Cisco Secure ACS for Windows の RADIUS 認証を使用した VPN 3000 コンセントレータの PPTP の設定

内容

概要

Cisco VPN 3000 コンセントレータは、ネイティブの Windows クライアントに対して Point-to-Point Tunnel Protocol（PPTP）トンネリングをサポートしています。このコンセントレータは、保護された信頼性のある接続のために 40 ビットと 128 ビットの暗号化をサポートしています。このドキュメントでは、RADIUS 認証のために Cisco Secure ACS for Windows で VPN 3000 コンセントレータ上に PPTP を設定する方法について説明します。

PIX への PPTP 接続の設定方法についての詳細は、『PPTP を使用するための Cisco Secure PIX Firewall の設定方法』を参照してください。

ルータへの PC 接続を設定する方法についての詳細は、『Cisco Secure ACS for Windows とルータの PPTP 認証の設定』を参照してください。ここでは、Cisco Secure Access Control System（ACS）3.2 for Windows サーバへのユーザ認証を提供してから、ユーザにネットワークへの参加を許可します。

はじめに

表記法

ドキュメント表記の詳細は、『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。

前提条件

このドキュメントでは、Cisco Secure ACS for Windows RADIUS 認証を追加する前に、ローカル PPTP 認証が動作していることを前提としています。ローカル PPTP 認証の詳細は、『ローカル認証での VPN 3000 Concentrator PPTP の設定方法』を参照してください。要件と制限事項の詳細なリストは、『Cisco VPN 3000 コンセントレータで PPTP 暗号化がサポートされる条件』を参照してください。

使用するコンポーネント

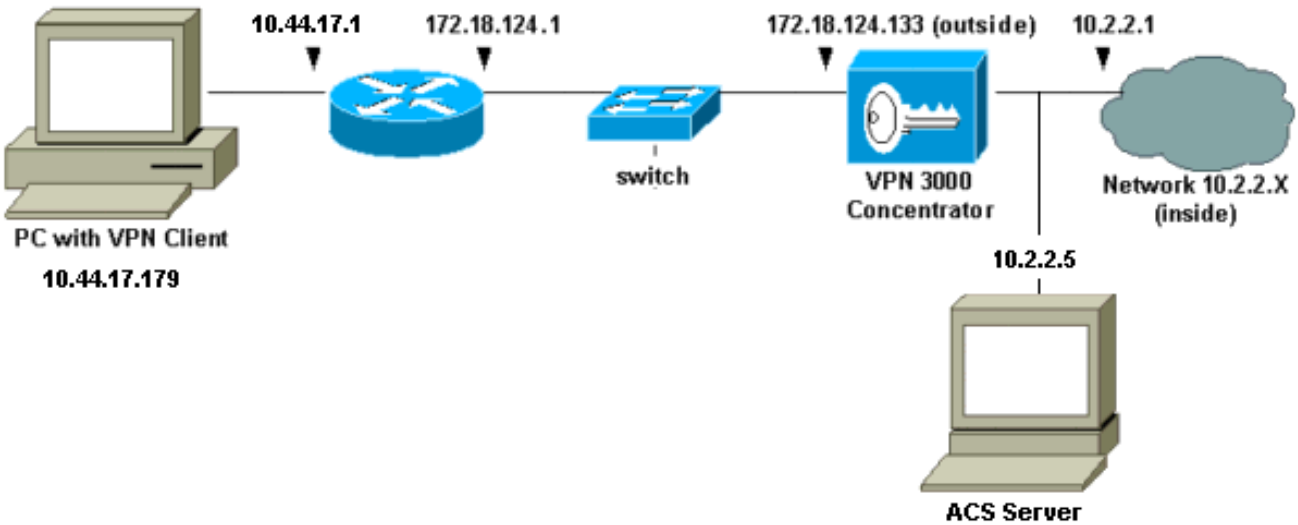
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS for Windows バージョン 2.5 以降
- VPN 3000 コンセントレータ バージョン 2.5.2.C 以降 (この設定はバージョン 4.0.x で確認されています)

