



## 複数の UDP ポート用の RADIUS

RADIUS セキュリティサーバは、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。

- [機能情報の確認 \(1 ページ\)](#)
- [複数の UDP ポート用の RADIUS の前提条件 \(2 ページ\)](#)
- [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 \(5 ページ\)](#)
- [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 \(6 ページ\)](#)

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

## 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 サーバソフトウェアを実行するマルチユーザシステムです。RADIUS サーバ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 サーバデー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 サーバを対象にしたグローバル設定、サーバ別設定、またはグローバル設定とサーバ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別設定）できます。デバイスにグローバル機能とサーバ別機能の両方を設定する場合、サーバ別のタイマー、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す。

## 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 モードをイネーブルにします。 ・パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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 server-name</b> 例：  Device(config)# radius server rad1	RADIUS サーバの名前を指定します。
ステップ 4	<b>address ipv4 ip-address</b> 例：  Device(config-radius-server)# address ipv4 10.45.1.2	RADIUS サーバに IP アドレスを割り当てます。
ステップ 5	<b>key {0 string   7 string   string}</b> 例：  Device(config-radius-server)# key myRaDIUSpassword	デバイスと RADIUS サーバ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 retries</b> 例：  Device(config-radius-server)# retransmit 25	デバイスからサーバに対して各 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 サーバに対してグローバルに設定されます。
ステップ 7	<b>timeout seconds</b> 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：	特権 EXEC モードに戻ります。

コマンドまたはアクション	目的
Device(config)# exit	

## 複数の UDP ポート用の RADIUS の設定例

### 例：デバイスと RADIUS サーバの通信

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：サーバ固有の値を指定した RADIUS サーバ

次に、172.31.39.46 という IP アドレスの RADIUS サーバについて、サーバ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>

関連項目	マニュアルタイトル
セキュリティコマンド	<ul style="list-style-type: none"> <li>『Cisco IOS Security Command Reference: Commands A to C』</li> <li>『Cisco IOS Security Command Reference: Commands D to L』</li> <li>『Cisco IOS Security Command Reference: Commands M to R』</li> <li>『Cisco IOS Security Command Reference: Commands S to Z』</li> </ul>
AAA	『Authentication, Authorization, and Accounting Configuration Guide』 (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
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。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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
複数の UDP ポート用の RADIUS		<p>RADIUS セキュリティ サーバは、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上の複数の UDP ポートに、RADIUS 要求を送信できます。</p> <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>

