複数の RADIUS サーバー間での認証および認可

複数の RADIUS サーバー間での認証および認可について

Catalyst アクセスポイント上のシスコ組み込み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 サーバー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 サーバーに分割することができます。

RADIUS サーバーは、認証サーバー、認可サーバー、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 サーバーで行う場合は、 組み込みワイヤレスコントローラ上の Session Aware Network（SANet）コンポーネントによって、クライアントが 組み込みワイヤレスコントローラに参加するときに一方のサーバーで認証を行い、別のサーバー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 サーバーを使用して実行できます。認証サーバーで認証が成功すると、組み込みワイヤレスコントローラは、認証サーバーから受信した属性を、認可サーバーとして指定された別の RADIUS サーバーに中継します。

その後、認可サーバーは次の処理を実行します。

- サーバー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、 組み込みワイヤレスコントローラに返す。

（注） 認証と認可の分割設定では、両方のサーバーを使用可能にする必要があります。また、組み込みワイヤレスコントローラがセッションを受け入れられるように、両方のサーバーで 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ーの分割による 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ー 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 サーバーのタイプをクリックします。

- RADIUS
- TACACS+
- LDAP

この手順では、RADIUS サーバー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 サーバーの名前と、サーバーの 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 サーバー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 サーバー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 サーバー 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 サーバーに送信される 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 サーバー 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ー 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、サーバー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、サーバー グループに含めるサーバーを選択し、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ーリストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** > **[Servers/Groups]** 選択します。

ステップ 2 [RADIUS] > [Servers] タブを選択します。

ステップ 3 [Add] をクリックして新しいサーバーを追加するか、既存のサーバーをクリックします。

ステップ 4 [Name]、[Server Address]、[Key]、[Confirm Key]、[Auth Port]、[Acct Port] を入力します。[PAC Key] チェックボックスをオンにして、[PAC key] と [Confirm PAC Key] を入力します。

ステップ 5 [Apply to Device] をクリックします。

ステップ 6 [RADIUS] > [Server Groups] を選択し、[Add] をクリックして新しいサーバーグループを追加するか、既存のサーバーグループをクリックします。

ステップ 7 サーバーグループの [Name] を入力し、そのサーバーグループに含めるサーバーを [Available Servers] リストから選択し、[Assigned Servers] リストに移動します。

ステップ 8 [Apply to Device] をクリックします。

明示的な認証サーバーリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**radius server** *server-name* 例： デバイス(config)# **radius server free-radius-authc-server**	RADIUS サーバー名を指定します。
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： デバイス(config-radius-server)# **address ipv4 9.2.62.56 auth-port 1812 acct-port 1813**	RADIUS サーバーのパラメータを指定します。
ステップ 5	[**pac**] **key** *key* 例： デバイス(config-radius-server)# **key cisco**	デバイスと、RADIUS サーバー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	**exit** 例： デバイス(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	**aaa group server radius** *server-group* 例： デバイス(config)# **aaa group server radius authc-server-group**	RADIUS サーバ グループの ID を作成します。 *server-group* はサーバー グループ名です。有効な範囲は 1 ～ 32 文字の英数字です。 コントローラに定義されたルートに RADIUS サーバーの IP アドレスが追加されていない場合、デフォルトルートが使用されます。AAA サーバーグループで定義された SVI からトラフィックを送信する特定のルートを定義することをお勧めします。
ステップ 8	**server name** *server-name* 例： デバイス(config)# **server name free-radius-authc-server**	サーバー名を設定します。
ステップ 9	**end** 例： デバイス(config)# **end**	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。

	コマンドまたはアクション	目的
		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ーリストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** > **[Servers/Groups]** 選択します。

ステップ 2 [RADIUS] > [Servers] タブを選択します。

ステップ 3 [Add] をクリックして新しいサーバーを追加するか、既存のサーバーをクリックします。

ステップ 4 [Name]、[Server Address]、[Key]、[Confirm Key]、[Auth Port]、[Acct Port] を入力します。[PAC Key] チェックボックスをオンにして、[PAC key] と [Confirm PAC Key] を入力します。

ステップ 5 [Apply to Device] をクリックします。

ステップ 6 [RADIUS] > [Server Groups] を選択し、[Add] をクリックして新しいサーバーグループを追加するか、既存のサーバーグループをクリックします。

ステップ 7 サーバーグループの [Name] を入力し、そのサーバーグループに含めるサーバーを [Available Servers] リストから選択し、[Assigned Servers] リストに移動します。

ステップ 8 [Apply to Device] をクリックします。

明示的な認可サーバーリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**radius server** *server-name* 例： `デバイス(config)# radius server cisco-dnac-authz-server`	RADIUS サーバー名を指定します。

	コマンドまたはアクション	目的
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： `デバイス(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	RADIUS サーバーのパラメータを指定します。
ステップ 5	[**pac**] **key** *key* 例： `デバイス(config-radius-server)# pac key cisco`	デバイスと、RADIUS サーバー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	**exit** 例： `デバイス(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	**aaa group server radius** *server-group* 例： `デバイス(config)# aaa group server radius authz-server-group`	RADIUS サーバ グループの ID を作成します。
ステップ 8	**server name** *server-name* 例： `デバイス(config)# server name cisco-dnac-authz-server`	
ステップ 9	**end** 例： `デバイス(config)# end`	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（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 5 [Apply to Device] をクリックします。

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	**enable** 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	**configure terminal** 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	**wlan** *wlan-name wlan-id SSID-name* 例： `デバイス(config)# wlan wlan-foo 222 foo-ssid`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：設定されている WLAN の名前です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 4	**security dot1x authentication-list** *authenticate-list-name* 例： `デバイス(config-wlan)# security dot1x authentication-list authc-server-group`	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	**security dot1x authorization-list** *authorize-list-name* 例： `デバイス(config-wlan)# security dot1x authorization-list authz-server-group`	dot1x セキュリティ用の認可リストを指定します。 **Cisco Digital Network Architecture Center**（**DNAC**）の詳細については、DNAC のマニュアルを参照してください。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `デバイス(config-wlan)# end`	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ーの分割による WLAN の Web 認証の設定

Web 認証用の認証および認可リストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [Layer2] タブで、[WPA Policy]、[AES]、および [802.1x] チェックボックスをオフにします。

ステップ 5 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストから認可リストを選択します。

ステップ 6 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 7 [Apply to Device] をクリックします。

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	**enable** 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	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**wlan** *wlan-name wlan-id SSID-name* 例： `デバイス(config)# wlan wlan-bar 1 bar-ssid`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：設定されている WLAN の名前です。 • *wlan-id*：ワイヤレス LAN の ID です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 4	**no security wpa** 例： `デバイス(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `デバイス(config-wlan)# no security wpa akm dot1x`	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	**no security wpa wpa2** 例： `デバイス(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*} 例： `デバイス(config-wlan)# security web-auth authentication-list authc-server-group`	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。 （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。 *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*

	コマンドまたはアクション	目的
ステップ 8	**end** 例： デバイス(config-wlan)# **end**	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 認証およびサーバー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 サーバーを使用した認証のための Catalyst アクセスポイント上のシスコ組み込み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 サーバーを使用した認証のための Catalyst アクセスポイント上のシスコ組み込み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 Catalyst アクセスポイント上のシスコ組み込み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 Catalyst アクセスポイント上のシスコ組み込み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
```

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。