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

ネットワーク図

このドキュメントでは次の図に示すネットワーク構成を使用しています。



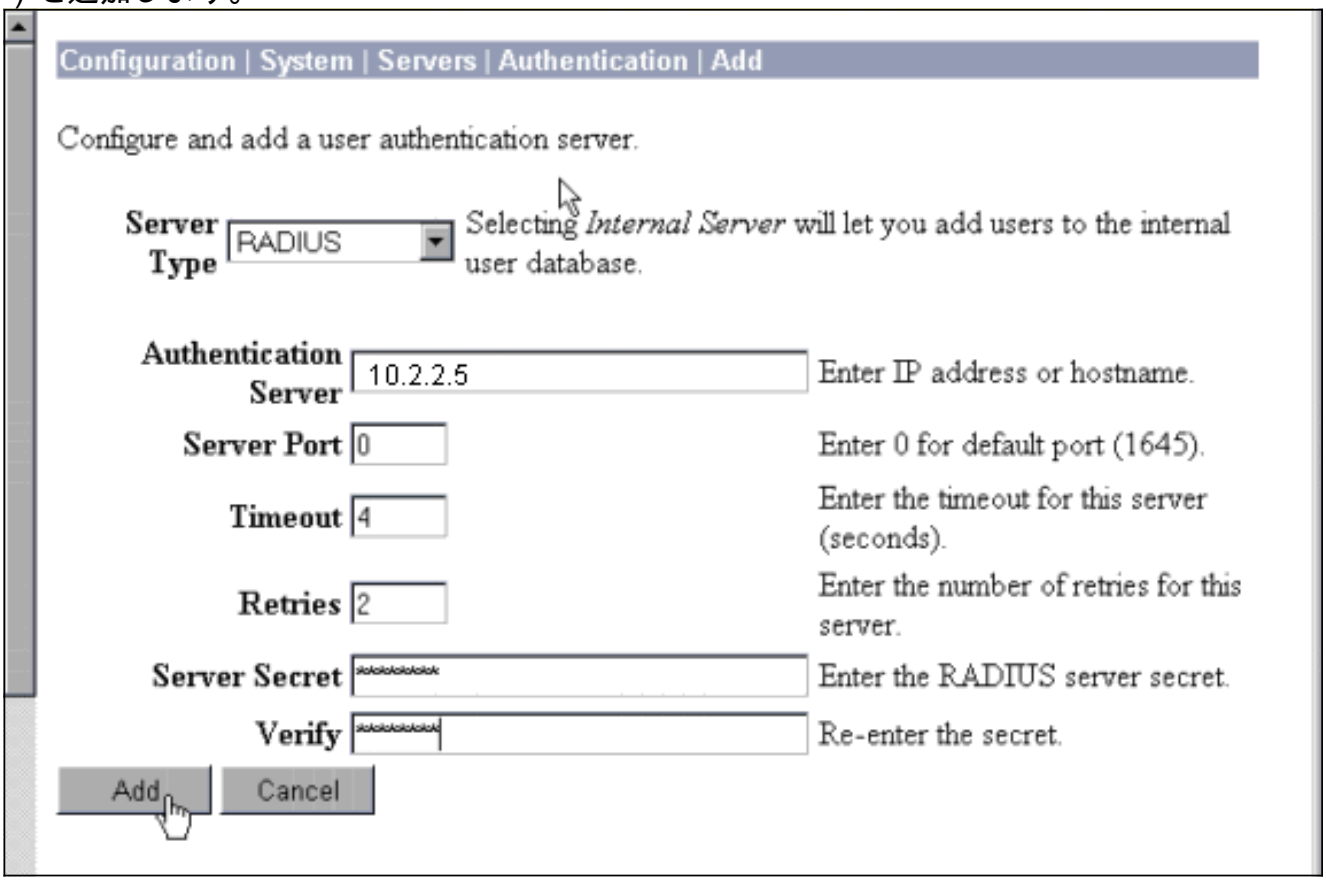
VPN 3000 コンセントレータの設定

Cisco Secure ACS for Windows の追加と設定

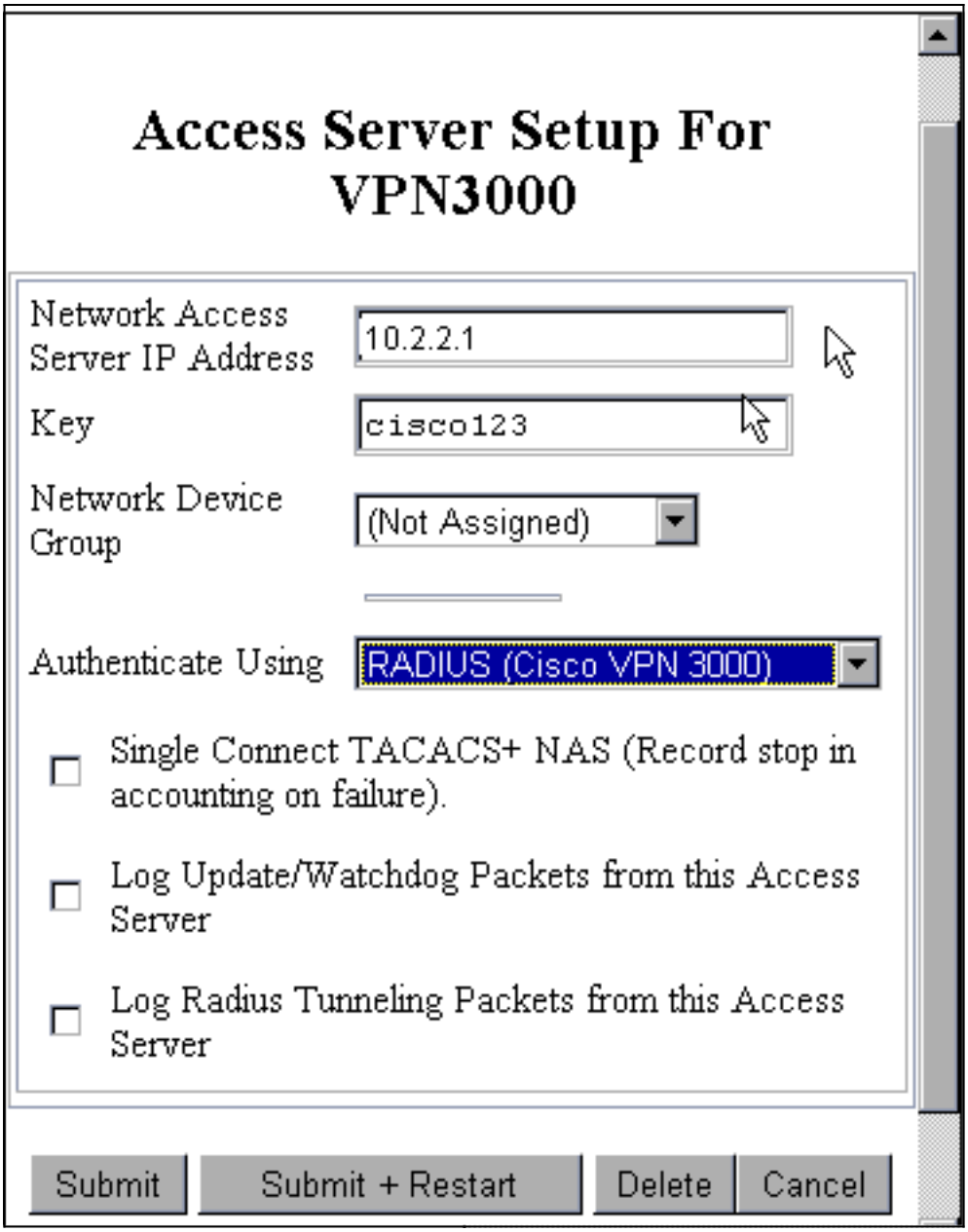
Cisco Secure ACS for Windows を使用するには、次のステップに従って VPN コンセントレータ

を設定します。

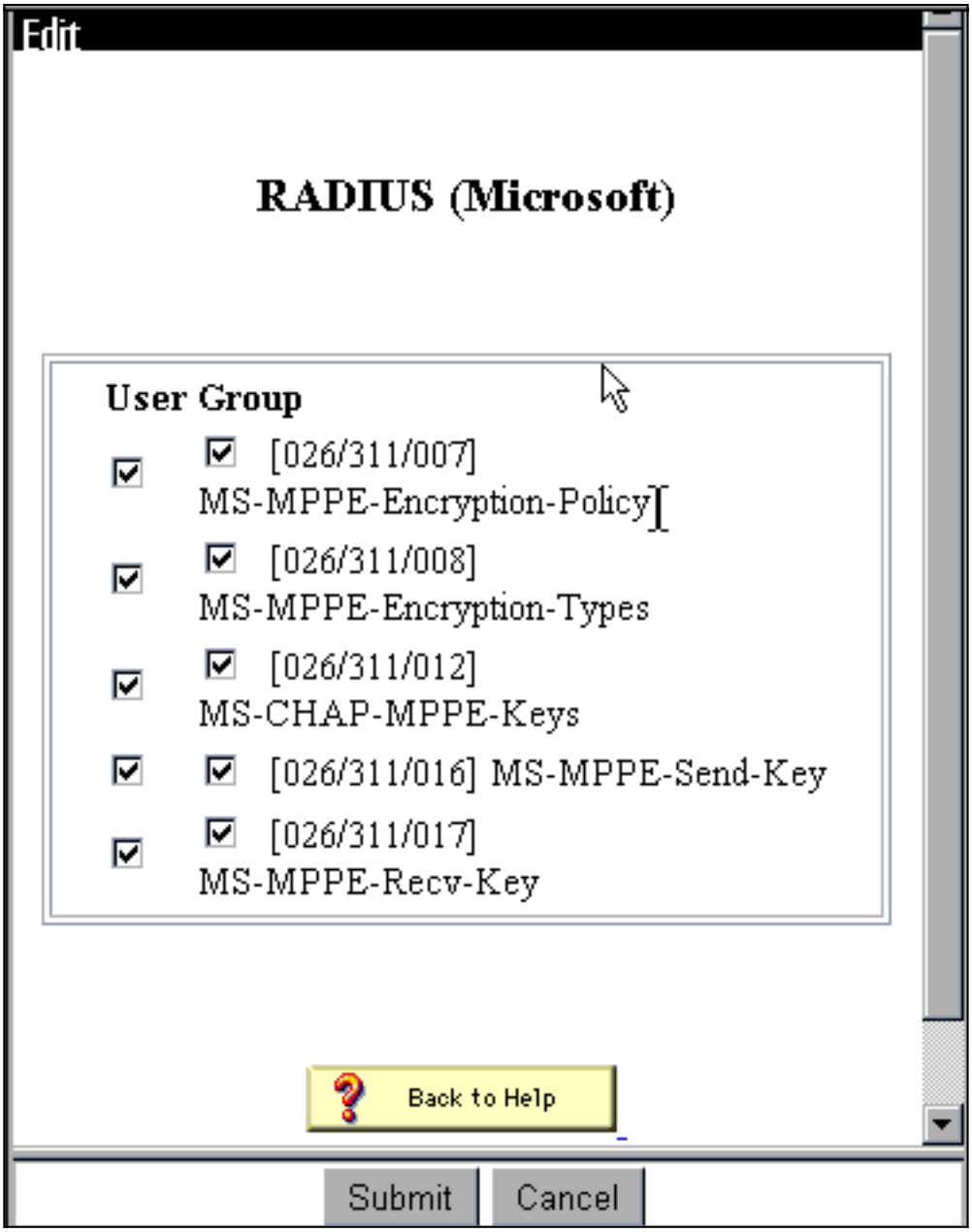
1. VPN 3000コンセントレータで、**[Configuration] > [System] > [Servers] > [Authentication Servers]に移動**し、Cisco Secure ACS for Windowsサーバとキー（この例では「cisco123」）を追加します。



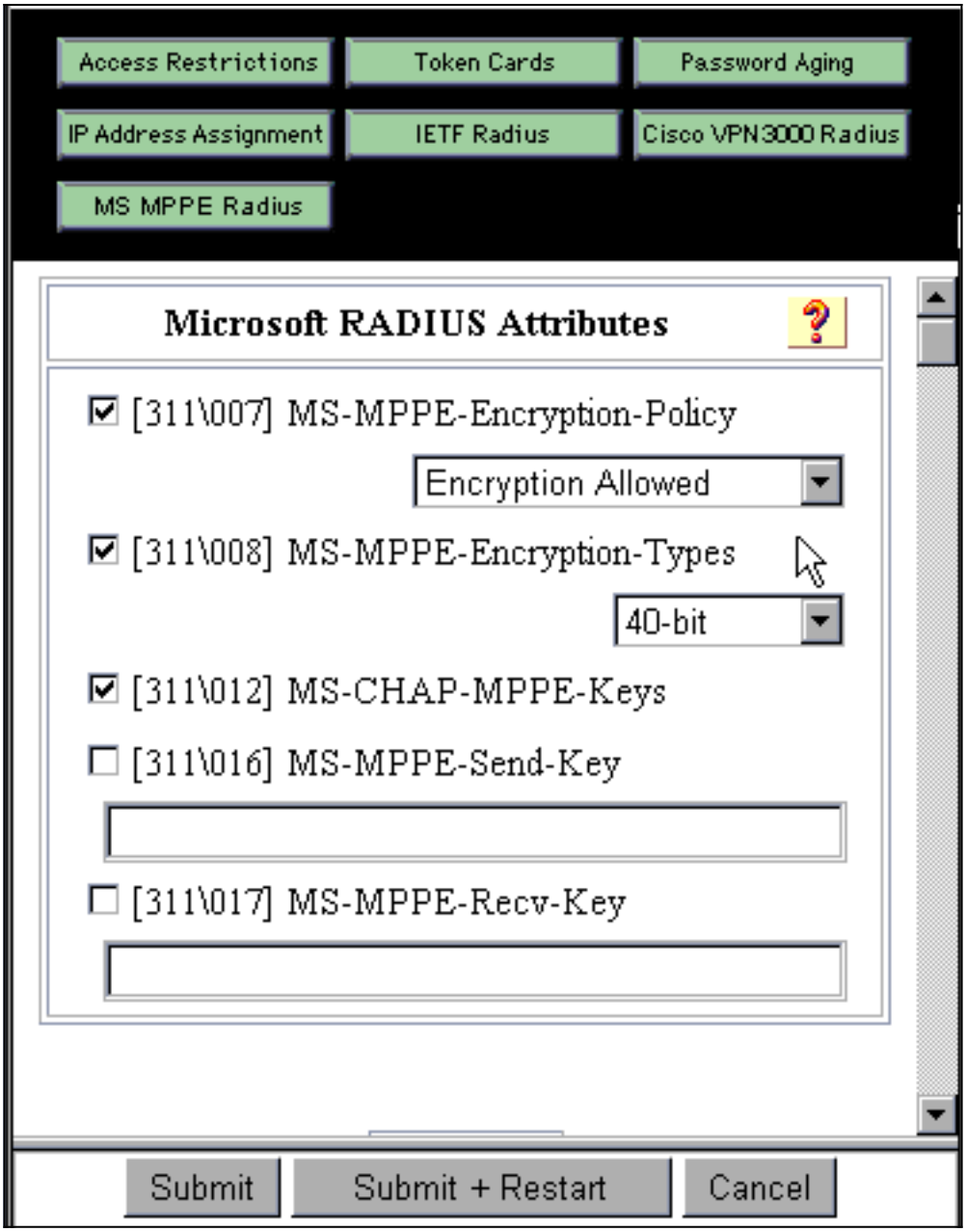
2. Cisco Secure ACS for Windows で、ACS サーバのネットワーク設定に VPN コンセントレータを追加し、辞書タイプを特定します。



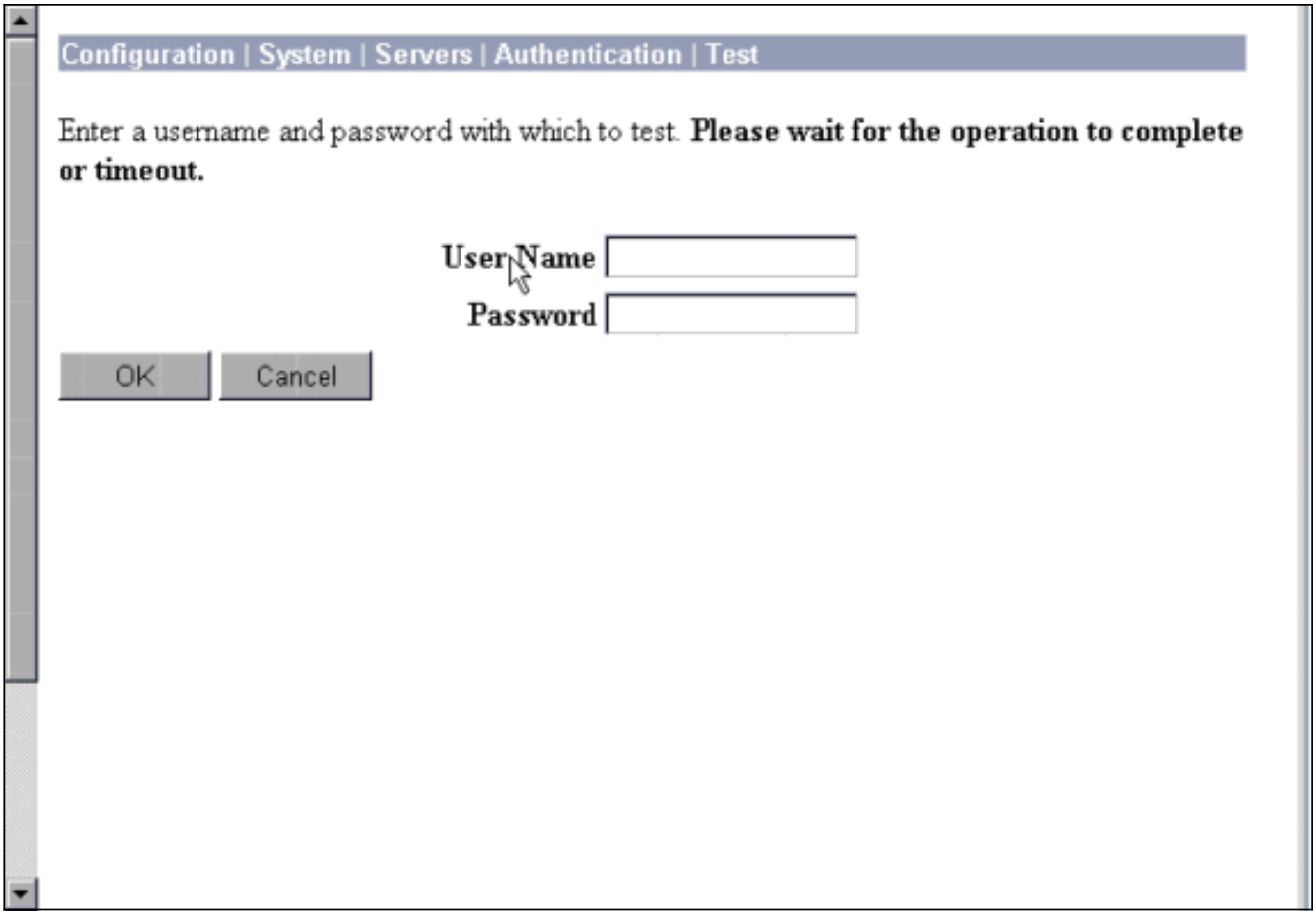
3. Cisco Secure ACS for Windows で、属性がグループ インターフェイスで表示されるように、[Interface Configuration] > [RADIUS (Microsoft)] の順に選択し、[Microsoft Point-to-Point Encryption (MPPE)] 属性にチェックマークを付けます。



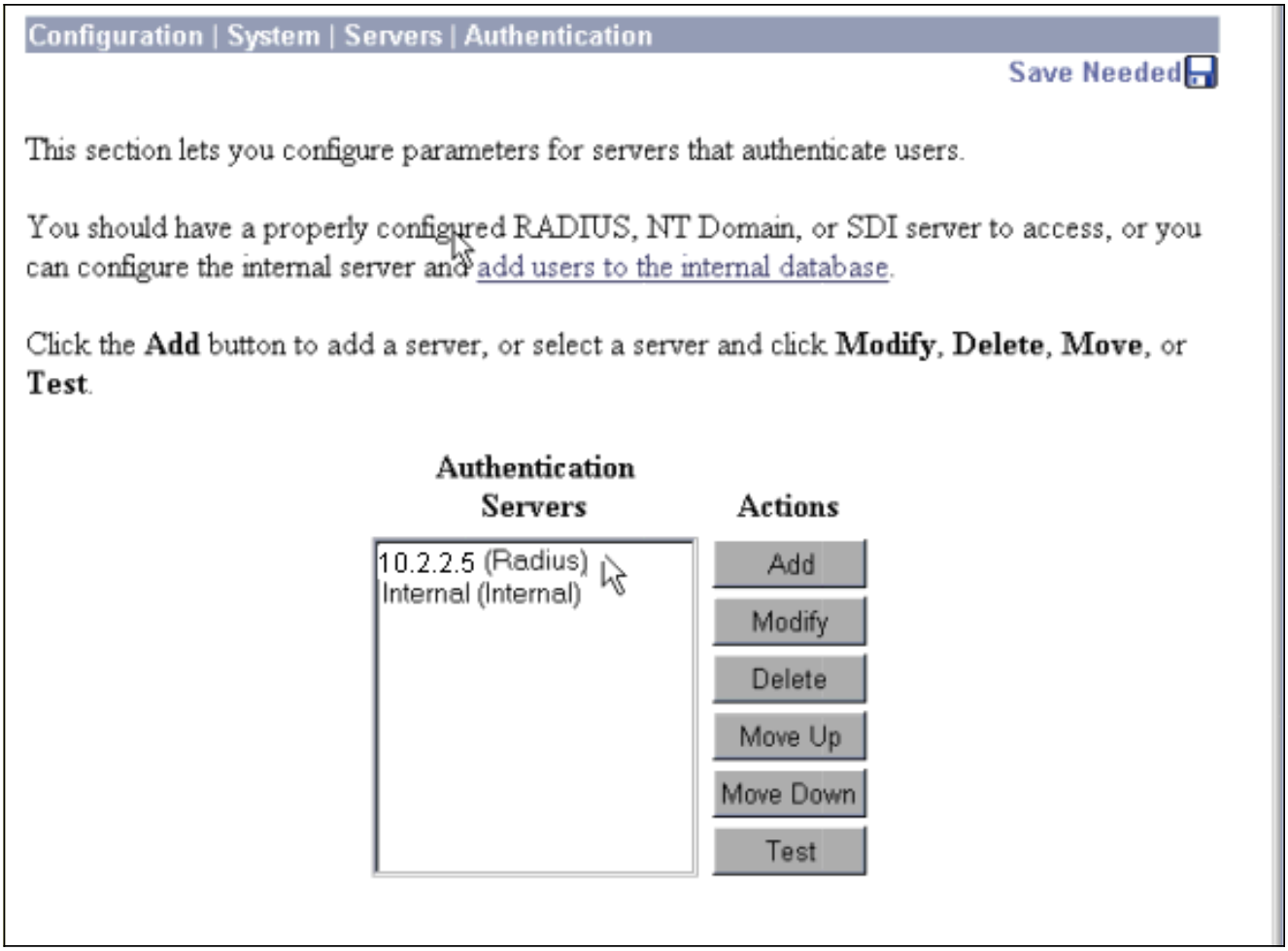
4. Cisco Secure ACS for Windows でユーザを追加します。ユーザのグループで、後で暗号化が必要になる場合のために MPPE（Microsoft RADIUS）属性を追加します。



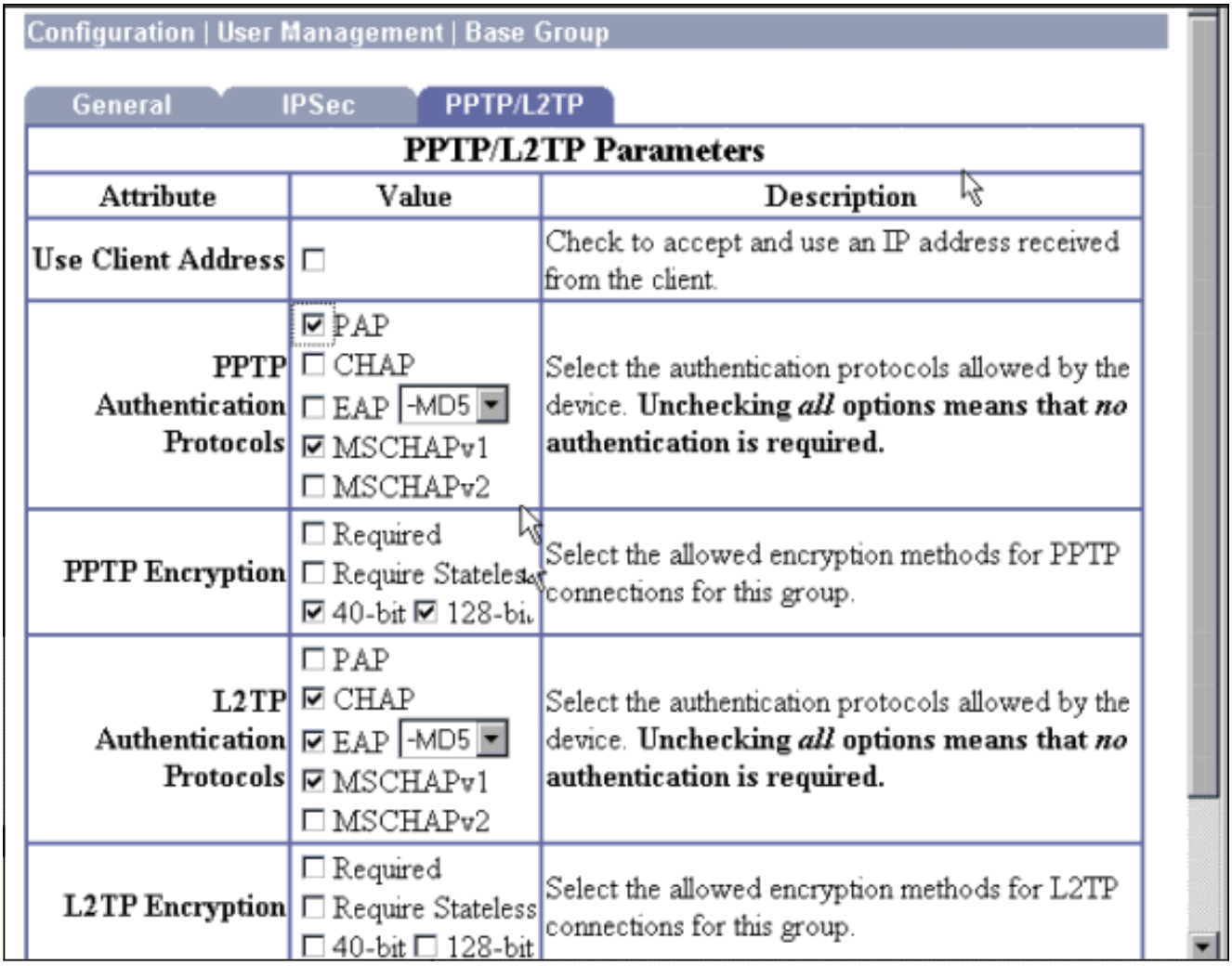
5. VPN 3000 コンセントレータで、[Configuration] > [System] > [Servers] > [Authentication Servers] を順に選択します。リストから認証サーバを選択して、[Test] を選択します。ユーザ名とパスワードを入力することで、VPN コンセントレータから Cisco Secure ACS for Windows サーバへの認証をテストします。正常な認証が行われると、VPN コンセントレータは「Authentication Successful」メッセージを表示します。Cisco Secure ACS for Windows での障害は、[Reports and Activity] > [Failed Attempts] に記録されます。デフォルトのインストール環境では、これらのレポートはディスクの C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts に格納されます。



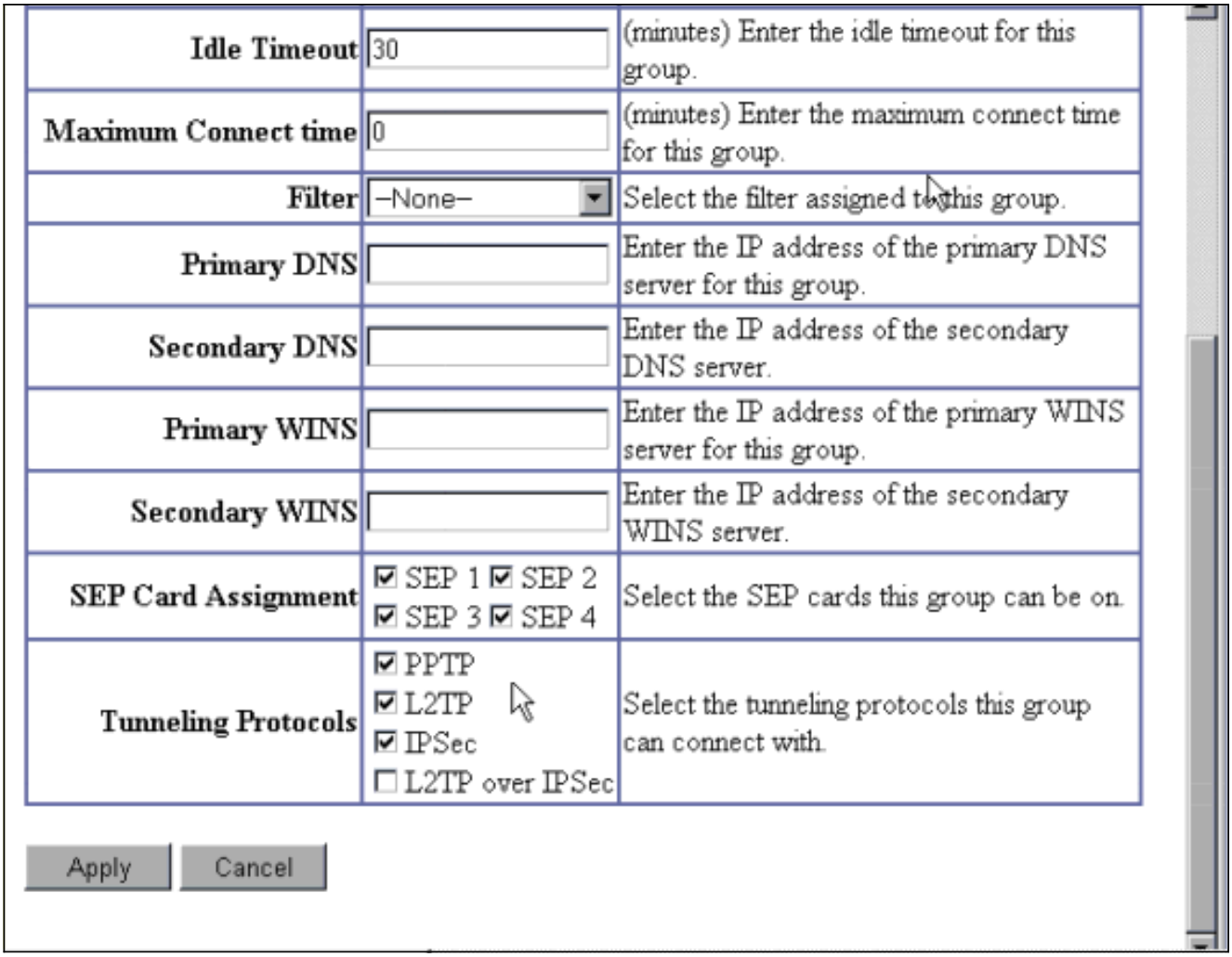
6. PC から VPN コンセントレータへの認証動作と、コンセントレータから Cisco Secure ACS for Windows サーバへの認証を確認したので、Cisco Secure ACS for Windows サーバをサーバ リストの先頭に移動することで、VPN コンセントレータを再設定して PPTP ユーザを Cisco Secure ACS for Windows RADIUS に送信できます。VPN コンセントレータでこれを実行するには、[Configuration] > [System] > [Servers] > [Authentication Servers] を順に選択します。



7. [Configuration] > [User Management] > [Base Group] を順に選択して、[PPTP/L2TP] タブを選択します。VPN コンセントレータのベース グループで、PAP と MSCHAPv1 のオプションがイネーブルになっていることを確認します。



8. [General] タブを選択して、PPTP が [Tunneling Protocols] セクションで許可されていることを確認します。

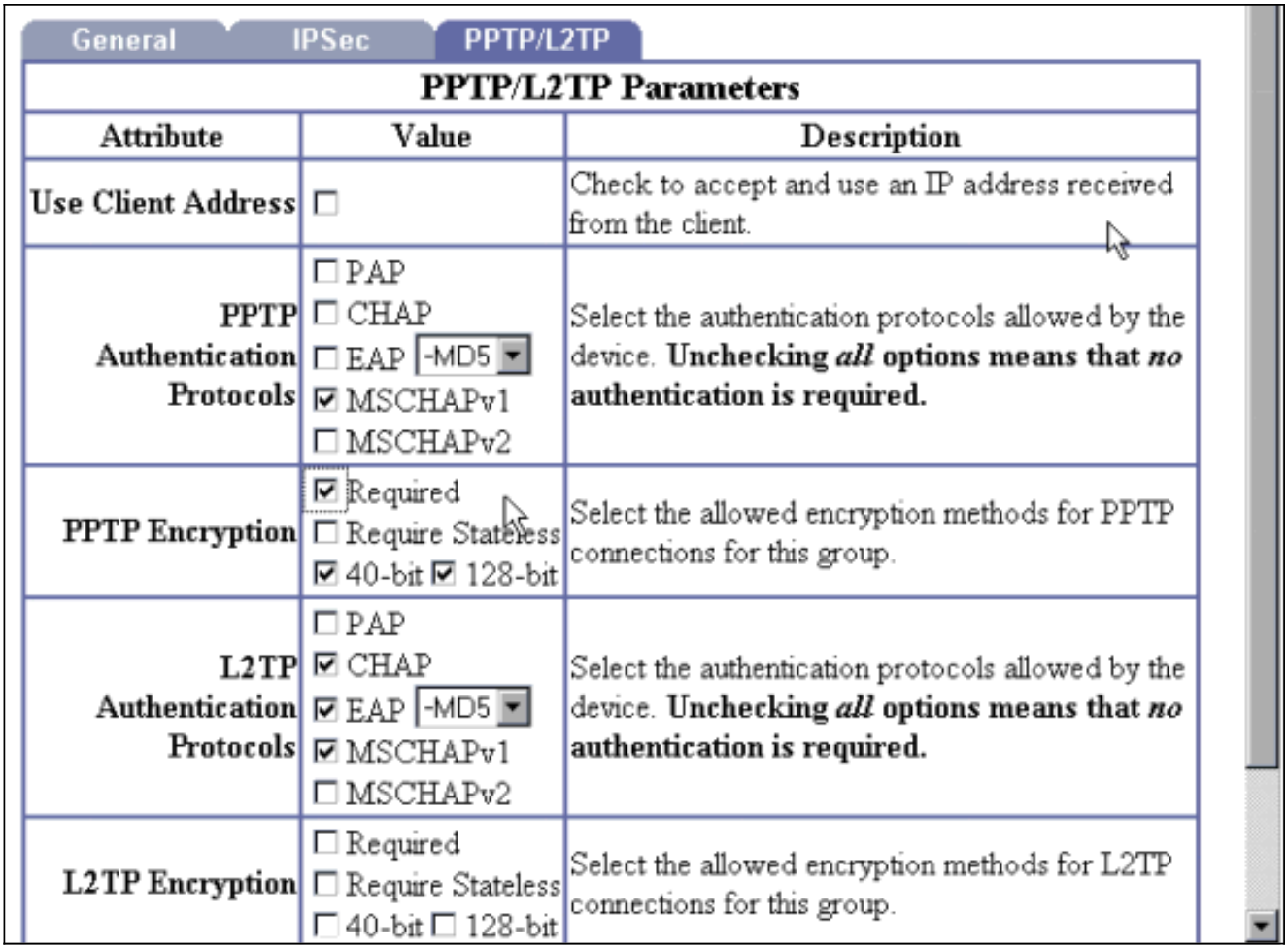


9. PPTP 認証を、Cisco Secure ACS for Windows RADIUS サーバのユーザでテストします。これが動作しない場合は、「デバッグ」セクションを参照してください。

MPPE（暗号化）の追加

暗号化のない状態で Cisco Secure ACS for Windows RADIUS PPTP 認証が動作する場合、VPN 3000 コンセントレータに MPPE を追加できます。

1. VPN コンセントレータで、[Configuration] > [User Management] > [Base Group] を順に選択します。
2. [PPTP Encryption]のセクションで、[**Required**]、[**40-bit**]、および[**128-bit**]のオプションをオンにします。すべての PC が 40 ビットと 128 ビットの暗号化の両方をサポートするわけではないので、ネゴシエーションを許可するように両方のオプションにチェックマークを付けます。
3. [PPTP Authentication Protocols] のセクションの下で、[MSCHAPv1] 用オプションのチェックマークを付けます（以前のステップで暗号化用の Cisco Secure ACS for Windows 2.5 ユーザ属性をすでに設定しています）。



General | IPSec | PPTP/L2TP

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	☐	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☐ PAP ☐ CHAP ☐ EAP -MD5 ☑ MSCHAPv1 ☐ MSCHAPv2	Select the authentication protocols allowed by the device. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☑ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	☐ PAP ☑ CHAP ☑ EAP -MD5 ☑ MSCHAPv1 ☐ MSCHAPv2	Select the authentication protocols allowed by the device. **Unchecking *all* options means that *no* authentication is required.**
L2TP Encryption	☐ Required ☐ Require Stateless ☐ 40-bit ☐ 128-bit	Select the allowed encryption methods for L2TP connections for this group.

注：PPTPクライアントは、最適または必要なデータ暗号化とMSCHAPv1（オプションの場合）を認識する必要があります。

アカウンティングの追加

認証を確立した後は、VPN コンセントレータにアカウンティングを追加できます。[Configuration] > [System] > [Servers] > [Accounting Servers] を順に選択して、Cisco Secure ACS for Windows サーバを追加します。

Cisco Secure ACS for Windows で、アカウンティング記録は次のように表示されます。

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
   Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
   Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
   PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
   PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

確認

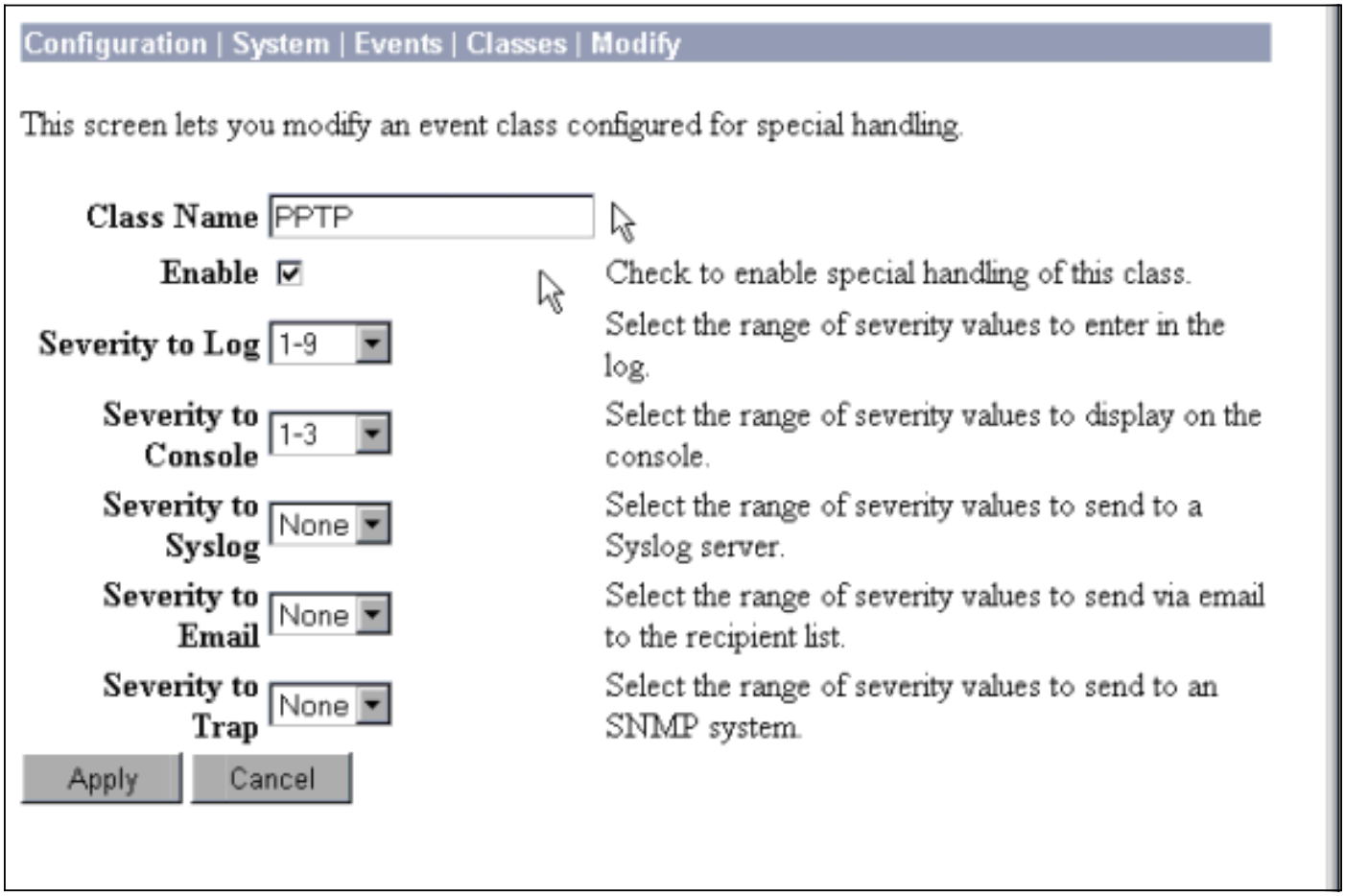
現在、この設定に使用できる確認手順はありません。

トラブルシュート

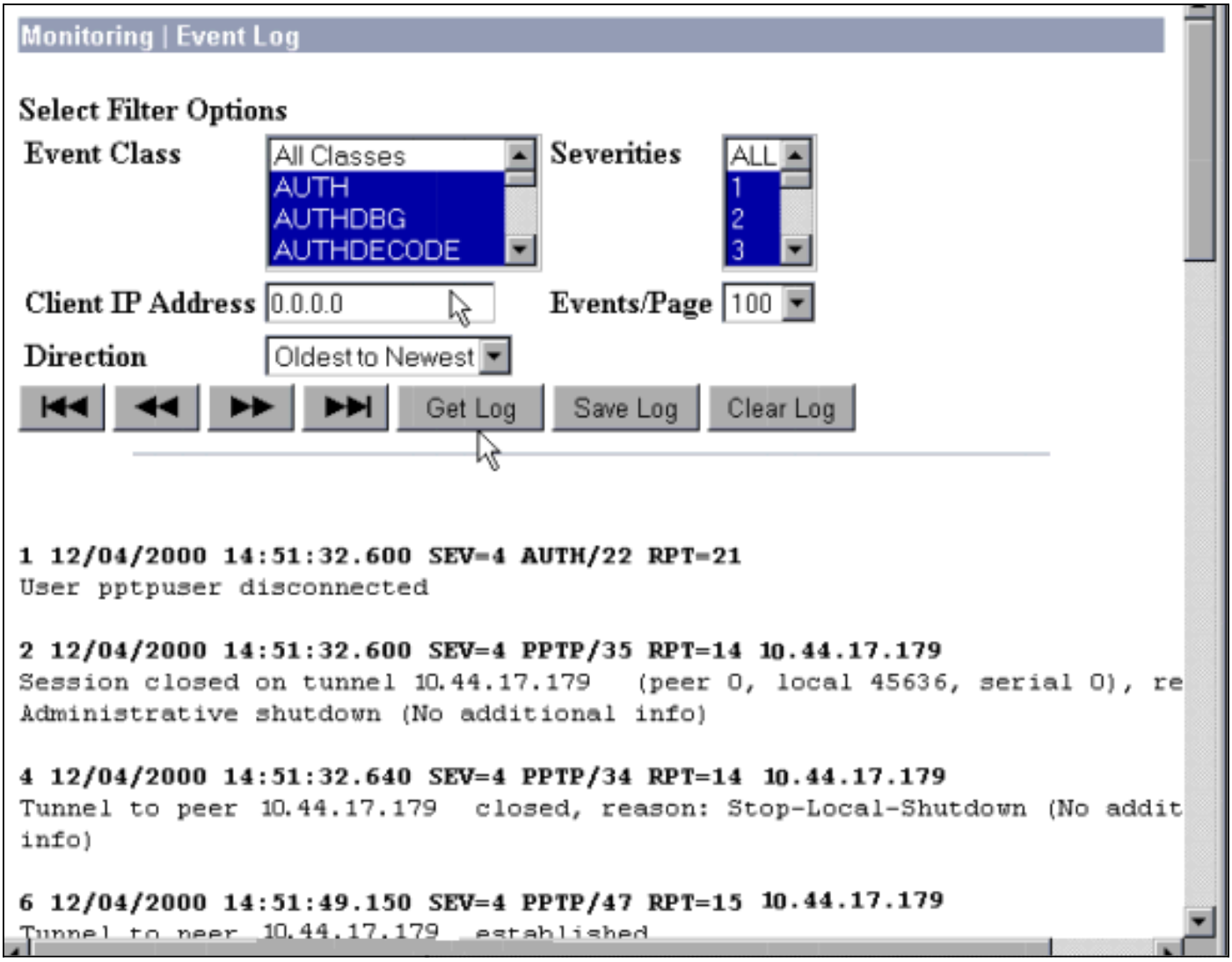
ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバッグのイネーブル

接続が動作しない場合、[Configuration] > [System] > [Events] > [Classes] > [Modify] に順に移動することで、VPN コンセントレータに PPTP と AUTH のイベント クラスを追加できます。PPTPDBG、PPTPDECODE、AUTHDBG、AUTHDECODE のイベント クラスも追加できますが、これらのオプションは過剰な情報を提供する可能性があります。



イベント ログは、[Monitoring] > [Event Log] を選択することで取得できます。



デバッグ：良好な認証

VPN コンセントレータに対する良好なデバッグは、次のようなものです。

```
1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected
```

発生する可能性のあるエラー

次のようなエラーを検出する可能性があります。

Cisco Secure ACS for Windows RADIUS サーバのユーザ名またはパスワードが不良

- VPN 3000 コンセントレータ デバッグ出力

```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established

7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179

8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23

9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser

11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )

12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```

- Cisco Secure ACS for Windows ログ出力

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

- ユーザに表示されるメッセージ（Windows 98 から）

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

[MPPE Encryption Required] がコンセントレータで選択されても、Cisco Secure ACS for Windows サーバは MS-CHAP-MPPE-Keys や MS-CHAP-MPPE-Types に設定されない

- VPN 3000 コンセントレータ デバッグ出力AUTHDECODE（1 ~ 13 の重大度）と PPTP デバッグ（1 ~ 9 の重大度）がオンになっている場合、ログは Cisco Secure ACS for Windows サーバがベンダ固有の属性 26（0x1A）をサーバからの access-accept （部分的なログ）に送信していないことを示しています。

```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE     .N.,..u.l6Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C     m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF                 ../.........

2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```

- Cisco Secure ACS for Windows ログ出力は障害を表示していません。
- ユーザに表示されるメッセージ

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

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 シリーズ クライアントに関するサポート ページ
- IPSec に関するサポート ページ
- Cisco Secure ACS for Windows に関するサポート ページ
- RADIUS に関するサポート ページ

- PPTP に関するサポート ページ
- RFC 2637:Point-to-Point Tunneling Protocol（PPTP）
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems