Cisco VPN 3000コンセントレータでHTTPを使用してCRLチェックを行う

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[ネットワーク図](#)
[VPN 3000 コンセントレータの設定](#)
[手順ごとの説明](#)
[モニタリング](#)
[確認](#)
[コンセントレータからのログ](#)
[正常なコンセントレータ ログ](#)
[失敗したログ](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、HTTP モードを使用して Cisco VPN 3000 コンセントレータにインストールされた認証局（CA）の証明書に関する証明書失効リスト（CRL）のチェック機能をイネーブルにする方法について説明します。

証明書は通常、その有効期間の間は有効であると予想されます。ただし、名前の変更、サブジェクトとCAの関連付けの変更、セキュリティ侵害などの理由で証明書が無効になると、CAは証明書を無効にします。X.509では、CAは署名されたCRLを定期的に発行して証明書を失効させます。ここで、各失効された証明書はシリアル番号で識別されます。CRLチェックを有効にすると、VPNコンセントレータが認証に証明書を使用するたびに、検証される証明書が失効していないことを確認するためにCRLもチェックされます。

CAは、Lightweight Directory Access Protocol(LDAP)/HTTPデータベースを使用してCRLを保存および配布します。また、他の方法を使用する場合もありますが、VPNコンセントレータはLDAP/HTTPアクセスに依存しています。

HTTP CRLチェックは、VPNコンセントレータバージョン3.6以降で導入されています。ただし、LDAPベースのCRLチェックは、以前の3.xリリースで導入されました。このドキュメントでは、HTTPを使用したCRLチェックについてのみ説明します。

注：VPN 3000シリーズコンセントレータのCRLキャッシュサイズはプラットフォームによって異

なり、管理者の希望に従って設定することはできません。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- インターネットキーエクスチェンジ(IKE)認証の証明書を使用して、VPN 3.xハードウェアクライアントからIPsecトンネルを正常に確立しました（CRLチェックは有効になっていません）。
- VPNコンセントレータは、常にCAサーバに接続できます。
- CAサーバがパブリックインターフェイスに接続されている場合は、必要なルールをパブリック（デフォルト）フィルタで開いています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VPN 3000コンセントレータバージョン4.0.1 C
- VPN 3.xハードウェアクライアント
- Windows 2000サーバで実行される証明書の生成とCRLチェック用のMicrosoft CAサーバ。

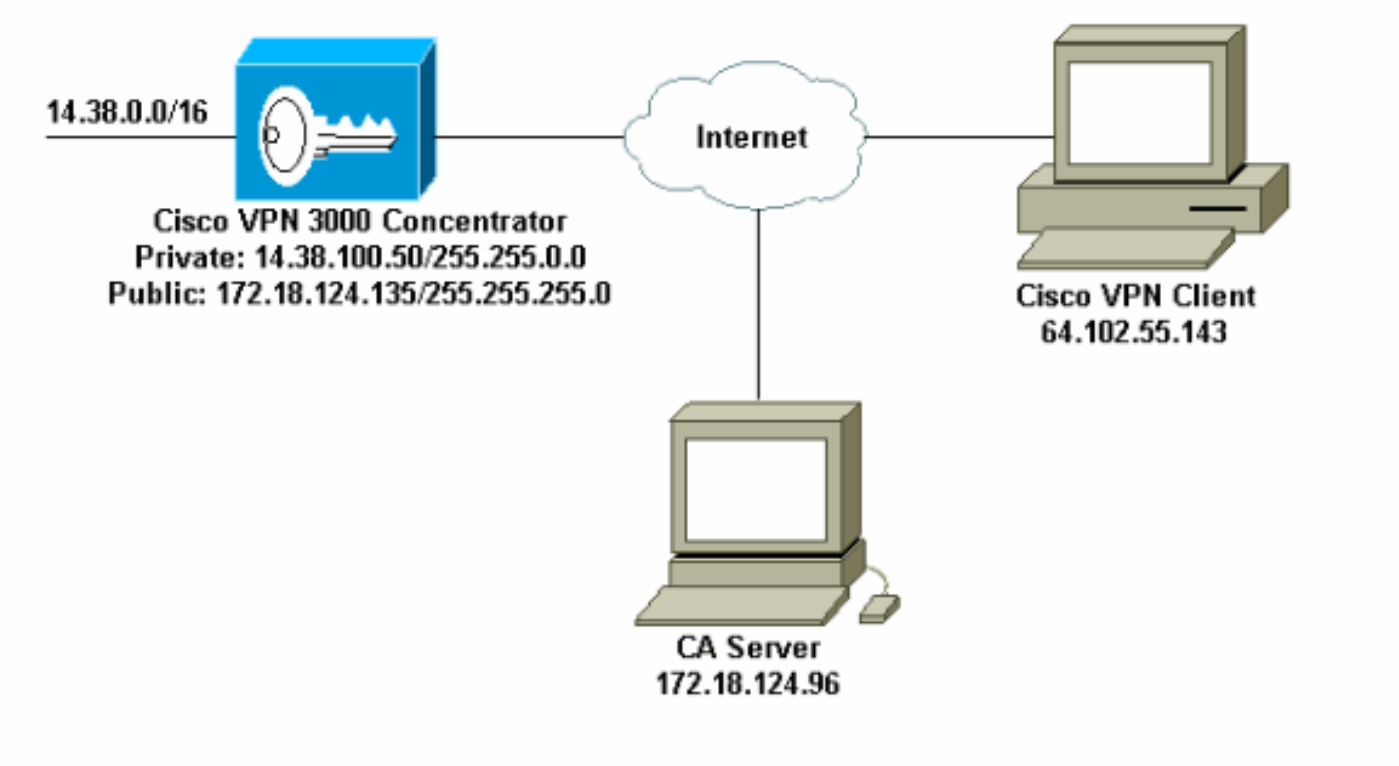
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

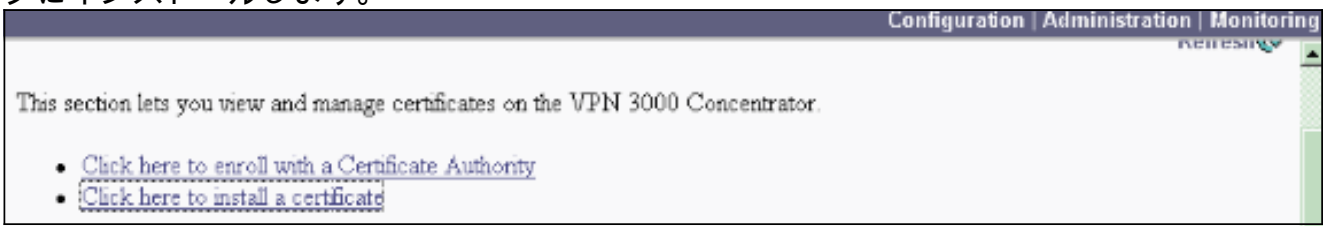


VPN 3000 コンセントレータの設定

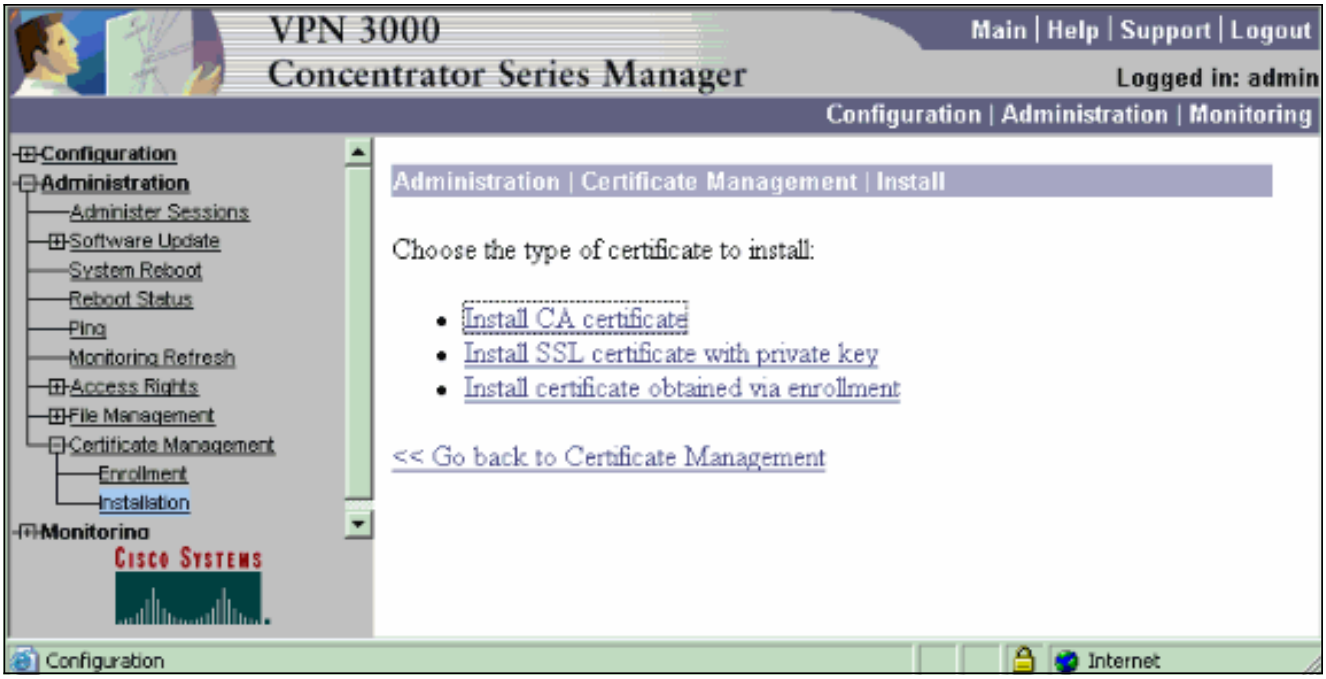
手順ごとの説明

VPN 3000コンセントレータを設定するには、次の手順を実行します。

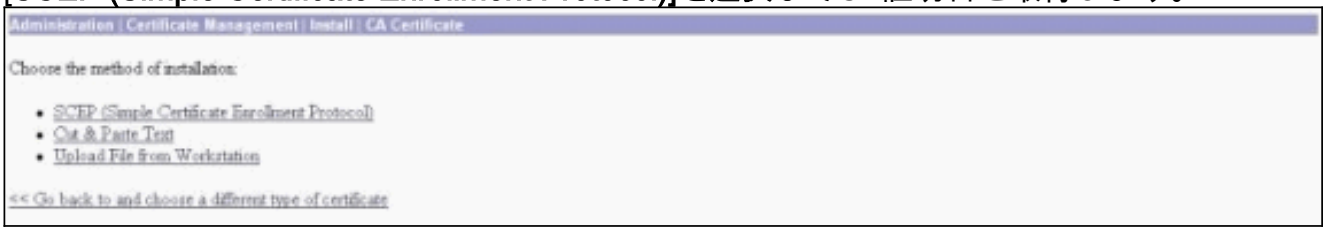
1. 証明書がない場合は、[Administration] > [Certificate Management] を選択して証明書を要求します。[Click here **to install a certificate]を選択して、ルート証明書を**VPNコンセントレータにインストールします。



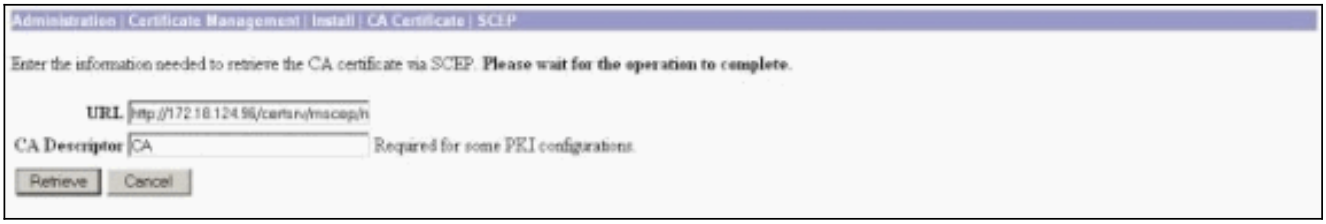
2. **[Install CA certificate]を選択します。**



3. [SCEP (Simple Certificate Enrollment Protocol)]を選択してCA証明書を取得します。

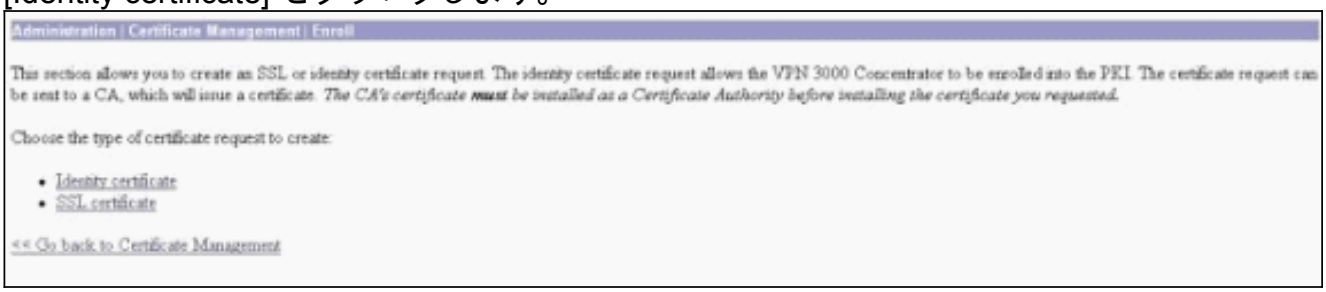


4. [SCEP]ウィンドウで、[URL]ダイアログボックスにCAサーバの完全なURLを入力します。この例では、CAサーバのIPアドレスは172.18.124.96です。この例ではMicrosoftのCAサーバを使用しているため、完全なURLはhttp://172.18.124.96/certsrv/mscep/mscep.dllです。次に、[CA Descriptor]ダイアログボックスに1ワードの記述子を入力します。この例ではCAを使用しています。

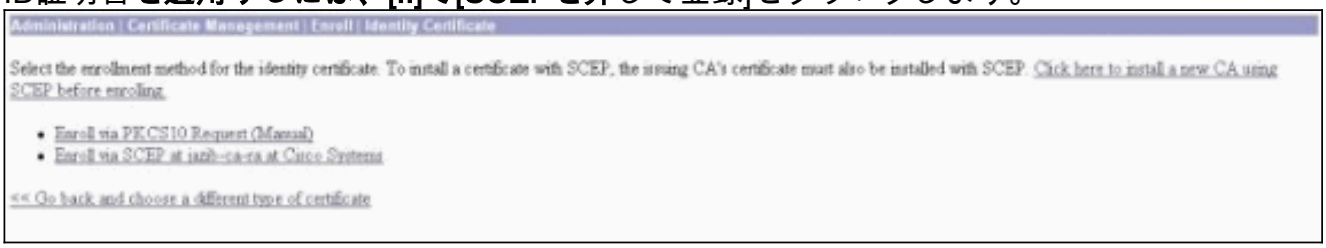


5. [Retrieve] をクリックします。CA証明書が[Administration] > [Certificate Management]ウィンドウに表示されます。証明書が表示されない場合、手順 1 に戻り、手順を繰り返します。

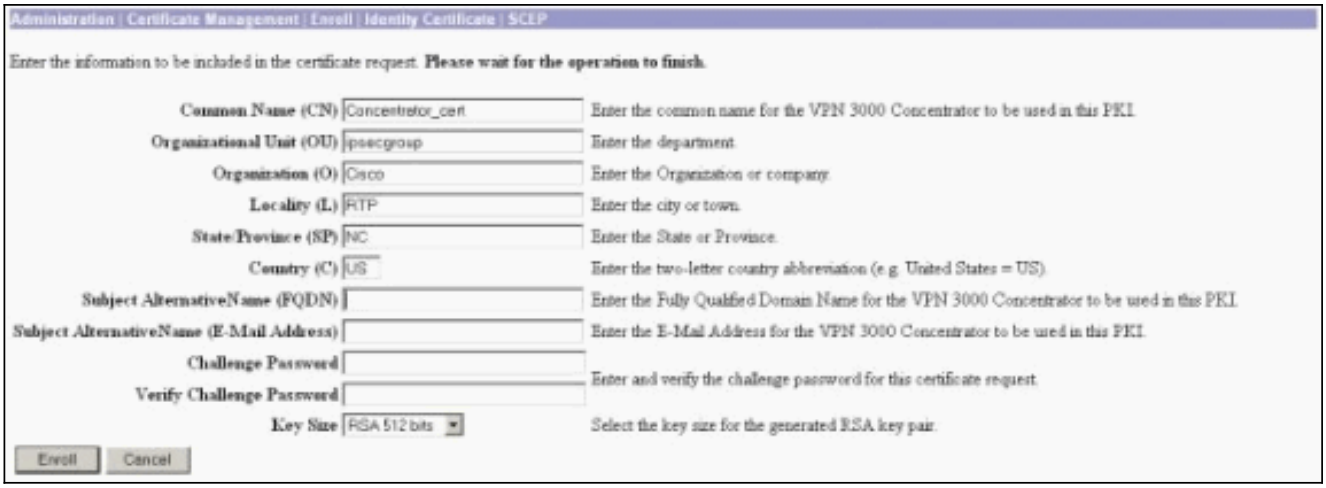
6. CA証明書を取得したら、[Administration] > [Certificate Management] > [Enroll] を選択し、[Identity certificate] をクリックします。



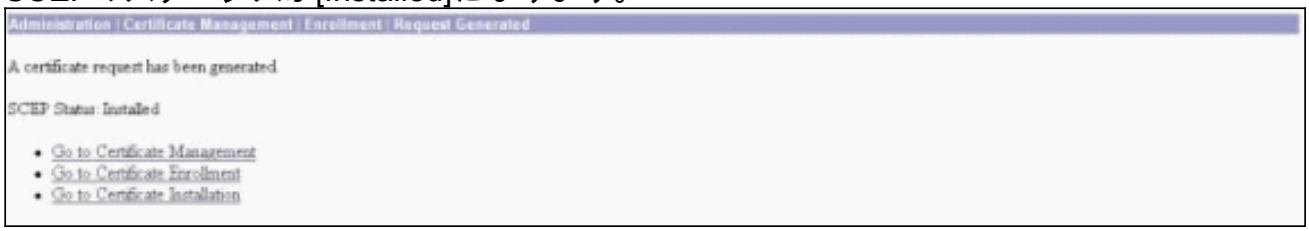
7. ID証明書を適用するには、[..]で[SCEPを介して登録]をクリックします。



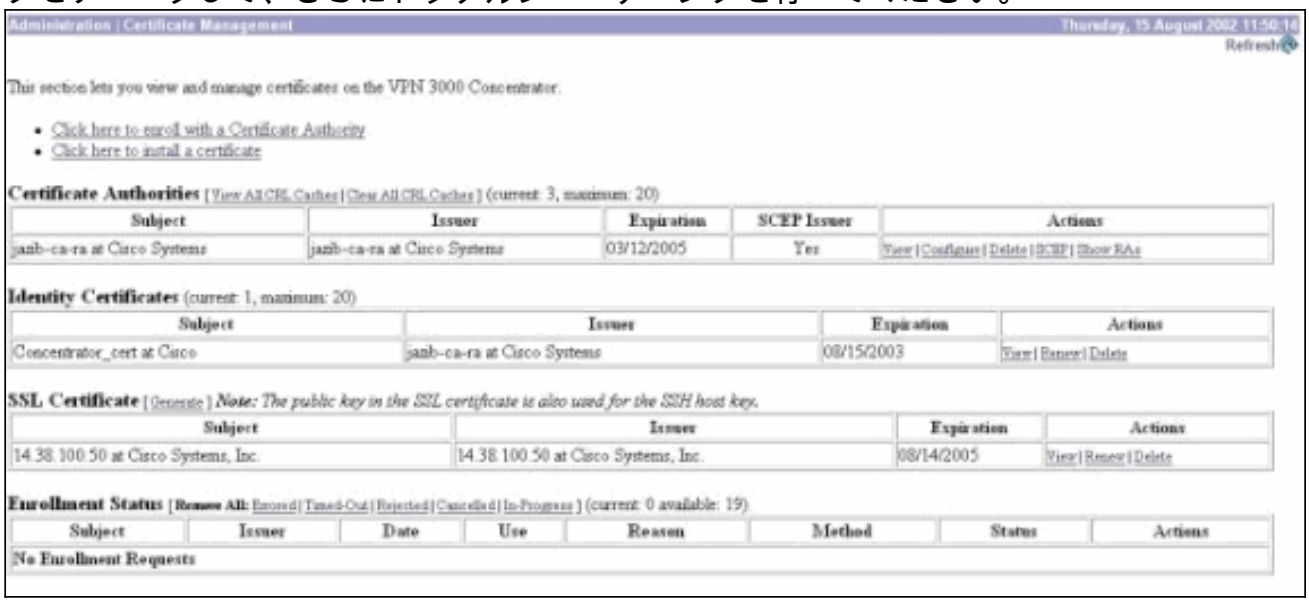
8. 登録フォームに入力するには、次の手順を実行します。Common Name (CN)フィールドに、公開キーインフラストラクチャ(PKI)で使用するVPNコンセントレータの共通名を入力します。[組織単位(OU)]フィールドに部署を入力します。OUは、設定されているIPsecグループ名と一致している必要があります。[組織(O)]フィールドに組織または会社を入力します。[Locality (L)]フィールドに都市または町を入力します。[State/Province (SP)]フィールドに都道府県を入力します。[国(C)]フィールドに国を入力します。PKIで使用するVPNコンセントレータの完全修飾ドメイン名(FQDN)を[Fully Qualified Domain Name (FQDN)]フィールドに入力します。PKIで使用するVPNコンセントレータの電子メールアドレスを[Subject Alternative Name (email Address)]フィールドに入力します。[Challenge Password]フィールドに、証明書要求のチャレンジパスワードを入力します。[Verify Challenge Password]フィールドにチャレンジパスワードを再入力します。[Key Size]ドロップダウンリストから、生成されたRSAキーペアのキーサイズを選択します。



9. [Enroll]を選択し、ポーリング状態のSCEPステータスを表示します。
10. CA サーバに移動し、アイデンティティ証明書を承認します。CAサーバで承認されると、SCEPのステータスが[Installed]になります。

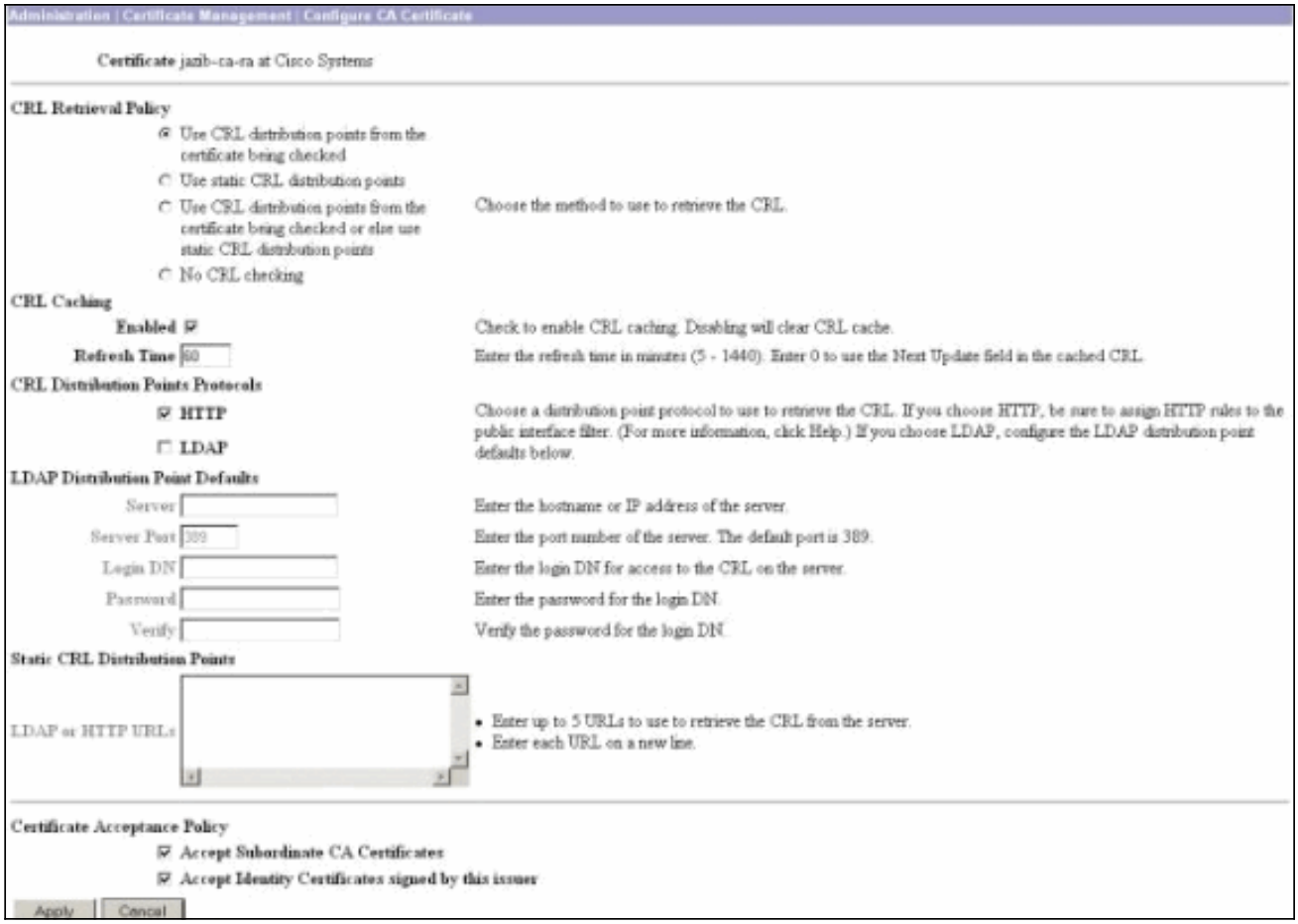


11. [Certificate Management]に、ID証明書が表示されます。そうでない場合は、CAサーバのログをチェックして、さらにトラブルシューティングを行ってください。



12. 受信した証明書の[表示(View)]を選択して、証明書にCRL分散ポイント(CDP)があるかどうかを確認します。CDPは、この証明書の発行者からのすべてのCRL分散ポイントをリストします。証明書にCDPがあり、DNS名を使用してCAサーバにクエリを送信する場合は、VPNコンセントレータでIPアドレスを使用してホスト名を解決するためにDNSサーバが定義されていることを確認します。この場合、CAサーバの例のホスト名はjazib-pcで、DNSサーバのIPアドレス172.18.124.96に解決されます。

13. 受信した証明書のCRLチェックを有効にするには、CA証明書の[**Configure**]をクリックします。受信した証明書にCDPがあり、それを使用する場合は、チェックする証明書から**Use CRL distribution pointsを選択します**。システムはネットワーク分散ポイントからCRLを取得して確認する必要があるため、CRLチェックを有効にすると、システムの応答時間が遅くなる可能性があります。また、ネットワークが低速または輻輳している場合、CRLチェックが失敗する可能性があります。CRLキャッシュを有効にして、これらの潜在的な問題を軽減します。これにより、取得したCRLがローカルの揮発性メモリに保存されるため、VPNコンセントレータは証明書の失効状態をより迅速に確認できます。CRLキャッシュが有効な場合、VPNコンセントレータは最初に必要なCRLがキャッシュに存在するかどうかを確認し、証明書のシリアル番号をCRLのシリアル番号のリストと照合して、証明書の失効状態を確認します。シリアル番号が見つかった場合、証明書は失効したと見なされます。VPNコンセントレータは、キャッシュ内に必要なCRLが見つからない場合、キャッシュされたCRLの有効期間が切れた場合、または設定された更新時間が経過した場合に、外部サーバからCRLを取得します。VPNコンセントレータは、外部サーバから新しいCRLを受信すると、新しいCRLでキャッシュを更新します。キャッシュには最大64のCRLを格納できます。**注：CRLキ**ャッシュはメモリに存在します。したがって、VPNコンセントレータをリブートすると、CRLキャッシュがクリアされます。VPNコンセントレータは、新しいピア認証要求を処理するため、更新されたCRLをCRLキャッシュに再入力します。[静的CRL配布ポイ**ントを使用する]を選択する**と、このウィンドウで指定した静的CRL配布ポイントを最大5つ使用できます。このオプションを選択する場合は、少なくとも1つのURLを入力する必要があります。チェックする証明書か**ら[Use CRL distribution points from the certificate]を選択するか、[Use static CRL distribution points]**を選択する**こともできます**。VPNコンセントレータが証明書内に5つのCRL分散ポイントを見つけることができない場合、スタティックCRL分散ポイントが追加されます。上限は5です。このオプションを選択した場合は、少なくとも1つのCRL Distribution Point Protocol(DSCP)を有効にします。また、少なくとも1つ（および5つ以下の）静的CRL分散ポイントを入力する必要があります。CRLチェッ**クを無効にする**場合は、[CRLチェックなし]を選択します。[CRL Caching]で[**Enabled**]ボックスを選択し、取得したCRLをVPNコンセントレータでキャッシュできるようにします。デフォルトでは、CRLキャッシュは有効になりません。CRLキャッシュを無効にすると（ボックスの選択を解除すると）、CRLキャッシュがクリアされます。チェックする証明書からCRL分散ポイントを使用するCRL取得ポリシーを設定した場合は、CRLの取得に使用する分散ポイントプロトコルを選択します。この場合**はHTTP**を選択してCRLを取得します。CAサーバがパブリックインターフェイスに向いている場合は、HTTPルールをパブリックインターフェイスフィルタに割り当てます。



モニタリング

[Administration] > [Certificate Management] を選択し、[View All CRL caches] をクリックして、VPNコンセントレータがCAサーバからCRLをキャッシュしたかどうかを確認します。

確認

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

コンセントレータからのログ

CRLチェックが機能することを確認するには、VPNコンセントレータでこれらのイベントを有効にします。

1. [Configuration] > [System] > [Events] > [Classes] の順に選択して、ロギングレベルを設定します。
2. [Class Name]で、[IKE]、[IKEDBG]、[IPSEC]、[IPSECDBG]、または[CERT]を選択します。
3. [Add] または[Modify] をクリックし、[Severity to Log]オプション1-13を選択します。
4. 変更する場合は[適用]をクリックし、新しいエントリを追加する場合は[追加]をクリックします。

正常なコンセントレータ ログ

CRLチェックが成功すると、これらのメッセージがフィルタ可能イベントログに表示されます。

```
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=61521511000000000086)
```

正常なコンセントレータログの完全な出力については、『正常なコンセントレータログ』を参照してください。

失敗したログ

CRLのチェックインが失敗した場合、これらのメッセージはフィルタ可能イベントログに表示されます。

```
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.
```

失敗したコンセントレータログの完全な出力については、『失効したコンセントレータログ』を参照してください。

成功したクライアントログの完全な出力については、「成功したクライアントログ」を参照してください。

失敗したクライアントログの完全な出力については、「取り消されたクライアントログ」を参照してください。

トラブルシュート

トラブルシューティングの詳細は、『VPN 3000コンセントレータの接続に関する問題のトラブルシューティング』を参照してください。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 クライアントに関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems