

Microsoft RADIUS での Cisco VPN 3000 コンセントレータの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[Windows 2000およびWindows 2003でのRADIUSサーバのインストールと設定](#)

[RADIUSサーバのインストール](#)

[IASを使用したMicrosoft Windows 2000 Serverの設定](#)

[IASを使用したMicrosoft Windows 2003 Serverの設定](#)

[RADIUS認証用のCisco VPN 3000コンセントレータの設定](#)

[確認](#)

[トラブルシューティング](#)

[WebVPN 認証の失敗](#)

[Active Directoryに対するユーザ認証の失敗](#)

[関連情報](#)

概要

Microsoft Internet Authentication Server (IAS) と Microsoft Commercial Internet System (MCIS 2.0) が現在利用できます。Microsoft RADIUSサーバは、ユーザデータベースにプライマリドメインコントローラのActive Directoryを使用するため、便利です。個別のデータベースを維持する必要がありません。また、ポイントツーポイントトンネリングプロトコル (PPTP) VPN 接続用に 40 ビットおよび 128 ビットの暗号化をサポートしています。[Microsoft](#)のチェックリストを参照してください。[ダイヤルアップとVPNアクセス用のIASの設定に関するドキュメントを参照してください。](#)

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

Windows 2000およびWindows 2003でのRADIUSサーバのインストールと設定

RADIUSサーバのインストール

RADIUSサーバ(IAS)がインストールされていない場合は、次の手順を実行してインストールします。RADIUSサーバがすでにインストールされている場合は、設定手順に進みます。

1. Windows Serverコンパクトディスクを挿入し、セットアッププログラムを開始します。
2. [アドオンコンポーネントのインストール]をクリックし、[Windowsコンポーネントの追加と削除]をクリックします。
3. [コンポーネント]で、[ネットワークサービス]をクリックし (チェックボックスをオンまたはオフにしない)、[詳細]をクリックします。
4. [Internet Authentication Service]をオンにし、[OK]をクリックします。
5. [next] をクリックします。

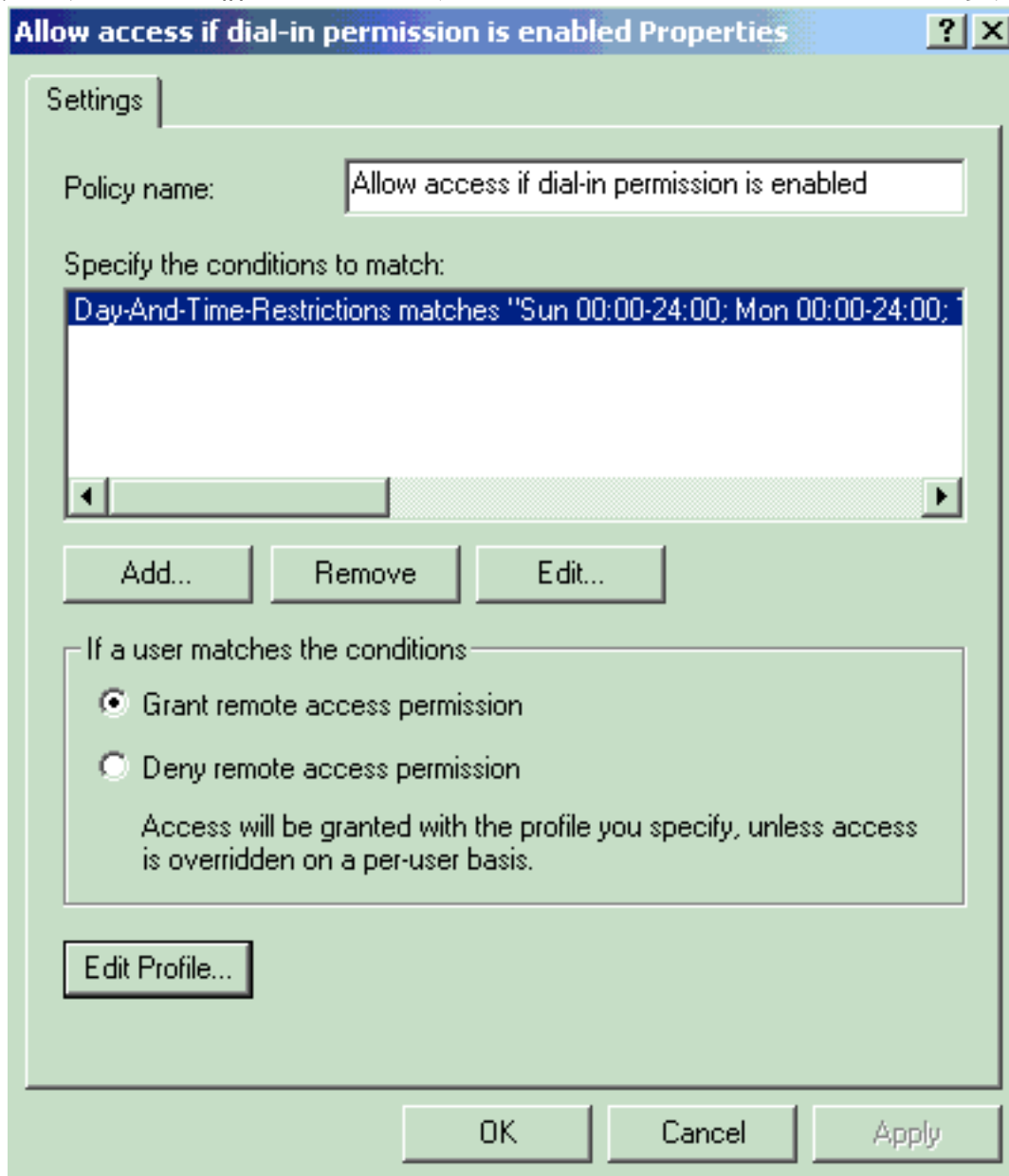
IASを使用したMicrosoft Windows 2000 Serverの設定

RADIUSサーバ(IAS)を設定し、サービスを開始して、VPNコンセントレータでユーザを認証できるようにします。

1. Start > Programs > Administrative Tools > Internet Authentication Serviceの順に選択します。
2. [Internet Authentication Service]を右クリックし、表示されるサブメニューから[Properties]をクリックします。
3. [RADIUS]タブに移動して、ポートの設定を確認します。RADIUS認証およびRADIUSアカウントティングUser Datagram Protocol(UDP)ポートが、認証およびアカウントティングで指定されたデフォルト値 (1812および1645、1813および1646) と異なる場合は、ポート設定を入力します。完了したら、[OK] をクリックします。注：デフォルトのポートは変更しないでください。認証またはアカウントティング要求に複数のポート設定を使用するには、カンマを使用してポートを分割します。
4. [Clients] を右クリックし、[New Client] を選択して、VPNコンセントレータを認証、許可、アカウントティング(AAA)クライアントとしてRADIUSサーバ(IAS)に追加します。注：2つのCisco VPN 3000コンセントレータ間に冗長性が設定されている場合は、バックアップCisco VPN 3000コンセントレータもRADIUSクライアントとしてRADIUSサーバに追加する必要があります。
5. フレンドリ名を入力し、[プロトコルRADIUS]を選択します。
6. 次のウィンドウで、IPアドレスまたはDNS名を使用してVPNコンセントレータを定義します。
7. [Client-Vendor]スクロールバーから[Cisco]を選択します。
8. 共有秘密を入力します。注：使用する秘密を正確に覚えておく必要があります。VPNコンセントレータを設定するには、次の情報が必要です。

9. [Finish] をクリックします。

10. [Remote Access Policies]をダブルクリックし、ウィンドウの右側に表示されるポリシーをダブルクリックします。注：IASをインストールした後、リモートアクセスポリシーがすでに存在している必要があります。Windows 2000では、ユーザアカウントおよびリモートアクセスポリシーのダイヤルインプロパティに基づいて許可が付与されます。リモートアクセスポリシーは、ネットワーク管理者が接続試行をより柔軟に承認できる一連の条件と接続設定です。Windows 2000 Routing and Remote AccessサービスとWindows 2000 IASは、どちらもリモートアクセスポリシーを使用して、接続試行を受け入れるか拒否するかを決定します。どちらの場合も、リモートアクセスポリシーはローカルに保存されます。接続試行の処理方法の詳細については、Windows 2000 IASのドキュメントを参照してください。



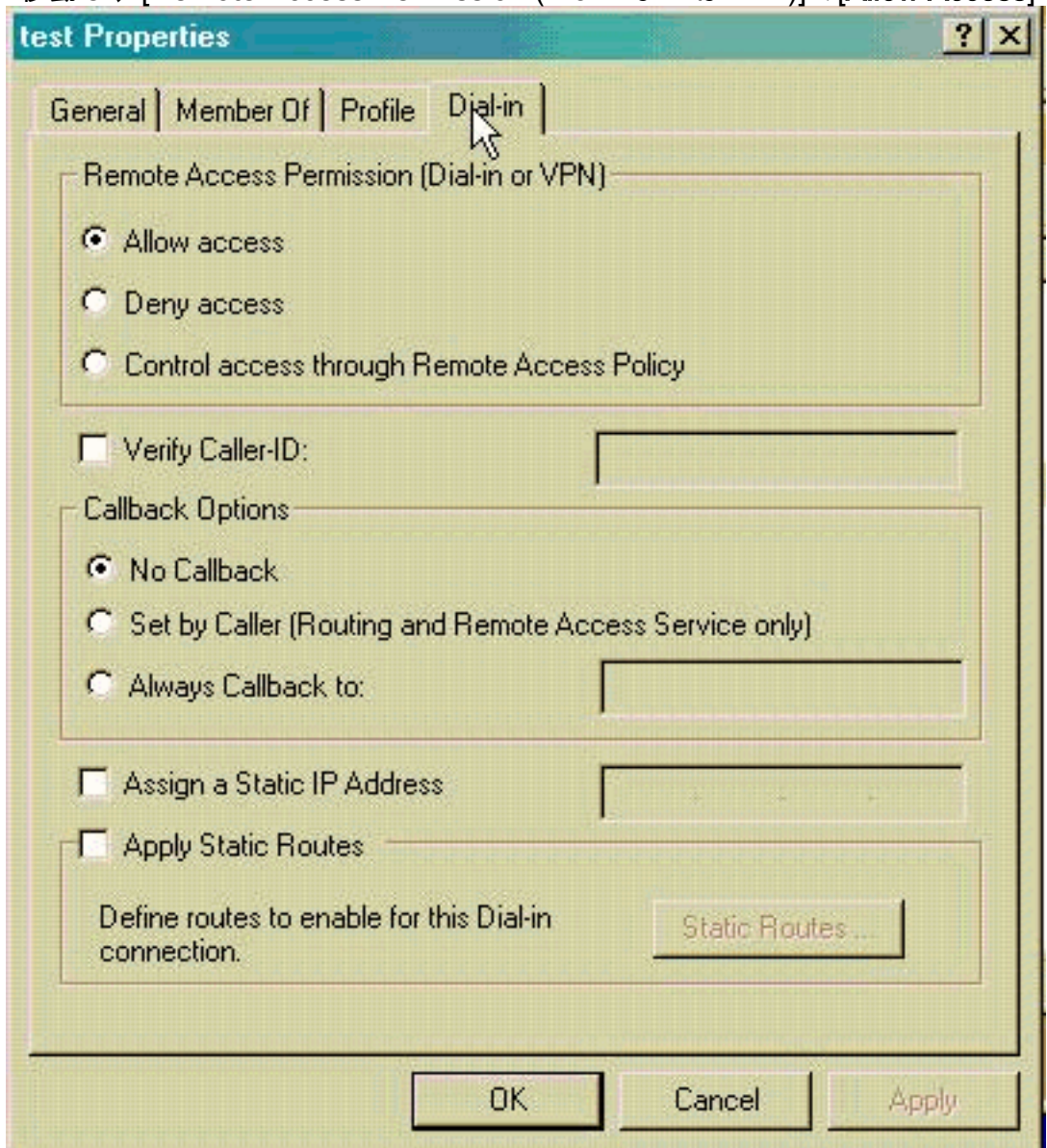
い。

11. [Grant remote access permission]を選択し、[Edit Profile]をクリックしてダイヤルインプロパティを設定します。

12. [Authentication]タブで、認証に使用するプロトコルを選択します。[Microsoft Encrypted Authentication version 2]にチェックマークを付け、他のすべての認証プロトコルのチェックマークを外します。注：このダイヤルインプロファイルの設定は、VPN 3000コンセントレータ設定およびダイヤルインクライアントの設定と一致している必要があります。この例では、PPTP暗号化のないMS-CHAPv2認証が使用されています。

13. [Encryption]タブで、[No Encryption only]をオンにします。

14. [OK]をクリックしてダイヤルインプロファイルを閉じ、[OK]をクリックしてリモートアクセスポリシーウィンドウを閉じます。
15. コンソール・ツリーで[Internet Authentication Service]を右クリックし、[Start Service]をクリックします。注：この機能を使用してサービスを停止することもできます。
16. 接続を許可するようにユーザを変更するには、次の手順を実行します。[コンソール]>[スナップインの追加と削除]を選択します。[Add]をクリックし、[Local Users and Groups]スナップインを選択します。[Add] をクリックします。[ローカルコンピュータ]を選択してください[Finish]、[OK]の順にクリックします。
17. [ローカルユーザーとグループ]を展開し、左側のペインの[ユーザー]フォルダをクリックします。右側のペインで、アクセスを許可するユーザ (VPNユーザ) をダブルクリックします。
18. [Dial-in]タブに移動し、[Remote Access Permission (Dial-inまたはVPN)]で[Allow Access]を



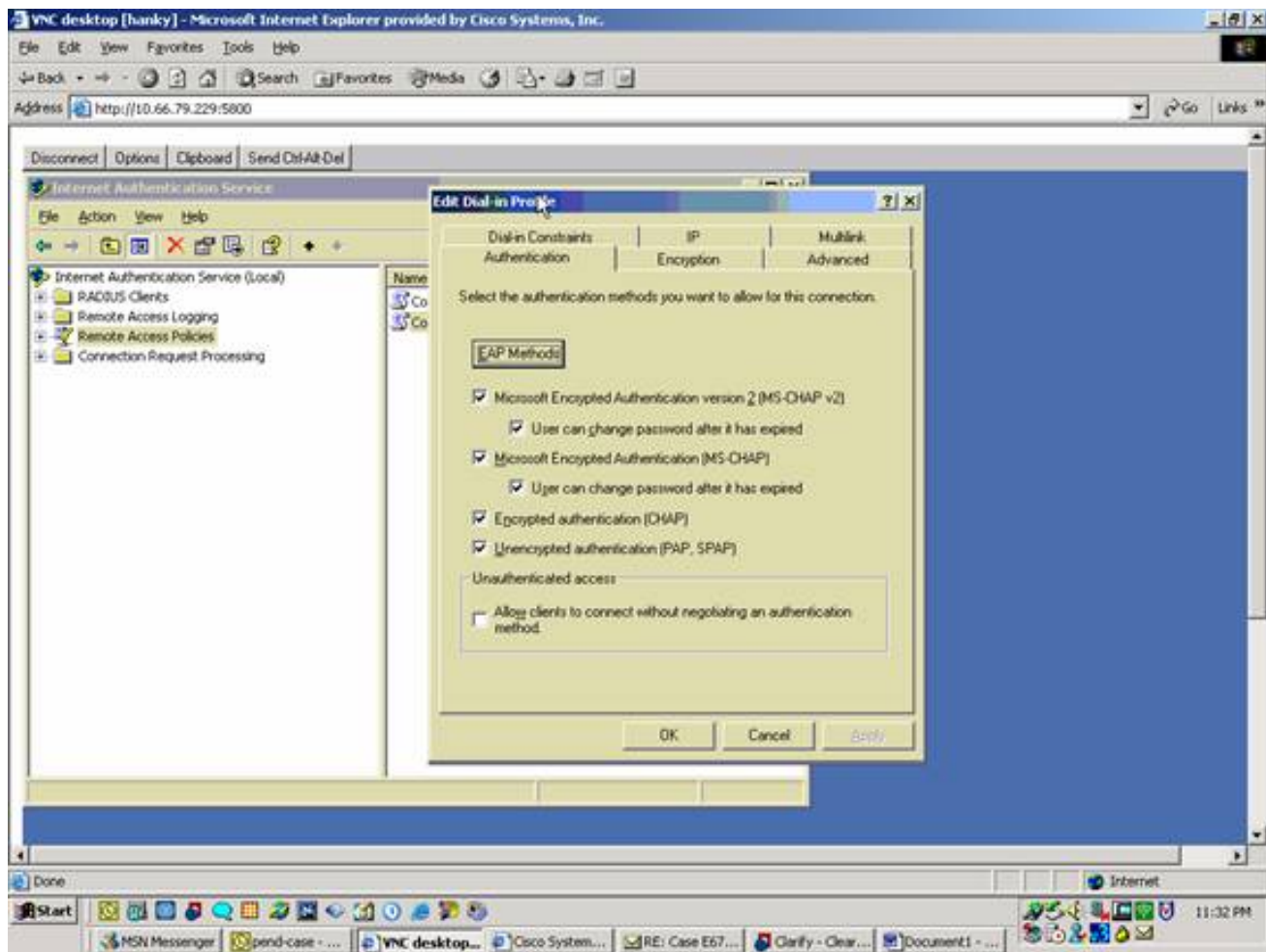
選択します。

19. [Apply]をクリックして、[OK]をクリックして操作を完了します。必要に応じて、[Console Management]ウィンドウを閉じてセッションを保存できます。変更したユーザは、VPN Clientを使用してVPN Concentratorにアクセスできるようになります。IASサーバはユーザ情報のみを認証することに注意してください。VPNコンセントレータは、引き続きグループ認証を行います。

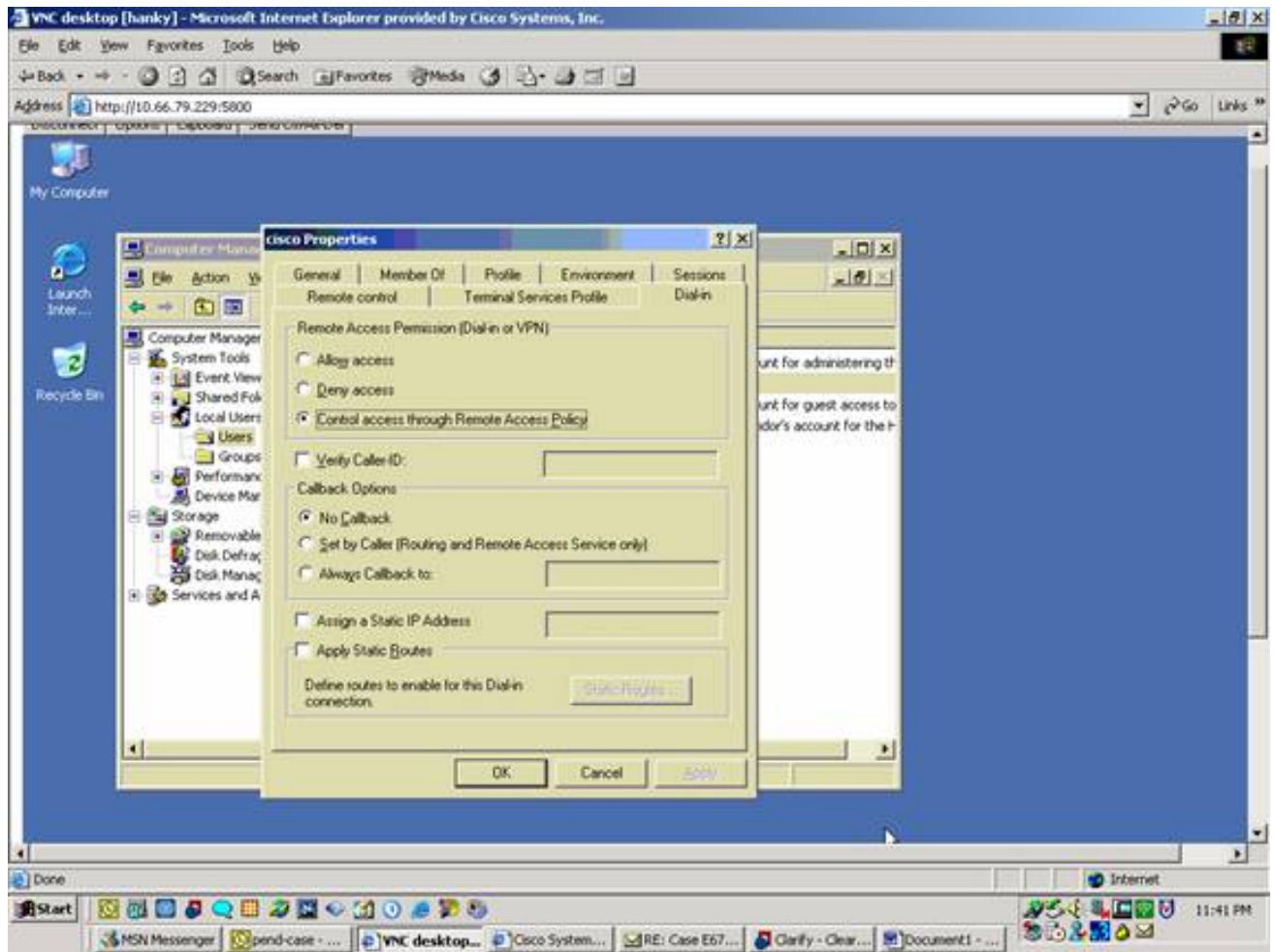
IAS がインストールされた Microsoft Windows 2003 サーバを設定するには、次の手順を実行します。

注：これらの手順では、IASがすでにローカルマシンにインストールされていることを前提としています。まだインストールされていない場合は、**Control Panel > Add/Remove Programs** の順に選択して、IAS を追加してください。

1. **[Administrative Tools] > [Internet Authentication Service]**を選択して、**[RADIUS Client]**を右クリックして、新しいRADIUSクライアントを追加します。クライアント情報を入力したら、**OK** をクリックします。
2. フレンドリ名を入力します。
3. 次のウィンドウで、IPアドレスまたはDNS名を使用してVPNコンセントレータを定義します。
4. **[Client-Vendor]**スクロールバーから**[Cisco]**を選択します。
5. 共有秘密を入力します。**注：**使用する秘密を正確に覚えておく必要があります。VPNコンセントレータを設定するには、次の情報が必要です。
6. **[OK]** をクリックして完了します。
7. **[Remote Access Policies]**に移動し、**[Connections to Other Access Servers]**を右クリックし、**[Properties]**を選択します。
8. **[Grant remote access permission]**を選択し、**[Edit Profile]**をクリックしてダイアログボックスを設定します。
9. **[Authentication]**タブで、認証に使用するプロトコルを選択します。**[Microsoft Encrypted Authentication version 2]**にチェックマークを付け、他のすべての認証プロトコルのチェックマークを外します。**注：**このダイアログボックスの設定は、VPN 3000コンセントレータ設定およびダイアログボックスクライアントの設定と一致している必要があります。この例では、PPTP暗号化のないMS-CHAPv2認証が使用されています。
10. **[Encryption]**タブで、**[No Encryption only]**をオンにします。
11. 完了したら、**[OK]** をクリックします。



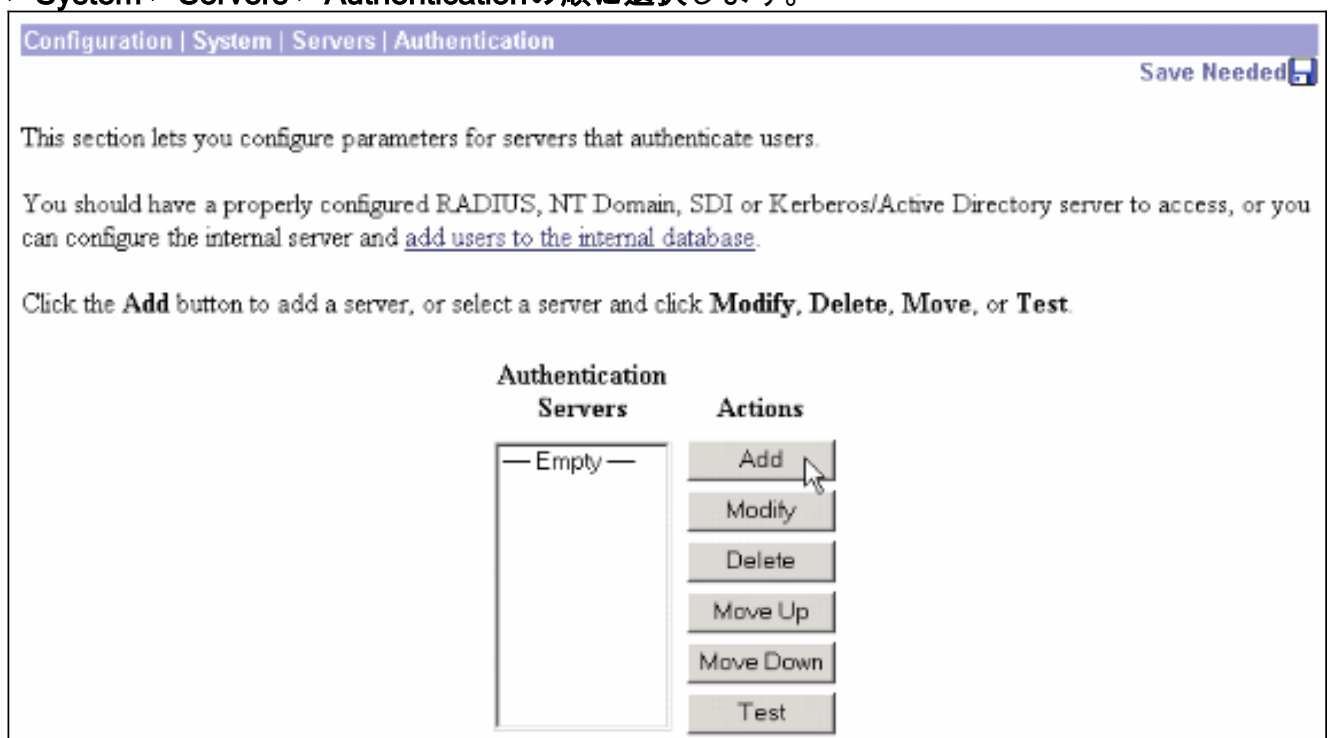
12. コンソール・ツリーで[Internet Authentication Service]を右クリックし、[Start Service]をクリックします。注：この機能を使用して、サービスを停止することもできます。
13. [Administrative Tools] > [Computer Management] > [System Tools] > [Local Users and Groups]の順に選択し、[Users]を右クリックし、[New Users]を選択してローカルコンピュータアカウントにユーザを追加します。
14. シスコパスワード「vpnpassword」を持つユーザを追加し、このプロファイル情報を確認します。General タブで、User Must Change Password のオプションではなく、**Password Never Expired** のオプションが選択されていることを確認します。[ダイヤルイン]タブで、[アクセスを許可する]オプションを選択します(または、既定の設定の[リモートアクセスポリシーによるコントロールアクセス]のままにします)。完了したら、[OK] をクリックします。



RADIUS認証用のCisco VPN 3000コンセントレータの設定

RADIUS認証用にCisco 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. WebブラウザでVPNコンセントレータに接続し、左側のフレームメニューから**Configuration > System > Servers > Authentication**の順に選択します。



2. [Add]をクリックし、これらの設定を構成します。サーバタイプ=RADIUS認証サーバ=RADIUSサーバ(IAS)のIPアドレスまたはホスト名サーバポート= 0 (0=デフォルト=1645) サーバシークレット= 「RADIUSサーバの設定」のセクションのステップ8と同じです。

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.

Authentication Server Enter IP address or hostname.

Used For Select the operation(s) for which this RADIUS server will be used.

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

3. [Add]をクリックして、実行コンフィギュレーションに変更を追加します。
4. [Add]をクリックし、[Server Type]に[Internal Server]を選択し、[Apply]をクリックします。IPsecグループを設定するには、後で必要になります ([Server Type] = [Internal Server]のみ)。

Configuration | System | Servers | Authentication | Add


Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

5. PPTPユーザまたはVPN Clientユーザ用にVPNコンセントレータを設定します。PPTPPPTPユーザを設定するには、次の手順を実行します。[Configuration] > [User Management] > [Base Group]の順に選択し、[PPTP/L2TP]タブをクリックします。[MSCHAPv2]を選択し、[PPTP Authentication Protocols]セクションの他の認証プロトコルのチェックを外します。

Configuration User Management Base Group		
General IPSec Client Config Client FW HW Client PPTP/L2TP WebVPN NAC		
PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MSCHAPv1 <input checked="" type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	Check to enable MPPC compression for L2TP connections for this group.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

ページ下部の[Apply]をクリックして、実行コンフィギュレーションに変更を追加します。PPTPユーザが接続すると、RADIUSサーバ(IAS)によって認証されます。VPN クライアントVPN Clientユーザ用に設定するには、次の手順を実行します。[Configuration] > [User Management] > [Groups]を選択し、[Add]をクリックして新しいグループを追加します。

Configuration User Management Groups		
Save Needed 		
<p>This section lets you configure groups. A group is a collection of users treated as a single entity.</p> <p>Click the Add Group button to add a group, or select a group and click Delete Group or Modify Group. To modify other group parameters, select a group and click the appropriate button.</p>		
Actions <input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	Current Groups <div style="border: 1px solid gray; padding: 5px; min-height: 100px;"> <p style="text-align: center;">— Empty —</p> </div>	Modify <input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

グループ名 (IPsecUsersなど) とパスワードを入力します。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters		
Attribute	Value	Description
Group Name	IPSecUsers	Enter a unique name for the group.
Password	●●●●●●	Enter the password for the group.
Verify	●●●●●●	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

このパスワードは、トンネルネゴシエーションの事前共有キーとして使用されます。
 [IPsec]タブに移動し、[Authentication]を[RADIUS]に設定します。

Configuration | Administration | Monitoring

below as needed.

Remote Access Parameters		
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/> Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/> Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/> If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/> Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/> For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	<input checked="" type="checkbox"/> Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/> Check to reauthenticate the user on an IKE (Phase-1) rekey.

Permit or deny VPN Clients according to

これにより、RADIUS認証サーバ経由でIPsecクライアントを認証できます。ページ下部の [Add]をクリックして、実行コンフィギュレーションに変更を追加します。これで、IPsecクライアントが接続し、設定したグループを使用すると、RADIUSサーバによって認証されます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

WebVPN 認証の失敗

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

- **問題**：WebVPNユーザはRADIUSサーバに対して認証できませんが、VPNコンセントレータのローカルデータベースで正常に認証できます。「Login failed」などのエラーと、このメッ



セージが表示されます。

原因

：このような問題は、コンセントレータの内部データベース以外のデータベースが使用されている場合によく発生します。WebVPNユーザは、コンセントレータに最初に接続するときにベースグループをヒットし、デフォルトの認証方式を使用する必要があります。この方法は、コンセントレータの内部データベースに設定され、設定されたRADIUSまたはその他のサーバではないことがよくあります。ソリューション：WebVPNユーザが認証すると、コンセントレータは[Configuration] > [System] > [Servers] > [Authentication]で定義されたサーバのリストを確認し、上位のサーバを使用します。WebVPN ユーザを認証するサーバを必ずこのリストの最初に移動してください。たとえば、RADIUS を認証方式にする場合は、認証を処理するためにリストの一番上に RADIUS サーバを移動する必要があります。注：WebVPNユーザが最初にベースグループにヒットしたからといって、ベースグループに限定されているわけではありません。コンセントレータで追加のWebVPNグループを設定でき、RADIUSサーバによってユーザに割り当てることができます。RADIUSサーバには、OU=groupnameという属性25が設定されています。詳細については、「[RADIUS サーバを使用した VPN 3000 コンセントレータ グループへのユーザのロック](#)」を参照してください。

Active Directoryに対するユーザ認証の失敗

Active Directoryサーバで、失敗したユーザの[User Properties]の[Account]タブに、次のチェックボックスが表示されます。

事前認証は不要

このチェックボックスがオフの場合は、オンにして、このユーザに対して再度認証を試みます。

関連情報

- [Cisco VPN 3000 シリーズ コンセントレータ](#)
- [Cisco VPN 3002 Hardware Client](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [RADIUS\(Remote Authentication Dial-In User Service\)に関するサポートページ](#)
- [Remote Authentication Dial-In User Service \(RADIUS \)](#)

- [テクニカル サポートとドキュメント – Cisco Systems](#)