



## 複数の UDP ポート用の RADIUS

RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号を組み合わせることによって、異なるポートを特定の認証、認可、およびアカウントティング (AAA) サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス (たとえば認証など) を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウントティング サービスの提供に失敗すると、ネットワーク アクセスサーバーは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウントティング サービスを提供するように試行します。

- [複数の UDP ポート用の RADIUS の前提条件 \(1 ページ\)](#)
- [複数の UDP ポート用の RADIUS に関する情報 \(2 ページ\)](#)
- [複数の UDP ポート用の RADIUS を設定する方法 \(3 ページ\)](#)
- [複数の UDP ポート用の RADIUS の設定例 \(4 ページ\)](#)
- [その他の参考資料 \(5 ページ\)](#)
- [複数の UDP ポート用の RADIUS の機能情報 \(6 ページ\)](#)

## 複数の UDP ポート用の RADIUS の前提条件

シスコ デバイスまたはアクセス サーバーで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

# 複数の UDP ポート用の RADIUS に関する情報

## デバイスと RADIUS サーバーの通信

通常、RADIUS ホストは、シスコ（CiscoSecure ACS）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバー ソフトウェアを実行するマルチユーザー システムです。RADIUS サーバーとの通信のためにデバイスを設定するには、次のような要素があります。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- タイムアウト時間
- 再送信回数
- キー文字列

RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティングサービスの提供に失敗すると、ネットワーク アクセス サーバーは同じデバイスに設定されている 2 番目のホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

RADIUS サーバーとシスコ デバイスは、共有秘密テキスト文字列を使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバー デモンが稼働するホストと、そのホストがデバイスと共有する秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト値、再送信値、および暗号キー値には、すべての RADIUS サーバーを対象にしたグローバル設定、サーバー別設定、またはグローバル設定とサーバー別設定の組み合わせを使用できます。デバイスと通信するすべての RADIUS サーバーにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバル コマンドを使用します。特定の RADIUS サーバーにこれらの値を適用するには、**radius-server host** コマンドをグローバル コンフィギュレーション モードで使用します。



- (注) 同じシスコ製ネットワーク アクセス サーバーで、タイムアウト、再送信、およびキー値のコマンドを同時に設定（グローバル設定およびサーバー別設定）できます。デバイスにグローバル機能とサーバー別機能の両方を設定する場合、サーバー別のタイマー、再送信、およびキー値のコマンドが、グローバルのタイマー、再送信、およびキー値のコマンドよりも優先されません。

## 複数の UDP ポート用の RADIUS を設定する方法

### デバイスと RADIUS サーバーの通信の設定

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **address ipv4** *ip-address*
5. **key** {*0 string* | *7 string* | *string*}
6. **retransmit** *retries*
7. **timeout** *seconds*
8. **exit**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>radius server</b> <i>server-name</i> 例：  Device(config)# radius server rad1	RADIUS サーバーの名前を指定します。
ステップ 4	<b>address ipv4</b> <i>ip-address</i> 例：	RADIUS サーバーに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
	Device(config-radius-server)# address ipv4 10.45.1.2	
ステップ 5	<b>key</b> { <b>0 string</b>   <b>7 string</b>   <i>string</i> } 例 : Device(config-radius-server)# key myRaDIUSpassword	デバイスと RADIUS サーバーの間で使用する共有秘密テキスト文字列を指定します。 (注) この手順では、暗号キーの値は、すべての RADIUS サーバーに対してグローバルに設定されます。 • <b>0 string</b> オプションを使用して、暗号化されていない共有秘密を設定します。 <b>7 string</b> オプションを使用して、暗号化された共有秘密を設定します。
ステップ 6	<b>retransmit</b> <i>retries</i> 例 : Device(config-radius-server)# retransmit 25	デバイスからサーバーに対して各 RADIUS 要求を送信する回数の上限を指定します (デフォルトは 3 です)。 (注) この手順では、再送信の値は、すべての RADIUS サーバーに対してグローバルに設定されます。
ステップ 7	<b>timeout</b> <i>seconds</i> 例 : Device(config-radius-server)# timeout 6	デバイスが RADIUS 要求に対する応答を待機して、要求を再送信するまでの時間 (秒数) を指定します。 (注) この手順では、タイムアウト値は、すべての RADIUS サーバーに対してグローバルに設定されます。
ステップ 8	<b>exit</b> 例 : Device(config)# exit	特権 EXEC モードに戻ります。

## 複数の UDP ポート用の RADIUS の設定例

### 例 : デバイスと RADIUS サーバーの通信

次に、固有のタイムアウト、再送信、およびキー値を指定した2つの RADIUS サーバーを設定する例を示します。この例では、**aaa new-model** コマンドを使用してデバイス上の AAA サービスを有効化し、特定の AAA コマンドで AAA サービスを定義します。**retransmit** コマンド

で、すべての RADIUS サーバーについて、グローバル再送信値を 4 に変更します。host コマンドで、IP アドレスが 172.16.1.1 と 172.29.39.46 の RADIUS サーバー ホストについて、特定のタイムアウト、再送信、およびキーの値を設定します。

```
! Enable AAA services on the device and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
Device(config)# radius server rad1
Device(config-radius-server)# address ipv4 10.45.1.2
Device(config-radius-server)# key myRaDIUSpassword
Device(config-radius-server)# retransmit 25
Device(config-radius-server)# timeout 6
Device(config)# exit
```

## 例：サーバー固有の値を指定した RADIUS サーバー

次に、172.31.39.46 という IP アドレスの RADIUS サーバーについて、サーバー固有のタイムアウト、再送信、およびキー値を設定する例を示します。

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Command List, All Releases</a> 』
セキュリティコマンド	<ul style="list-style-type: none"> <li>『<a href="#">Cisco IOS Security Command Reference: Commands A to C</a>』 [英語]</li> <li>『<a href="#">Cisco IOS Security Command Reference: Commands D to L</a>』 [英語]</li> <li>『<a href="#">Cisco IOS Security Command Reference: Commands M to R</a>』 [英語]</li> <li>『<a href="#">Cisco IOS Security Command Reference: Commands S to Z</a>』 [英語]</li> </ul>
AAA	『 <a href="#">Authentication, Authorization, and Accounting Configuration Guide</a> 』 (Securing User Services Configuration Library の一部)

## シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

## 複数の UDP ポート用の RADIUS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 1: 複数の UDP ポート用の RADIUS の機能情報

機能名	リリース	機能情報
<p>複数の UDP ポート用の RADIUS</p>		<p>RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。</p> <ul style="list-style-type: none"> <li>• Catalyst 3850 シリーズ スイッチ</li> <li>• Catalyst 3650 シリーズ スイッチ</li> </ul> <p>次のコマンドが導入または変更されました。<b>radius-server host</b></p>





## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。