

Cisco Unified Wireless Network TACACS+ の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[コントローラでの TACACS+ の実装](#)

[\[Authentication\]](#)

[許可](#)

[アカウントिंग](#)

[WLC での TACACS+ 設定](#)

[TACACS+ 認証サーバの追加](#)

[TACACS+ 認可サーバの追加](#)

[TACACS+ アカウントिंगサーバの追加](#)

[認証順序の設定](#)

[設定の確認](#)

[Cisco Secure ACS サーバの設定](#)

[ネットワーク設定](#)

[インターフェイス設定](#)

[ユーザ/グループ設定](#)

[Cisco Secure ACS のアカウントिंगレコード](#)

[WCS での TACACS+ 設定](#)

[仮想ドメインを使用した WCS](#)

[Cisco Secure ACS が WCS を使用する設定](#)

[ネットワーク設定](#)

[インターフェイス設定](#)

[ユーザ/グループ設定](#)

[デバッグ](#)

[WLC からの role1=ALL のデバッグ](#)

[WLC からの複数のロールのデバッグ](#)

[WLC からの認可エラーのデバッグ](#)

[関連情報](#)

概要

このドキュメントでは、Cisco ワイヤレス LAN コントローラ (WLC) での Terminal Access Controller Access Control System Plus (TACACS+) と、Cisco Unified Wireless Network の

Cisco Wireless Control System (WCS) の設定例について説明します。このドキュメントでは、基本的なトラブルシューティングのヒントのいくつかを説明します。

TACACS+ はクライアント/サーバ プロトコルであり、ルータまたはネットワーク アクセス サーバに管理アクセスしようとするユーザに、一元化されたセキュリティを提供します。TACACS+ は次の AAA サービスを提供します。

- ネットワーク機器にログインしようとするユーザの認証
- ユーザに許可するアクセスレベルを決める認可
- ユーザが行うすべての変更を追跡するアカウントिंग

AAA サービスおよび TACACS+ 機能の詳細については、「[TACACS+ の設定](#)」を参照してください。

TACACS+ と RADIUS の比較については、「[TACACS+ と RADIUS の比較](#)」を参照してください。

[前提条件](#)

[要件](#)

次の項目に関する知識があることが推奨されます。

- WLC と Lightweight アクセス ポイント (LAP) の基本動作のための設定方法に関する知識
- Lightweight アクセス ポイント プロトコル (LWAPP) とワイヤレスのセキュリティ方式に関する知識
- RADIUS および TACACS+ の基礎知識
- Cisco ACS 設定の基礎知識

[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 Secure ACS for Windows バージョン 4.0
- バージョン4.1.171.0が稼働するCisco Wireless LAN Controller。WLCのTACACS+機能は、ソフトウェアバージョン4.1.171.0以降でサポートされています。
- バージョン4.1.83.0が稼働するCisco Wireless Control System。WCSのTACACS+機能は、ソフトウェアバージョン4.1.83.0以降でサポートされています。

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ました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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。

[コントローラでの TACACS+ の実装](#)

[Authentication]

認証は、ユーザ名とパスワードを使用するローカル データベース、RADIUS、TACACS+ サーバのいずれかで実行できます。実装は完全にモジュール単位というわけではありません。認証サービスと認可サービスは相互に拘束されます。たとえば、RADIUS/ローカル データベースで認証を実行した場合、認可は TACACS+ で実行されません。ローカル データベースか RADIUS データベースでユーザに関連している、読み取り専用または読み取りと書き込みなどの権限が使用されます。認証を TACACS+ で実行すると、認可は TACACS+ に拘束されます。

複数のデータベースが設定されている場合は、バックエンド データベースが参照される順序を指示するために CLI が提供されます。

許可

認可はタスク ベースであり、実際のコマンドごとの認可ではありません。タスクはさまざまなタブにマッピングされており、現在の Web GUI に表示される 7 個のメニュー バー項目に対応します。そのメニュー バー項目は次のとおりです。

- MONITOR
- WLANS
- CONTROLLER
- WIRELESS
- SECURITY
- MANAGEMENT
- COMMAND

このようにマッピングされているのは、多くのお客様が CLI の代わりに Web インターフェイスを使用してコントローラを設定するためです。

ロビー管理者権限のみが必要なユーザは、ロビー管理者管理 (LOBBY) の別のロールを使用できます。

ユーザに資格があるタスクは、Attribute-Value (AV) ペアを使用して TACACS+ (ACS) サーバで設定します。ユーザは、1 つ以上のタスクに認可できます。最小の認可は MONITOR のみであり、最大の認可は ALL (7 個すべてのタブを実行する認可) です。ユーザに特定のタスクの資格がない場合でも、ユーザは読み取り専用モードでそのタスクにアクセスできます。認証が有効であり、認証サーバに到達できなくなったか、認証サーバが認可できない場合、ユーザはコントローラにログインできません。

注：TACACS+による基本管理認証が成功するには、WLCで認証サーバと認可サーバを設定する必要があります。アカウントिंगの設定は任意です。

アカウントिंग

特定のユーザが開始した操作が正常に実行されるたびに、アカウントिंगが発生します。変更された属性は、TACACS+ アカウントिंग サーバに次のものとともに記録されます。

- 変更した個人のユーザ ID
- ユーザがログインしたりリモート ホスト
- コマンドが実行された日時
- ユーザの認可レベル

• どの操作が実行されたか、および指定された値に関する情報を提供する文字列
アカウントिंग サーバに到達できなくなっても、ユーザはセッションを続けることができます。

注：アカウントングレコードは、ソフトウェアリリース4.1以降ではWCSから生成されません。

WLC での TACACS+ 設定

WLC ソフトウェア リリース 4.1.171.0 以降では、CLI と Web GUI の新しい変更が導入され、WLC で TACACS+ 機能が有効になります。導入された CLI は、このセクションで参照用にリストされています。Web GUI で対応する変更は、[Security] タブに追加されています。

このドキュメントでは、WLC の基本的な設定がすでに完了していることが想定されています。

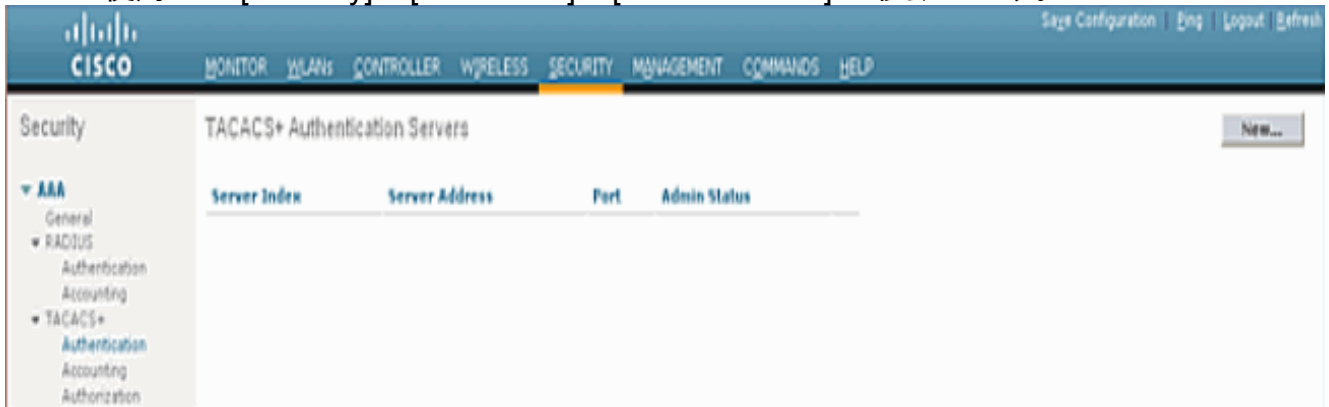
WLC コントローラで TACACS+ を設定するには、次の手順を実行する必要があります。

1. [TACACS+ 認証サーバの追加](#)
2. [TACACS+ 認可サーバの追加](#)
3. [TACACS+ アカウントング サーバの追加](#)
4. [認証順序の設定](#)

TACACS+ 認証サーバの追加

TACACS+ 認証サーバを追加するには、次の手順を実行します。

1. GUI を使用して [Security] > [TACACS+] > [Authentication] に移動します。



2. TACACS+ サーバの IP アドレスを追加し、共有秘密鍵を入力します。必要に応じて、デフォルト ポート TCP/49 を変更します。

3. [Apply] をクリックします。CLI からこれを実行するには、コマンド `config tacacs auth add <Server Index> <IP addr> <port> [ascii/hex] <secret>` を使用します。

