外部認証を使用する Cisco VPN 5000 コンセントレータを Microsoft Windows 2000 IAS RADIUS サーバに設定する方法

内容

概要

このドキュメントでは、外部認証を使用する Cisco VPN 5000 コンセントレータを RADIUS を使用する Microsoft Windows 2000 Internet Authentication Server（IAS）に設定する手順について説明します。

注：チャレンジハンドシェーク認証プロトコル(CHAP)は機能しません。パスワード認証プロトコル(PAP)のみを使用します。 詳細については、Cisco Bug ID CSCdt96941(登録ユーザ専用)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情報は次のソフトウェア バージョンに基づいています。

- Cisco VPN 5000 コンセントレータ ソフトウェア バージョン 6.0.16.0001

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。

Cisco VPN 5000 Concentrator 設定

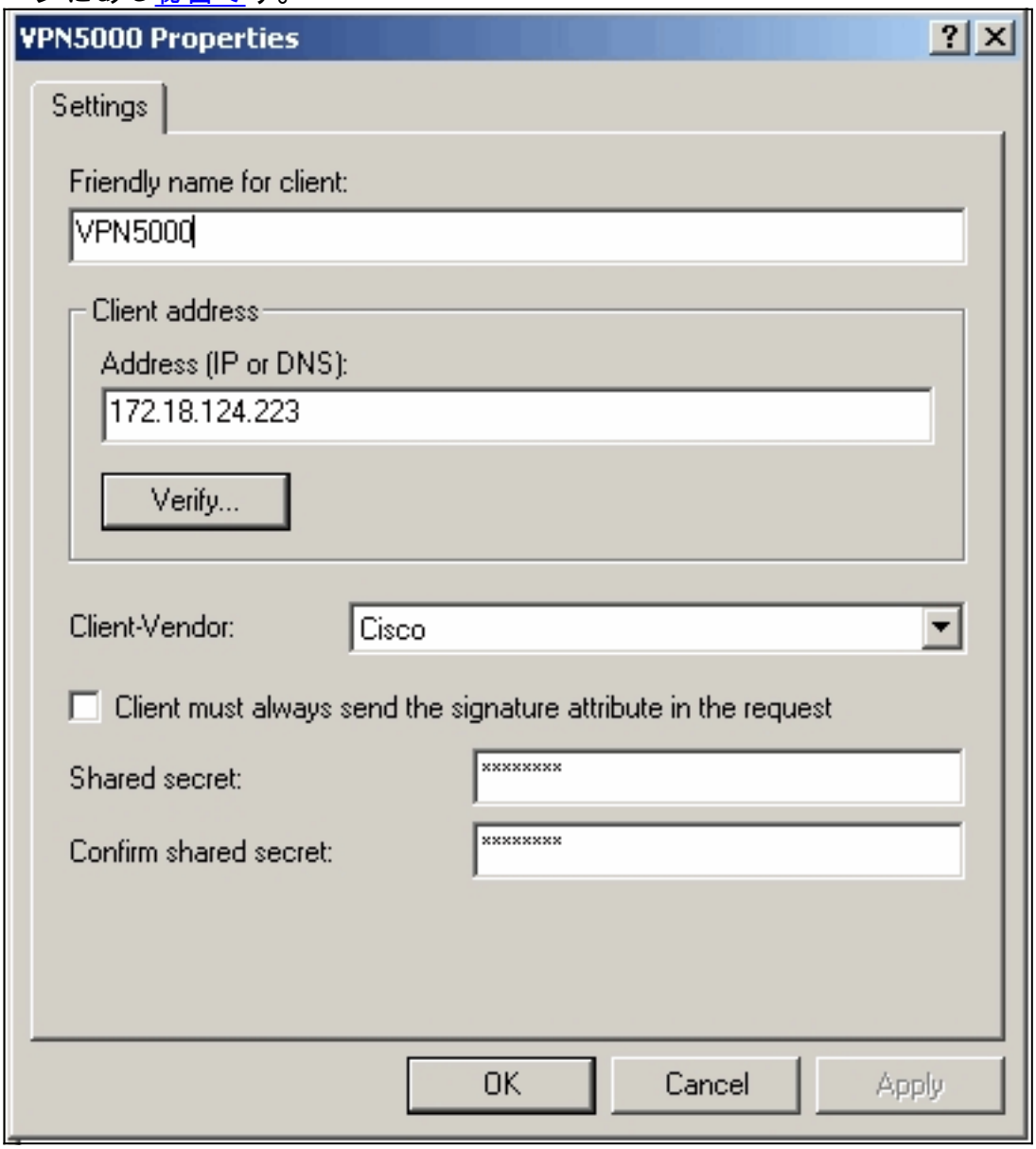
VPN5001_4B9CBA80

```
VPN5001_4B9CBA80> show config
Enter Password:

Edited Configuration not Present, using Running

[ General ]
EthernetAddress          = 00:02:4b:9c:ba:80
DeviceType               = VPN 5001 Concentrator
ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
EnablePassword           =
Password                 =

[ IP Ethernet 0 ]
Mode                     = Routed
SubnetMask               = 255.255.255.0
IPAddress                = 172.18.124.223

[ IP Ethernet 1 ]
Mode                     = Off

[ IKE Policy ]
Protection               = MD5_DES_G1

[ VPN Group "rtp-group" ]
BindTo                   = "ethernet0"
Transform                = esp(md5,des)
LocalIPNet               = 10.1.1.0/24
MaxConnections           = 10
IPNet                    = 0.0.0.0/0

[ RADIUS ]
BindTo                   = "ethernet0"
ChallengeType            = PAP
PAPAuthSecret            = "pappassword"
PrimAddress              = "172.18.124.108"
Secret                   = "radiuspassword"
UseChap16                = Off
Authentication           = On

[ Logging ]
Level                    = 7
Enabled                  = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

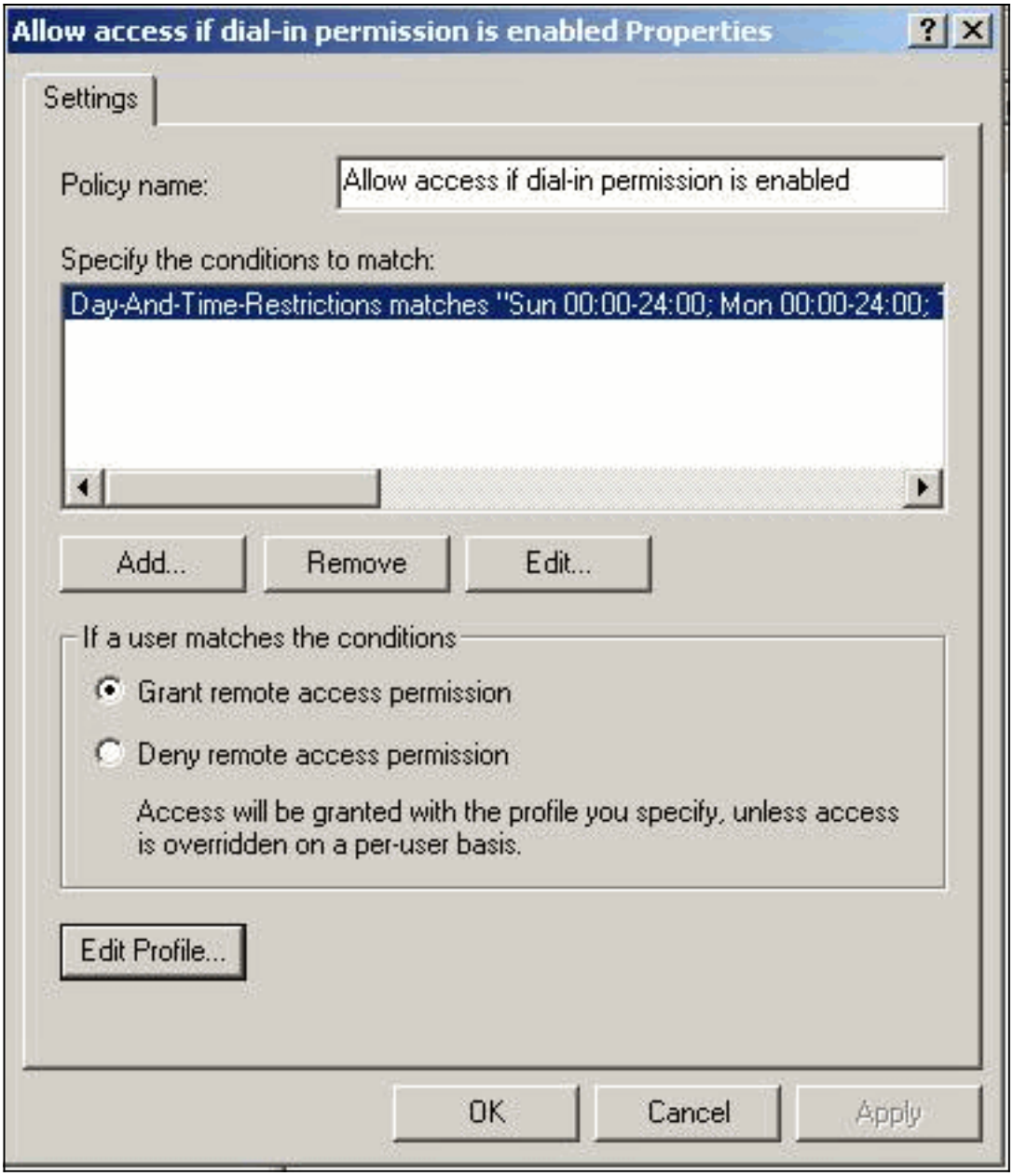
Microsoft Windows 2000 IAS RADIUSサーバの設定

次の手順に従って、簡単なMicrosoft Windows 2000 IAS RADIUSサーバ設定を行います。

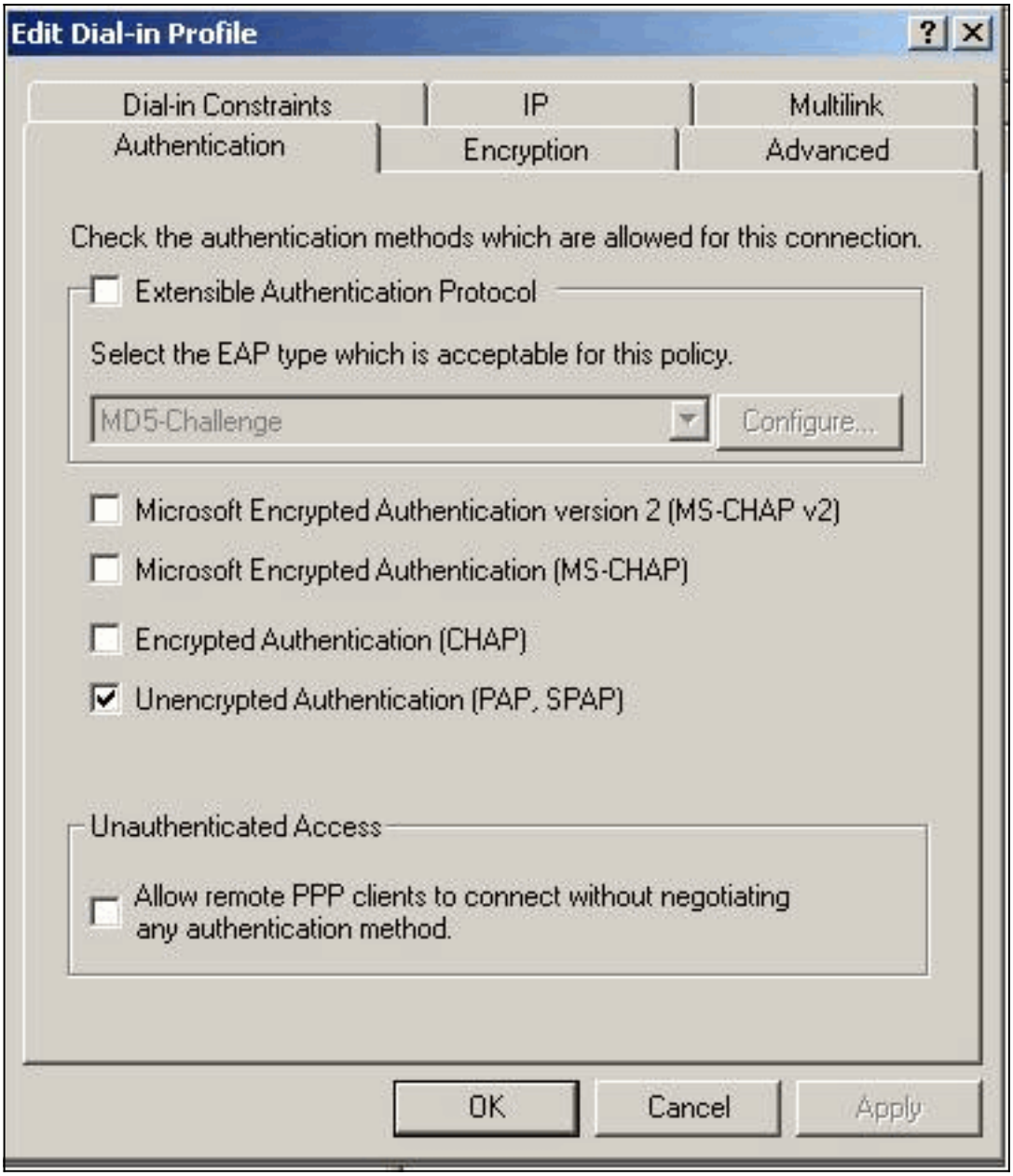
1. Microsoft Windows 2000 IASのプロパティで、[Clients]を選択し、新しいクライアントを作成します。この例では、VPN5000という名前のエントリが作成されます。Cisco VPN 5000コンセントレータのIPアドレスは172.18.124.223です。[Client-Vendor]ドロップダウンボックスで、[Cisco]を選択します。共有秘密は、VPNコンセントレータの設定の[RADIUS]ョンにある秘密です。



2. リモートアクセスポリシーのプロパティで、[ユーザーが条件に一致する場合]セクションの[リモートアクセス許可の付与]を選択し、[プロファイルの編集]をクリックします。

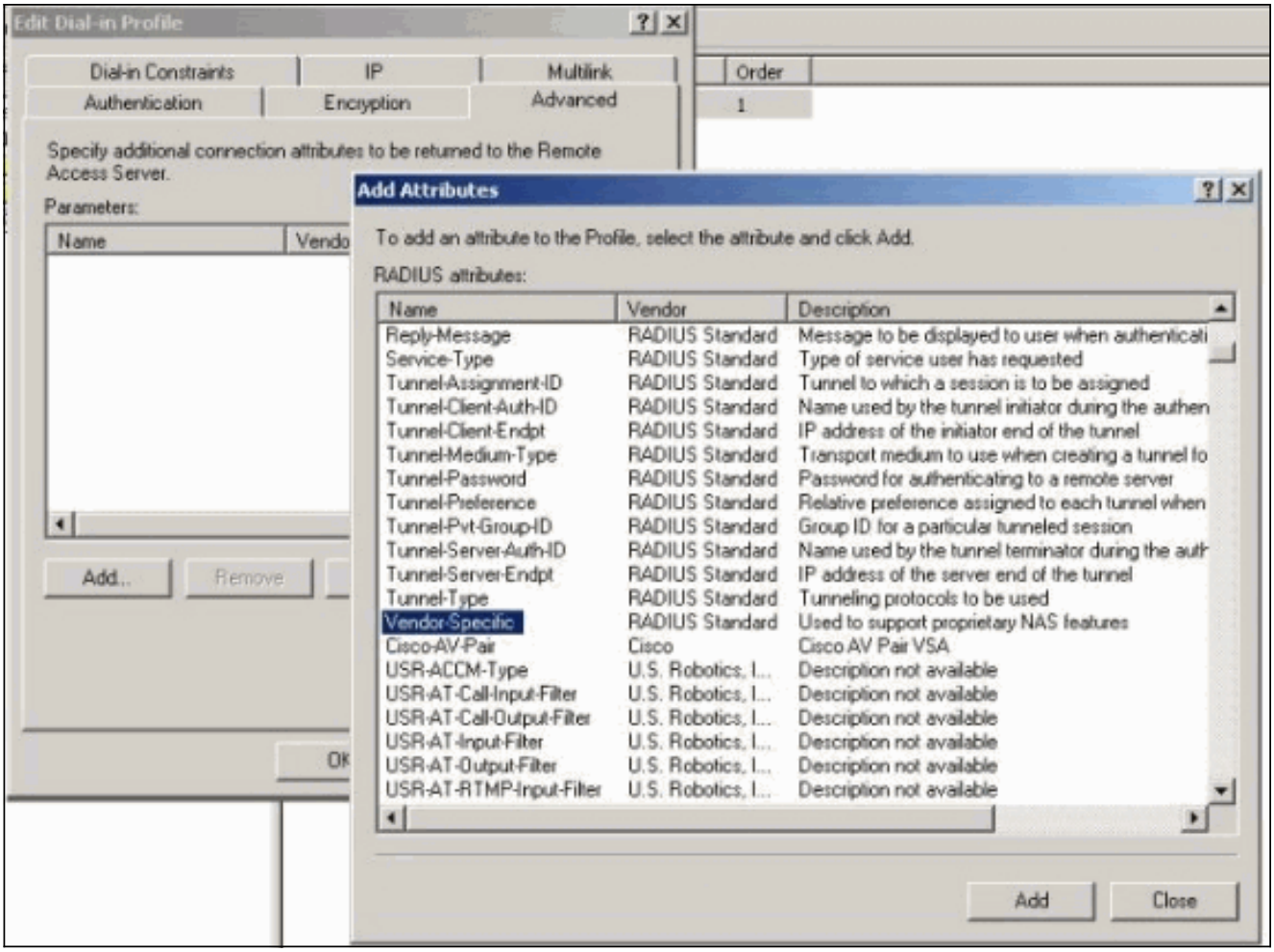


3. 「認証」タブをクリックし、「非暗号化認証(PAP、SPAP)」のみが選択されていることを

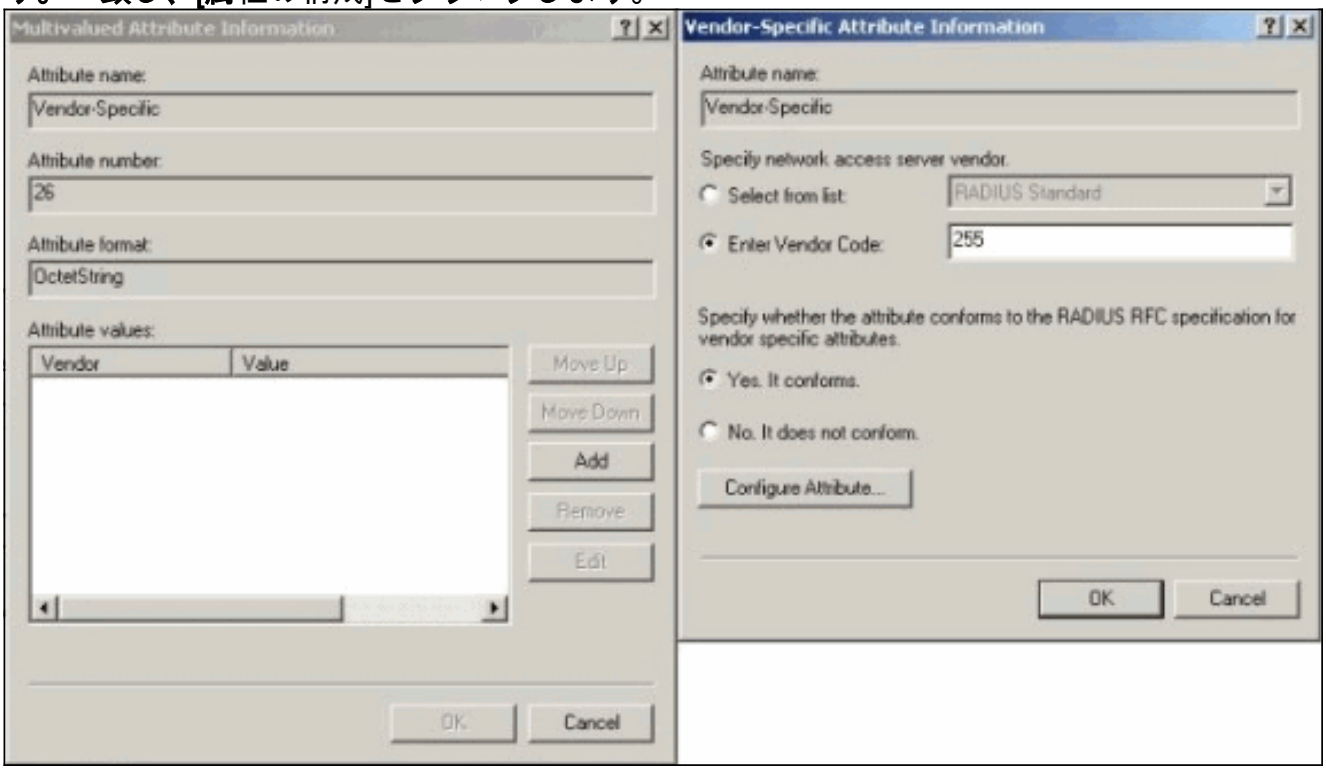


確認します。

4. [Advanced]タブを選択し、[Add]をクリックし、[Vendor-Specific]を選択します。



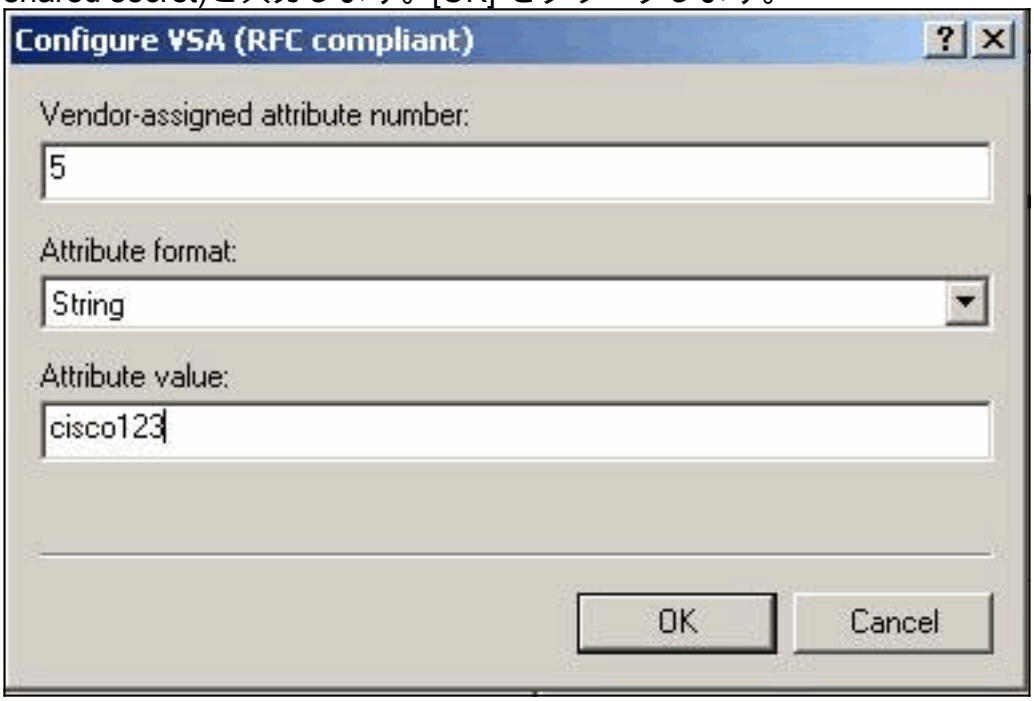
5. Vendor-Specific属性の[Multivalued Attribute Information]ダイアログボックスで、[**Add**]をクリックして、[Vendor-Specific Attribute Information]ダイアログボックスに移動します。[Enter **Vendor Code]を選択**し、横のボ**ックスに**255と入力します。次に、[はい]を選択**します。一致し、[属**性の構成]を**クリックします。**



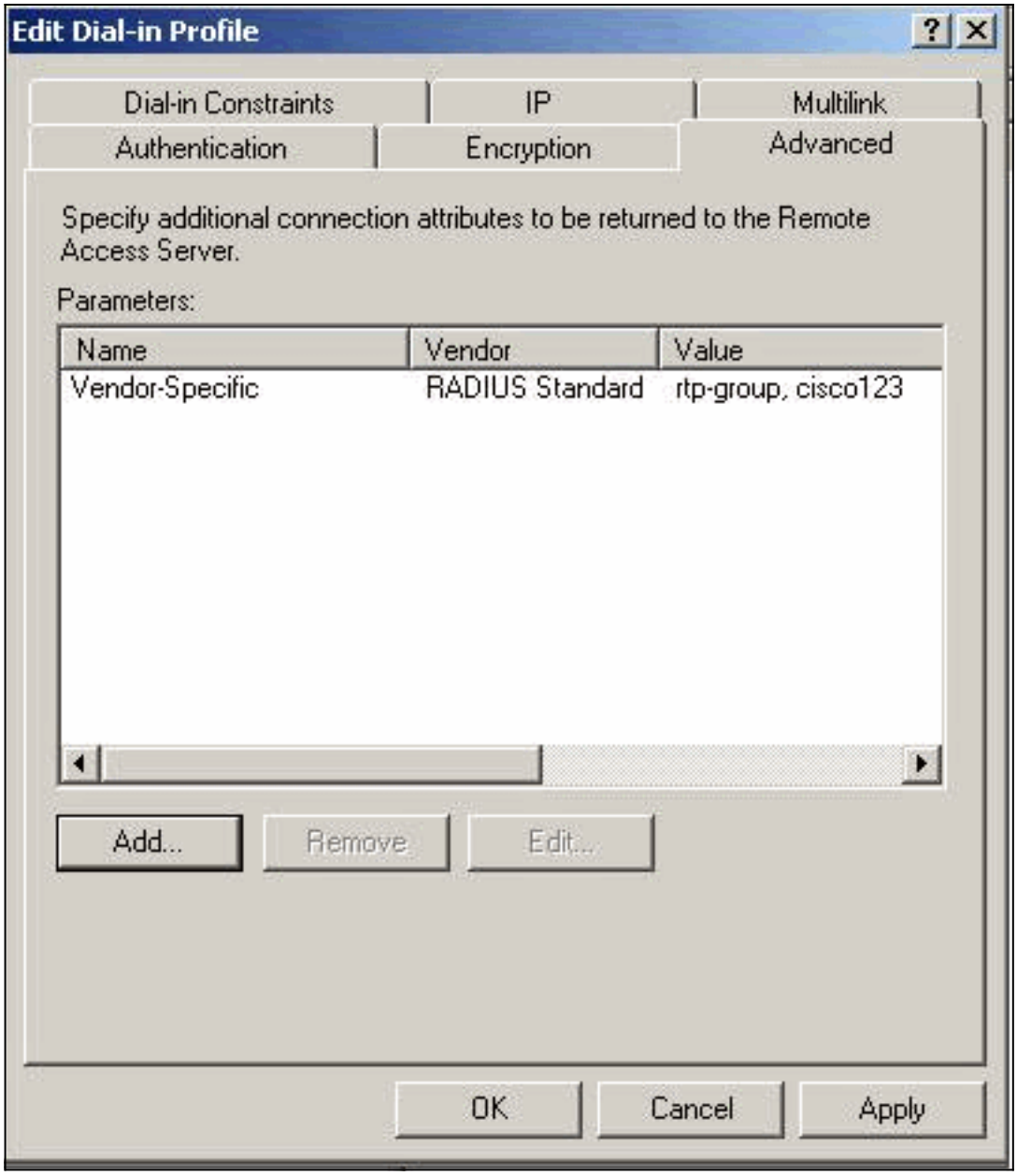
6. [Configure VSA (RFC compliant)]ダイアログボックスで、[Vendor-assigned attribute number]に**4**と入力し、[Attribute format]に**String**と入力し、[Attribute value]に**rtp-group**（Cisco VPN 5000コンセントレータのVPNグループののグループの名）とです。

[OK]をクリックし、手順5を繰り返します。

7. [Configure VSA (RFC compliant)]ダイアログボックスで、[Vendor-assigned attribute number]に**4**と入力し、[Attribute format]に**String**と入力し、[Attribute value]に**cisco123** (client shared secret)と入力します。[OK] をクリックします。

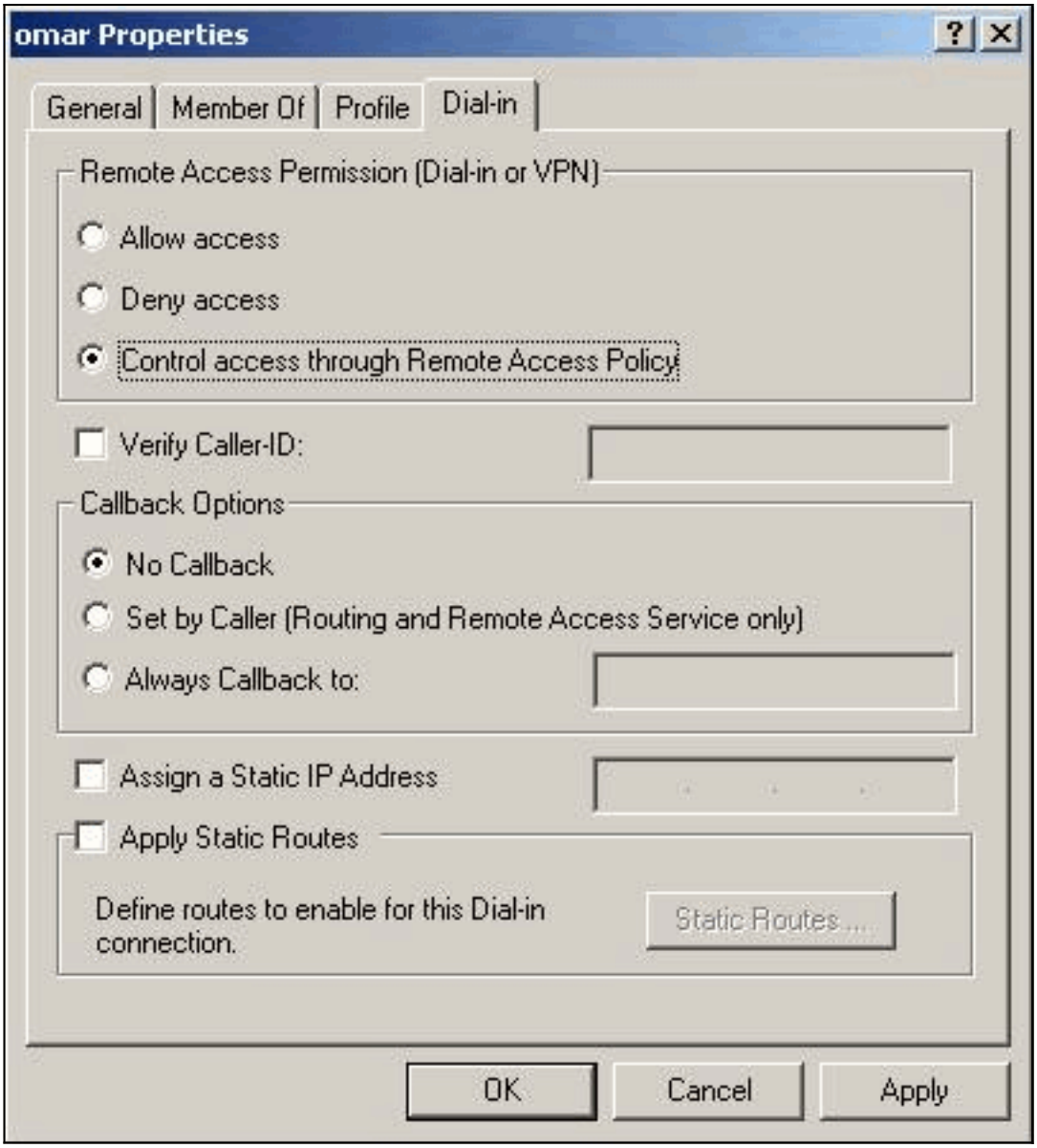


8. ベンダー固有属性に2つの値（グループとVPNパスワード）が含まれていることがわかりま



す。

9. ユーザーのプロパティの下で、[ダイヤルイン]タブをクリックし、[リモート**アクセスポリシーによるアクセスの制御]が選択**されていることを確認します。



結果の確認

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供しています。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show radius statistics**:VPNコンセントレータとRADIUSセクションで識別されるデフォルトのRADIUSサーバ間の通信に関するパケット統計情報を表示します。
- **show radius config**:RADIUSパラメータの現在の設定を表示します。

次に、**show radius statistics**コマンドの**出力を示**します。

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting              Primary       Secondary
Requests                   0             na
```

```
Responses                0             na
Retransmissions          0             na
Bad Authenticators       0             na
Malformed Responses      0             na
Packets Dropped          0             na
Pending Requests         0             na
Timeouts                 0             na
Unknown Types            0             na


Authentication        Primary       Secondary
Requests                 3             na
Accepts                  3             na
Rejects                  0             na
Challenges               0             na
Retransmissions          0             na
Bad Authenticators       0             na
Malformed Responses      0             na
Packets Dropped          0             na
Pending Requests         0             na
Timeouts                 0             na
Unknown Types            0             na



VPN5001_4B9CBA80>
```

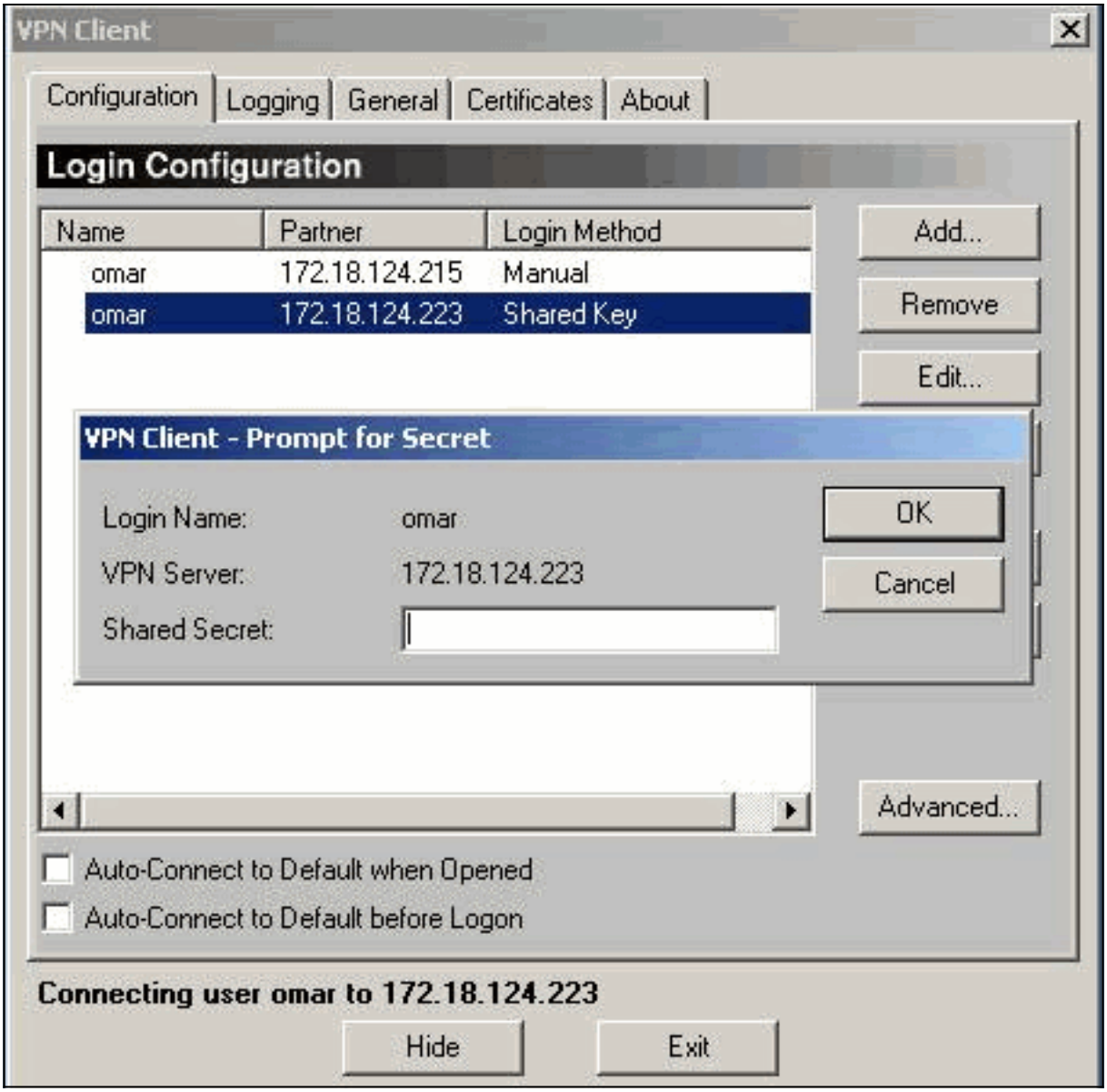
次に、**show radius config**コマンドの出力を示します。

```
RADIUS           State    UDP  CHAP16
Authentication   On      1812  No
Accounting       Off     1813  n/a
Secret           'radiuspassword'

Server     IP address      Attempts  AcctSecret
Primary    172.18.124.108         5  n/a
Secondary  Off
```

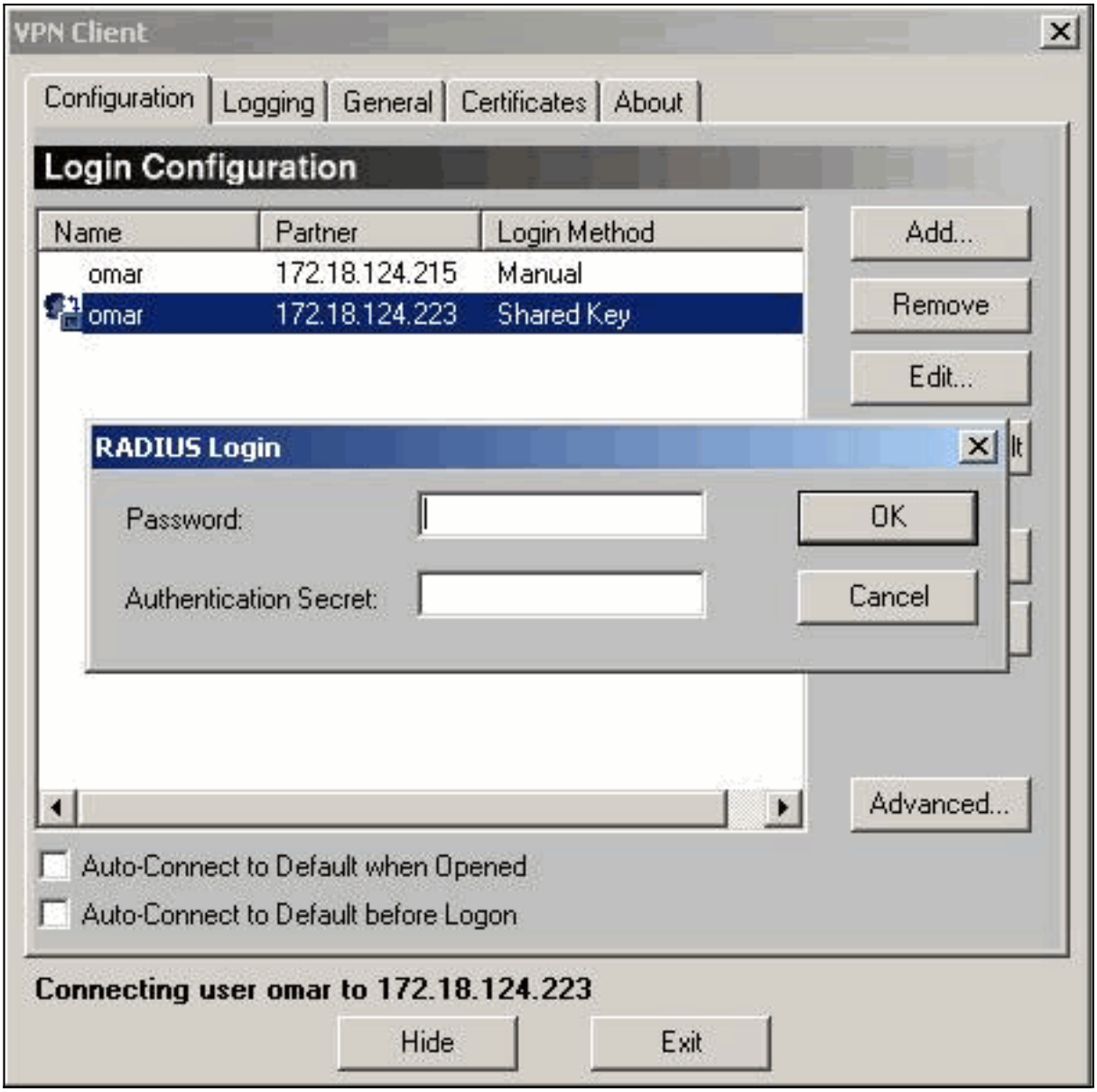
VPN クライアントの設定

この手順では、VPN Clientの設定について説明します。

1. [VPN Client]ダイアログボックスで、[Configuration]タブを選択します。次に、[VPN Client-Prompt for Secret]ダイアログボックスで、VPN Serverの下に共有秘密を入力します。VPN Clientの共有秘密は、VPNコンセントレータで属性5のVPNパスワードに入力した値です。



2. 共有秘密を入力すると、パスワードと認証秘密の入力を求められます。パスワードはそのユーザのRADIUSパスワードで、認証シークレットはVPNコンセントレータの[RADIUS]セクションにあるPAP認証シークレットです。



コンセントレータ ログ

```
Notice    4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar
Debug     4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108
Debug     4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contacting
server
Notice    4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108.
Debug     4088.8 seconds Client's local broadcast address = 172.18.124.255
Notice    4088.8 seconds User assigned IP address 10.1.1.1
Info      4094.49 seconds Command loop started from 10.1.1.1 on PTY2
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- Cisco VPN 5000 コンセントレータに関するサポートページ

- Cisco VPN 5000 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
- テクニカルサポート - Cisco Systems