

# NAC ( CCA ) : ACS を使用した Clean Access Manager ( CAM ) の認証の設定

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[ACS で CCA の認証を設定するステップ](#)

[ACS の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この資料に Cisco Secure Access Control Server ( ACS ) で Clean Access Manager ( CAM ) の認証を設定する方法を記述されています。ACS 5.x およびそれ以降を使用して同じような設定に関しては、[NAC \( CCA \)](#) を参照して下さい: [ACS 5.x およびそれ以降で Clean Access Manager の認証を設定して下さい](#)。

## 前提条件

### 要件

この設定は CAM バージョン 3.5 以降に適用されます。

### 使用するコンポーネント

このドキュメントの情報は、CAM バージョン 4.1 に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

## ACS で CCA の認証を設定するステップ

次の手順を実行します。

1. **新しいロールの追加 管理ロールの作成** CAM で、> **ユーザの役割** > **新しいロール** 『User Management』 を選択して下さい。[Role Name] フィールドに、そのロールの固有の名前 ( **admin** ) を入力します。オプションの [Role Description] に「**Admin User Role**」と入力します。[Role Type] で [Normal Login Role] を選択します。適切な VLAN でアウトオブバンド ( OOB ) ユーザ ロール VLAN を設定します。たとえば、[VLAN ID] を選択して、「10」として ID を指定します。完了したら、[Create Role] をクリックします。フォームのデフォルト プロパティを復元するには、[Reset] をクリックします。「[OOB ロール ベース マッピングの VLAN のタグ付け](#)」セクションに示されているように、ロールが [List of Roles] タブに表示されます。**ユーザ ロールの作成** CAM で、> **ユーザの役割** > **新しいロール** 『User Management』 を選択して下さい。[Role Name] フィールドに、そのロールの固有の名前 ( **users** ) を入力します。オプションの [Role Description] に「**Normal User Role**」と入力します。適切な VLAN でアウトオブバンド ( OOB ) ユーザ ロール VLAN を設定します。たとえば、[VLAN ID] を選択して、「20」として ID を指定します。完了したら、[Create Role] をクリックします。フォームのデフォルト プロパティを復元するには、[Reset] をクリックします。「[OOB ロール ベース マッピングの VLAN のタグ付け](#)」セクションに示されているように、ロールが [List of Roles] タブに表示されます。
2. **OOB ロール ベース マッピングの VLAN のタグ付け** CAM で、> **ユーザの役割** > **ロールのリスト** ロールのリストをこれまでのところ見るために『User Management』 を選択して下さい。
3. **RADIUS 認証サーバ ( ACS ) の追加**[User Management] > [Auth Servers] > [New] の順に選択します。[Authentication Type] ドロップダウン メニューから [Radius] を選択します。[Provider Name] に「**ACS**」と入力します。[Server Name] に「**auth.cisco.com**」と入力します。[Server Port] : RADIUS サーバがリッスンするポート番号 ( **1812** ) を入力します。[Radius Type] : RADIUS 認証方式。サポート対象は、EAPMD5、PAP、CHAP、MSCHAP、および MSCHAP2 の方式です。ACS へのマッピングが正しく定義または設定されていない場合、あるいは ACS で RADIUS 属性が正しく定義または設定されていない場合、[Default Role] が使用されます。[Shared Secret] : 指定されたクライアントの IP アドレスにバインドされた RADIUS 共有秘密キー。[NAS-IP-Address] : すべての RADIUS 認証パケットとともに送信される値。[Add Server] をクリックします。
4. **ACS ユーザの CCA ユーザ ロールへのマッピング** ACS の管理ユーザを CCA 管理ユーザに

マップするには、[User Management] > [Auth Servers] > [Mapping Rules] > [Add Mapping Link] の順に選択します。ACS の通常のユーザを CCA ユーザ ロールにマップするには、[User Management] > [Auth Servers] > [Mapping Rules] > [Add Mapping Link] の順に選択します。ユーザ ロールのマッピングの概要を次に示します。

5. [User Page] での代替プロバイダーの有効化ユーザ ログイン ページで代替プロバイダーを有効にするには、[Administration] > [User Pages] > [Login Page] > [Add] > [Content] の順に選択します。

## ACS の設定

1. RADIUS ( IETF ) クラス属性 [025] が有効になることを確かめるために『Interface Configuration』を選択して下さい。
2. ACS サーバに RADIUSクライアントを追加して下さい示されているように AAA クライアント CAM を追加するために『Network Configuration』を選択して下さい:[Submit + Restart] をクリックします。注: ことを AAA クライアントが付いている RADIUS 鍵マッチ確かめ、RADIUS ( IETF ) を使用します。示されているように AAA クライアント CAS を追加するために『Network Configuration』を選択して下さい:[Submit + Restart] をクリックします。注: 説明する VPNゲートウェイ RADIUS に関しては CCA ポリシーは CAS IP アドレスからの RADIUS 説明パケット ( UDP 1646/1813 ) が ACS サーバのIPアドレスに非認証を通るようになる必要があります。示されているように AAA クライアント ASA を追加するために『Network Configuration』を選択して下さい:ユーザ左側 PIX/ASA インターフェイス アドレス ( 一般的に 内部インターフェイス ) RADIUS ( Cisco IOS/PIX ) へのセット型。
3. ACS サーバに /Configure グループを追加して下さいAdmin group を作成して下さいグループ値を割り当てるために IETF RADIUS クラス属性 [025] を設定して下さい。値は CAS マッピングで設定されるそれを一致する必要があります。ユーザグループを作成して下さい各 Clean Access ユーザの役割のためのグループを追加して下さい/マッピングされるために設定して下さい。ACS サーバの追加して下さい/設定 ユーザ各 Clean Access ユーザ向けの ACS ユーザを追加して下さい/ACS によって認証されるために設定して下さい。ACS 団体会員を設定して下さい。ACS はまた他の外部サーバにプロキシ認証をサポートします。

## 確認

ここでは、設定が正常に動作していることを確認します。

セクションを監察する ACS では渡される示されているように認証の情報を表示できます:

同様に、RADIUS 会計についてはスクリーン ショットを次のように表示できます:

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco NAC アプライアンスに関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)