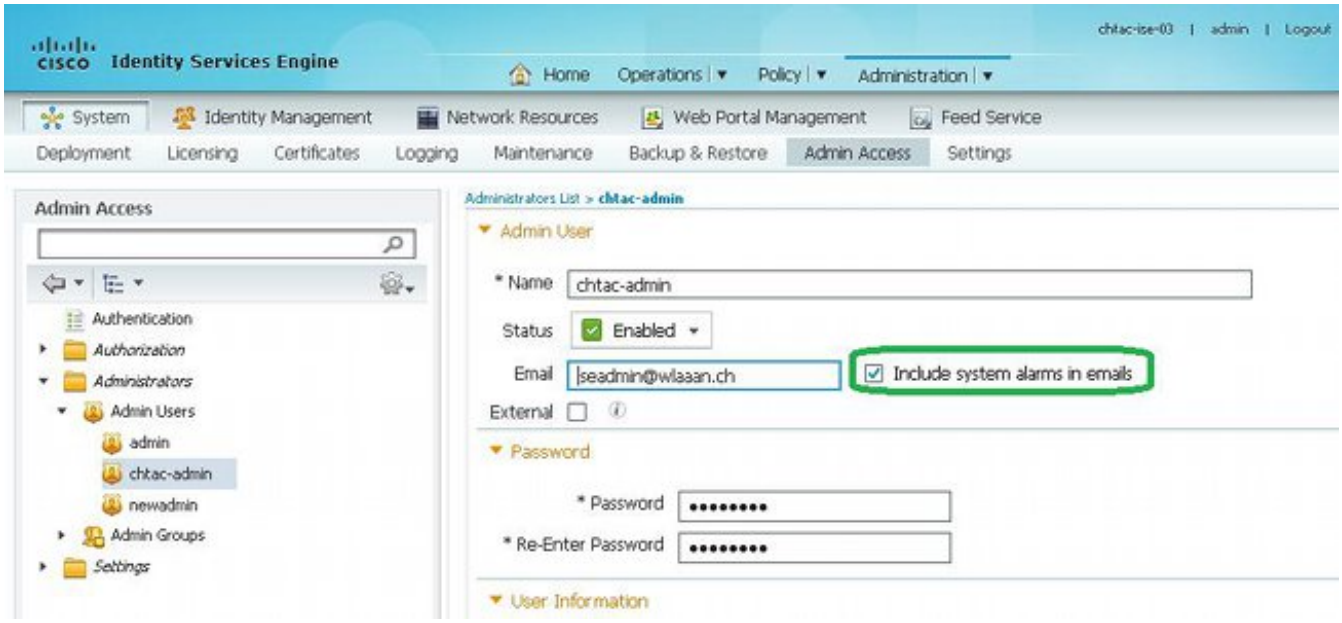


有两种方式您能设置通知：

- 请使用Admin访问为了通知管理员：

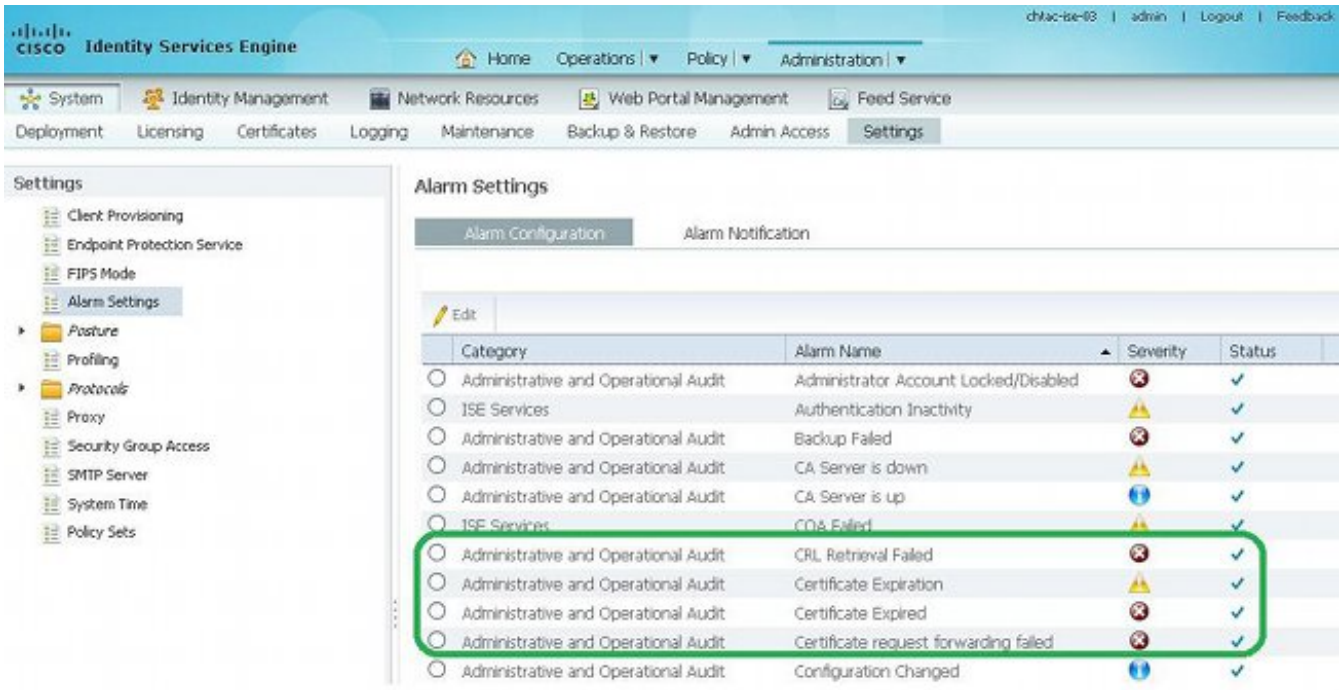
  连接给**管理>System > Admin访问>管理员>管理员用户**。

  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*-。

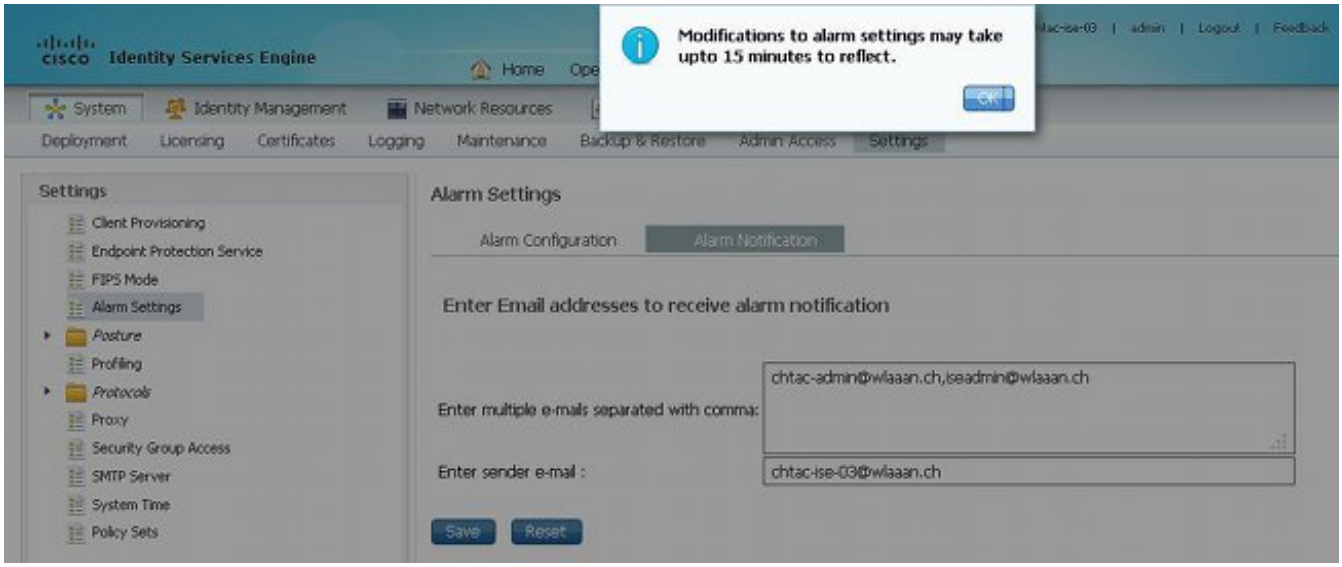


- 配置ISE告警设置为了通知用户：

连接对**管理>System >设置>告警设置>警报配置**：



Note:如果希望防止警报该类别，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被通知，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。

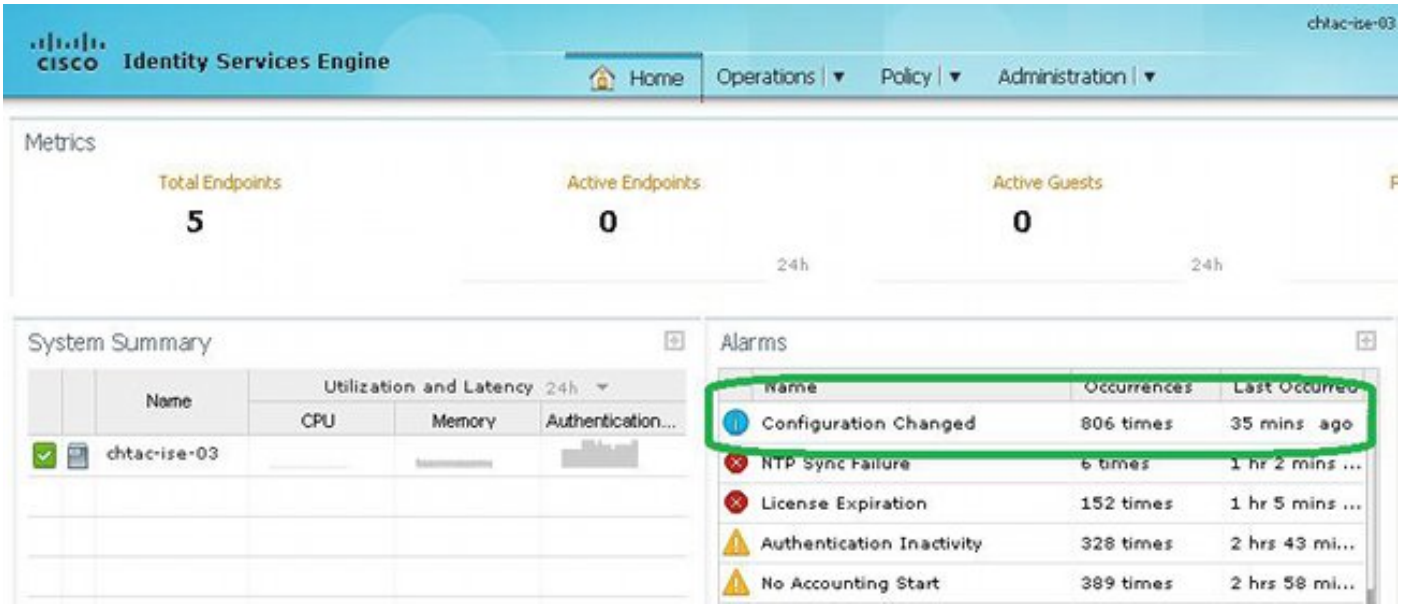


Verify

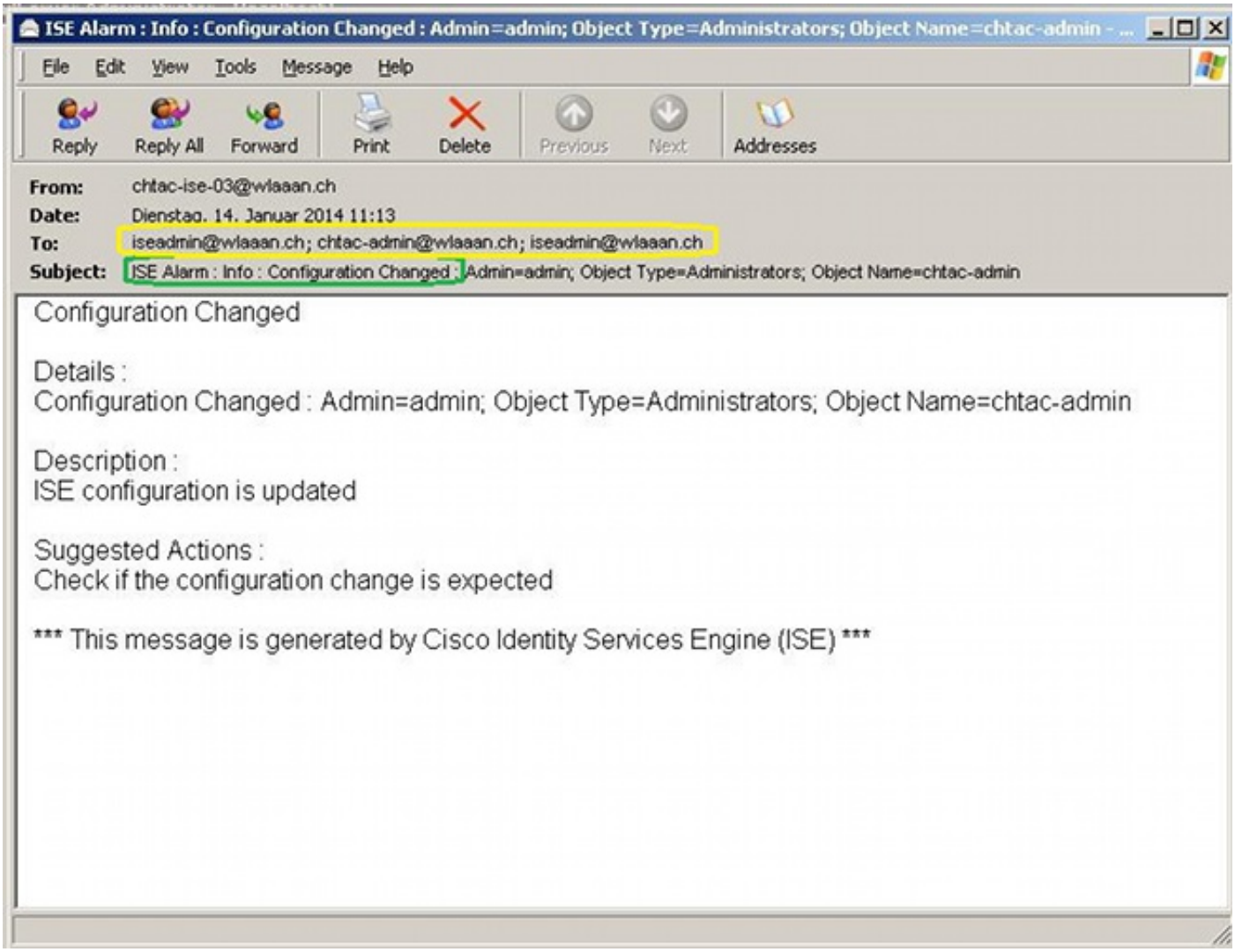
使用本部分可确认配置能否正常运行。

验证警报系统

验证警报系统正确地运作。在本例中，配置更改生成与信息的告警级别的一次戒备。(信息警报是最低的严重性，而证书到期生成警告的一个高严重程度级别。)



这是ISE发送电子邮件警报的示例：



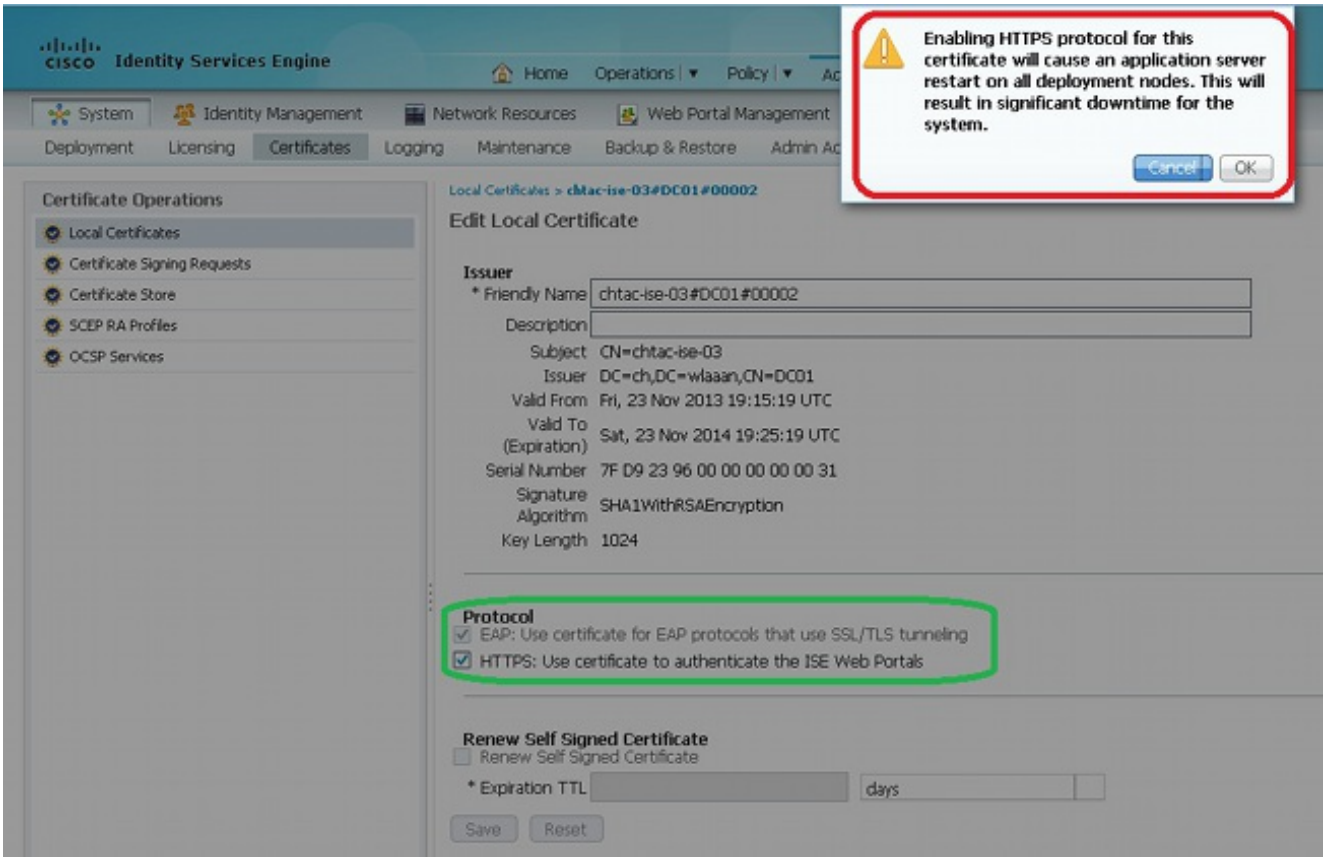
Note:在本例中， ISE两次发电子邮件告警消息到iseadmin@wlaaan.ch，如用黄色表示。此电子邮件地址用解释的两个方法设置接收通知配置警报系统。

验证认证更改

此程序描述如何验证正确地安装认证和如何更改EAP和HTTPS的协议：

1. 在ISE控制台上，请连接对**Administration >证书>本地证书**，并且选择新证书为了查看详细资料。

   警告：如果enable (event) HTTPS协议， ISE服务重新启动，导致服务器停工期。



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. 对于一个被分配的部署方案，请连接对在ISE控制台的**管理>System >配置> Status节点**，并且验证Status节点。

5. 检查终端用户认证是成功的。在ISE控制台上，请连接对**操作>认证**，并且查看Protected Extensible Authentication Protocol (PEAP) /EAP传输层安全(TLS)认证的认证。

验证认证

如果要检查认证外部，您能使用嵌入式微软视窗工具或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专用的CA，您在一个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。

为了得到关于认证的概要和验证它，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
```

Troubleshoot

目前没有针对此配置的故障排除信息。

结论

由于您能在ISE上安装新证书，在是活跃的前， Cisco建议您安装新证书，在老认证到期前。在老证书到期到期日和新证书起始日期之间的此重叠周期提供您时刻更新证书和计划他们的安装用很少或不停工期。一旦新证书输入其有效日期范围， enable (event) EAP和HTTPS协议。切记，如果您enable (event) HTTPS，有服务重新启动。