在ISE中删除过期的内部OCSP响应器证书

目录

简介

本文档介绍如何在思科身份服务引擎(ISE)中删除过期和/或即将过期OCSP响应方证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)的基本知识。
- 证书的基本知识。
- 在线证书状态协议(OCSP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎3.x

本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备都以清除（默认）配置开始。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

使用思科身份服务引擎(ISE)的客户面临的常见问题是收到指示证书已过期的警报，特别是当OCSP响应器证书已过期或即将过期且找不到证书时。这种情况通常会导致客户打开TAC案例以寻求帮助。本指南的目标是使客户能够自行查找和删除这些已过期或即将过期的OCSP响应方证书，从而避免提出TAC案例。

在线证书状态协议(OCSP)是用于检查x.509数字证书状态的协议。此协议是证书撤销列表(CRL)的替代协议，用于解决导致处理CRL的问题。思科ISE能够通过HTTP与OCSP服务器通信，以验证身份验证中的证书状态。OCSP配置配置在一个可重用的配置对象中，该对象可以从思科ISE中配置的任何证书颁发机构(CA)证书引用。

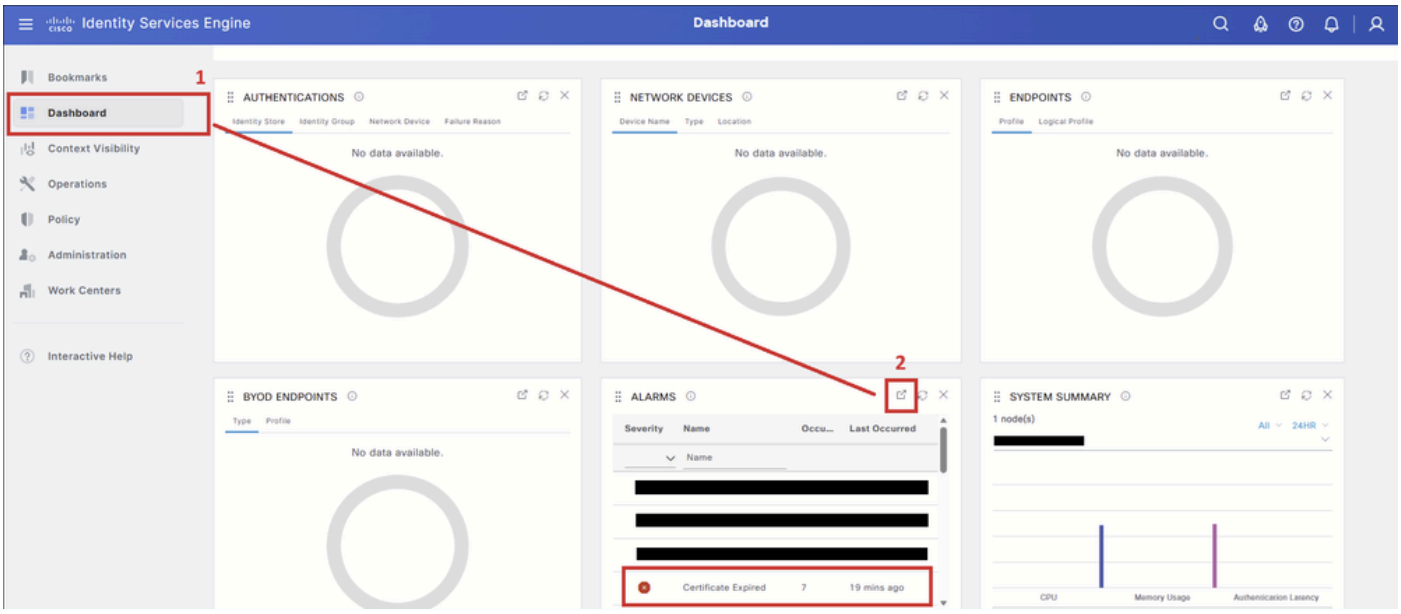
在每个Cisco ISE部署中，OCSP（在线证书状态协议）响应器证书默认作为内部CA（证书颁发机构）基础设施的一部分存在。这些证书由思科ISE内部CA在PPAN（主要策略管理节点）上颁发，并为部署中的每个节点(包括PAN和所有PSN（策略服务节点）)自动生成。

管理这些OCSP Responder证书非常重要，因为过期或即将过期的证书可能会触发Cisco ISE控制面板中的Certificate Expired警报。虽然Cisco ISE自动重新生成新的OCSP响应方证书，但过期的条目仍保留在受信任证书库中，直到手动删除它们。

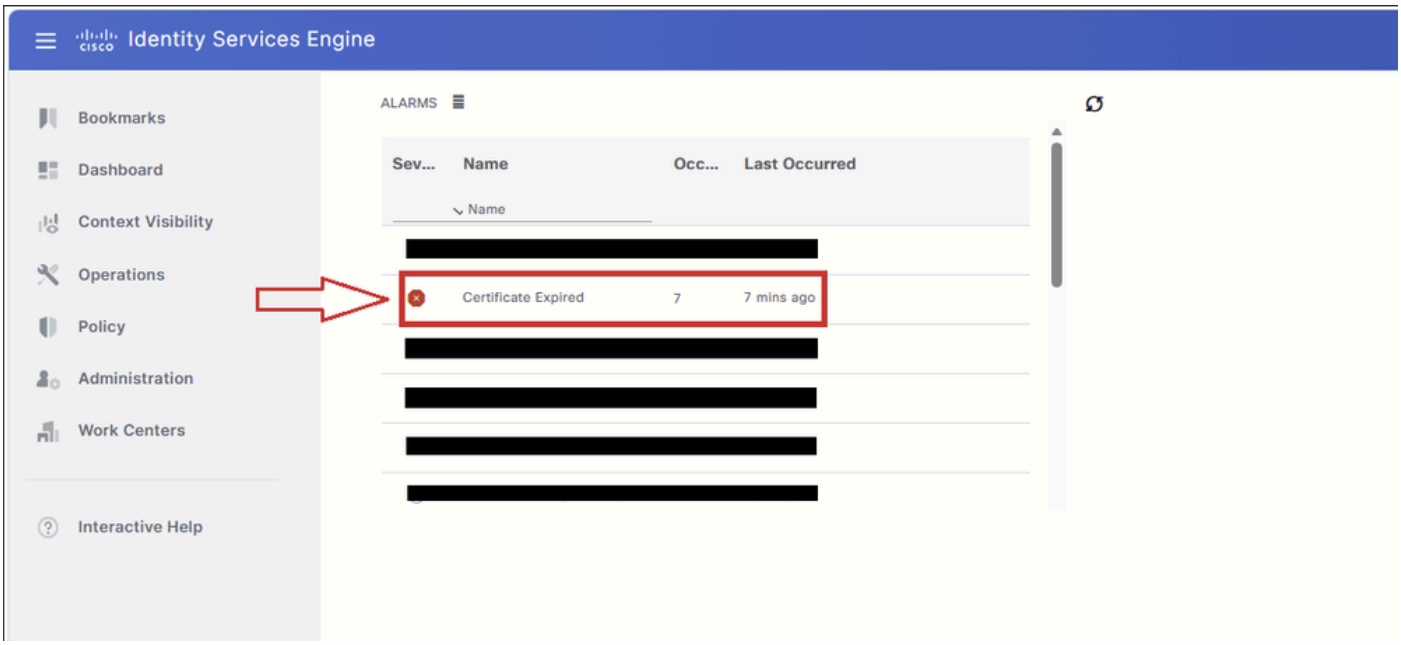
配置

第1步 — 检验过期的OCSP证书

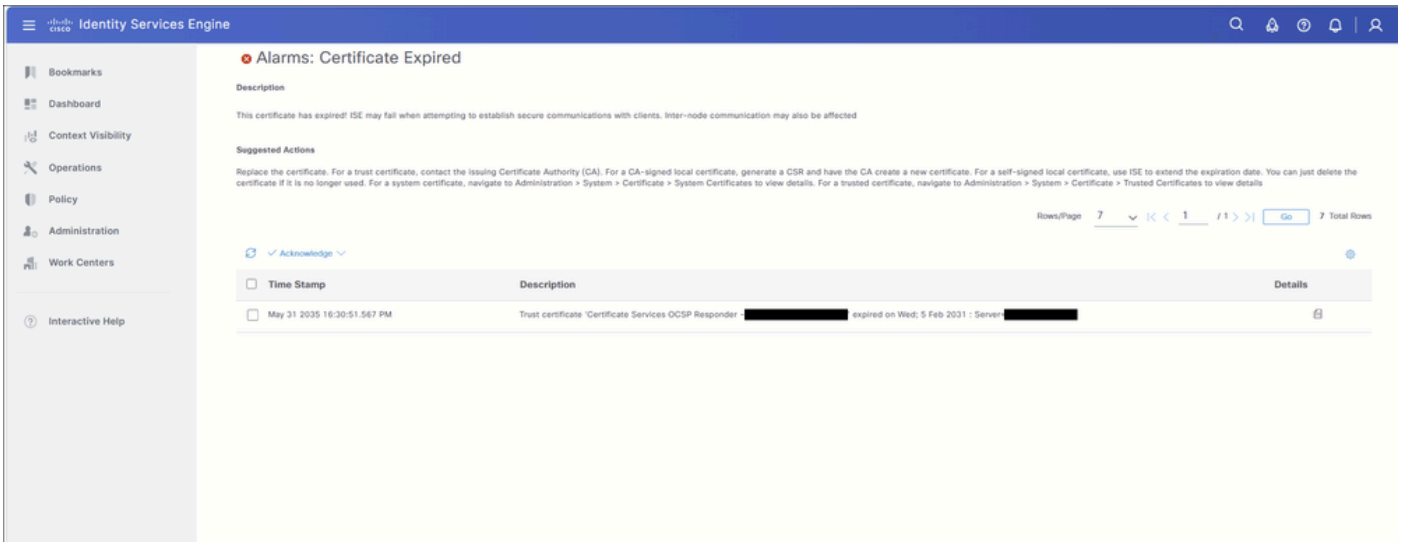
在PPAN(主要策略管理节点)GUI中，导航到控制面板选项卡(1)。 在Alarms dashlet中，单击Detach按钮(2)以展开警报表。



单击Certificate Expired警报以展开表并显示与警报关联的证书条目。



所有触发证书过期警报的证书都显示在此表中。本指南仅重点介绍OCSP Responder证书。如果表包含其他过期的证书类型，例如EAP、SAML、Admin或其他系统证书，请参阅相关思科文档和Cisco ISE管理员指南获取有关这些证书类型的指导。



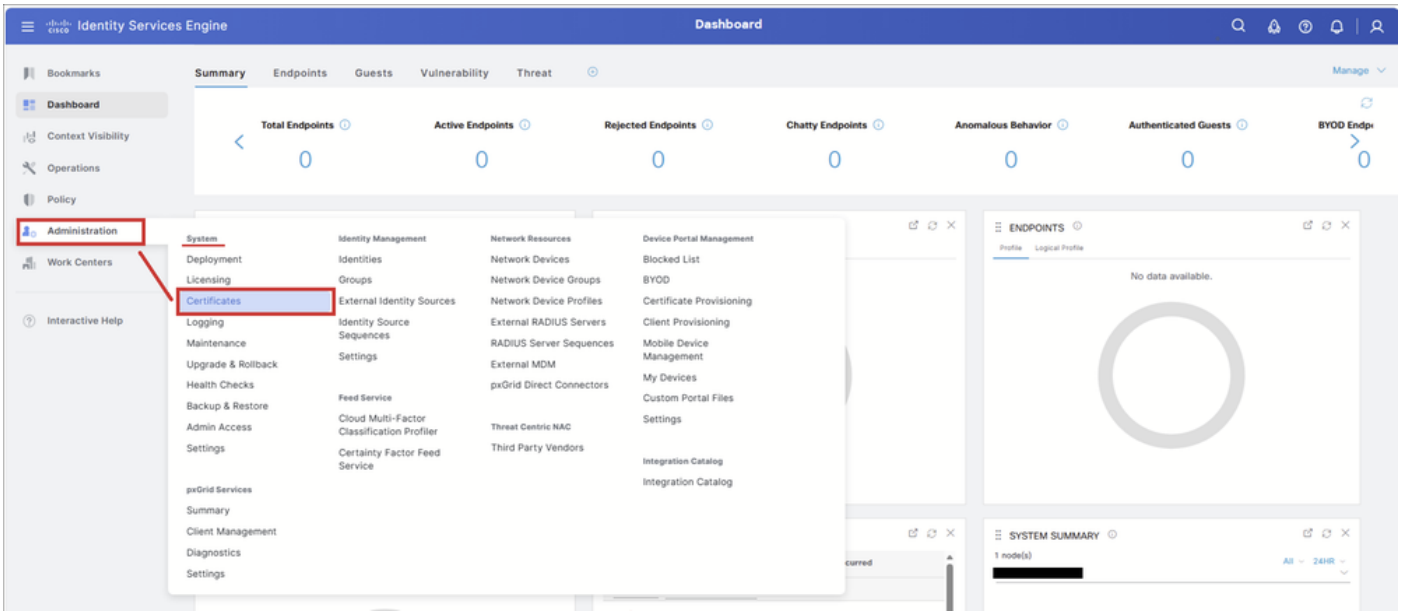
查看警报说明，确定已到期的证书，或者在某些情况下即将到期的证书。

在本示例中，过期证书为：证书服务OCSP响应器 — <node-name>#00004。

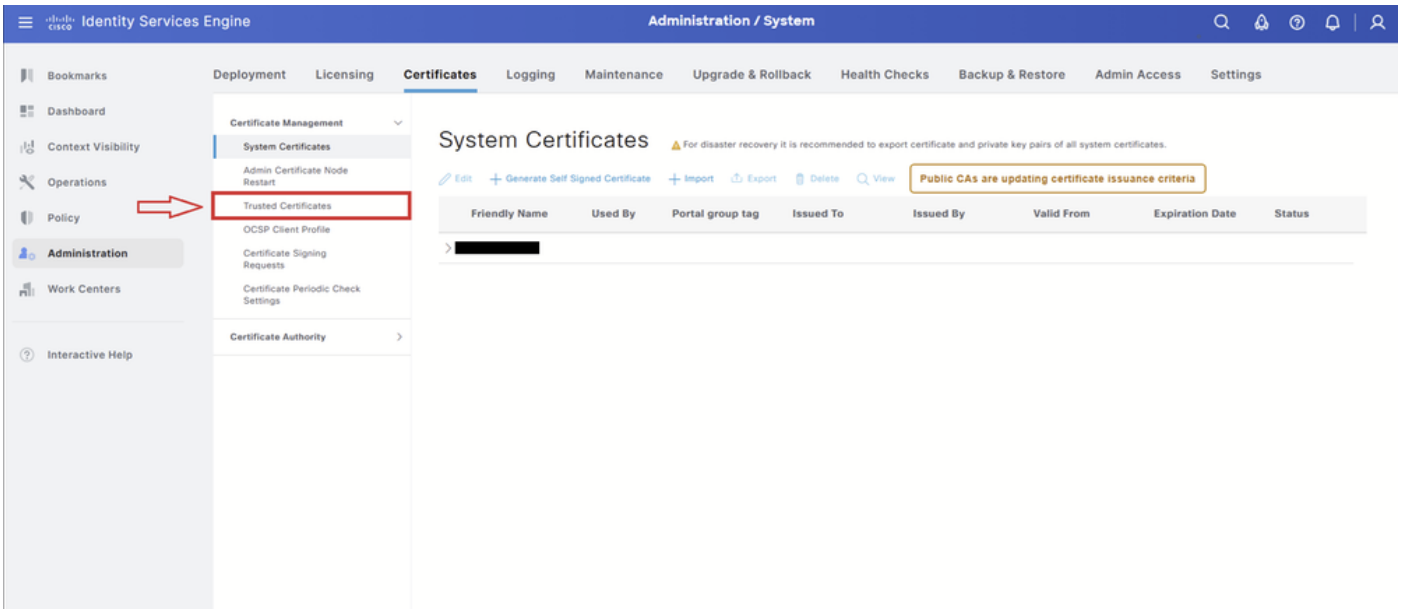
记下证书名称。此名称用于后续步骤以从受信任证书存储区查找和删除证书。

第2步 — 查找并删除过期的OCSP证书

导航至：Administration > System > Certificates:



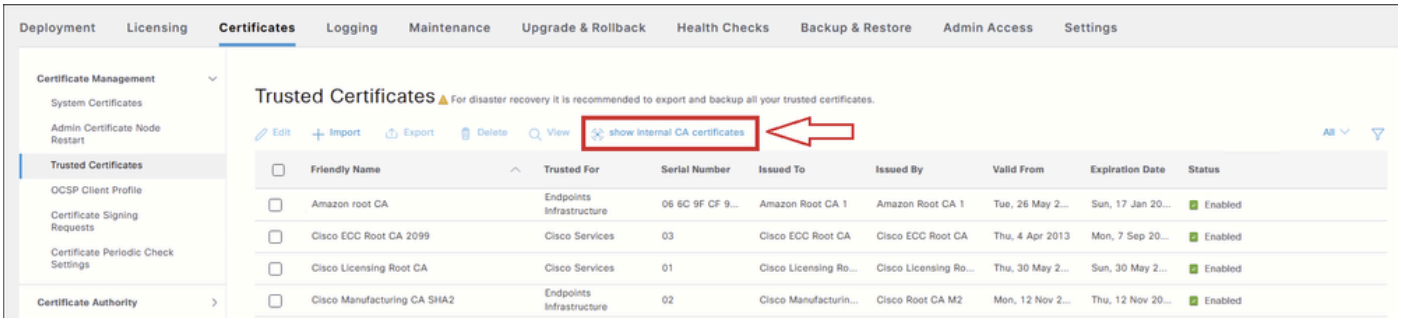
选择Trusted Certificates选项卡。



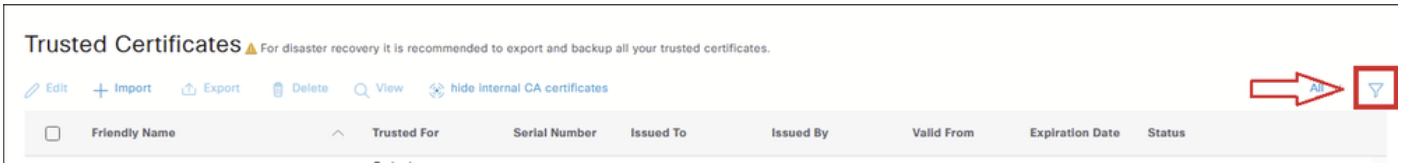
在Trusted Certificates页面上，选择show internal CA certificates。这将显示思科ISE内部CA（证书颁发机构）证书，包括默认隐藏的OCSP响应方证书。

选中后，该按钮将更改以隐藏内部CA证书。

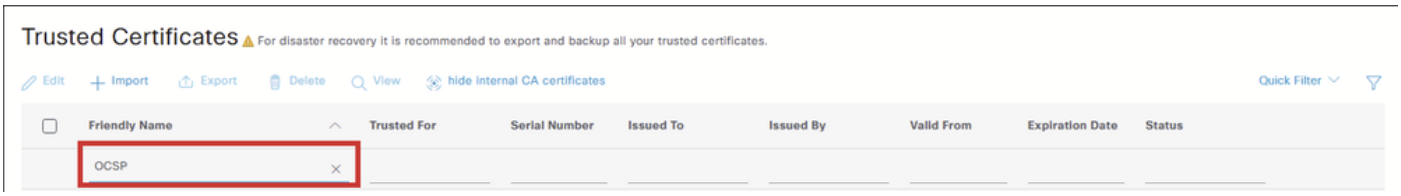
警告：此步骤是必需的。如果未选择show internal CA certificates，则OCSP Responder证书不会显示在受信任证书存储表中。



在Trusted Certificate Store表中，选择Filter图标搜索必须删除的证书。

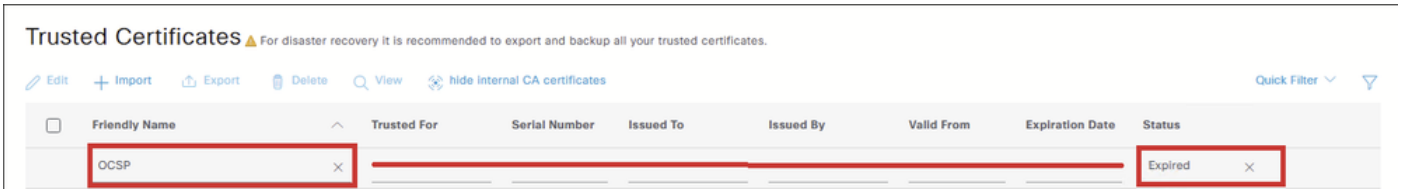


如果OCSP Responder证书即将过期，请仅按“友好名称”下的OCSP进行过滤。如果OCSP Responder证书已过期，请继续执行下一步操作。



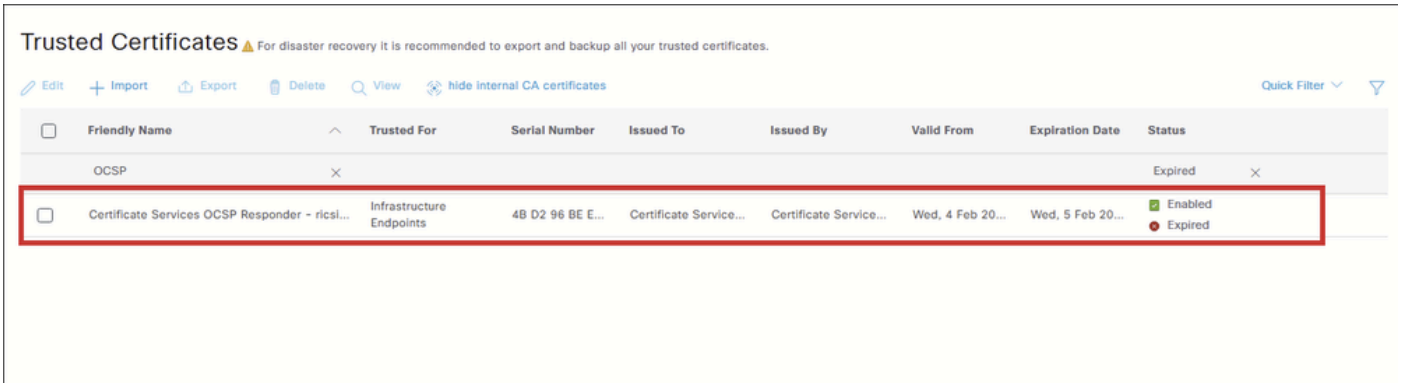
要查找已过期的OCSP响应器证书，请输入以下过滤器：

- 友好名称：OCSP
- 状态:已到期

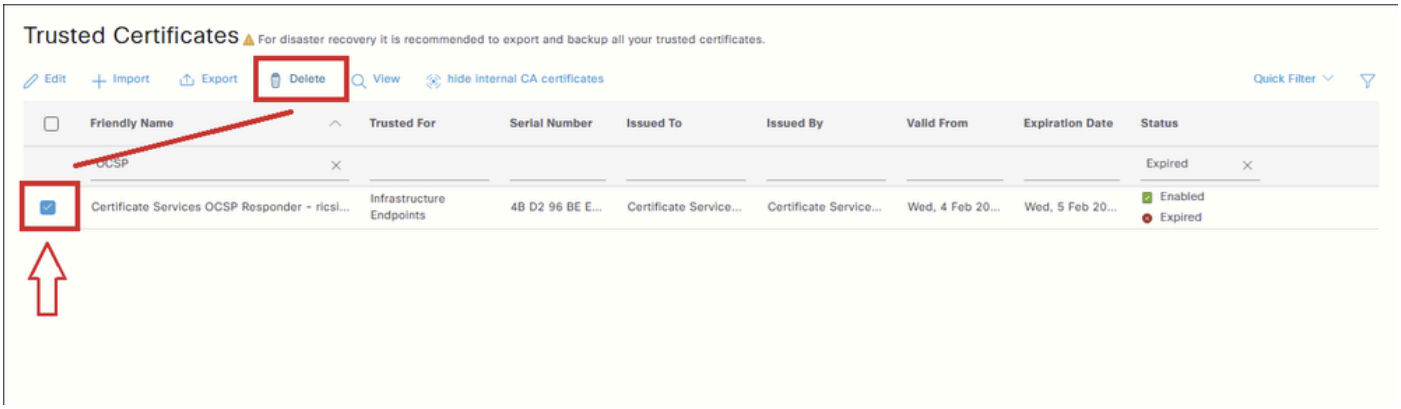


该表显示过期的OCSP响应方证书。

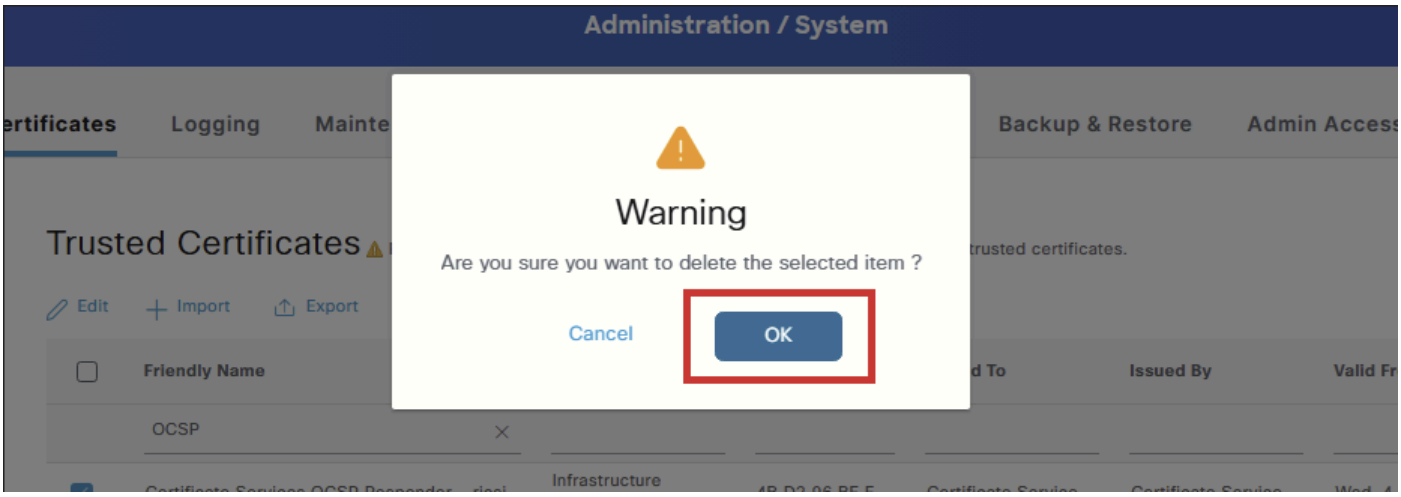
提示：如果您正在搜索即将到期的OCSP响应器证书，则可以显示多个证书，尤其是在具有多个思科ISE节点的部署中。要识别正确的证书，请勿仅按OCSP过滤。相反，按步骤1中警报详细信息中显示的完整证书名称进行过滤。



选中必须删除的OCSP Responder证书旁边的复选框，然后单击Delete。



在确认警告上选择OK以继续删除证书。



在删除证书之前，必须了解OCSP响应器证书是ISE内部CA基础设施的一部分。

删除过程中出现的警告是通用的，适用于所有内部CA相关证书。其目的是警告不要在内部CA层次结构内删除证书，因为其中某些证书签署用于服务（例如BYOD、pxGrid）的终端证书，或依赖ISE内部CA颁发的证书的其他功能。

过期的OCSP响应器证书也会影响ISE内部CA颁发的证书。当客户端或服务查询该CA颁发的证书的状态时，OCSP服务会返回一个错误，因为OCSP响应器证书已过期，这可能导致证书状态验证失败。

选择Delete时，将显示两个选项：

- 删除证书：此选项从受信任证书库删除思科ISE内部CA证书。删除内部CA证书后，该CA签名的所有终端证书将失效，受影响的终端将无法访问网络。此操作是可逆的：通过将同一内部CA证书导入回受信任证书存储区，可以恢复网络访问。
- 删除和撤销证书：此选项删除和撤销思科ISE内部CA证书。与Delete选项一样，由内部CA签名的所有终端证书都变为无效，受影响的终端将失去网络访问权限。但是，此操作是不可逆的。撤销后，您必须替换整个思科ISE根证书链，部署才能恢复功能。

为过期OCSP响应器证书选择哪个选项？

所述影响适用于主动签署终端证书的内部CA证书。OCSP Responder证书不对终端证书签名，它用于OCSP通信。虽然过期的OCSP响应器证书可能导致内部CA颁发的证书的证书状态验证失败，但证书已过期，因此不再提供有效的OCSP响应。删除它不会产生任何其他影响。

由于此场景中的OCSP响应器证书已过期，因此它不再有效。在这种情况下，“删除”和“删除和撤消”都会产生相同的结果，因为没有任何有效内容可供撤消。

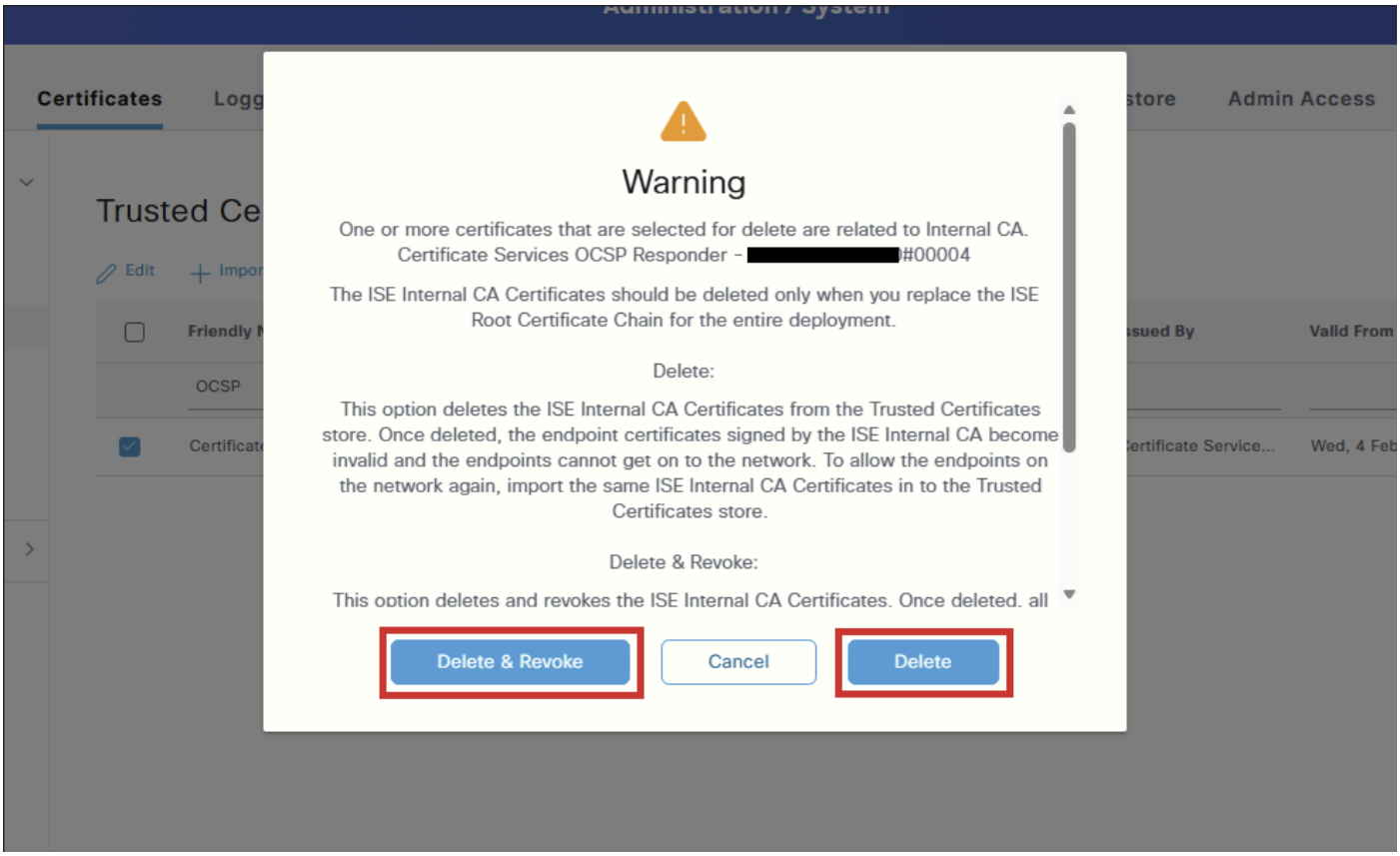
因此，建议使用Delete选项，因为它是更简单的操作，而且可以避免生成不必要的撤销条目。

注意：在正常操作期间，不会重新生成OCSP响应器证书。只有在安装了补丁时才重新生成：
— 在多节点部署中，通过GUI安装补丁时会重新生成证书。
— 在独立部署中，通过GUI或CLI安装补丁后重新生成证书。

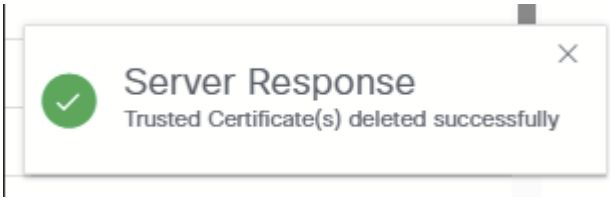
仅在下次安装补丁时生成新的OCSP Responder证书。

警告：确保受影响节点在受信任证书存储区中具有有效的活动OCSP响应器证书。如果有效证书不存在且使用OCSP验证ISE内部CA签名的证书，则验证失败，直到生成新的OCSP响应器证书。

如果有效的OCSP响应器证书不存在，请从PPAN（主策略管理节点）续订OCSP响应器证书，如下所述：
1.访问ISE PPAN GUI。
2.转至Administration > System > Certificates。
3.选择左侧的Certificate Signing Requests。
4.单击生成CSR。对于Usage，选择Renew ISE OCSP Responder。
5.单击Renew ISE OCSP Responder Certificates完成此过程。



删除证书后，系统将显示服务器响应通知，指示已成功删除受信任证书：



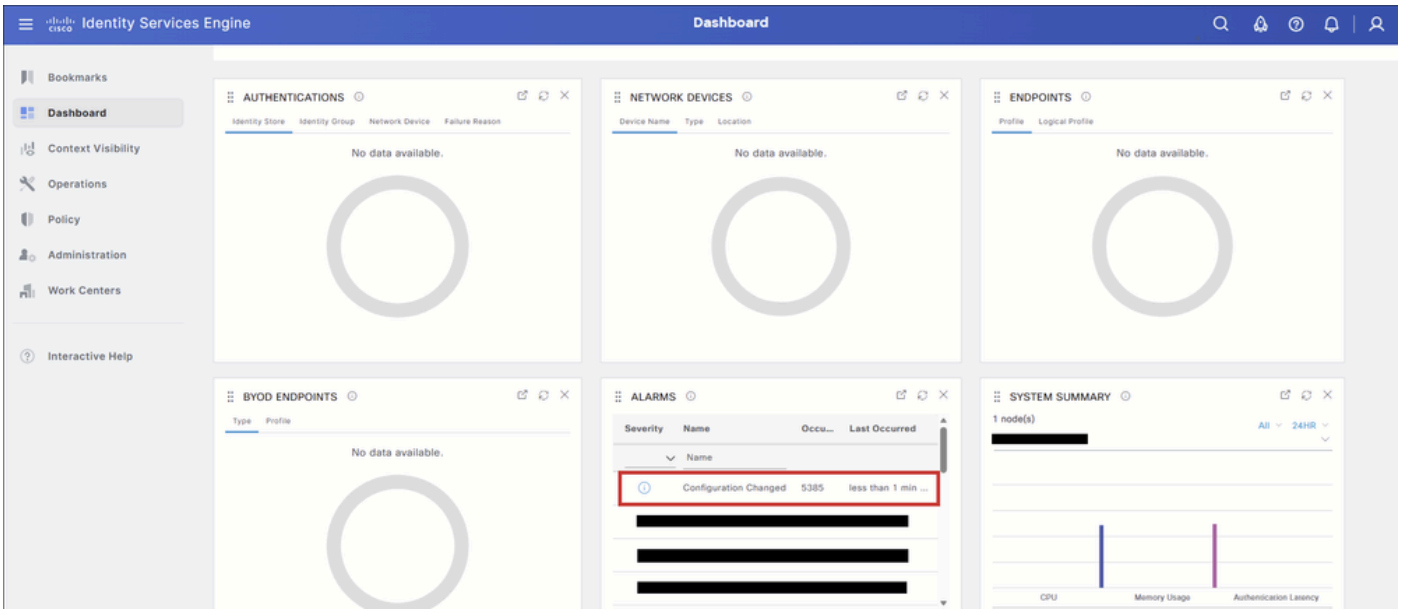
验证

删除证书后，您可以使用其中一种或两种方法来验证操作是否成功。

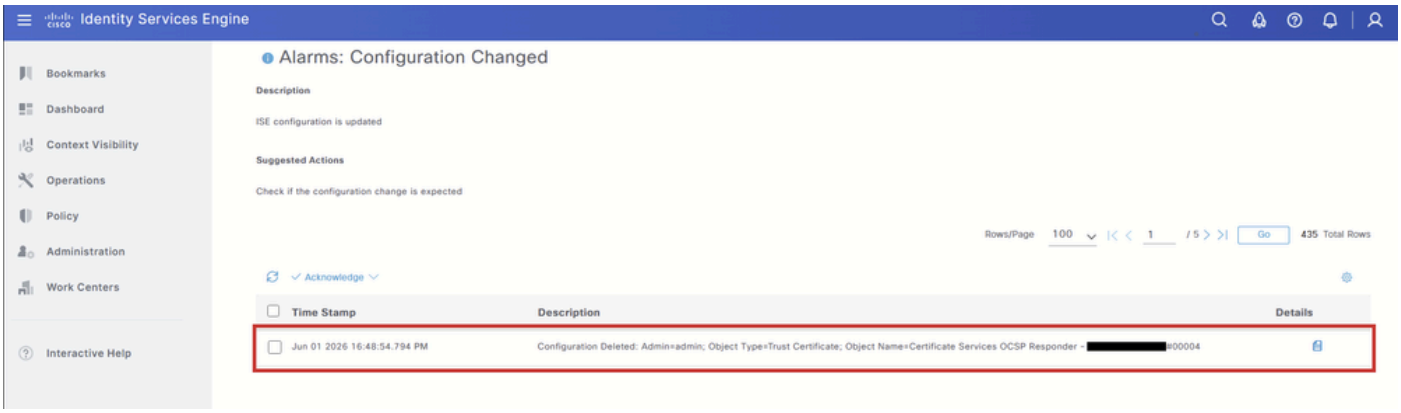
选项1 — 从控制面板警报中验证

导航到Dashboard页面。

在Alarms(警报)Dashlet（小面板）中，找到Configuration Changed（配置更改）警报。选择警报以显示详细信息。



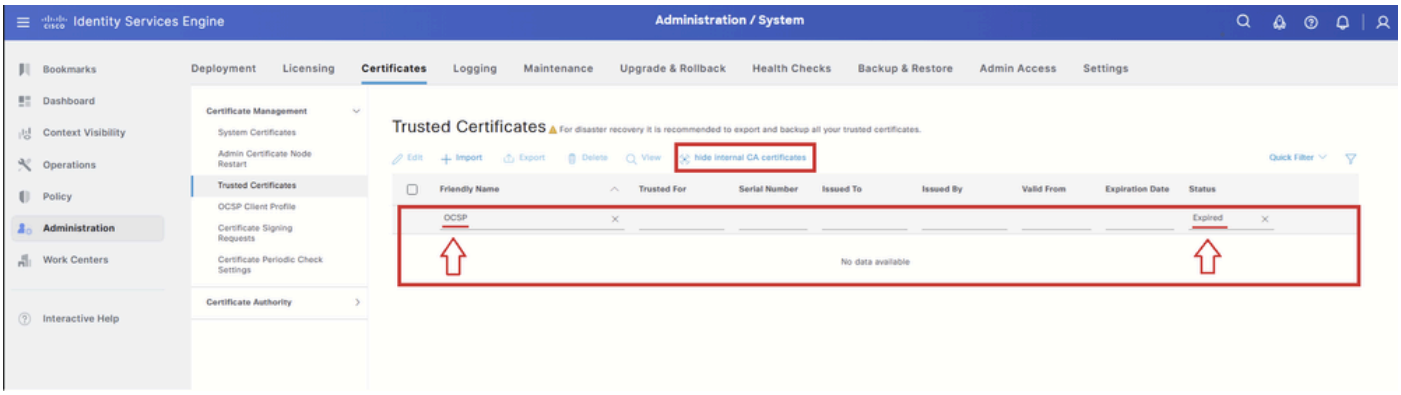
必须出现一个条目，指示已删除配置对象。对象名称必须与已删除的OCSP响应器证书匹配。



选项2 — 从受信任证书库进行验证

作为额外的步骤，导航回Trusted Certificate Store表并过滤OCSP Responder证书。由于证书已被删除，该表必须显示“无可用数据”。

注意：请记得选择show internal CA certificates。


Identity Services Engine
Administration / System
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade & Rollback
Health Checks
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settings
Certificate Authority
Trusted Certificates
For disaster recovery it is recommended to export and backup all your trusted certificates.
Edit
Import
Export
Delete
View
Hide Internal CA certificates
Quick Filter
Friendly Name
Trusted For
Serial Number
Issued To
Issued By
Valid From
Expiration Date
Status
OCSP
Expired
No data available

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）。