# 在 Cisco VPN 3000 集中器上通过 HTTP 检查 CRL

## 目录



## 简介

本文描述如何启用检查认证机构(CA)证书的证书撤销列表(CRL)安装在Cisco VPN 3000集中器使用HTTP模式。

证书通常预计是有效在其整个有效性周期内。然而，如果证书变为无效由于这样事作为名称更改，关联更改在主题和CA之间的和安全妥协， CA废除证书。在X.509下， CA通过周期地发出签字的CRL废除证书，每取消的证书由其序列号识别。启用CRL检查含义那，在VPN集中器使用证书验证时候，它也检查CRL保证验证的证书未取消。

CA用轻量级目录访问协议(LDAP)存储和分配Crl的/HTTP数据库。他们也许也使用其它方法，但是VPN集中器依靠LDAP/HTTP访问。

HTTP CRL检查在VPN集中器版本3.6或以上介绍。然而，基于LDAP的CRL检查在初期的3.x版本介绍。使用HTTP，本文只讨论CRL检查。

**注意：** CRL缓存容量VPN 3000系列集中器取决于平台，并且不可能根据管理员的希望配置。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- 您成功设立从使用证书的VPN 3.x硬件客户端的IPSec隧道Internet Key Exchange (IKE)验证(没有启用的CRL检查)。
- 您的VPN集中器一直有连接到CA服务器。
- 如果您的CA服务器连接对公共接口，则您打开在公共(默认)过滤器的必要的规则。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- VPN 3000集中器版本4.0.1 C
- VPN 3.x硬件客户端
- 证书生成和CRL检查运行的Microsoft CA服务器在Windows 2000服务器。

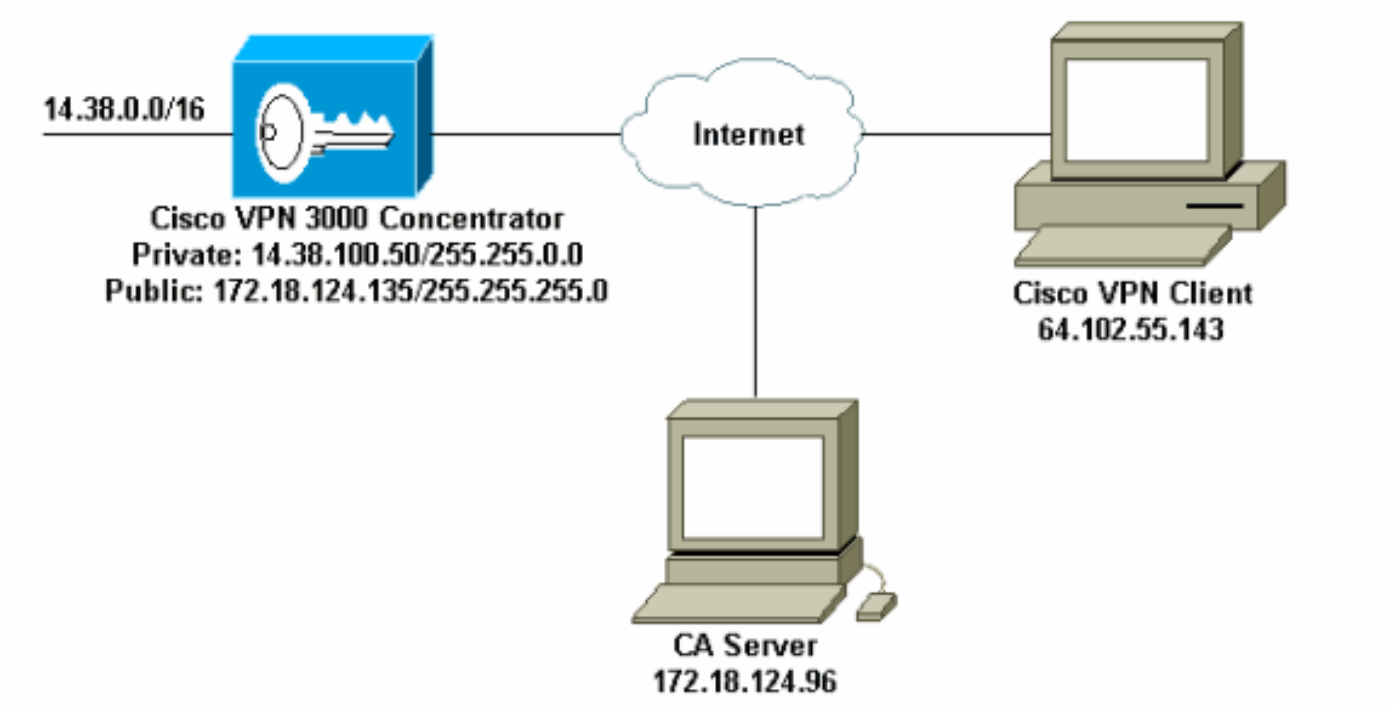
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## 网络图

本文档使用以下网络设置：

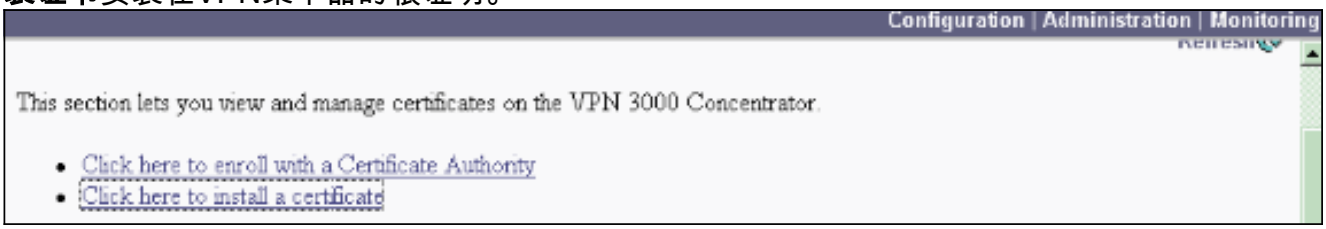



# 配置VPN 3000集中器

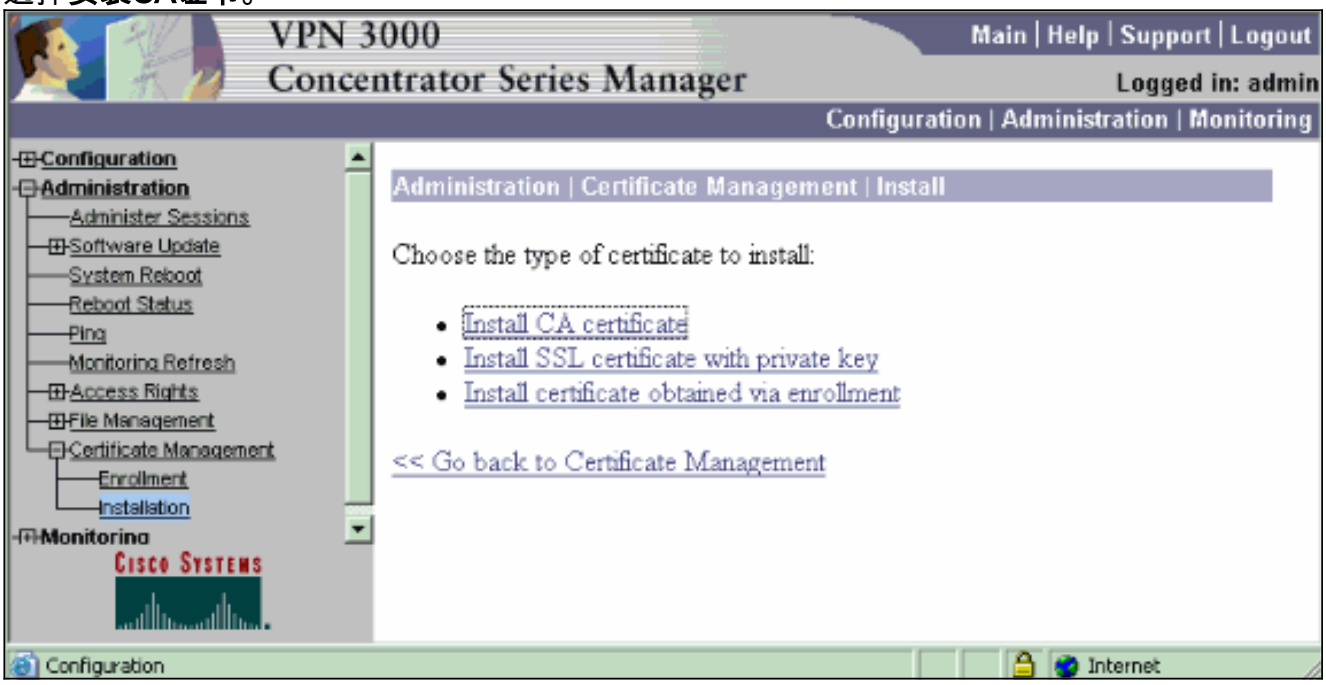
## 逐步指导

完成以下步骤以配置 VPN 3000 集中器：

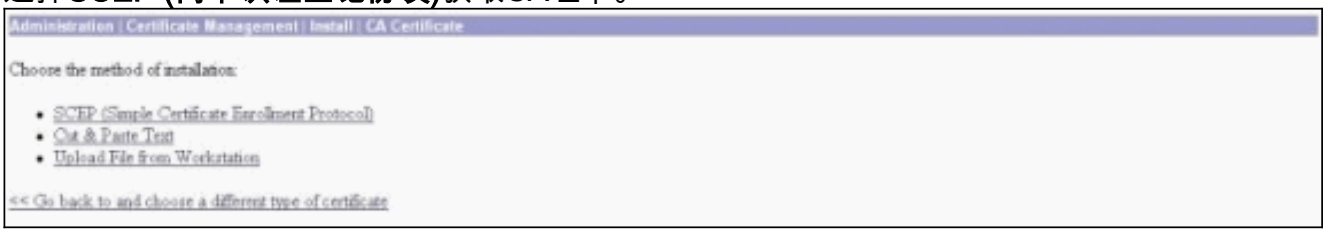
1. 如果没有一证书，请选择**Administration > Certificate Management**请求证书。选择**点击此处安装证书**安装在VPN集中器的根证明。



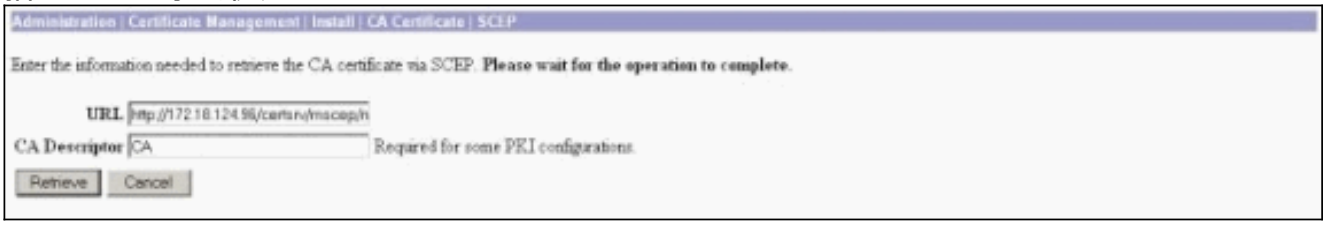

2. 选择**安装CA证书**。




3. 选择**SCEP (简单认证登记协议)**获取CA证书。

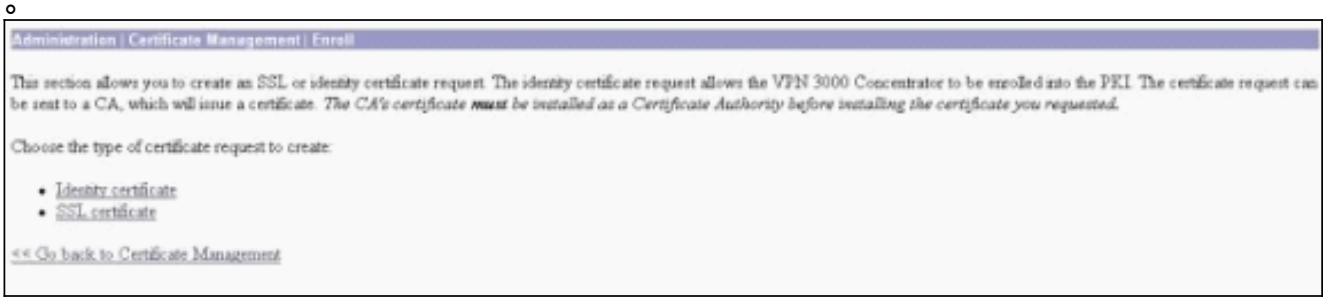



4. 从SCEP窗口，请输入CA服务器的完整URL在URL对话框的。在本例中， CA服务器IP地址是172.18.124.96。因为此示例使用Microsoft的CA服务器，完整URL是http://172.18.124.96/certsrv/mscep/mscep.dll。其次，请输入在CA Descriptor对话框的一个词描述符。此示例使用CA。

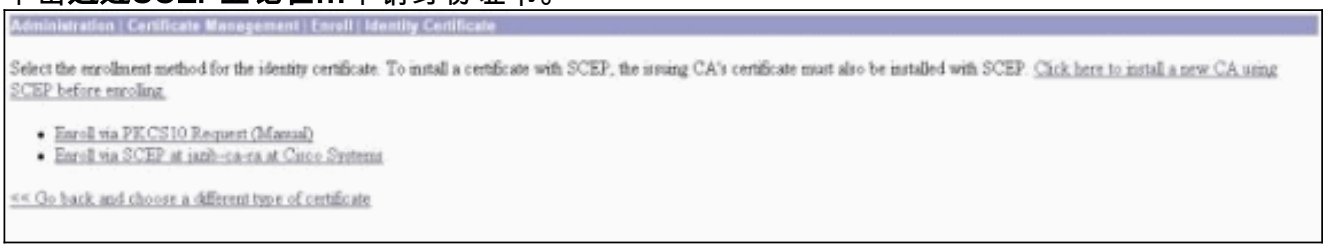



5. 单击 Retrieve（检索）。您的CA证书应该出现在Administration > Certificate Management窗口下。如果看不到证书，去上一步Step1并且再遵从步骤。

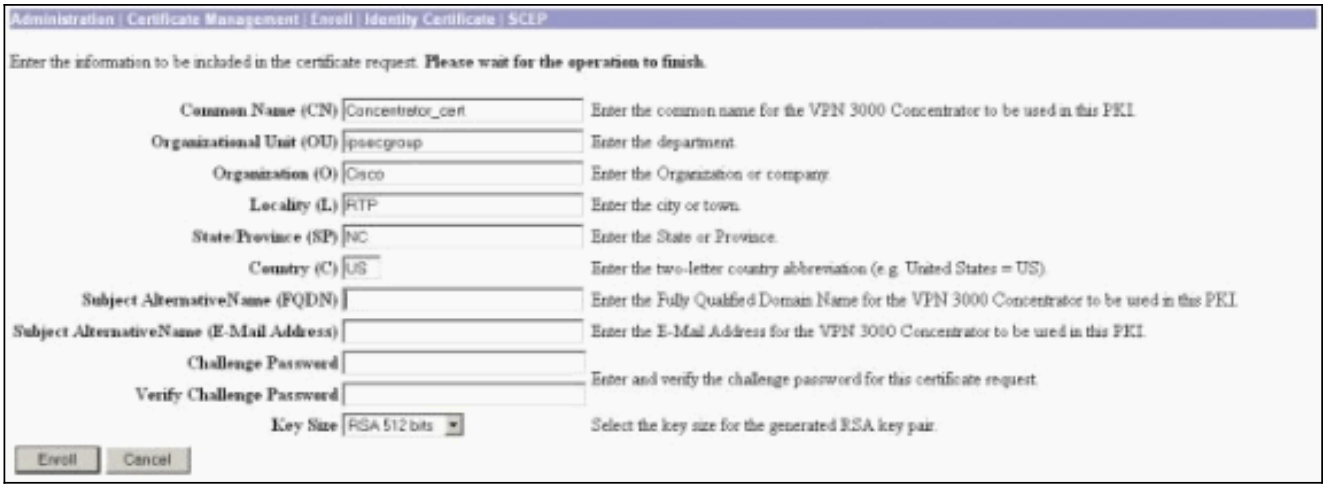

6. 一旦有CA证书，请选择**Administration > Certificate Management > Enroll**，并且点击**身份证书**。



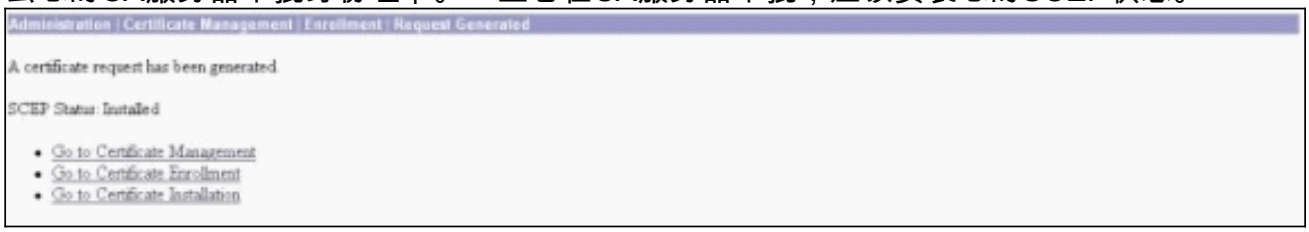

7. 单击**通过SCEP登记在...**申请身份证书。



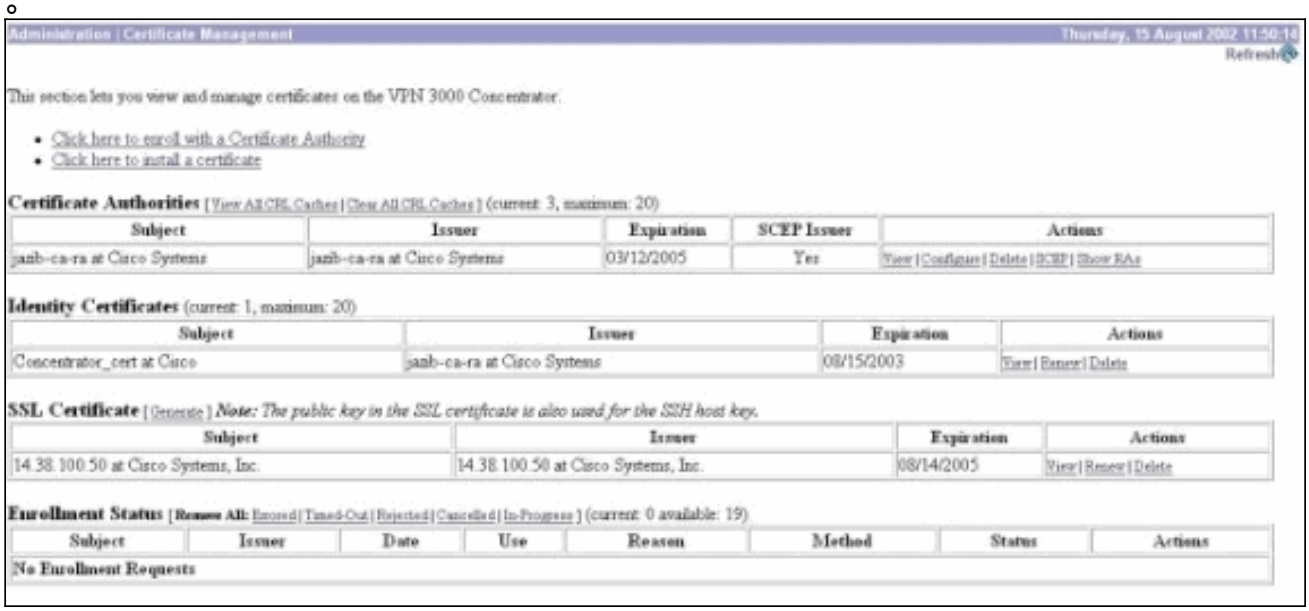

8. 完成这些步骤填好表格登记：在共同名称(CN)字段输入用于公共密钥基础设施(PKI)能的VPN集中器的公用名称。在组织单位(OU)字段送进您的部门。OU应该匹配配置的IPSec组名。在组织(o)字段进入您的组织或公司。在现场(l)字段进入您的城市或城镇。在State/Province(SP)字段进入您的状态或省。在国家(c)字段进入您的国家。在完全合格的域名(FQDN)字段输入用于PKI能的VPN集中器的完全合格的域名(FQDN)。在附属的替代方案名称(电子邮件地址)字段输入用于PKI能的VPN集中器的电子邮件地址。输入证书请求的私钥保护密码在Challenge Password字段。重新输入私钥保护密码在Verify Challenge Password字段。选择生成的RSA密钥对的密钥大小从密钥大小下拉列表。




9. 在轮询状态选择**登记**并且查看SCEP状态。
10. 去您的CA服务器审批身份证书。一旦它在CA服务器审批，应该安装您的SCEP状态。

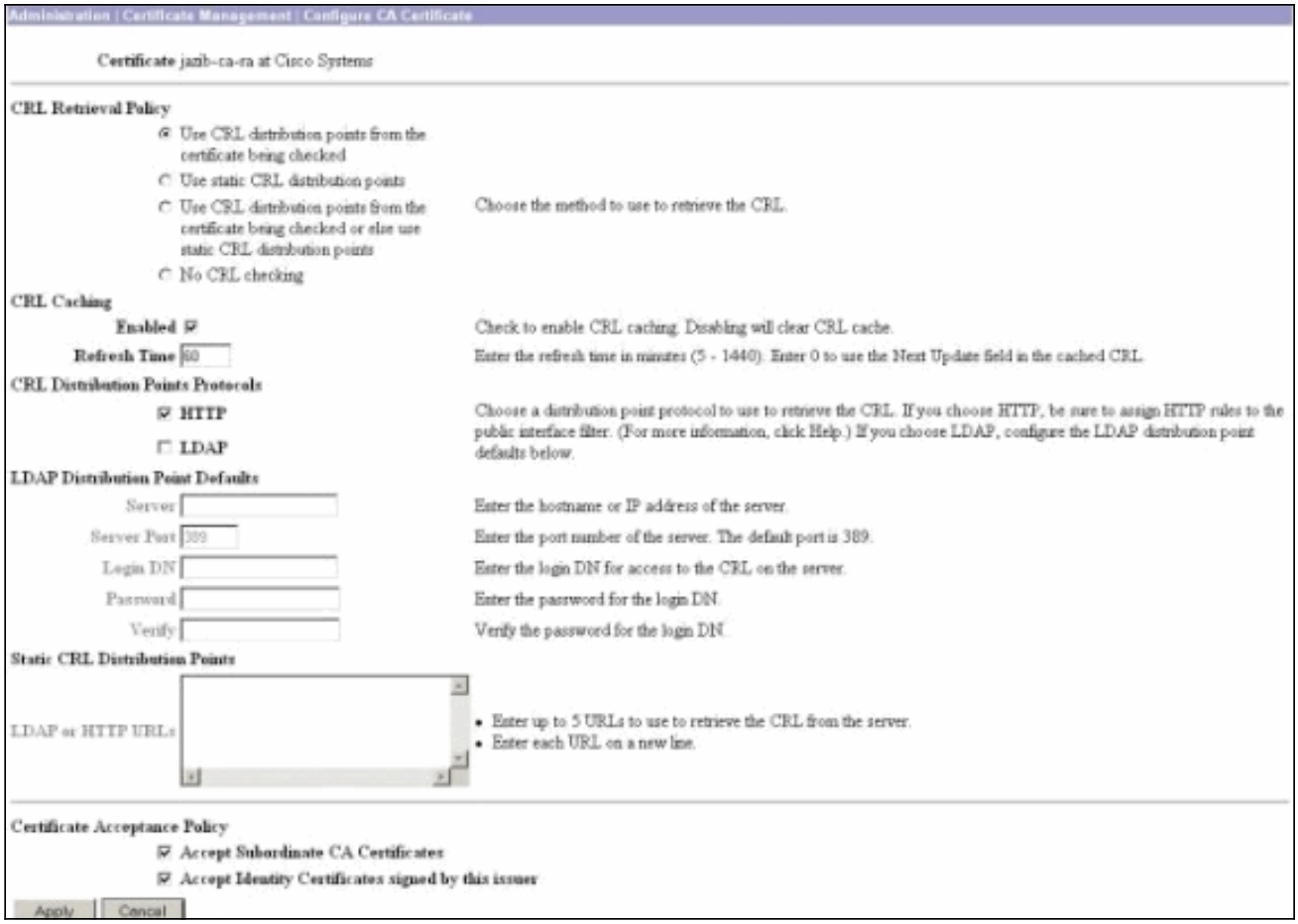



11. 在证书管理下，您应该看到您的身份证书。如果不，检查注册您的更多故障排除的CA服务器。




12. 选择在您的已接收证书的**视图**发现您的证书是否有控制分配点(CDP)。CDP列出从此证书发布者的所有CRL分布点。如果有在您的证书的CDP，并且使用一个DNS名发送查询到CA服务器，请确保您安排DNS服务器定义在您的VPN集中器解决主机名用IP地址。在这种情况下，解决对172.18.124.96的IP地址在DNS服务器的示例CA服务器的主机名是jazib-pc。


13. 单击**配置**在您的CA证书启用在已接收证书的CRL检查。如果有在您的已接收证书的CDP，并且希望使用它，则请选择**从被检查的证书的使用CRL分布点**。因为系统必须从网络分布点获取和检查CRL，启用CRL检查也许减慢系统响应时间。并且，如果网络是慢或拥塞， CRL检查也许发生故障。减轻这些潜在问题的Enable (event) CRL高速缓冲存储。这存储在本地易失性存储器的获取的Crl并且允许VPN集中器迅速验证证书废止状态。当CRL高速缓冲存储启用， VPN集中器首先检查需要的CRL是否在缓存存在并且根据序列号列表在CRL的检查证书的序列号，当需要检查证书的废止状态时。如果找到，证书被认为取消其序列号。VPN集中器从外部服务器获取CRL二者之一，当没在缓存时找到需要的CRL，当被缓存的CRL的有效性周期超时时，或者，当已配置的刷新时间流逝了时。当VPN集中器接收从外部服务器时的新的CRL，更新有新的CRL的缓存。缓存能包含64 Crl。**注意：** CRL缓存在内存存在。所以，重新启动VPN集中器清除CRL缓存。当处理新建对等体验证请求， VPN集中器重新填充有更新Crl的CRL缓存。如果选择**使用静态CRL分布点**，则您在此窗口能使用五静态CRL分布点，如指定。如果选择此选项，您必须输入至少一个URL。您能也选择**从被检查的证书的使用CRL分布点**，或者请选择**使用静态CRL分布点**。如果VPN集中器找不到证书的五CRL分布点，添加静态CRL分布点，至限制五。如果选择此选项，请启用至少一份控制分配点协议。您必须也进入一个(和不大于五)至少静态CRL分布点。如果要禁用CRL检查，请勿选择**CRL检查**。在CRL高速缓冲存储下，请选择**已启用**方框允许VPN集中器缓存获取的Crl。默认不是启用CRL高速缓冲存储。当您禁用CRL高速缓冲存储(请取消选择方框)，清除CRL缓存。如果配置使用从被检查的证书的CRL分布点的CRL检索策略，请选择分布点协议使用获取CRL。在这种情况下选择**HTTP**获取CRL。如果您的CA服务器是往公共接口，请分配HTTP规则到公共接口过滤器。




## 监控

选择**Administration > Certificate Management**并且点击**视图所有CRL缓存**发现您的VPN集中器是否缓存了从CA服务器的任何Crl。

# 验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

## 从集中器的日志

使在VPN集中器的这些事件为了确保， CRL检查工作。

1. 选择**Configuration > System > Events > Classes**设置日志级别。
2. 在类名称下请选择**IKE**、**IKEDBG**、**IPSEC**、**IPSECDBG**或者**CERT**。
3. 单击**添加**或**修改**，并且选择**严重性记录选项1-13**。
4. 请单击**应用，**如果要修改，或者**添加**是否想要添加一个新的条目。

## 成功的集中器日志

如果您的CRL检查是成功的，这些消息在可过滤事件日志被看到。

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl
```

```
1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=615215110000000000086)
```

参考一本成功的集中器日志的完整输出的成功的集中器日志。

### 失败的日志

如果您的在不成功的CRL检查，这些消息在可过滤事件日志被看到。

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

一本失败的集中器日志的完整输出的参考的无效的集中器日志。

参考一本成功的客户端日志的完整输出的成功的客户端日志。

一本失败的客户端日志的完整输出的参考的无效的客户端日志。

## 故障排除

参考在VPN 3000集中器的故障排除连接问题欲知更多故障排除信息。

## 相关信息

- Cisco VPN 3000 系列集中器支持页面
- Cisco VPN 3000 Client 支持页
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems