

配置WLC和ACS以驗證管理使用者

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[WLC配置](#)

[配置WLC以透過Cisco Secure ACS伺服器接受管理](#)

[Cisco Secure ACS配置](#)

[將WLC作為AAA客戶端增加到RADIUS伺服器](#)

[配置使用者及其相應的RADIUS IETF屬性](#)

[設定具有讀寫存取權的使用者](#)

[設定具有唯讀存取權的使用者](#)

[在本機以及透過RADIUS伺服器管理WLC](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何配置WLC和Cisco Secure ACS，以使AAA伺服器能夠對控制器上的管理使用者進行身份驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何在WLC上配置基本引數
- 瞭解如何配置RADIUS伺服器 (如Cisco Secure ACS)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本7.0.216.0的Cisco 4400無線LAN控制器
- 運行軟體版本4.1的Cisco Secure ACS，在此配置中用作RADIUS伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

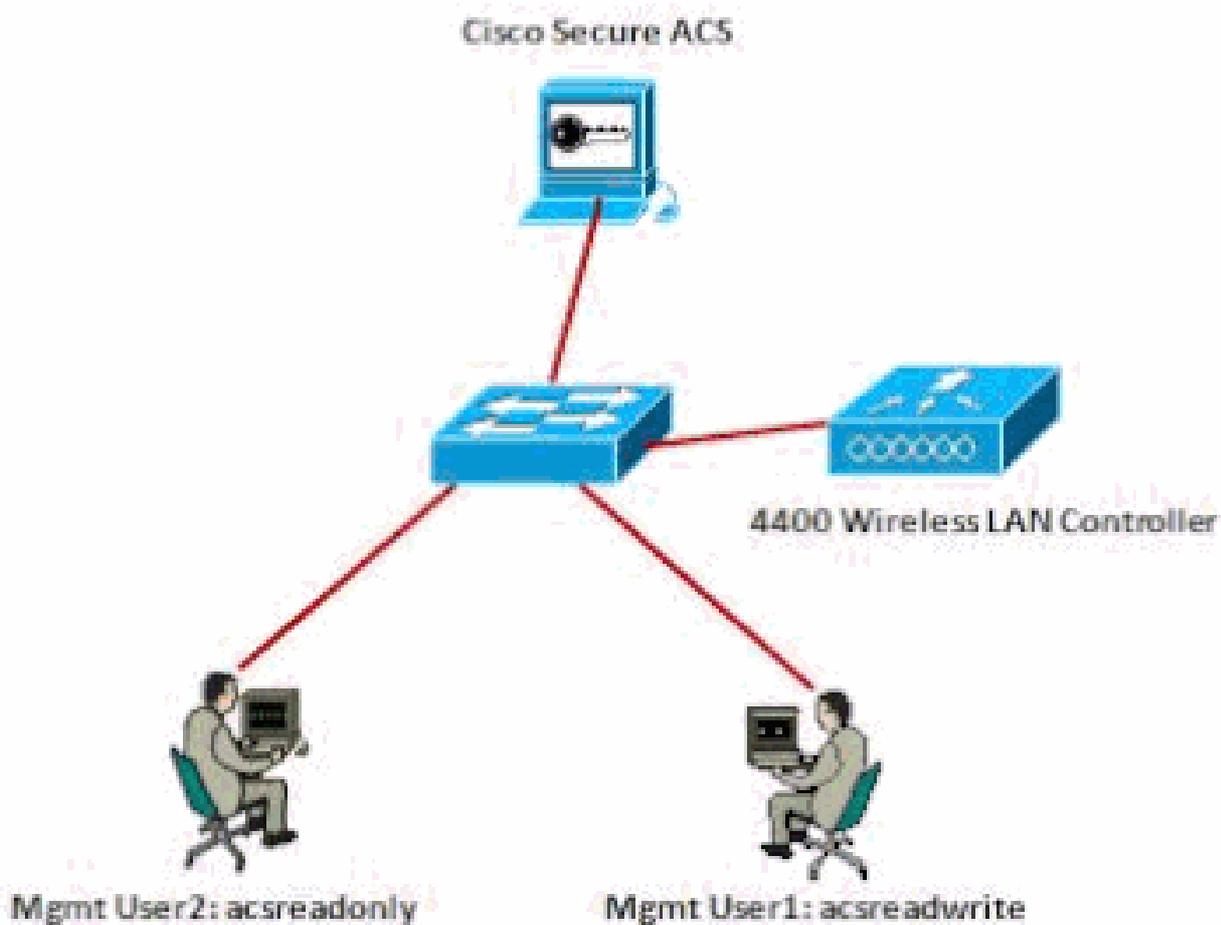
本文說明如何設定無線LAN控制器(WLC)和存取控制伺服器(Cisco Secure ACS)，以便驗證、授權和計量(AAA)伺服器能對控制器上的管理使用者進行驗證。本文檔還說明了不同的管理使用者如何使用Cisco Secure ACS RADIUS伺服器返回的供應商特定屬性(VSA)獲得不同的許可權。

設定

本節提供如何根據本文檔中所述目的配置WLC和ACS的資訊。

網路圖表

此文件使用以下網路設定：



網路圖表

此組態範例使用以下引數：

- Cisco Secure ACS的IP地址—172.16.1.1/255.255.0.0
- 控制器的管理介面IP地址— 172.16.1.30/255.255.0.0
- 在存取點(AP)和RADIUS伺服器上使用的共用金鑰- asdf1234
- 以下是該示例在ACS上配置的兩名使用者的憑據：
 - 使用者名稱- acsreadwrite
密碼- acsreadwrite
 - 使用者名稱- acsreadonly
密碼- acsreadonly

您需要配置WLC和Cisco Secure Cisco Secure ACS以便：

- 任何使用使用者名稱和口令acsreadwrite登入到WLC的使用者都可以對WLC進行完全管理訪問。
- 任何使用使用者名稱和口令acsreadonly登入到WLC的使用者都可以以只讀方式訪問WLC。

組態

本檔案使用下列組態：

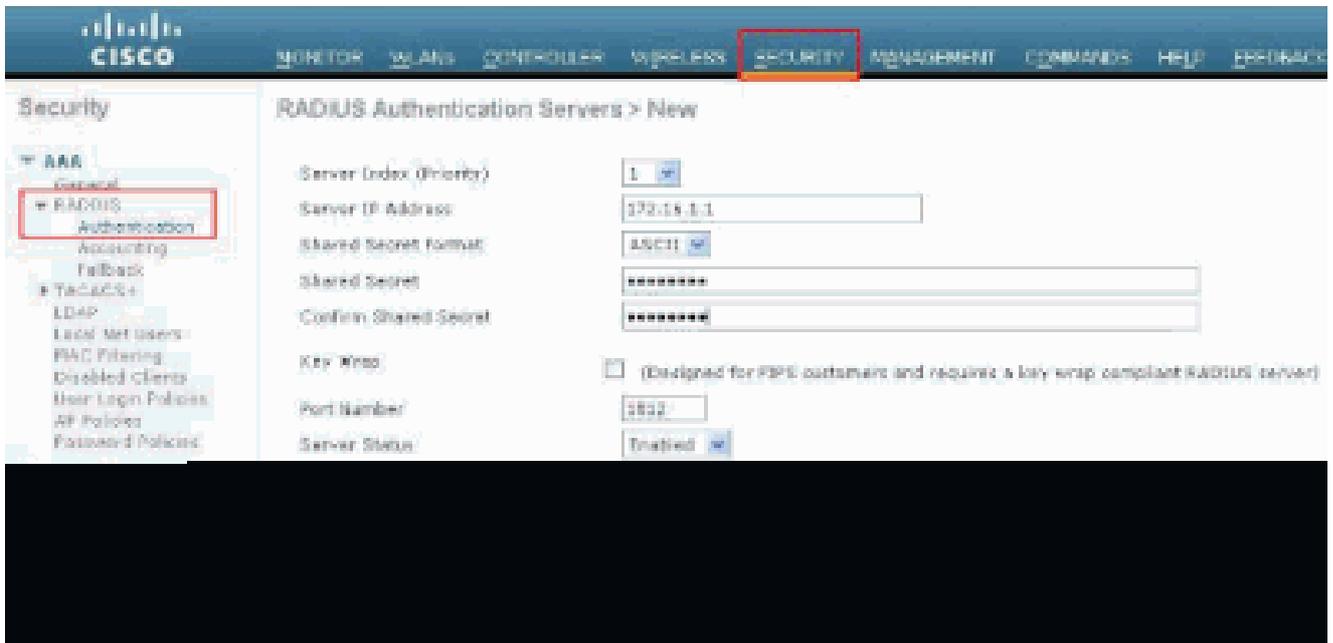
- [WLC配置](#)
- [Cisco Secure ACS配置](#)

WLC配置

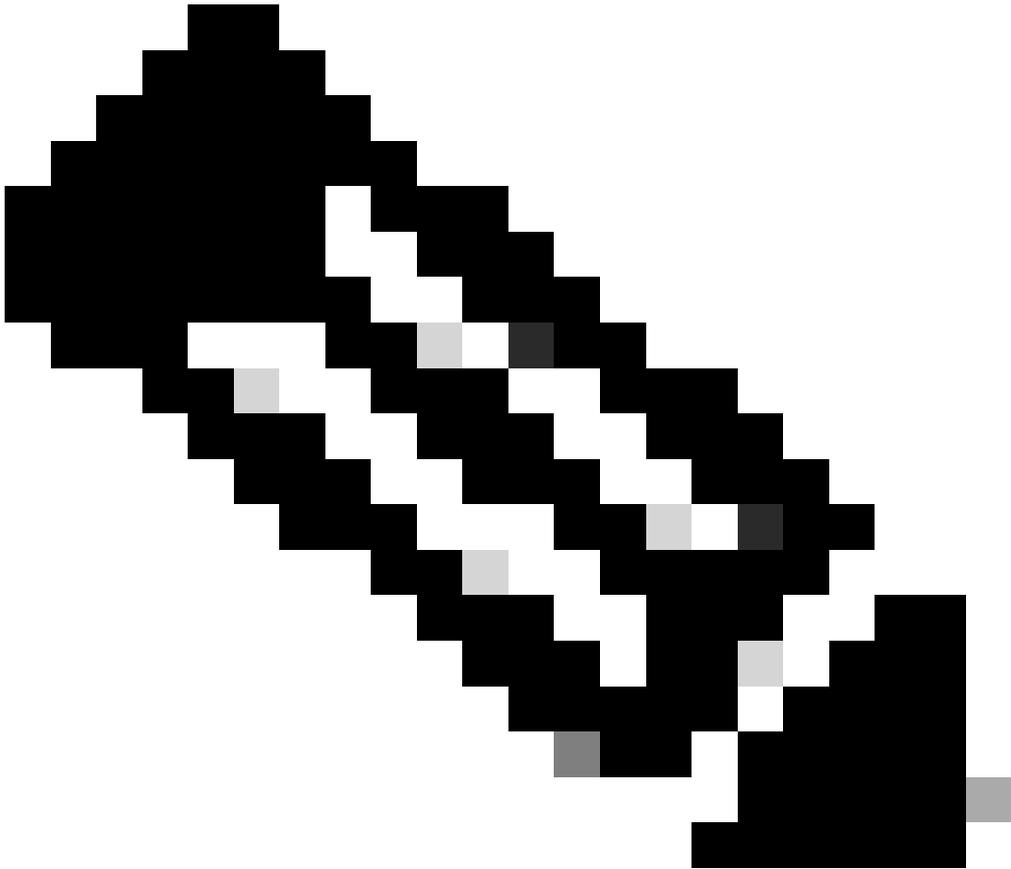
配置WLC以透過Cisco Secure ACS伺服器接受管理

完成以下步驟以配置WLC使其與RADIUS伺服器通訊：

1. 從WLC GUI中，按一下Security。 從左側選單中按一下RADIUS > Authentication。 將會顯示RADIUS Authentication servers 頁。要增加新的RADIUS伺服器，請按一下New。在RADIUS Authentication Servers > New 頁中，輸入特定於RADIUS伺服器的引數。以下提供範例。

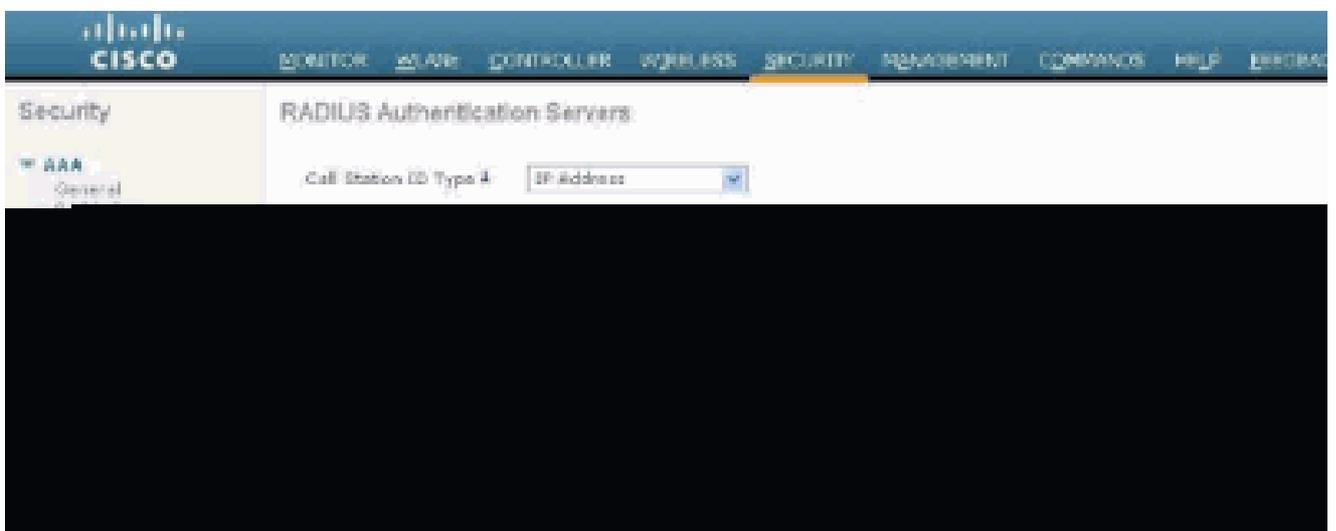


2. 選中Management 單選按鈕以允許RADIUS伺服器對登入到WLC的使用者進行身份驗證。



注意：請確保此頁上配置的共用金鑰與RADIUS伺服器上配置的共用金鑰匹配。只有這樣WLC才能與RADIUS伺服器通訊。

3. 驗證WLC是否配置為由Cisco Secure ACS管理。為此，請在WLC GUI中按一下Security。顯示的GUI視窗與本範例類似。



可以看到RADIUS伺服器172.16.1.1啟用了Management覈取方塊。這說明，允許ACS對WLC上的管理使用者進行身份驗證。

Cisco Secure ACS配置

完成以下部分中的步驟以配置ACS：

1. [將WLC作為AAA客戶端增加到RADIUS伺服器。](#)
2. [配置使用者及其相應的RADIUS IETF屬性。](#)
3. [設定具有讀寫存取權的使用者。](#)
4. [配置具有只讀訪問許可權的使用者。](#)

將WLC作為AAA客戶端增加到RADIUS伺服器

要在Cisco Secure ACS中將WLC增加為AAA客戶端，請完成以下步驟：

1. 從ACS GUI中，按一下Network Configuration。
2. 在AAA Clients下，按一下Add Entry。
3. 在Add AAA Client窗口中，輸入WLC主機名、WLC的IP地址和共用金鑰。

在此範例中，設定如下：

- AAA Client Hostname is WLC-4400
- 172.16.1.30/16是AAA使用者端IP位址，在本案例中為WLC。
- 共用金鑰為「asdf1234」。

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

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

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

增加AAA客戶端窗口

此共用金鑰必須與您在WLC上配置的共用金鑰相同。

4. 從Authenticate Using下拉選單中，選擇RADIUS (Cisco Airespace)。
5. 按一下Submit + Restart以儲存配置。

配置使用者及其相應的RADIUS IETF屬性

若要透過RADIUS伺服器驗證使用者，對於控制器登入和管理，您必須根據使用者許可權，將具有IETF RADIUS attributeService-Typeset的使用者新增至RADIUS資料庫。

- 若要設定使用者的讀取/寫入許可權，請將Service-TypeAttribute設定為Administrative。
- 要為使用者設定只讀許可權，請將Service-TypeAttribute設定為NAS-Prompt。

設定具有讀寫存取權的使用者

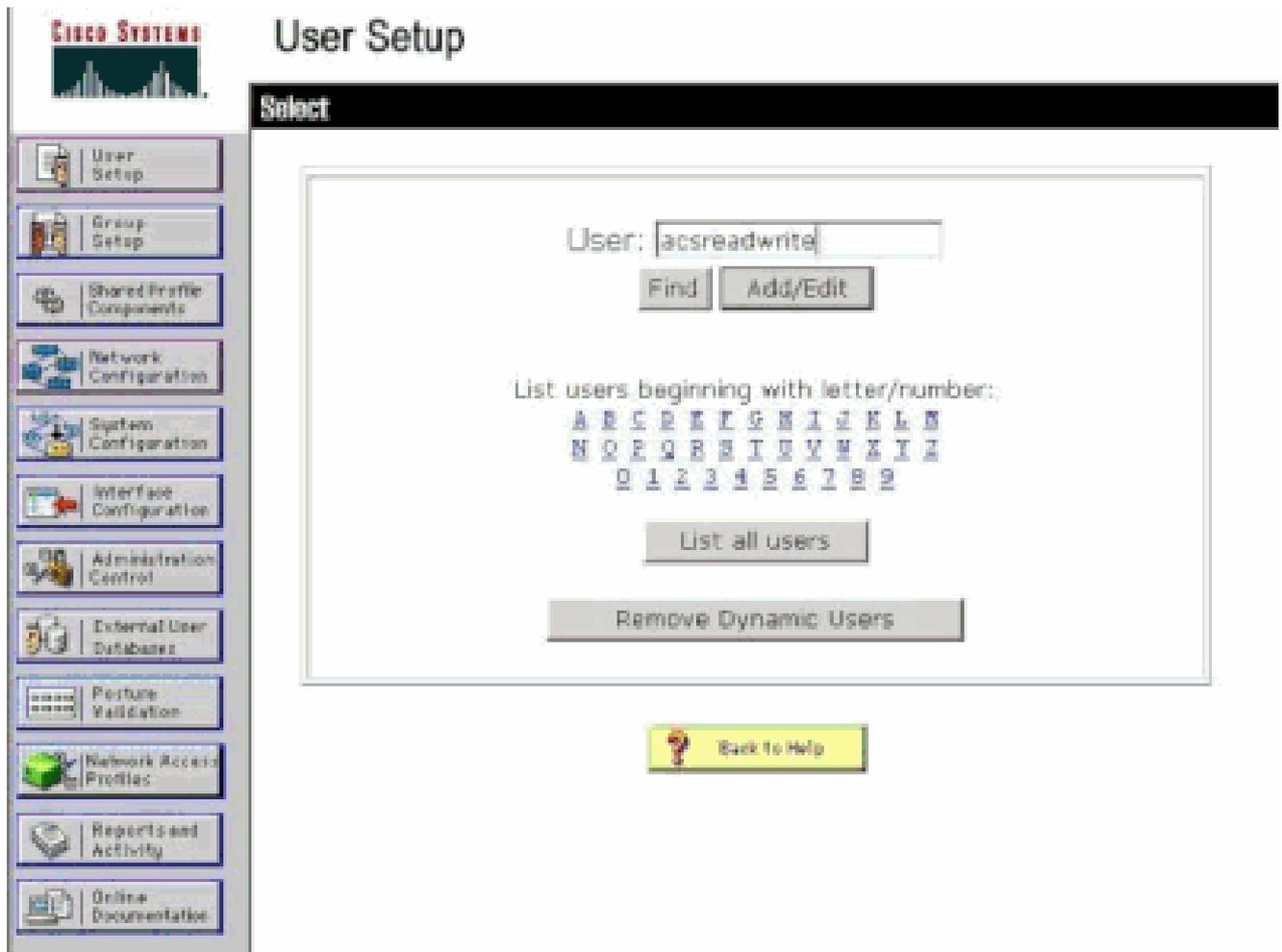
第一個範例顯示具有WLC完整存取權的使用者組態。當此使用者嘗試登入控制器時，RADIUS伺服器會驗證並向此使用者提供完整的管理存取許可權。

