

GUI を使用した Aironet アクセス ポイントでのログイン認証用 TACACS+ の設定例

目次

[はじめに](#)

[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 4.1 を使用したログイン認証用の TACACS+ サーバの設定](#)

[ACS 5.2 を使用したログイン認証用の TACACS+ サーバの設定](#)

[TACACS+ 認証用の Aironet AP の設定](#)

[確認](#)

[ACS 5.2 の検証](#)

[トラブルシューティング](#)

[関連情報](#)

[はじめに](#)

このドキュメントでは、TACACS Plus (TACACS+) サーバを使用してログイン認証を実行するために、Cisco Aironet Access Point (AP; アクセス ポイント) 上で TACACS+ サービスを有効にする方法について説明しています。

[前提条件](#)

[要件](#)

この設定を行う前に、次の要件が満たされていることを確認します。

- Aironet AP での基本的なパラメータの設定方法に関する知識
- Cisco Secure Access Control Server (ACS) のような TACACS+ サーバを設定する方法に関する知識
- TACACS+ の概念に関する知識

TACACS+ の動作の仕組みについては、『[RADIUS サーバと TACACS+ サーバの設定](#)』の「[TACACS+ について](#)」の項を参照してください。

[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くものです。

- Cisco Aironet 1240/1140 シリーズ アクセス ポイント
- ソフトウェア バージョン 4.1 が稼働する ACS
- ソフトウェア バージョン 5.2 が稼働する ACS

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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

このセクションでは、TACACS+ ベースのログイン認証用に Aironet AP および TACACS+ サーバ（ACS）を設定する方法について説明しています。

この設定例では、次のパラメータを使用します。

- ACS の IP アドレス：172.16.1.1/255.255.0.0
- AP の IP アドレス：172.16.1.30/255.255.0.0
- AP と TACACS+ サーバで使用される共有秘密キー：**Example**

この例で ACS に設定するユーザのクレデンシャルは次のとおりです。

- ユーザ名：**User1**
- パスワード：**Cisco**
- グループ：**AdminUsers**

Web インターフェイスまたは Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して AP に接続しようとするユーザを検証するように、TACACS+ 機能を設定する必要があります。この設定を実現するには、次の作業を行う必要があります。

1. [ログイン認証用の TACACS+ サーバの設定](#)。
2. [TACACS+ 認証用の Aironet AP の設定](#)。

注: このドキュメント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 4.1 を使用したログイン認証用の TACACS+ サーバの設定

最初に、AP へのアクセスを試みるユーザを検証するように、TACACS+ デーモンを設定します。TACACS+ 認証用に ACS を設定し、ユーザ データベースを作成する必要があります。任意の TACACS+ サーバを使用できます。この例では、ACS を TACACS+ サーバとして使用しています。次の手順を実行します。

1. 次の手順を実行して、AP を Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) クライアントとして追加します。ACS の GUI で、**Network Configuration** タブをクリックします。AAA Clients の下で **[Add Entry]** をクリックします。Add AAA Client ウィンドウで、AP ホスト名、AP の IP アドレス、および共有秘密キーを入力します。この共有秘密キーは、AP に設定する共有秘密キーと一致する必要があります。**Authenticate Using** ドロップダウン メニューから、**TACACS+ (Cisco IOS)** を選択します。設定を保存するには、**Submit + Restart** をクリックします。次に例を示します。

The screenshot shows the CiscoSecure ACS GUI in Microsoft Internet Explorer. The main window is titled 'Network Configuration' and contains a sub-window 'Add AAA Client'. The 'Add AAA Client' window has the following fields and options:

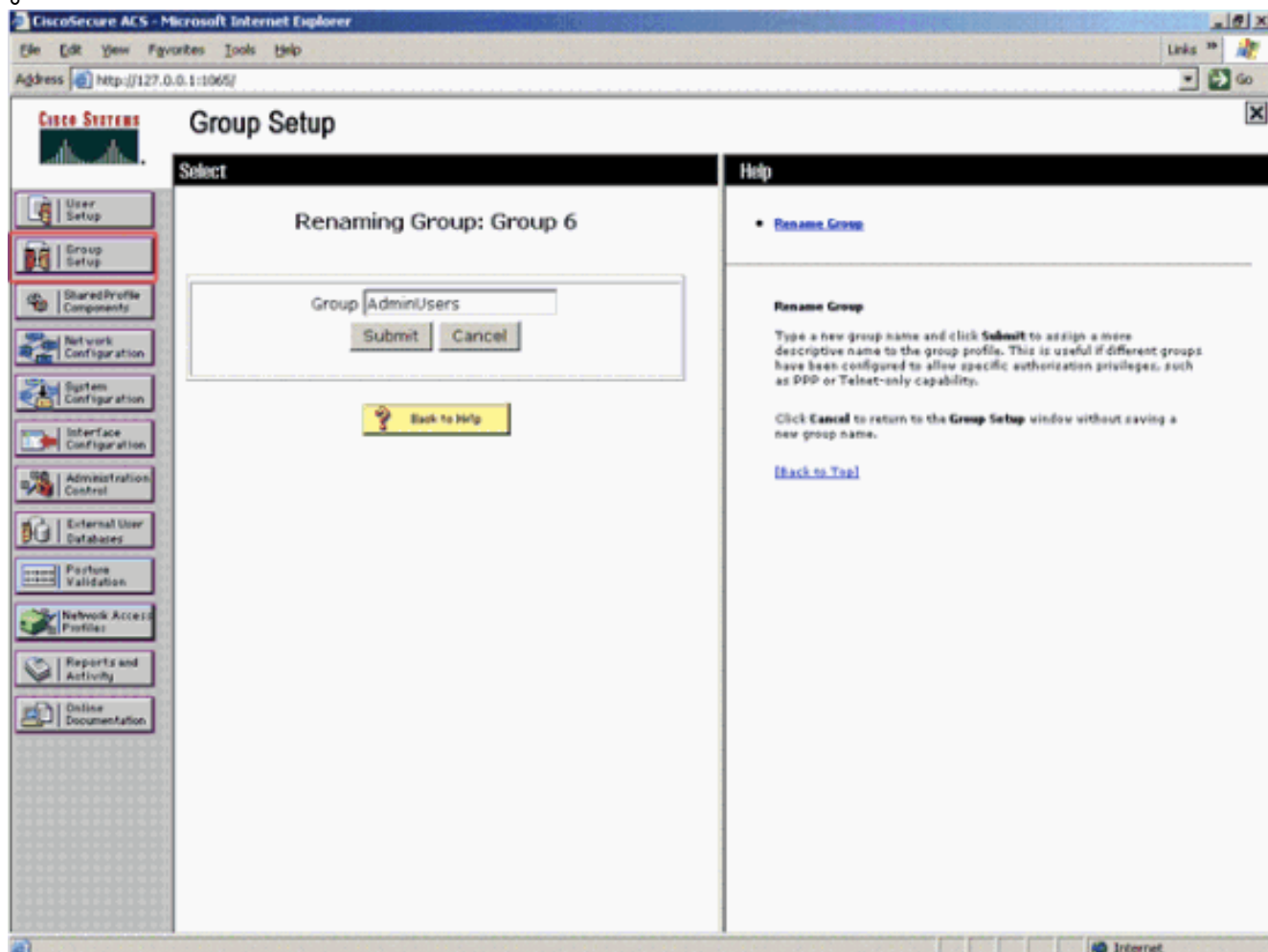
- AAA Client Hostname: AccessPoint
- AAA Client IP Address: 172.16.1.30
- Shared Secret: Example
- RADIUS Key Wrap: Key Encryption Key, Message Authenticator Code, Key, Key Input Format (ASCII/Hexadecimal)
- Authenticate Using: TACACS+ (Cisco IOS) (highlighted with a red oval)
- Single Connect TACACS+ 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:

At the bottom of the window, there are three buttons: 'Submit', 'Submit + Apply' (highlighted with a red oval), and 'Cancel'. A 'Help' sidebar is visible on the right side of the window.

この例では次の設定を使用しています。AAA クライアントのホスト名 : **AccessPoint** AAA クライアントの IP アドレス : **172.16.1.30/16** 共有秘密キー : **Example**

2. 次の手順を実行して、すべての管理 (admin) ユーザを含むグループを作成します。左側の

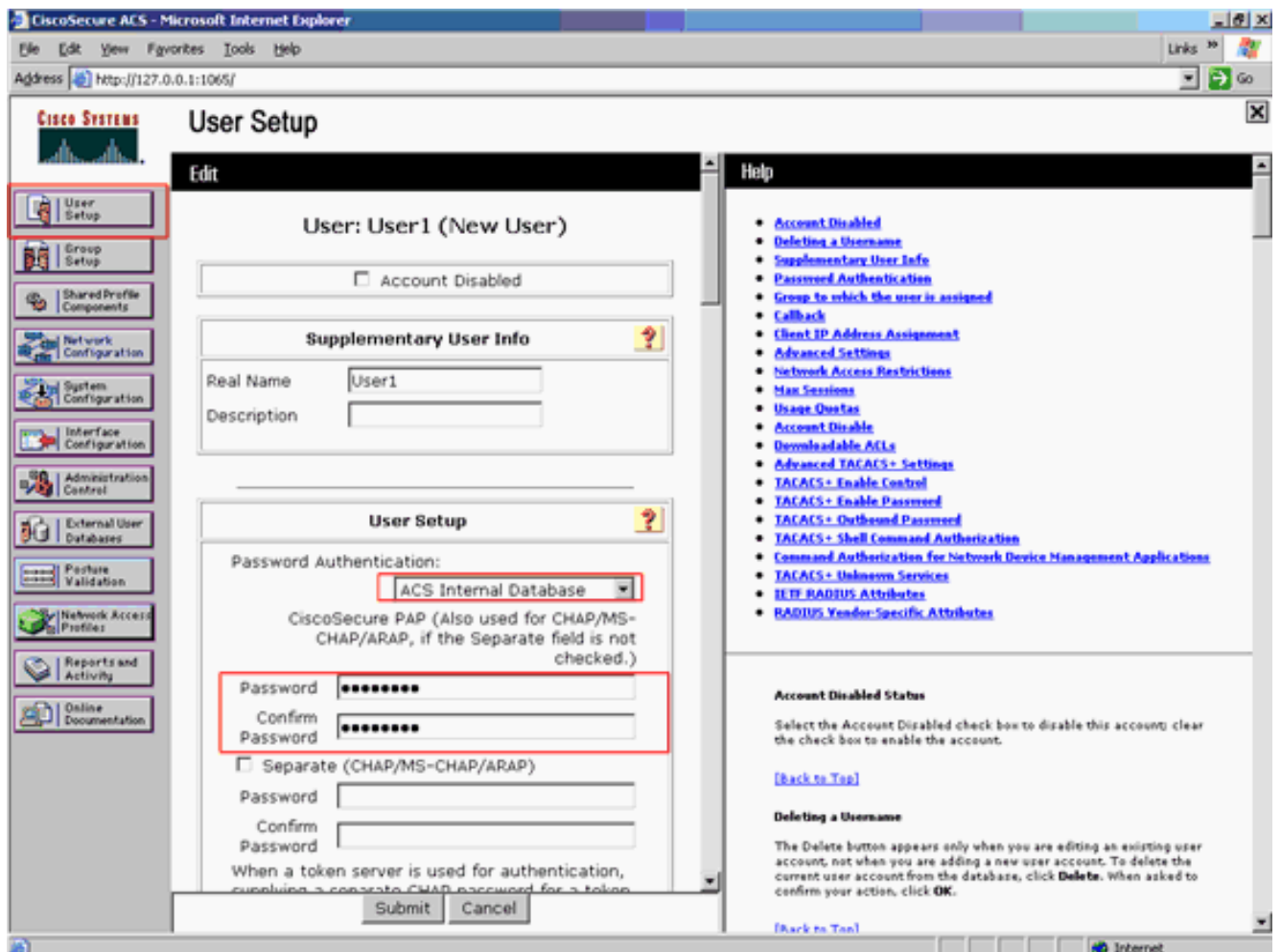
メニューで **Group Setup** をクリックします。新しいウィンドウが表示されます。**Group Setup** ウィンドウで、設定するグループをドロップダウンメニューから選択して、**Rename Group** をクリックします。この例では、Group 6 をドロップダウンメニューから選択し、グループの名前を AdminUsers に変更します。[Submit] をクリックします。次に例を示します。



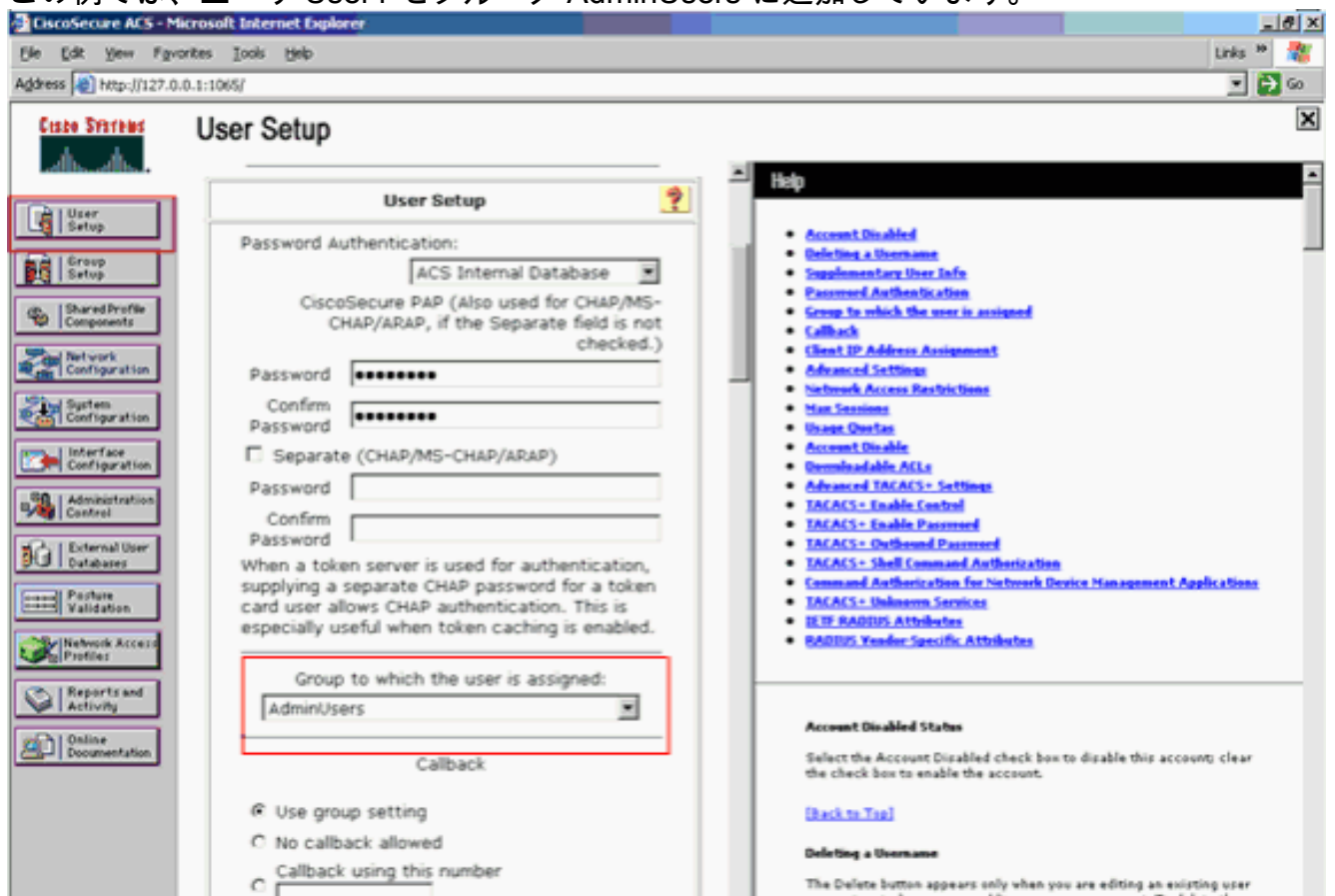
3. 次の手順を実行して、TACACS+ データベースにユーザを追加します。**User Setup** タブをクリックします。新しいユーザを作成するには、**User** フィールドにユーザ名を入力し、**Add/Edit** をクリックします。ここで、**User1** を作成する例を示します。

Add/Edit をクリックすると、このユーザに対する Add/Edit ウィンドウが表示されます。

4. このユーザに固有のクレデンシャルを入力し、Submit をクリックして設定を保存します。入力できるクレデンシャルは次のものです。補足ユーザ情報ユーザ設定ユーザが割り当てられているグループ次に例を示します。



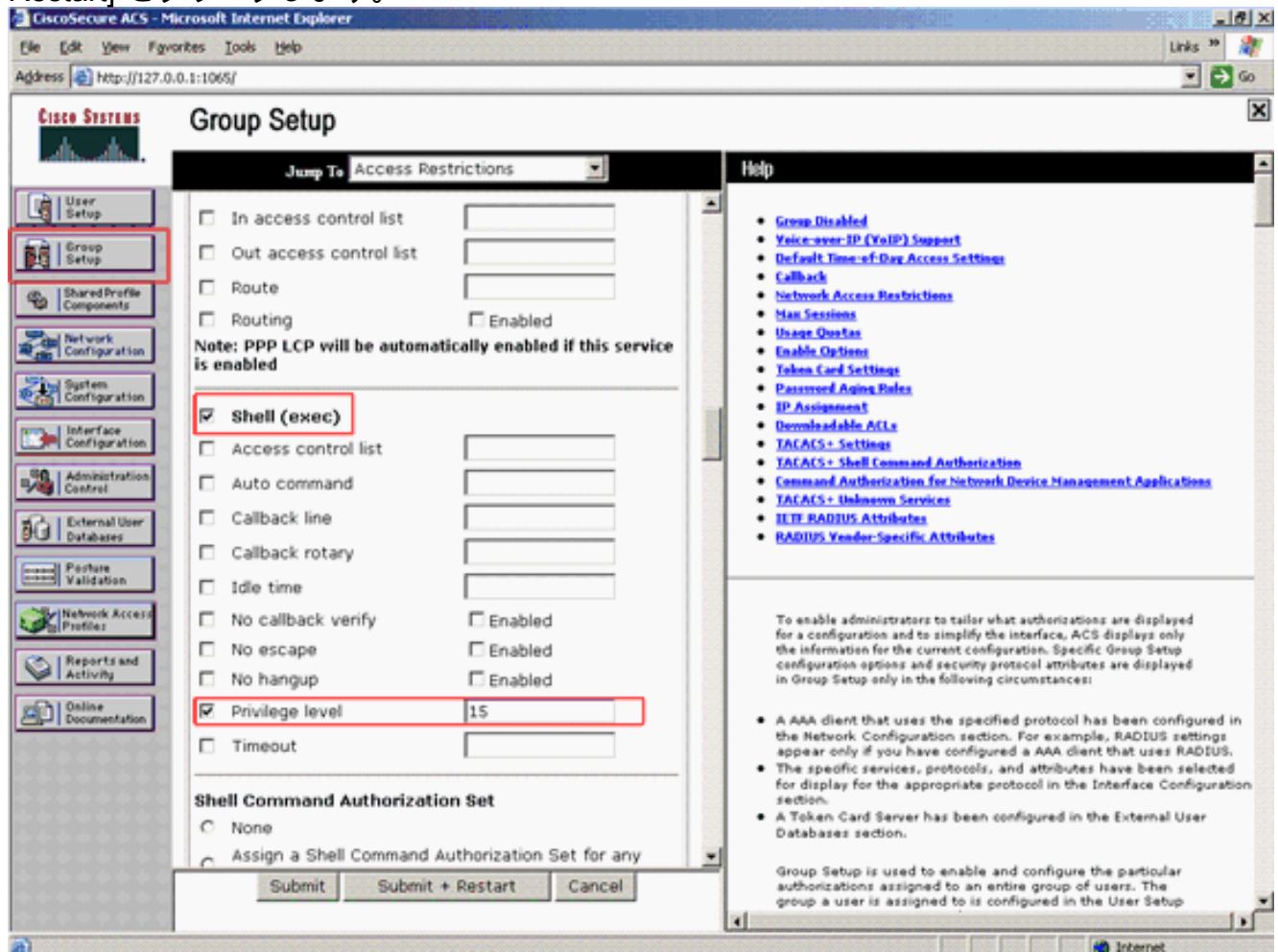
この例では、ユーザ User1 をグループ AdminUsers に追加しています。



