



# 複数の RADIUS サーバ間での認証および認可

- [複数の RADIUS サーバ間での認証および認可について \(1 ページ\)](#)
- [認証および認可サーバの分割による WLAN の 802.1X セキュリティの設定 \(2 ページ\)](#)
- [認証および認可サーバの分割による WLAN の Web 認証の設定 \(6 ページ\)](#)
- [認証と認可の分割設定の確認 \(8 ページ\)](#)
- [設定例 \(9 ページ\)](#)

## 複数の RADIUS サーバ間での認証および認可について

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、認証と認可の両方を組み合わせた単一の RADIUS サーバと要求および応答トランザクションを行うアプローチを使用します。コントローラでの認証と認可は、複数の RADIUS サーバに分割することができます。

RADIUS サーバは、認証サーバ、認可サーバ、またはその両方の役割を担うことができます。認証と認可を異なる RADIUS サーバで行う場合は、コントローラ上の Session Aware Network (SANet) コンポーネントによって、クライアントがコントローラに参加するとき一方のサーバで認証を行い、別のサーバで認可を行うことが可能になりました。

認証は、Cisco ISE、Cisco DNAC、Free Radius、または任意のサードパーティ製 RADIUS サーバを使用して実行できます。認証サーバで認証が成功すると、コントローラは、認証サーバから受信した属性を、認可サーバとして指定された別の RADIUS サーバに中継します。

その後、認可サーバは次の処理を実行します。

- サーバで定義されている他のポリシーやルールを使用して、受信した属性を処理する。
- 認証応答の一部として属性を導出し、コントローラに返す。



(注) 認証と認可の分割設定では、両方のサーバを使用可能にする必要があります。また、コントローラがセッションを受け入れられるように、両方のサーバで ACCESS-ACCEPT を使用して認証と認可を正常に行う必要があります。

# 認証および認可サーバの分割による WLAN の 802.1X セキュリティの設定

## 明示的な認証および認可サーバリストの設定 (GUI)

### 手順

- ステップ 1 [Configuration] > [Security] > [AAA] の順に選択します。
  - ステップ 2 [Authentication Authorization and Accounting] ページで、[Servers/Groups] タブをクリックします。
  - ステップ 3 次のオプションから、設定する AAA サーバのタイプをクリックします。
    - RADIUS
    - TACACS+
    - LDAP
- この手順では、RADIUS サーバの設定について説明します。
- ステップ 4 [RADIUS] オプションを選択した状態で、[Add] をクリックします。
  - ステップ 5 RADIUS サーバの名前と、サーバの IPv4 または IPV6 アドレスを入力します。
  - ステップ 6 デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを入力します。PAC キーまたは非 PAC キーのどちらを使用するかを選択できます。
  - ステップ 7 サーバのタイムアウト値を入力します。有効な範囲は 1 ~ 1000 秒です。
  - ステップ 8 再試行回数を入力します。有効な範囲は 0 ~ 100 です。
  - ステップ 9 [Support for CoA] フィールドは [Enabled] 状態のままにしておきます。
  - ステップ 10 [Save & Apply to Device] をクリックします。
  - ステップ 11 [Authentication Authorization and Accounting] ページで、[RADIUS] オプションを選択した状態で、[Server Groups] タブをクリックします。
  - ステップ 12 [Add] をクリックします。
  - ステップ 13 表示される [Create AAA RADIUS Server Group] ウィンドウで、RADIUS サーバグループの名前を入力します。
  - ステップ 14 [MAC-Delimiter] ドロップダウン リストから、RADIUS サーバに送信される MAC アドレスで使用される区切り文字を選択します。
  - ステップ 15 [MAC Filtering] ドロップダウン リストから、MAC アドレスをフィルタリングするための基準値を選択します。
  - ステップ 16 サーバグループのデッドタイムを設定し、稼働特性が異なる別のサーバグループに AAA トラフィックを転送するには、[Dead-Time] フィールドに、サーバが停止していると見なされる時間を分単位で入力します。

ステップ 17 [Available Servers] リストから、サーバグループに含めるサーバを選択し、それらを [Assigned Servers] リストに移動します。

ステップ 18 [Save & Apply to Device] をクリックします。

## 明示的な認証サーバリストの設定 (CLI)

### 手順

	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）。
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 free-radius-authc-server	RADIUS サーバ名を指定します。
ステップ 4	<b>address ipv4 address auth-port auth_port_number acct-port acct_port_number</b> 例： Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813	RADIUS サーバのパラメータを指定します。
ステップ 5	<b>[pac] key key</b> 例： Device(config-radius-server)# key cisco	デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 6	<b>exit</b> 例： Device(config-radius-server)# exit	コンフィギュレーション モードに戻ります。
ステップ 7	<b>aaa group server radius server-group</b> 例：	RADIUS サーバグループの ID を作成します。

## 明示的な認可サーバリストの設定 (CLI)

	コマンドまたはアクション	目的
	Device (config) # <b>aaa group server radius authc-server-group</b>	(注) <i>server-group</i> はサーバグループ名です。有効な範囲は 1 ~ 32 文字の英数字です。
ステップ 8	<b>server name server-name</b> 例 : Device (config) # <b>server name free-radius-authc-server</b>	
ステップ 9	<b>end</b> 例 : Device (config) # <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。  詳細については、「外部認証用の AAA の設定」を参照してください。

## 明示的な認可サーバリストの設定 (CLI)

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	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)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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) # <b>radius server cisco-dnac-authz-server</b>	RADIUS サーバ名を指定します。
ステップ 4	<b>address ipv4 address auth-port auth_port_number acct-port acct_port_number</b> 例 : Device (config-radius-server) # <b>address ipv4 9.4.62.32 auth-port 1812 acct-port 1813</b>	RADIUS サーバのパラメータを指定します。

	コマンドまたはアクション	目的
ステップ 5	<b>[pac] key <i>key</i></b> 例： Device(config-radius-server)# <b>pac key</b> <b>cisco</b>	デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認可および暗号キーを指定します。
ステップ 6	<b>exit</b> 例： Device(config-radius-server)# <b>exit</b>	コンフィギュレーション モードに戻ります。
ステップ 7	<b>aaa group server radius <i>server-group</i></b> 例： Device(config)# <b>aaa group server radius</b> <b>authz-server-group</b>	RADIUS サーバグループの ID を作成します。 (注) <i>server-group</i> はサーバグループ名です。有効な範囲は 1 ~ 32 文字の英数字です。
ステップ 8	<b>server name <i>server-name</i></b> 例： Device(config)# <b>server name</b> <b>cisco-dnac-authz-server</b>	
ステップ 9	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

## 802.1X セキュリティ用の認証および認可リストの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	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）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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>wlan <i>wlan-name wlan-id SSID-name</i></b> 例：	WLAN コンフィギュレーション サブモードを開始します。

	コマンドまたはアクション	目的
	<pre>Device(config)# wlan wlan-foo 222 foo-ssid</pre>	<ul style="list-style-type: none"> <li>• <i>wlan-name</i> : 設定されている WLAN の名前です。</li> <li>• <i>wlan-id</i> : ワイヤレス LAN の ID です。範囲は 1 ~ 512 です。</li> <li>• <i>SSID-name</i> : 最大 32 文字の英数字からなる SSID 名です。</li> </ul> <p>(注) すでにこのコマンドを設定している場合は、<b>wlan wlan-name</b> コマンドを入力します。</p>
ステップ 4	<pre>security dot1x authentication-list authenticate-list-name</pre> <p>例 :</p> <pre>Device(config-wlan)# security dot1x authentication-list authc-server-group</pre>	dot1x セキュリティ用の認証リストを有効にします。
ステップ 5	<pre>security dot1x authorization-list authorize-list-name</pre> <p>例 :</p> <pre>Device(config-wlan)# security dot1x authorization-list authz-server-group</pre>	dot1x セキュリティ用の認可リストを指定します。  <b>Cisco Digital Network Architecture Center (DNAC)</b> の詳細については、DNAC のマニュアルを参照してください。
ステップ 6	<pre>end</pre> <p>例 :</p> <pre>Device(config-wlan)# end</pre>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

## 認証および認可サーバの分割による WLAN の Web 認証の設定

- [#unique\\_789](#)
- [#unique\\_790](#)
- [Web 認証用の認証および認可リストの設定 \(7 ページ\)](#)

## Web 認証用の認証および認可リストの設定

### 手順

	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）。
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>wlan wlan-name wlan-id SSID-name</b> 例： Device(config)# <b>wlan wlan-bar 1 bar-ssid</b>	WLAN コンフィギュレーション サブモードを開始します。 <ul style="list-style-type: none"> <li>• <i>wlan-name</i> : 設定されている WLAN の名前です。</li> <li>• <i>wlan-id</i> : ワイヤレス LAN の ID です。</li> <li>• <i>SSID-name</i> : 最大 32 文字の英数字からなる SSID 名です。</li> </ul> (注) すでにこのコマンドを設定している場合は、 <b>wlan wlan-name</b> コマンドを入力します。
ステップ 4	<b>no security wpa</b> 例： Device(config-wlan)# <b>no security wpa</b>	WPA セキュリティを無効にします。
ステップ 5	<b>no security wpa akm dot1x</b> 例： Device(config-wlan)# <b>no security wpa akm dot1x</b>	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	<b>no security wpa wpa2</b> 例： Device(config-wlan)# <b>no security wpa wpa2</b>	WPA2 セキュリティを無効にします。

	コマンドまたはアクション	目的
ステップ 7	<pre>security web-auth {authentication-list authenticate-list-name   authorization-list authorize-list-name}  例 : Device(config-wlan)# security web-auth authentication-list authc-server-group</pre>	<p>dot1x セキュリティ用の認証または認可リストを有効にします。</p> <p>(注) WPA セキュリティ、dot1x の AKM、および WPA2 セキュリティを無効にしていない場合は、次のエラーが表示されます。</p> <pre>% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.</pre>
ステップ 8	<pre>end  例 : Device(config-wlan)# end</pre>	<p>特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。</p>

## 認証と認可の分割設定の確認

WLAN の詳細を表示するには、次のコマンドを使用します。

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

AAA 認証およびサーバの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
key cisco
!
radius server cisco-dnac-authz-server
address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
pac key cisco
!
!
aaa new-model
aaa session-id common
!
```



802.1Xセキュリティ用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name      : authc-server-group
802.1x authorization list name     : authz-server-group
802.1x                               : Enabled
```

Web 認証用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-bar | sec Webauth
Webauth On-mac-filter Failure      : Disabled
Webauth Authentication List Name   : authc-server-group
Webauth Authorization List Name    : authz-server-group
Webauth Parameter Map              : Disabled
```

## 設定例

サードパーティの RADIUS サーバを使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の設定 : 例

次に、サードパーティの RADIUS サーバを使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の設定例を示します。

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Cisco ISE または DNAC を使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の設定 : 例

次に、Cisco ISE または DNAC を使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の設定例を示します。

```
Device(config)# radius server cisco-dnac-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-dnac-authz-server
Device(config)# end
```