在本示例中，使用者名稱和口令為acsreadwrite。

在Cisco Secure ACS上完成以下步驟。

1. 從ACS GUI中，按一下User Setup。

2. 鍵入要增加到ACS的使用者名稱，如以下示例窗口所示。



使用者設定視窗

3. 按一下Add/Edit轉到「User Edit」頁。
4. 在「使用者編輯」頁面中，提供此使用者的實際名稱、說明和密碼詳細資訊。
5. 向下滾動到IETF RADIUS Attributes設定並選中Service-Type Attribute。
6. 由於在本示例中，需要向使用者acsreadwrite授予完全訪問許可權，因此請從「Service-Type」下拉選單中選擇Administrative，然後按一下Submit。

這可確保此特定使用者具有對WLC的讀寫訪問許可權。

The screenshot shows the Cisco ACS User Setup interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Feature Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is divided into two sections: 'Account Disable' and 'IETF RADIUS Attributes'. The 'Account Disable' section has a 'Never' radio button selected, and options for disabling the account based on date or failed attempts. The 'IETF RADIUS Attributes' section shows a list of attributes, with '[006] Service-Type' selected and a dropdown menu open showing various service types, with 'Administrative' highlighted.

ETF RADIUS屬性設定

有時，使用者設定下看不到此Service-Type屬性。在這種情況下，請完成以下步驟使其可見。

1. 從ACS GUI中，選擇Interface Configuration > RADIUS (IETF)以在使用者配置窗口中啟用IETF屬性。

這會顯示RADIUS (IETF) Settings頁面。

2. 在「RADIUS (IETF)設定」(RADIUS (IETF)設定頁面，您可以啟用需要顯示在使用者或組設定下的IETF屬性。對於此配置，請檢查User列的Service-Type，然後按一下Submit。此視窗顯示一個範例。



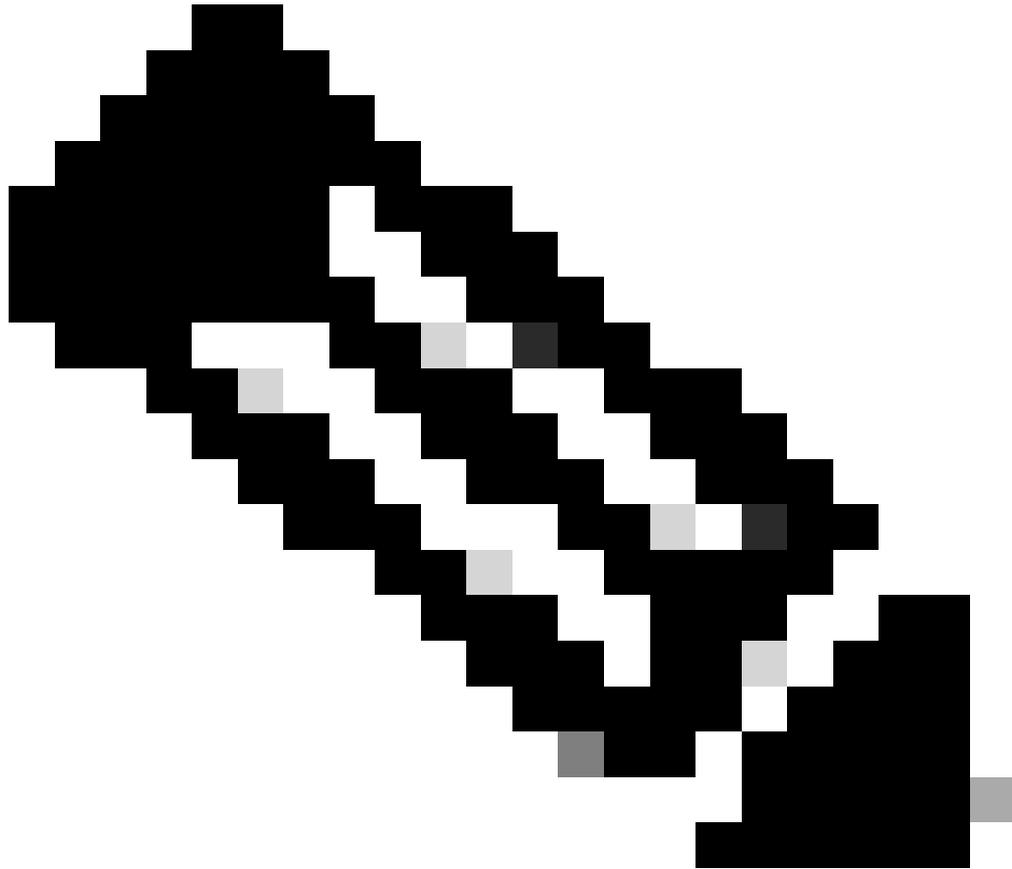
Interface Configuration

RADIUS (IETF)

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

| User | Group |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> [006] Service-Type |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [007] Framed-Protocol |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [009] Framed-IP-Netmask |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [010] Framed-Routing |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [011] Filter-Id |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [012] Framed-MTU |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [013] Framed-Compression |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [014] Login-IP-Host |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [015] Login-Service |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [016] Login-TCP-Port |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [018] Reply-Message |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [020] Callback-Id |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [022] Framed-Route |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [023] Framed-IPX-Network |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [024] State |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [025] Class |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [027] Session-Timeout |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> [028] Idle-Timeout |

RADIUS (IETF)設定値頁面



注意：此示例指定基於每個使用者的身份驗證。您也可以根據特定使用者所屬的組執行身份驗證。在這種情況下，請啟用「群組」核取方塊，以便此屬性在「群組設定」下可見。此外，如果身份驗證基於組，則需要將使用者分配到特定組，並配置組設定 IETF 屬性以提供對該組使用者的訪問許可權。有關如何配置和管理組的詳細資訊，請參閱組管理。

設定具有唯讀存取權的使用者

此範例顯示具有 WLC 唯讀存取權的使用者組態。當此使用者嘗試登入控制器時，RADIUS 伺服器會驗證並向此使用者提供唯讀存取權。

在本示例中，使用者名稱和口令為 `acsreadonly`。

在 Cisco Secure ACS 上完成以下步驟：

1. 從 ACS GUI 中，按一下 User Setup。
2. 鍵入要增加到 ACS 的使用者名稱，然後按一下 Add/Edit 以轉至 User Edit 頁。



User Setup

Select

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

User:

Find

Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

List all users

Remove Dynamic Users



Back to Help

增加使用者名稱

3. 提供此使用者的真實名稱、說明和密碼。此視窗顯示一個範例。

User Setup

User: acsreadonly (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a

提供新增使用者的實際名稱、說明和密碼

4. 向下滾動到IETF RADIUS Attributes設定並選中Service-Type Attribute。
5. 由於在本示例中，使用者acsreadonly需要具有只讀訪問許可權，因此從「Service-Type」下拉選單中選擇NAS Prompt，然後按一下Submit。

這可確保此特定使用者對WLC具有只讀訪問許可權。

Cisco Systems

User Setup

Account Disable

Never

Disable account if:

Date exceeds: Sep 22 2011

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit:

IETF RADIUS Attributes

[006] Service-Type

Authenticate only

NAS Prompt

Outbound

Callback NAS Prompt

Administrative

Callback Administrative

Callback login

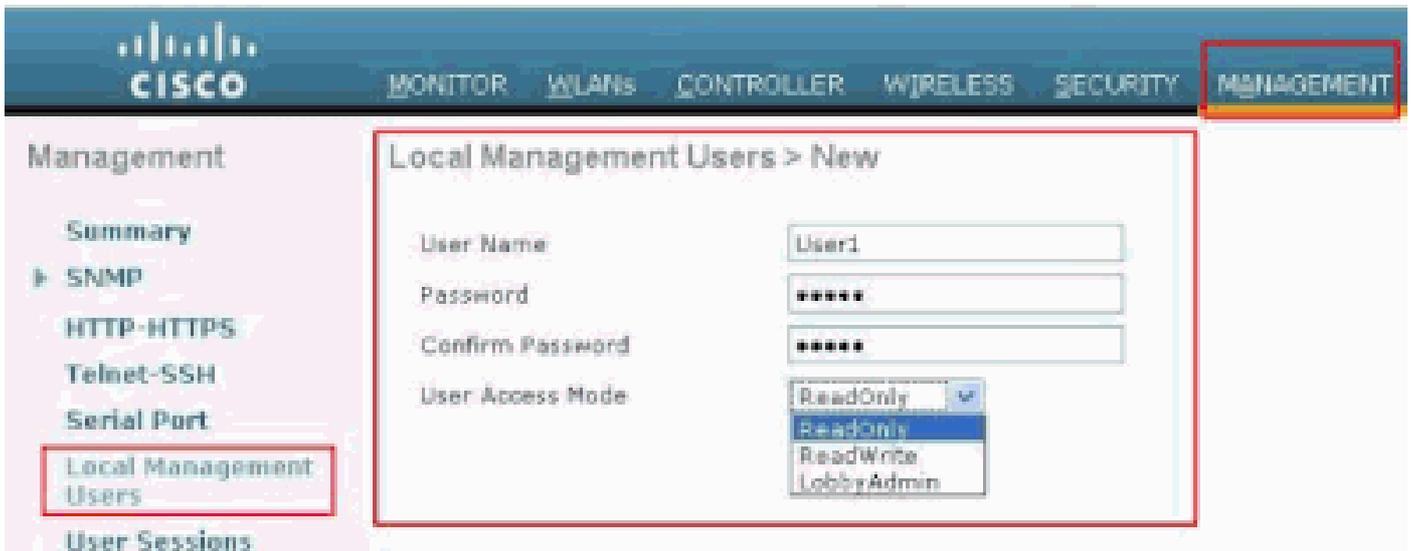
Framed

Back to Help

檢查服務型別屬性

在本機以及透過RADIUS伺服器管理WLC

您也可以在WLC本機上設定管理使用者。這可以在控制器GUI的Management > Local Management Users下完成。

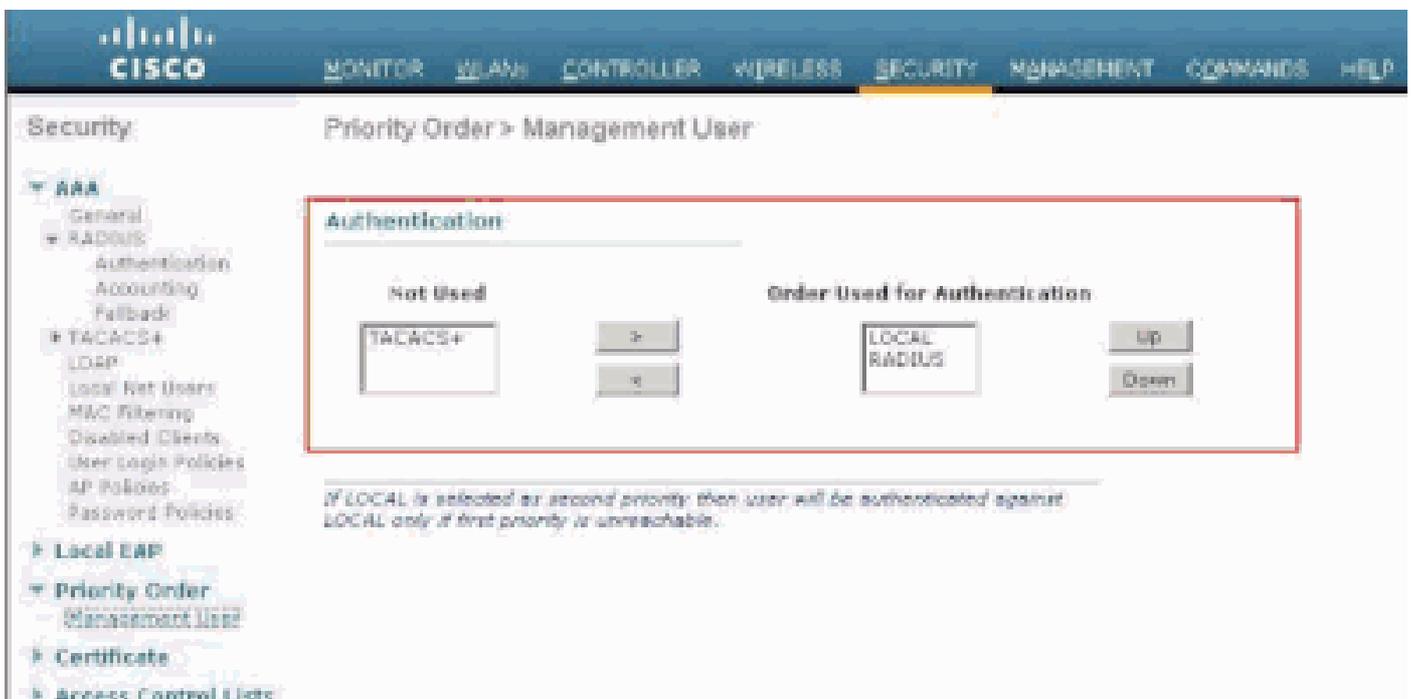


在WLC上本地組態管理使用者

假設WLC在本地以及RADIUS伺服器中配置了管理使用者，並啟用了Management覈取方塊。在此案例中，預設情況下，使用者嘗試登入WLC時，WLC會以下列方式運作：

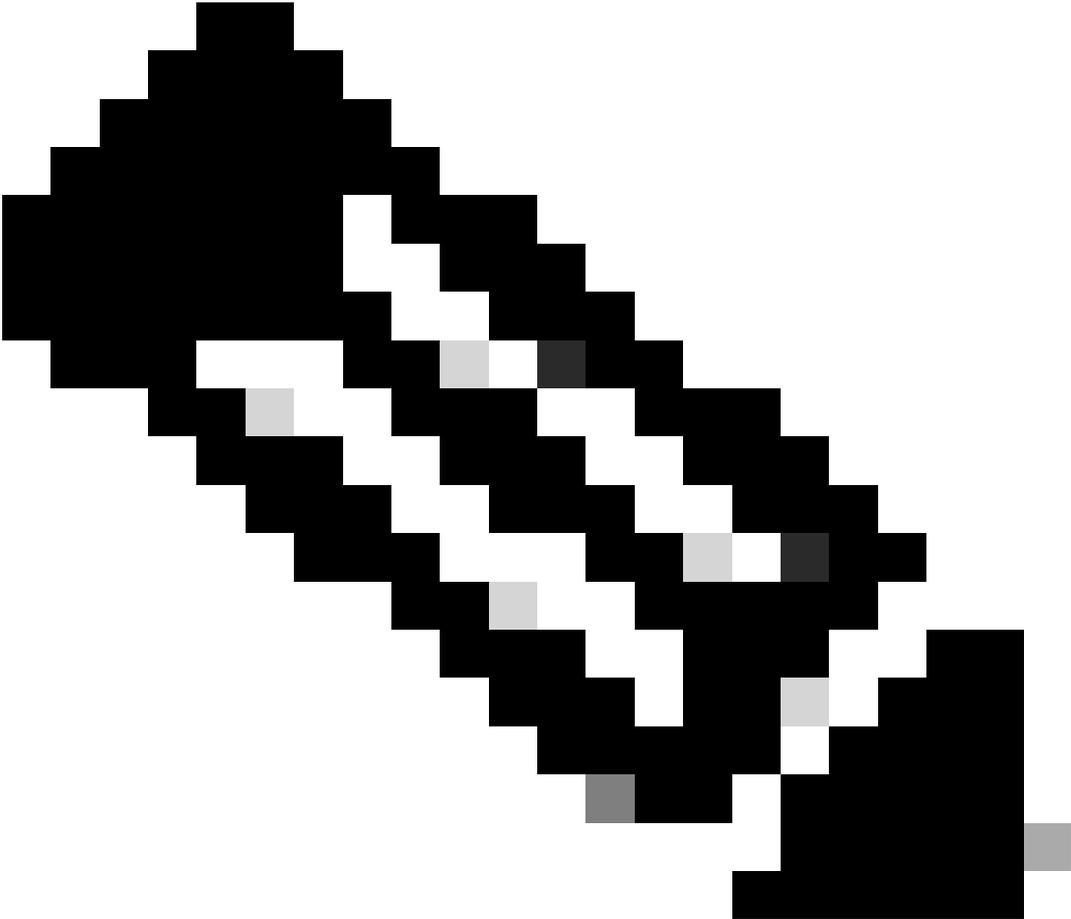
1. WLC首先檢視為驗證使用者而定義的本地管理使用者。如果該使用者存在於其本地清單中，則允許對該使用者進行身份驗證。如果此使用者未在本機顯示，則會尋找RADIUS伺服器。
2. 如果相同使用者存在本機和RADIUS伺服器，但具有不同的存取許可權，則WLC會使用本機指定的許可權驗證使用者。換句話說，與RADIUS伺服器相比，WLC上的本機組態永遠優先。

可以在WLC上更改管理使用者的身份驗證順序。為此，請從WLC上的Security頁面按一下Priority Order > Management User。 您可以在此頁面指定驗證的順序。以下提供範例。



Management User Selection" />

Priority Order > Management User Selection



注意：如果將LOCAL選為第二優先順序，則僅當定義為第一優先順序的方法(RADIUS/TACACS)不可達時，才使用此方法驗證使用者。

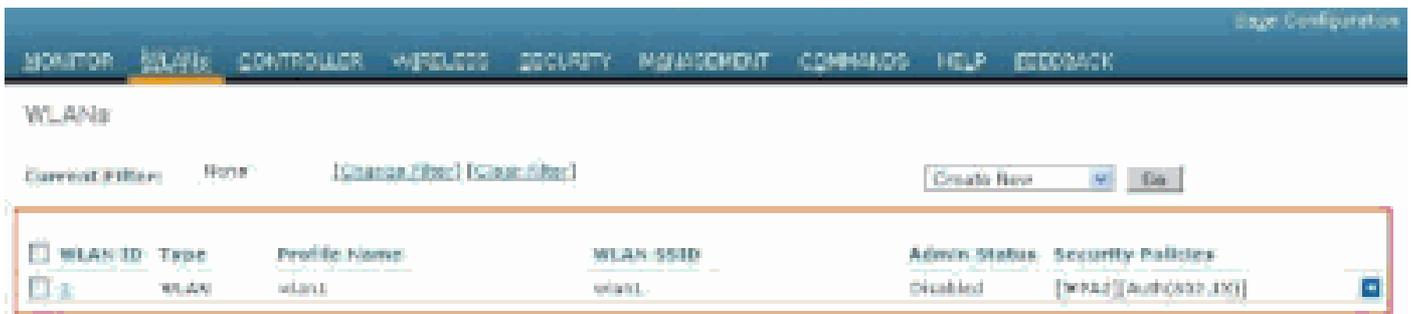
驗證

若要驗證組態是否正常運作，請透過CLI或GUI (HTTP/HTTPS)模式存取WLC。出現登入提示時，鍵入在Cisco Secure ACS上配置的使用者名稱和密碼。

如果您具有正確的組態，就會成功在WLC中透過驗證。

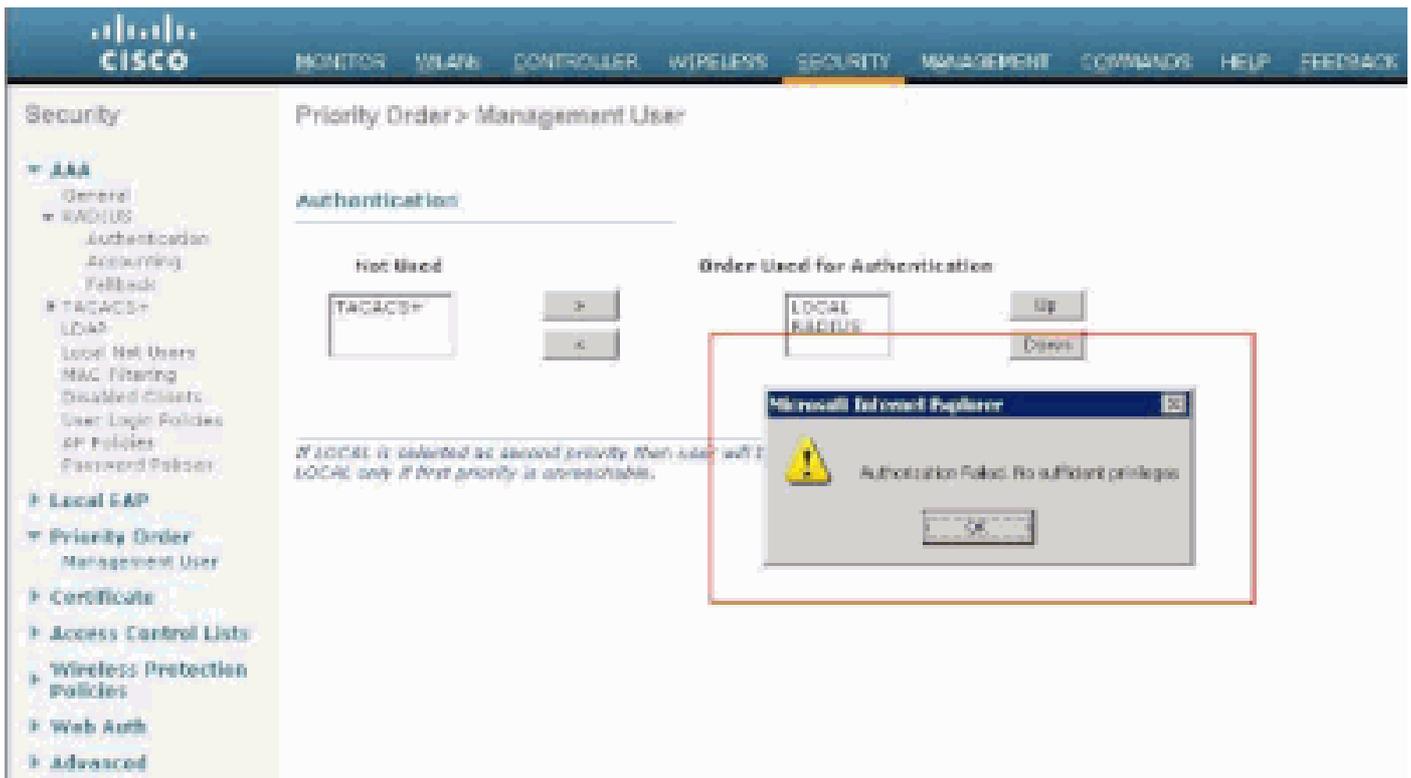
您還可以確保已驗證使用者是否受到ACS指定的訪問限制。為此，請透過HTTP/HTTPS存取WLC GUI (請確認WLC已設定為允許HTTP/HTTPS)。

在ACS中設定讀寫訪問許可權的使用者在WLC中具有若干可配置許可權。例如，讀寫使用者擁有在WLC的WLAN頁面下建立新WLAN的許可權。此視窗顯示一個範例。



WLC中的可配置許可權

當具有唯讀授權的使用者嘗試變更控制器上的組態時，使用者會看到此訊息。



無法以唯讀存取權更改控制器

這些存取限制也可透過WLC的CLI驗證。下面是一個輸出示例。

```
<#root>
```

```
(Cisco Controller) >
```

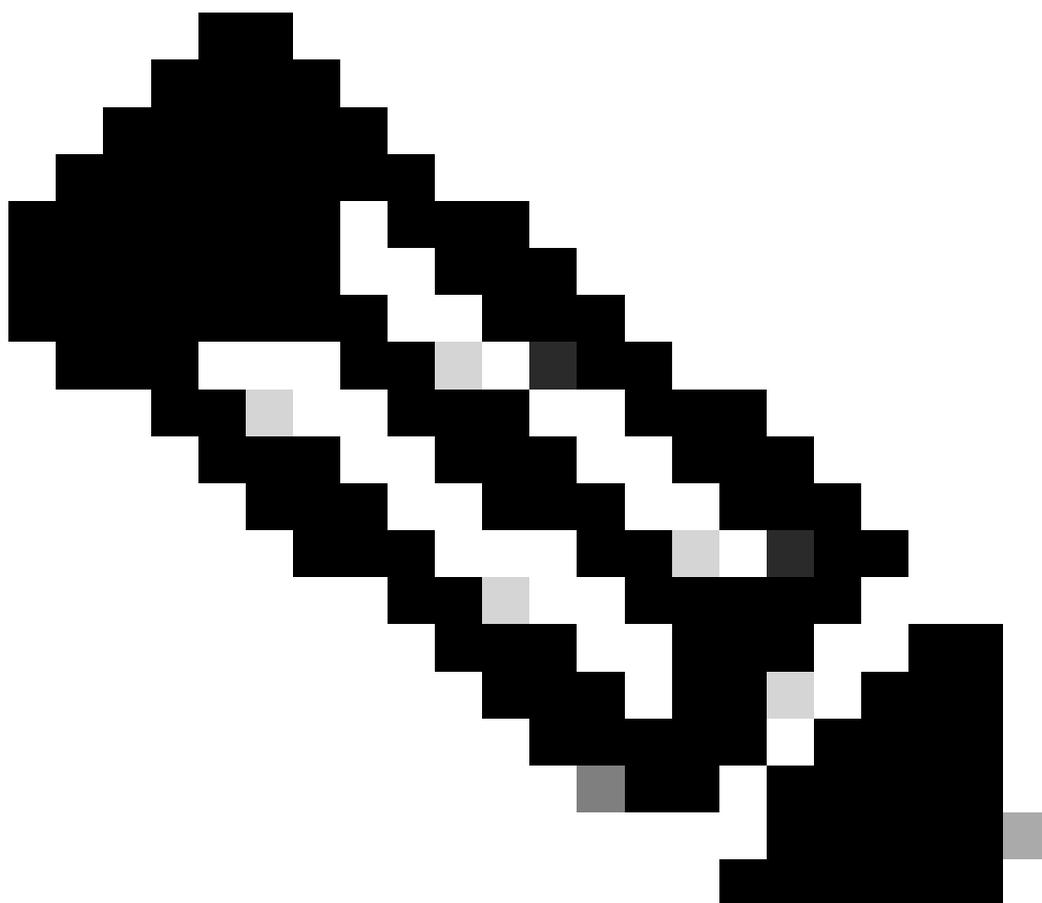
```
?
```

```
debug      Manages system debug options.
help       Help
linktest   Perform a link test to a specified MAC address.
logout     Exit this session. Any unsaved changes are lost.
show       Display switch options and settings.
```

```
(Cisco Controller) >config
```

```
Incorrect usage. Use the '?' or <TAB> key to list commands.
```

如以下示例輸出所示，控制器CLI中的？將顯示當前使用者可用的命令清單。另請注意，config 命令無法用於此示例輸出。這說明唯讀使用者沒有許可權在WLC上執行任何設定。但是，讀寫使用者擁有在控制器（GUI和CLI模式）上執行組態的許可權。



注意：即使您透過RADIUS伺服器對WLC使用者進行了身份驗證，當您逐頁瀏覽時，HTTP[S]伺服器仍會每次對客戶端進行完全身份驗證。不會在每個頁面上提示您進行驗證的唯一原因是您的瀏覽器會快取並重新顯示您的認證。

在某些情況下，控制器透過ACS對管理使用者進行身份驗證，身份驗證成功完成(access-accept)，並且您在控制器上未看到任何授權錯誤。但是，系統再次提示使用者進行身份驗證。

在這種情況下，不能解釋問題所在，以及為什麼使用者無法僅使用debug aaa events enable 命令登入到WLC。相反，控制器會顯示另一個身份驗證提示。

一個可能的原因是，即使ACS上正確配置了使用者名稱和密碼，ACS未配置為傳輸該特定使用者或組的Service-Type屬性。

debug aaa events enable

命令的輸出並不表明使用者沒有所需的屬性（例如，Service-Type屬性），即使access-accept 從AAA伺服器傳送回也是如此。此示例debug aaa events enable 命令輸出是一個示例。

```
<#root>
```

```
(Cisco Controller) >
```

```
debug aaa events enable
```

```
Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
Mon Aug 13 20:14:33 2011: Callback.....0x8250c40
Mon Aug 13 20:14:33 2011: protocolType.....0x00020001
Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00-00:00
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00
Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2
Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0
```

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520
Mon Aug 13 20:14:33 2011: structureSize.....28
Mon Aug 13 20:14:33 2011: resultCode.....0
Mon Aug 13 20:14:33 2011: protocolUsed.....0x00000001
Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00-00:00
Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

在此第一個示例 `debug aaa events enable` 命令輸出中，您看到 `Access-Accept` 已成功從 RADIUS 伺服器接收，但 `Service-Type` 屬性未傳遞到 WLC。這是因為 ACS 上沒有使用此屬性配置特定使用者。

需要將 Cisco Secure ACS 配置為在使用者身份驗證後返回 `Service-Type` 屬性。必須根據使用者許可權將 `Service-Type` 屬性值設定為 **Administrative** 或 **NAS-Prompt**。

第二個示例再次顯示了 `debug aaa events enable` 命令輸出。但是，這一次 ACS 上的 `Service-Type` 屬性設定為 **Administrative**。

```
<#root>
```

```
(Cisco Controller)>
```

```
debug aaa events enable
```

```
Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c
Mon Aug 13 20:17:02 2011: Callback.....0x8250c40
Mon Aug 13 20:17:02 2011: protocolType.....0x00020001
Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00
Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)
```

```
Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.....100

Mon Aug 13 20:17:02 2011: resultCode.....0

Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.....
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)
```

您可以看到在上一個範例輸出中，Service-Type屬性已傳遞到WLC。

相關資訊

- [配置無線區域網控制器-配置指南](#)
- [在無線區域網控制器上配置VLAN](#)
- [為動態VLAN分配配置RADIUS伺服器 and WLC](#)
- [設定無線區域網路控制器和輕量型存取點基礎操作](#)
- [使用無線區域網控制器配置AP組VLAN](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。