RADIUS レルム

RADIUS レルムについて

RADIUS レルム機能は、ユーザーのドメインに関連付けられています。クライアントはこの機能を使用して、認証とアカウンティングの処理に使用する RADIUS サーバーを選択できます。

モバイル クライアントが WLAN に関連付けられている場合、Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement（EAP-AKA）の ID 応答要求の一部として、認証要求パケット内で RADIUS レルムを受信します。WLAN のネットワーク アクセス ID（NAI）形式（EAP-AKA）は、*username@domain.com* として指定できます。NAI 形式のレルムは @ 記号の後ろに示され、domain.com として指定されます。ベンダー固有の属性が *test* として追加された場合は、NAI 形式は test@domain.com として表されます。

RADIUS レルム機能は、WLAN で有効または無効にすることができます。レルムが WLAN で有効になっている場合、対応するユーザーはユーザー名を NAI 形式で送信する必要があります。 組み込みワイヤレスコントローラは、クライアントから受信した NAI 形式のレルムが定められた標準に従っている場合にのみ、AAA サーバーに認証要求を送信します。認証とは別に、アカウンティング要求もレルム フィルタリングに基づいて AAA サーバーに送信する必要があります。

WLAN 上のレルム サポート

各 WLAN は NAI レルムをサポートするように設定されます。レルムが特定の SSID に対して有効になると、RADIUS サーバー上で設定されたレルムに対して EAP ID 応答で受信したレルムを照合するためのルックアップが実行されます。クライアントがレルムとともにユーザー名を送信しない場合は、WLAN で設定されているデフォルトの RADIUS サーバーが認証に使用

されます。クライアントから受信したレルムが、WLAN上で設定されているレルムと一致しない場合、クライアントは認証解除され、ドロップされます。

RADIUS レルム機能が WLAN で有効になっていない場合は、EAP ID 要求の一部として受信したユーザー名がユーザー名として直接使用され、設定されているRADIUSサーバーが認証およびアカウンティングに使用されます。デフォルトでは、RADIUS レルム機能は WLAN で無効になっています。

- **認証用のレルム照合**：EAP方式を使用したdot1x（EAP AKAと同様）では、ユーザー名がEAP ID 応答の一部として受信されます。レルムはユーザー名から抽出され、対応するRADIUS認証サーバーですでに設定されているレルムと照合されます。一致した場合は、認証要求がRADIUSサーバーに転送されます。一致しなかった場合は、クライアントが認証解除されます。
- **アカウンティング用のレルム照合**：クライアントのユーザ名がaccess-acceptメッセージを通じて受信されます。アカウンティングメッセージがトリガーされると、対応するクライアントのユーザー名からレルムが抽出され、RADIUSアカウンティング サーバー上で設定されたアカウンティング レルムと比較されます。一致した場合は、アカウンティング要求がRADIUSサーバーに転送されます。一致しなかった場合は、アカウンティング要求が破棄されます。

RADIUS レルムの有効化

RADIUS レルムを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless aaa policy** *aaa-policy* **例**： `Device(config)# wireless aaa policy policy-1`	新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** **例**： `Device(config-aaa-policy)# aaa-realm enable`	AAA RADIUS レルムの選択を有効にします。 （注） RADIUS レルムを無効にするには、**no aaa-realm enable** または **default aaa-realm enable** コマンドを使用します。

認証およびアカウンティング用に RADIUS サーバーと照合するためのレルムの設定

認証およびアカウンティング用にRADIUSサーバーと照合するようにレルムを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 3	**aaa authorization network default group** *radius-server-group* 例： `Device(config)# aaa authorization network default group aaa_group_name`	許可の方法を設定します。
ステップ 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication dot1x cisco.com group cisco1`	dot1x がレルム グループ RADIUS サーバーを使用する必要があることを示します。
ステップ 5	**aaa authentication login** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication login cisco.com group cisco1`	ログイン時の認証方法を定義します。
ステップ 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* 例： `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。

WLAN の AAA ポリシーの設定

WLAN の AAA ポリシーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless aaa policy** *aaa-policy-name* 例： `Device(config)# wireless aaa policy aaa-policy-1`	ワイヤレスの新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** 例： `Device(config-aaa-policy)# aaa-realm enable`	レルム別の AAA RADIUS サーバーの選択を有効にします。
ステップ 4	**exit** 例： `Device(config-aaa-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless profile policy** *wlan-policy-profile* 例： `Device(config)# wireless profile policy wlan-policy-a`	WLAN ポリシープロファイルを設定します。
ステップ 6	**aaa-policy** *aaa-policy* 例： `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	AAA ポリシーをマッピングします。
ステップ 7	**accounting-list** *acct-config-realm* 例： `Device(config-wireless-policy)# accounting-list cisco.com`	アカウンティング リストを設定します。
ステップ 8	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan wlan2 14 wlan-aaa`	WLAN を設定します。
ステップ 10	**security dot1x authentication-list** *auth-list-realm* 例： `Device(config-wlan)# security dot1x authentication-list cisco.com`	IEEE 802.1x のセキュリティ認証リストを有効にします。
ステップ 11	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**wireless tag policy** *policy* 例： `Device(config)# wireless tag policy tag-policy-1`	ポリシー タグを設定します。
ステップ 13	**wlan** *wlan-name* **policy** *policy-profile* 例： `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	ポリシープロファイルを WLAN にマッピングします。
ステップ 14	**exit** 例： `Device(config-policy-tag)# exit`	グローバル コンフィギュレーション モードに戻ります。

RADIUS レルム設定の確認

RADIUS レルム設定を確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail


Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
```

```
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 9.4.23.50
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
```

```
              VLAN            : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

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。