(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123

TACACS+ 認可サーバの追加

TACACS+ 認可サーバを追加するには、次の手順を実行します。

1. GUI から [Security] > [TACACS+] > [Authorization] に移動します。
2. TACACS+ サーバの IP アドレスを追加し、共有秘密鍵を入力します。必要に応じて、デフォルトポート TCP/49 を変更します。

3. [Apply] をクリックします。CLI からこれを実行するには、コマンド `config tacacs athr add <Server Index> <IP addr> <port> [ascii/hex] <secret>` を使用します。

(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123

TACACS+ アカウンティングサーバの追加

TACACS+ アカウンティングサーバを追加するには、次の手順を実行します。

1. GUI を使用して [Security] > [TACACS+] > [Accounting] に移動します。

2. サーバの IP アドレスを追加し、共有秘密鍵を入力します。必要に応じて、デフォルトポート TCP/49 を変更します。

The screenshot shows the Cisco GUI for configuring TACACS+ Accounting Servers. The page title is "TACACS+ Accounting Servers > New". The left sidebar shows the navigation menu with "TACACS+ Accounting" selected. The main content area contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.1.1.12
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Port Number: 49
- Server Status: Enabled
- Retransmit Timeout: 2 seconds

Buttons for "< Back" and "Apply" are visible in the top right corner.

3. [Apply] をクリックします。CLI からこれを実行するには、コマンド `config tacacs acct add <Server Index> <IP addr> <port> [ascii/hex] <secret>` を使用します。

(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123

認証順序の設定

この手順では、複数のデータベースが設定されているとき、認証の AAA 順序を設定する方法について説明します。認証の順序は、ローカルおよび RADIUS または ローカルおよび TACACS にすることができます。認証順序のデフォルト コントローラ設定はローカルおよび RADIUS です。

認証順序を設定するには、次の手順を実行します。

1. GUI から [Security] > [Priority Order] > [Management User] に移動します。
2. [Authentication Priority] を選択します。この例では TACACS+ が選択されています。
3. 選択を有効にするには、[Apply] をクリックします。

The screenshot shows the Cisco GUI for configuring Authentication Priority. The page title is "Priority Order > Management User". The left sidebar shows the navigation menu with "Priority Order" selected. The main content area contains the following fields:

- Authentication Priority: Radio buttons for RADIUS and TACACS+ (TACACS+ is selected).
- *Local is implicitly set as the first server to try for authentication.

An "Apply" button is visible in the top right corner.

`config aaa auth mgmt <server1> <server2>` コマンドを使用して CLI からこれを実行することができます。

(Cisco Controller) >config aaa auth mgmt tacacs local

設定の確認

このセクションでは、WLC での TACACS+ 設定の確認に使用するコマンドについて説明します。設定が正しいかどうかの判断に役立つ、便利な **show** コマンドは次のとおりです。

- **show aaa auth** : 認証順序に関する情報を表示します。

```
(Cisco Controller) >show aaa auth
Management authentication server order:
 1..... local
 2..... Tacacs
```

- **show tacacs summary** : TACACS+ サービスと統計情報の概要を表示します。

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2
```

```
Authorization Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2
```

```
Accounting Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2
```

- **show tacacs auth stats** : TACACS+ 認証サーバの統計情報を表示します。

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 7
Retry Requests..... 3
Accept Responses..... 3
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 12
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **show tacacs athr stats** : TACACS+ 認可サーバの統計情報を表示します。

```
(Cisco Controller) >show tacacs athr statistics
Authorization Servers:

Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 3
Retry Requests..... 3
Received Responses..... 3
Authorization Success..... 3
Authorization Failure..... 0
Challenge Responses..... 0
```

```
Malformed Msgs..... 0
Bad Athenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **show tacacs acct stats** : TACACS+ アカウンティング サーバの統計情報を表示します。

```
(Cisco Controller) >show tacacs acct statistics
Accounting Servers:
```

```
Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 133
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 399
Unknowntype Msgs..... 0
Other Drops..... 0
```

Cisco Secure ACS サーバの設定

このセクションでは、TACACS+ ACS サーバがサービスとカスタム属性を作成し、ユーザまたはグループにロールを割り当てることに関連する手順について説明します。

ユーザとグループの作成については説明しません。ユーザとグループは必要に応じて作成されていることが想定されています。ユーザとユーザグループの作成方法については詳しくは、『[Cisco Secure ACS for Windows Server 4.0 ユーザガイド](#)』を参照してください。

ネットワーク設定

次の手順を実行します。

コントローラ管理 IP アドレスを AAA クライアントとして、認証メカニズムを TACACS+ (Cisco IOS) として追加します。

CiscoSecure ACS - Microsoft Internet Explorer

Address <http://127.0.0.1:1479/>

Network Configuration

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
DOBSL12-2	10.22.8.21	TACACS+ (Cisco IOS)

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
wnbu-dt-srvr01	11.11.13.2	CiscoSecure ACS

Add Entry Search

Help

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Editing a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [Searching for Network Devices](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)
- [Editing a Proxy Distribution Table Entry](#)
- [Deleting a Proxy Distribution Table Entry](#)

Applet appPing started Internet

[インターフェイス設定](#)

次のステップを実行します。

1. [Interface Configuration] メニューで [TACACS+ (Cisco IOS)] リンクを選択します。
2. [New Services] を有効にします。
3. [User] チェック ボックスおよび [Group] チェック ボックスの両方をオンにします。
4. サービスに「**ciscowlc**」、プロトコルに「**common**」と入力します。
5. [Advanced TACACS+ Features] を有効にします。

Address <http://127.0.0.1:1767/> Go Links

CISCO SYSTEMS

Interface Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

Network Access Profiles

Reports and Activity

Online Documentation

TACACS+ Services

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Advanced Configuration Options

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. 変更を適用するには、[Submit] をクリックします。

ユーザ/グループ設定

次のステップを実行します。

1. 以前作成したユーザ/グループを選択します。
2. [TACACS+ Settings] に移動します。
3. インターフェイス設定で作成した *ciscowlc* サービスに対応するチェックボックスをオンにします。
4. [Custom attributes] チェックボックスを選択します。

Jump To Access Restrictions

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Shell Command Authorization Set

None
 Assign a Shell Command Authorization Set for any network device
 Per Group Command Authorization
 Unmatched Cisco IOS commands
 Permit
 Deny

Command:

 Arguments:

 Unlisted arguments
 Permit
 Deny

ciscowlc common
 Custom attributes

Wireless-WCS HTTP
 Custom attributes

IETF RADIUS Attributes ?

[006] Service-Type
Callback NAS Prompt

5. 作成したユーザが、WLAN、SECURITY、CONTROLLER のみにアクセスする必要がある場合は、[Custom attributes] の下にあるテキスト ボックスにテキスト「**role1=WLAN role2=SECURITY role3=CONTROLLER**」を入力します。ユーザが [SECURITY] タブのみにアクセスする必要がある場合は、テキスト「**role1=SECURITY**」を入力します。ロールは、コントローラ Web GUI の 7 個のメニューバー項目に対応します。メニューバー項目は、[MONITOR]、[WLAN]、[CONTROLLER]、[WIRELESS]、[SECURITY]、[MANAGEMENT]、[COMMAND] です。
6. ユーザに必要なロールを、[role1]、[role2] などに入力します。ユーザにすべてのロールが必要な場合は、キーワード「**ALL**」を使用します。ロビー管理者ロールの場合は、キーワード「**LOBBY**」を使用します。

Cisco Secure ACS のアカウントレコード

WLC からの TACACS+ アカウントレコードは、[Reports and Activity] の [TACACS+ Administration] の [Cisco Secure ACS] で利用できます。

The screenshot shows the Cisco Secure ACS web interface. The main content area displays a table of TACACS+ Administration records. The table has columns for Date, Time, User-name, Group-name, cmd, priv-lev, service, NAS-Portname, task_id, NAS-IP-Address, and reason. The records show various commands being executed by the 'tac' user from the 'Taccacs Group for WLC' group, such as 'wlan enable 1', 'wlan ldap delete 1 position 2', and 'wlan mac-filtering disable 1'.

Date	Time	User-name	Group-name	cmd	priv-lev	service	NAS-Portname	task_id	NAS-IP-Address	reason
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan enable 1	249	shell	---	224	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 2	249	shell	---	223	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 1	249	shell	---	222	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 0	249	shell	---	221	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan timeout 1 0	249	shell	---	220	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan mac-filtering disable 1	249	shell	---	219	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan security is NONE for wlan-id 1	249	shell	---	218	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan security Wf(WPA/RSN) disable 1	249	shell	---	217	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan aaa-overmode disable 1	249	shell	---	216	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan qos 1 platinum	249	shell	---	215	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan radio 1 all	249	shell	---	214	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan dhcp_server 1 0.0.0.0 required	249	shell	---	213	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan broadcast-ssid enable 1	249	shell	---	212	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan exclusionlist 1 0	249	shell	---	211	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan exclusionlist 1 disable	249	shell	---	210	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan act 1	249	shell	---	209	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan interface 1 100	249	shell	---	208	10.10.80.3	---
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan disable 1	249	shell	---	207	10.10.80.3	---

WCS での TACACS+ 設定

次のステップを実行します。

1. GUI からルート アカウントで WCS にログインします。
2. TACACS+ サーバを追加します。[Administration] > [AAA] > [TACACS+] > [Add TACACS+ Server] に移動します。



3. IP アドレス、ポート番号 (49 がデフォルト)、共有秘密鍵など、TACACS+ サーバの詳細を追加します。



4. WCS での管理用に TACACS+ 認証を有効にします。[Administration] > [AAA] > [AAA Mode] > [Select TACACS+] に移動します。



[仮想ドメインを使用した WCS](#)

仮想ドメインは、WCSバージョン5.1で導入された新機能です。WCS仮想ドメインは、デバイスとマップのセットで構成され、ユーザのビューをこれらのデバイスとマップに関連する情報に制限します。仮想ドメインを使用して、管理者はユーザが担当するデバイスおよびマップだけを表示できるようにすることができます。また、仮想ドメインのフィルタにより、ユーザはネットワークの割り当てられた部分だけについて、アラームを設定、表示およびレポートを生成できます。管理者は、許可した一連の仮想ドメインを各ユーザに指定します。ログインの際、ユーザについてこれらのドメインのうちアクティブとなるのは1つだけです。ユーザは、画面上部の [Virtual Domain] ドロップダウンメニューで別の有効な仮想ドメインを選択して、現在の仮想ドメインを変更できます。仮想ドメインによって、すべてのレポート、アラーム、およびその他の機能がフィルタ処理されます。

システムに定義されている仮想ドメインが1つだけ(ルート)であり、かつTACACS+/RADIUSサーバにカスタム属性の仮想ドメインがない場合、ユーザにはデフォルトでルートの仮想ドメインが割り当てられます。

仮想ドメインが複数あり、ユーザに指定された属性がない場合、ユーザのログインはブロックされます。ユーザがログインできるようにするには、仮想ドメインのカスタム属性をRADIUS/TACACS+サーバにエクスポートする必要があります。

[Virtual Domain Custom Attributes] ウィンドウを使用して、各仮想ドメインの適切なプロトコル固有のデータを指定することができます。[Virtual Domain Hierarchy] サイドバーの [Export] ボタンを使用して、RADIUS 属性および TACACS+ 属性を事前に設定できます。これらの属性を ACS サーバにコピーして貼り付けることができます。該当する仮想ドメインだけを ACS サーバの画面にコピーし、ユーザがこれらの仮想ドメインだけにアクセスできるようにすることができます。

フォーマット済み RADIUS 属性と TACACS+ 属性を ACS サーバに適用するには、「[仮想ドメインの RADIUS 属性および TACACS+ 属性](#)」で説明する手順を実行してください。

[Cisco Secure ACS が WCS を使用する設定](#)

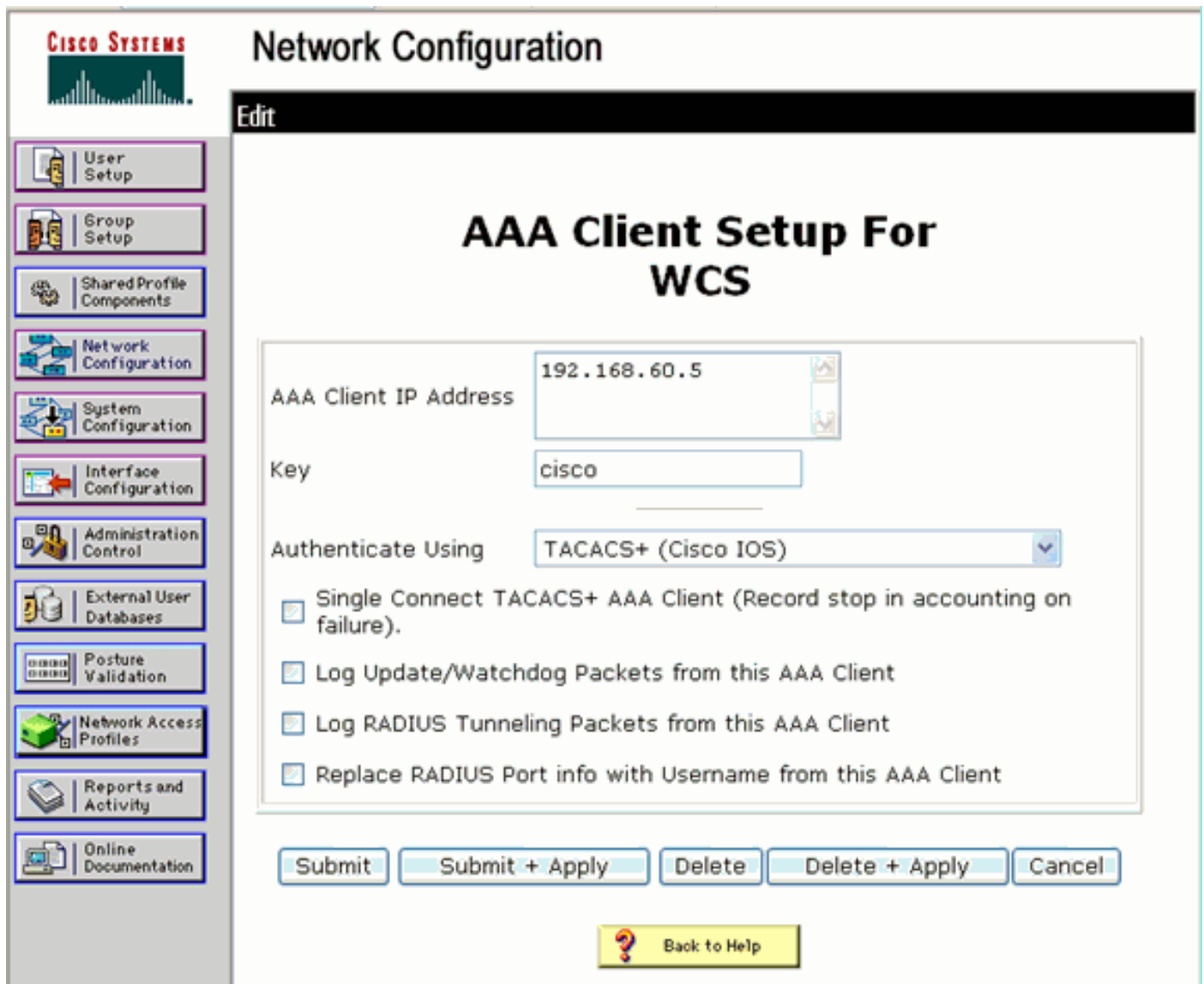
このセクションでは、TACACS+ ACS サーバがサービスとカスタム属性を作成し、ユーザまたはグループにロールを割り当てることに関連する手順について説明します。

ユーザとグループの作成については説明しません。ユーザとグループは必要に応じて作成されていることが想定されています。

ネットワーク設定

次の手順を実行します。

WCS IP アドレスを AAA クライアントとして、認証メカニズムを TACACS+ (Cisco IOS) として追加します。



The screenshot shows the Cisco Network Configuration interface. The main title is "Network Configuration" and the current page is "AAA Client Setup For WCS". The interface includes a sidebar with various configuration options and a main content area with the following fields and options:

- AAA Client IP Address:** 192.168.60.5
- Key:** cisco
- Authenticate Using:** TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom, there are buttons for "Submit", "Submit + Apply", "Delete", "Delete + Apply", and "Cancel". A "Back to Help" button is also present.

インターフェイス設定

次のステップを実行します。

1. [Interface Configuration] メニューで [TACACS+ (Cisco IOS)] リンクを選択します。
2. [New Services] を有効にします。
3. [User] チェック ボックスおよび [Group] チェック ボックスの両方をオンにします。
4. サービスに「Wireless-WCS」、プロトコルに「HTTP」と入力します。注：HTTPは

CAPSである必要があります。

5. [Advanced TACACS+ Features] を有効にします。

CISCO SYSTEMS

Interface Configuration

<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

	Service	Protocol
<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>		

Advanced Configuration Options

Advanced TACACS+ Features

6. 変更を適用するには、[Submit] をクリックします。

ユーザ/グループ設定

次のステップを実行します。

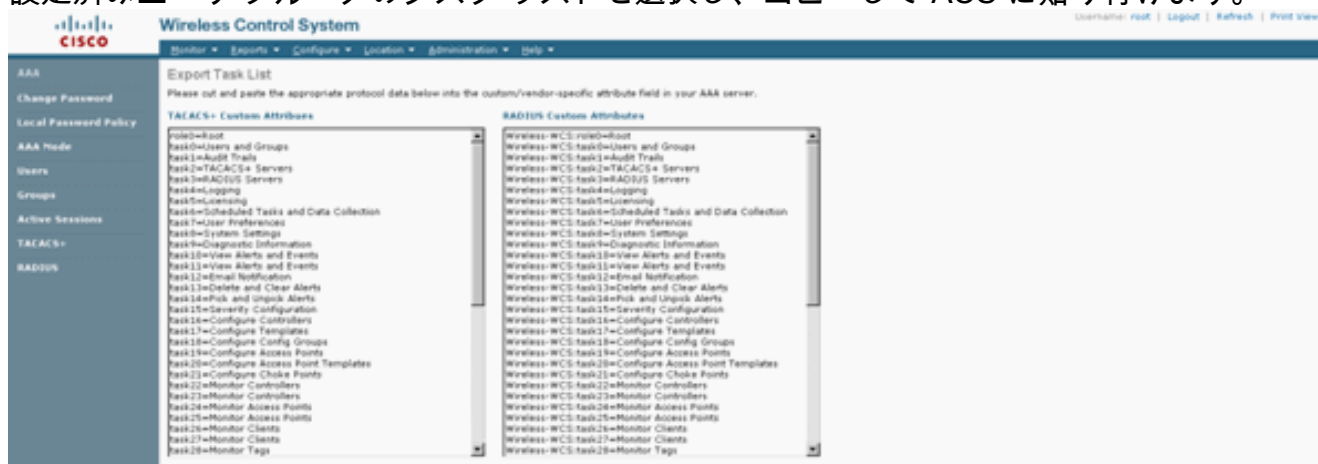
1. WCS GUI で [Administration] > [AAA] > [Groups] に移動し、WCS の SuperUsers などの設定済みユーザグループを選択します。

