

# 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

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[Cisco VPN 5000 Concentrator 設定](#)

[Microsoft Windows 2000 IAS RADIUSサーバを設定して下さい](#)

[結果の確認](#)

[VPN クライアントの設定](#)

[コンセントレータ ログ](#)

[トラブルシューティング](#)

[関連情報](#)

## 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:** Challenge Handshake Authentication Protocol ( CHAP ) ははたきません。 Password Authentication Protocol ( PAP ) だけ使用して下さい。 更に詳しい情報については Cisco バグ ID [CSCdt96941](#) ( [登録ユーザのみ](#) ) を参照して下さい。

## 前提条件

### 要件

このドキュメントに関する固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、次のソフトウェアのバージョンに基づくものです。

- 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たものです。こ

のドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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サーバを設定して下さい

これらのステップは簡単な Microsoft Windows 2000 IAS RADIUSサーバ設定によってガイドします。

1. Microsoft Windows 2000 IAS プロパティの下で、新しいクライアントを『Clients』を選択し、作成して下さい。この例では、VPN5000 と指名されるエントリは作成されます。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 ボックスの下で、『Cisco』を選択して下さい。共有秘密は [VPN コンセントレータ](#) 設定の[RADIUS]セクションのシークレットです。
2. リモートアクセスポリシーのプロパティの下で、ユーザが条件」セクションと一致し、『Edit Profile』をクリックしますの下で「『Grant remote access permission』を選択して下さい。
3. Authentication タブをクリックし、その非暗号化認証だけ ( PAP、SPAP ) 選択されます確認して下さい。
4. Advanced タブを選択し、『Add』をクリックし、『Vendor-Specific』を選択して下さい。
5. Vendor-specific属性のための Multivalued Attribute Information ダイアログボックスの下で、( Vendor-Specific Attribute Information ) ダイアログ ボックスに行くために『Add』をクリックして下さい。隣接したボックスで 255 を『Enter Vendor Code』を選択し、入力して下さい。次に、『Yes』を選択して下さい。それは準拠し、『Configure Attribute』をクリックします。

6. 設定 VSA ( 対応 RFC ) ダイアログボックスの下で、ベンダ割り当て 属性 番号のための 4 つを入力し、属性 の フォーマットのためのストリングを入力し、属性値のための `ntp` グループ ( Cisco VPN 5000 コンセントレータの VPNグループの名前 ) を入力して下さい。ステップ 5.を『OK』 をクリックし、繰り返して下さい。
7. 設定 VSA ( 対応 RFC ) ダイアログボックスの下で、ベンダ割り当て 属性 番号のための 4 つを入力し、属性 の フォーマットのためのストリングを入力し、属性値のための `cisco123` ( クライアント 共有秘密 ) を入力して下さい。[OK] をクリックします。
8. Vendor-specific属性が 2 つの値を示すことがわかります ( グループおよび VPN パスワード ) 。
9. ユーザ プロパティの下で、Dial-in タブをクリックし、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**が選択されるようにして下さい。

## 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。

特定の `show` コマンドは、[Output Interpreter Tool](#) ( [登録](#) ユーザ専用 ) によってサポートされています。このツールを使用すると、`show` コマンド出力の分析を表示できます。

- `show radius statistics` — RADIUS セクションによって識別される VPN コンセントレータとデフォルト ラジウス サーバ間のコミュニケーションのためのパケット統計情報を表示する。
- `show radius config` — RADIUS パラメータの現在の設定を示します。

これは `show radius statistics` コマンドの出力です。

```
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>
```

これは `show radius config` コマンドの出力です。

```
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

このプロシージャは VPN クライアントの設定によってガイドします。

1. VPN Client ダイアログボックスから、Configuration タブを選択して下さい。次に、秘密ダイアログボックスのためにクライアント敏速な VPN から VPN サーバの下で共有秘密を入力して下さい。VPN クライアント 共有秘密は VPN コンセントレータでアトリビュート 5 の VPN パスワードのために入る値です。
2. 共有秘密を入力した後、パスワードおよび認証 秘密のためにプロンプト表示されます。パスワードはそのユーザ向けの RADIUSパスワードであり、認証 秘密は [VPN コンセントレー](#)

タの[RADIUS]セクションの 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
```

## トラブルシューティング

現在のところ、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発表](#)
- [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](#)