

Cisco Access Control Server (ACS) を使用した 5760 Web インターフェイス特権レベルに基づ くアクセス制御の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[ACS での少数のテスト ユーザの作成](#)

[ポリシー要素とシェル プロファイルの設定](#)

[特権レベル 15 のシェル アクセス プロファイルの作成](#)

[管理者ユーザ用のコマンド セットの作成](#)

[読み取り専用ユーザのシェル プロファイルの作成](#)

[TACACS プロトコルに一致するサービス選択ルールの作成](#)

[フル管理アクセスのための認証ポリシーの作成](#)

[読み取り専用管理アクセスのための認証ポリシーの作成](#)

[TACACS に対応した 5760 の設定](#)

[2 つの異なるプロファイルを使用した同じ 5760 へのアクセス](#)

[関連するシスコ サポート コミュニティ ディスカッション](#)

概要

このドキュメントでは、さまざまな特権レベルの Cisco ACS TACACS+ 認証および認可プロファイルを作成し、WebUI へのアクセスのために 5760 に統合する方法について説明します。この機能は 3.6.3 以降でサポートされています (ただし、このドキュメントの執筆時点では 3.7.x ではサポートされていません)。

前提条件

要件

このドキュメントでは、読者が Cisco ACS および Converged Access コントローラ コンフィギュレーションを理解していることを前提としています。このドキュメントは、TACACS+ 認証における次の 2 つのコンポーネント間のインタラクションのみに重点を置いています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Converged Access 5760 リリース 3.6.3