Wireless Control System

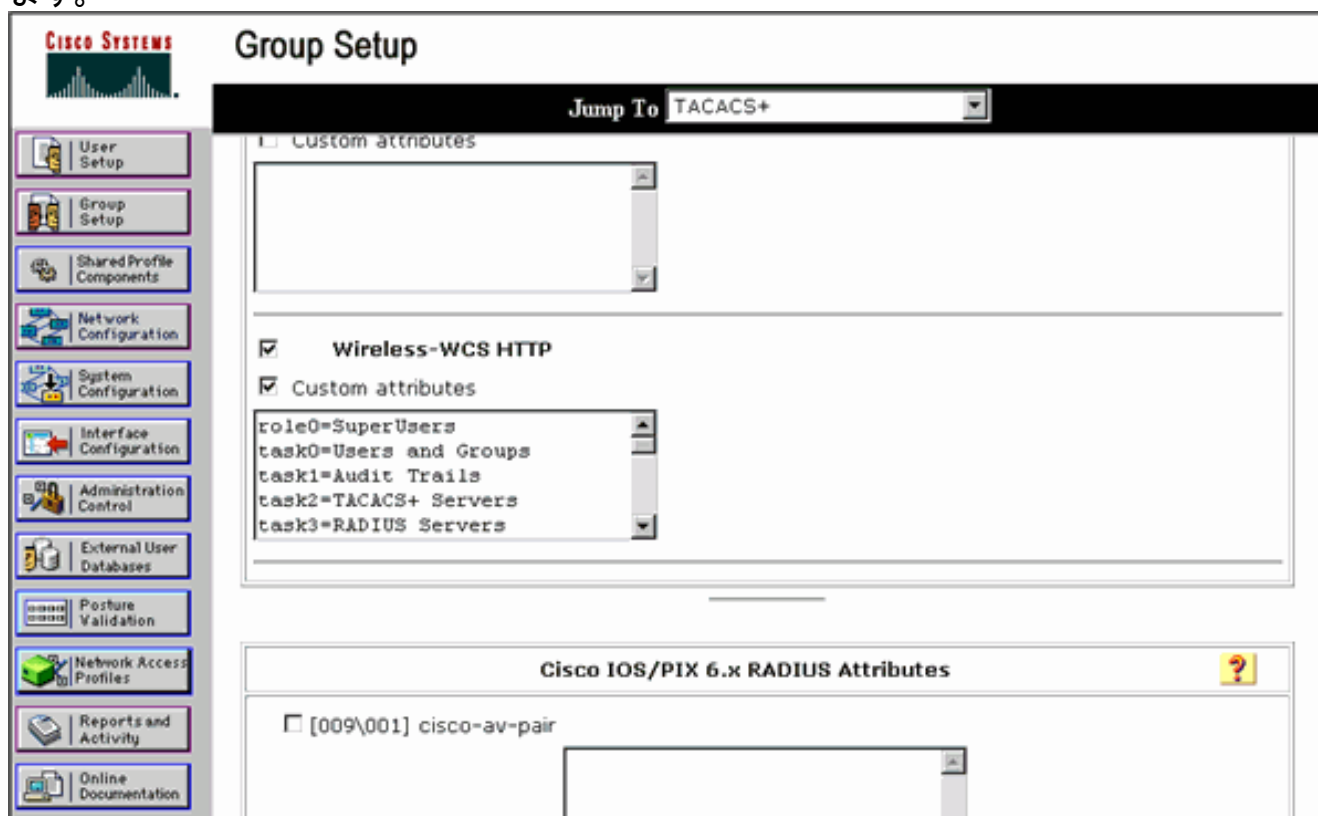
Administration > [AAA] > [Groups]

Group Name	Members	Audit Trail	Export
Admin	--		Task List
ConfAdmins	--		Task List
System Monitors	--		Task List
Users Assistant	--		Task List
WebAdmins	--		Task List
Monitor Logs	--		Task List
North Bound API	--		Task List
SuperUsers	--		Task List
Root	root --		Task List
User Defined 1	--		Task List
User Defined 2	--		Task List
User Defined 3	--		Task List
User Defined 4	--		Task List

2. 設定済みユーザグループのタスクリストを選択し、コピーして ACS に貼り付けます。



3. 以前作成したユーザグループを選択し、[TACACS+ Settings] に移動します。
4. ACS GUI で、以前作成した Wireless-WCS サービスに対応するチェックボックスをオンにします。
5. ACS GUI で [Custom attributes] ボックスをオンにします。
6. [Custom attributes] の下にあるテキストボックスに、WCS からコピーしたロールとタスクの情報を入力します。たとえば、SuperUsers によって許可されるタスクのリストを入力します。



7. ACS で新しく作成したユーザ名/パスワードで WCS にログインします。

デバッグ

WLC からの role1=ALL のデバッグ

```
(Cisco Controller) >debug aaa tacacs enable
```

```
(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
```



```
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole ffffffff8
```

WLC からの複数のロールのデバッグ

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

WLC からの認可エラーのデバッグ

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007: User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

関連情報

- [Web 認証用の Cisco ワイヤレス LAN コントローラ \(WLC \) および Cisco ACS 5.x \(TACACS+ \) の設定例](#)
- [TACACS+ の設定](#)

- [ACS 5.1 で Admin ユーザと Admin 以外のユーザに TACACS 認証と認可を設定する方法](#)
- [TACACS+ と RADIUS の比較](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)