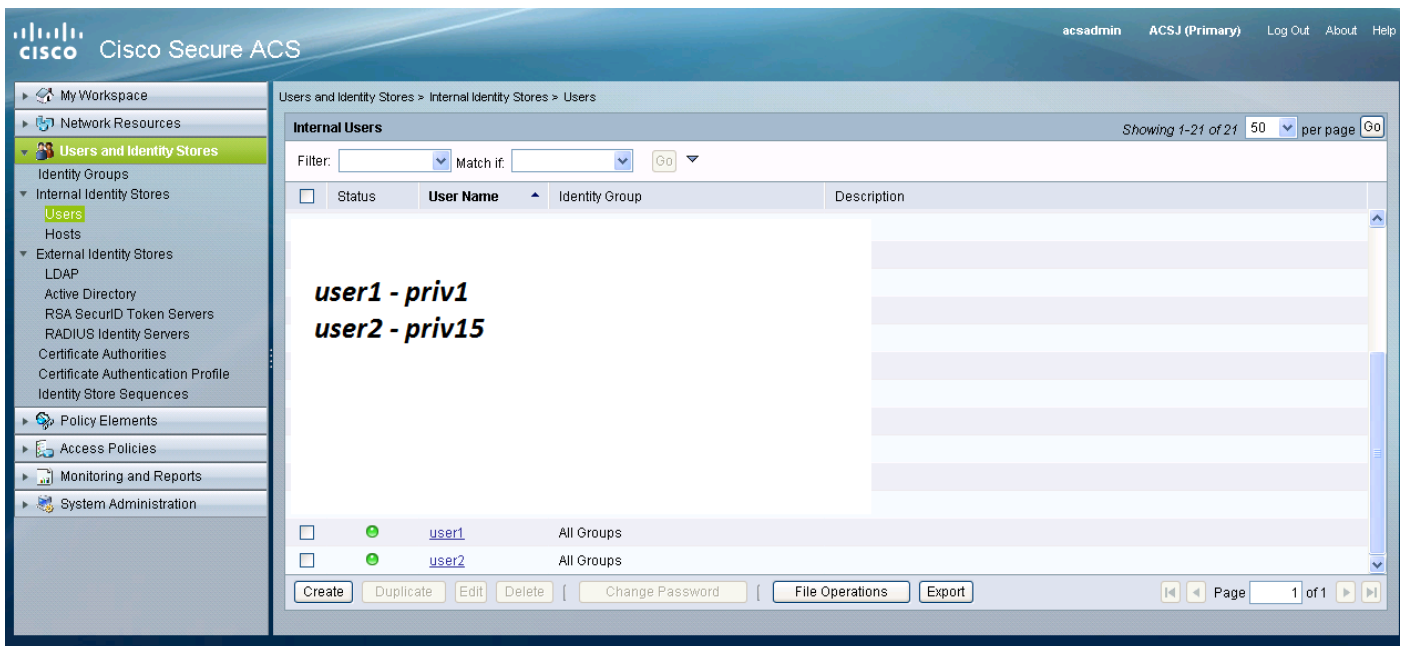
- Cisco Access Control Server (ACS) 5.2

コンフィギュレーション

ACS での少数のテスト ユーザの作成

[Users and Identity Stores] をクリックしてから、[Users] を選択します。

[Create] をクリックし、次に示すような少数のテスト ユーザを設定します。



ポリシー要素とシェル プロファイルの設定

cisco tacacsの世界で2種類のアクセス.Privilege 15用に2つのプロファイルを作成する必要があります。つまり、デバイスへのフルアクセスを制限なく提供します。一方、特権1では、ログインして実行できるコマンドの数は限られています。次に、シスコが提供するアクセスレベルの簡単な説明を示します。

特権レベル 1 = 特権なし (プロンプトは router>)、ログインのデフォルト レベル

特権レベル 15 = 特権あり (プロンプトは router#)、イネーブル モードに入った後のレベル

特権レベル 0 = ほとんど使用されませんが、5つのコマンド (disable、enable、exit、help、logout

5760では、レベル2 ~ 14はレベル1と同じとみなされます。これらのレベルには1と同じ権限が与えられます。5760で特定のコマンドに対してtacacs権限レベルを設定しないでください。タブによる UI アクセスは 5760 ではサポートされていません。フル アクセス (priv15) または [Monitor] タブへのアクセスのみ (priv1) のいずれかが設定されます。特権レベル 0 のユーザは、ログインできません。

特権レベル 15 のシェル アクセス プロファイルの作成

次に示す画面を使用してこのプロファイルを作成します。

[Policy Elements] をクリックします。 [Shell Profiles] をクリックします。

新しいプロファイルを作成します。

[Common Tasks] タブに移動し、デフォルト特権レベルおよび最大特権レベルを 15 に設定します。



管理者ユーザ用のコマンドセットの作成

コマンドセットは、すべてのTACACSデバイスで使用されるコマンドのセットです。特定のプロファイルが割り当てられている場合にユーザが使用できるコマンドを制限するために使用できます。5760では、渡された特権レベルに基づいて WebUI コードで制限が設定されるため、レベル 1 とレベル 15 の両方のコマンドセットは同一になります。

Cisco Secure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address https://9.10.40.56/acsadmin/

acesadmin ACSJ (Primary)

Cisco Secure ACS

Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Edit: "PermitAllCmds"

General

Name: PermitAllCmds

Description:

Permit any command that is not in the table below

Grant	Command	Arguments
-------	---------	-----------

Add A Edit V Replace A Delete

Grant Command Arguments

Permit

Submit Cancel

読み取り専用ユーザのシェル プロファイルの作成

読み取り専用ユーザのシェル プロファイルを作成します。このプロファイルは、特権レベルが 1 に設定されていることが異なります。

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "joseph1"

General **Common Tasks** Custom Attributes

Privilege Level

Default Privilege: Static Value 1

Maximum Privilege: Static Value 1

Shell Attributes

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use


No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

Callback Line: Not in Use

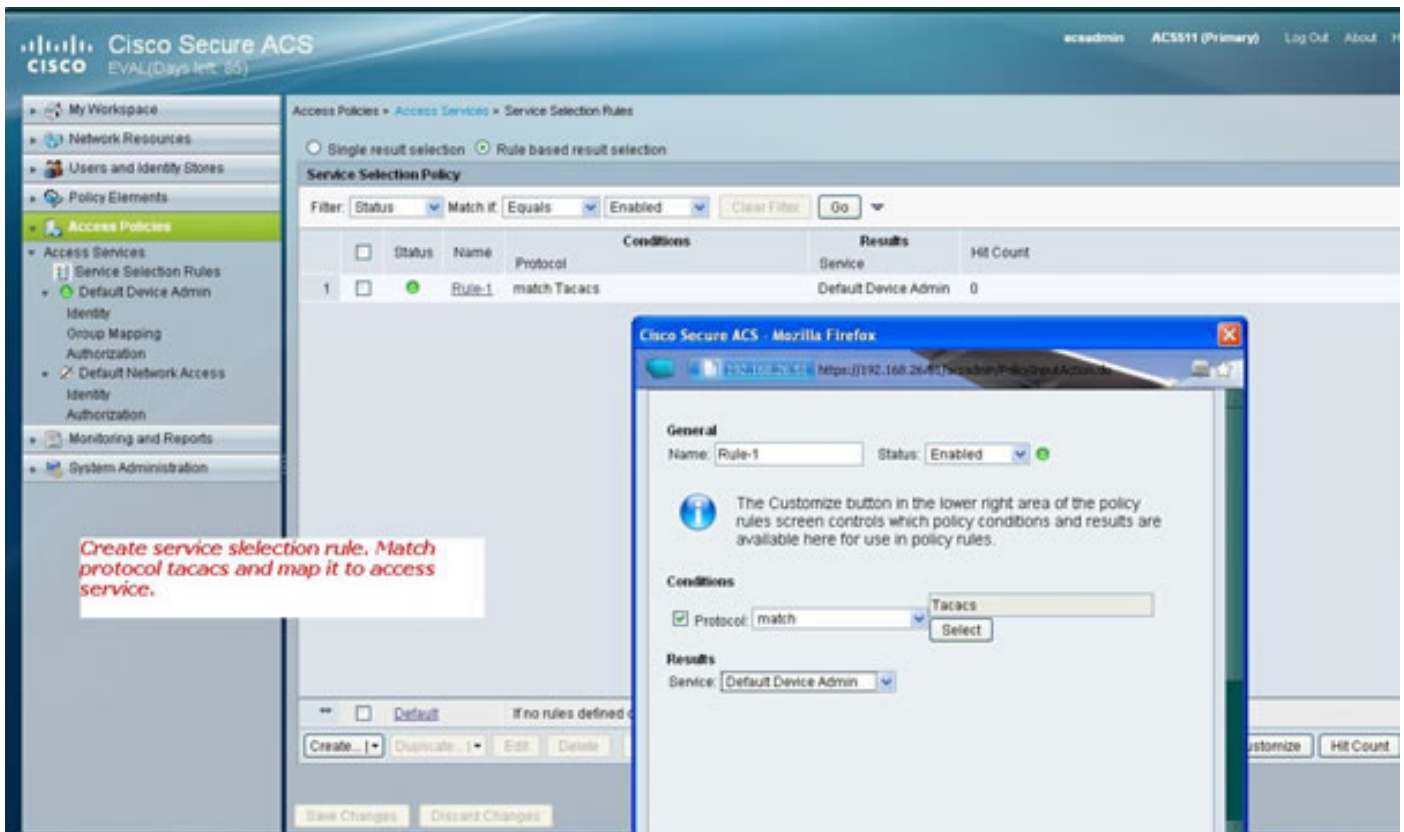
Callback Rotary: Not in Use

 = Required fields

Submit Cancel

TACACS プロトコルに一致するサービス選択ルールの作成

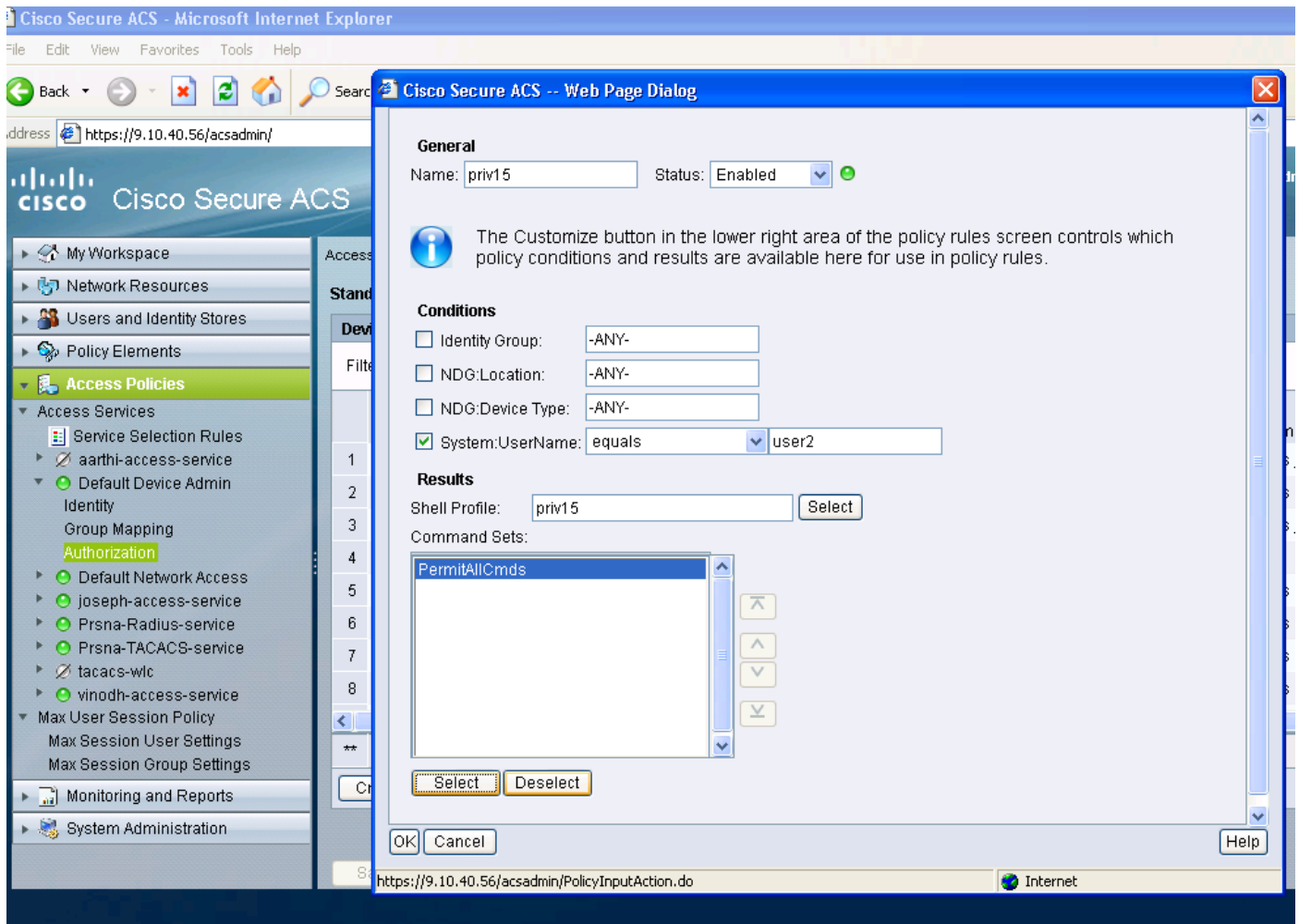
ポリシーと設定に基づき、5760 から送信される TACACS と一致するルールがあることを確認します。



フル管理アクセスのための認証ポリシーの作成

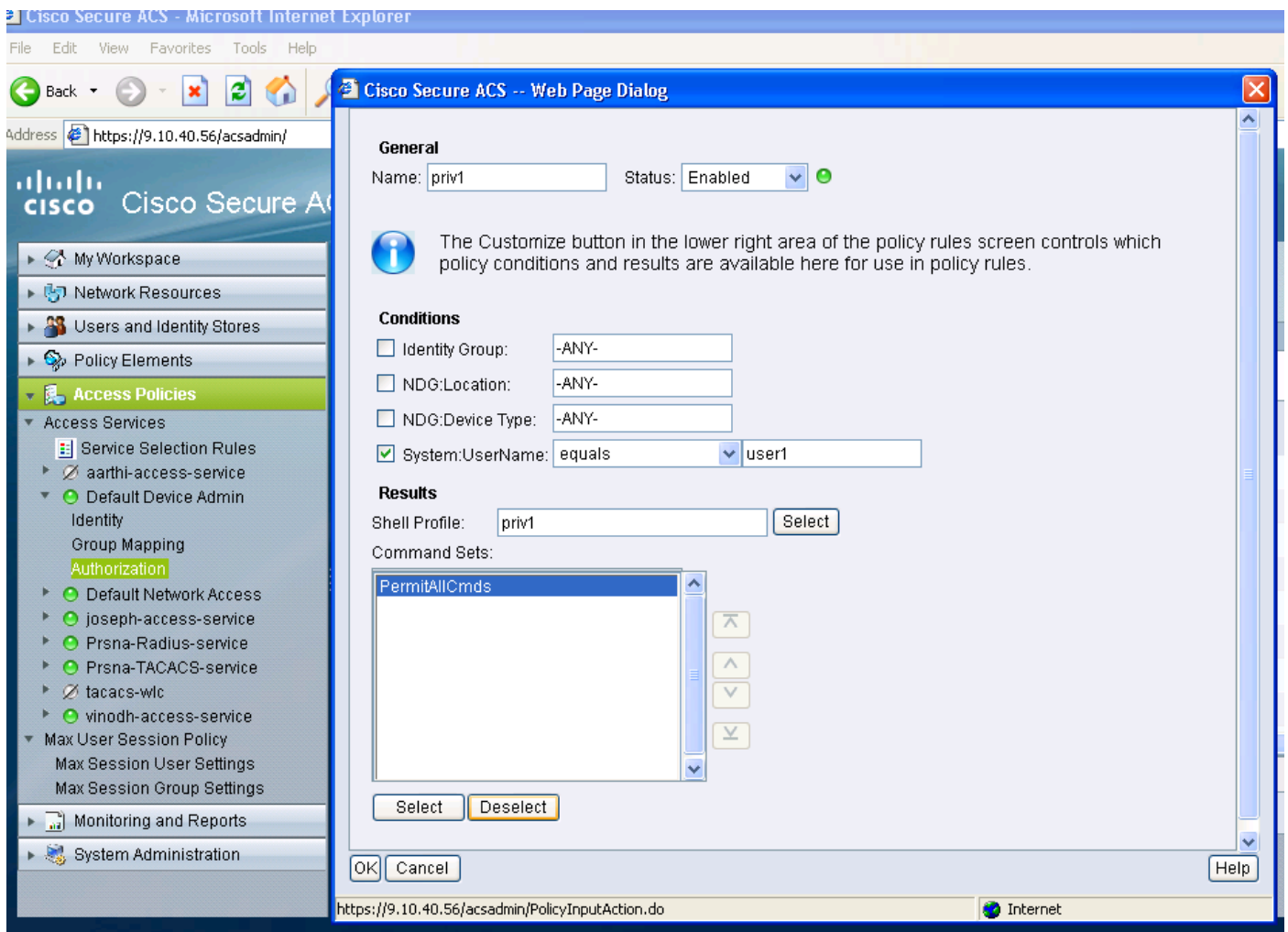
TACACS プロトコルの選択に使用する Default Device Admin ポリシーは、評価ポリシー プロセスの一部として選択されます。認証に TACACS プロトコルを使用する場合、選択されるサービス ポリシーは Default Device Admin ポリシーと呼ばれます。このポリシーは 2 つのセクションで構成されています。アイデンティティとは、ユーザが誰であるか、ユーザがどのグループに属しているか（ローカルまたは外部）、および設定されている認証プロファイルに基づいてユーザがどの操作を実行できるかを示します。設定するユーザに関連するコマンド セットを割り当てます。

。



読み取り専用管理アクセスのための認証ポリシーの作成

読み取り専用ユーザにも同様の内容が該当します。この例では、ユーザ 1 に特権レベル 1 シェルプロファイルを設定し、ユーザ 2 に特権レベル 15 シェルプロファイルを設定します。



TACACS に対応した 5760 の設定

1. RADIUS/TACACS サーバを設定する必要があります。

```
tacacs server tac_acct
```

```
address ipv4 9.1.0.100
```

```
key cisco
```

2. サーバグループの設定

```
aaa group server tacacs+ gtac
```

```
server name tac_acct
```

上記のステップまでは、前提条件はありません。

3. 認証および認可のメソッドリストを設定します。

```
aaa authentication login <method-list> group <srv-grp>
```

```
aaa authorization exec <method-list> group srv-grp>
```

```
aaa authorization exec default group <srv-grp> —httpでtacacsを取得するための回避策。
```

上記の3つのコマンドとその他のすべての認証および認可パラメータでは、同じデータベース

(RADIUS/TACACS またはローカル) を使用する必要があります。

たとえば、コマンド認可を有効にする必要がある場合は、コマンド認可が同じデータベースをポイントしている必要もあります。

例 :

aaa authorization commands 15 <method-list> group <srv-grp> →データベース (tacacs/radiusまたはローカル) を指すサーバグループは同じである必要があります。

4. 上記のメソッド リストを使用するように HTTP を設定します。

ip http authentication aaa login-auth <method-list> →方式リストが「デフォルト」であっても、ここで明示的に指定する必要があります。

```
ip http authentication aaa exec-auth <method-list>
```

** 注意点

- 「line vty」設定パラメータに対してメソッド リストを設定しないでください。上記の手順と line vty の設定が異なる場合は、line vty の設定が優先されます。
- データベースは SSH/Telnet や webui などのすべての管理設定タイプで同じにする必要があります。
- HTTP 認証では明示的にメソッド リストが定義されている必要があります。

2 つの異なるプロファイルを使用した同じ 5760 へのアクセス

限られたアクセス権限が付与される 特権レベル 1 ユーザからのアクセスを次に示します。

The screenshot shows the Cisco Wireless Controller web interface. The browser address bar displays the URL `9.12.137.95/wireless`. The navigation menu at the top includes `Home`, `Monitor`, and `Help`, with `Home` circled in red. The main content area is divided into two columns. The left column contains `System Summary` and `Access Point Summary`. The right column contains a search bar, `Top WLANs` table, and `AVC for WLAN : QM` section.

Profile Name	Number of Clients
QM	0
jalouisan	0

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

フル アクセス権限が付与される 特権レベル 15 ユーザからのアクセスを次に示します。

System Summary

System Time	18:51:40.772 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CTS760
Up Time	9 hours, 26 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	Detail

Access Point Summary

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

Client Summary

Protocol Statistics

Search

Username

Top WLANs

Profile Name	Number of Clients
QM	0
jolouisan	0

AVC for WLAN : QM

AVC is not enabled on this WLAN

Rogue APs

Active Rogue APs 207 [Detail](#)