注: 特定のグループを作成しないと、ユーザはデフォルトのグループに割り当てられます。

5. 次の手順を実行して、特権レベルを定義します。Group Setup タブをクリックします。この

ユーザに割り当ててあるグループを選択し、**Edit Settings** をクリックします。この例では、グループ AdminUsers を使用しています。[TACACS+ Settings] で、[Shell (exec)] チェックボックスと値を 15 にした [Privilege level] チェックボックスをオンにします。[Submit + Restart] をクリックします。



注: レベル 15 としてアクセスできるようにするには、GUI と Telnet に対して特権レベル 15 を定義する必要があります。このようにしないと、デフォルトにより、ユーザはレベル 1 としてのみアクセスできます。特権レベルを定義せず、ユーザが CLI で (Telnet を使用して) イネーブル モードに入ろうとすると、AP に次のエラーメッセージが表示されます。

```
AccessPoint>enable
% Error in authentication
```

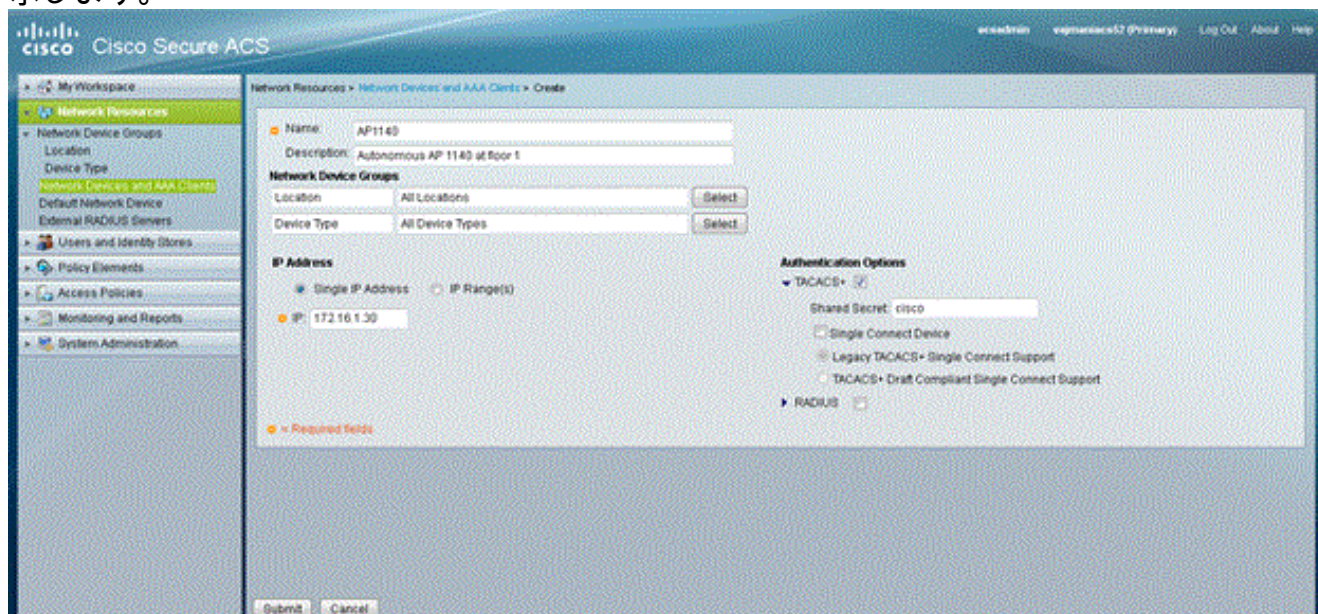
TACACS+ データベースにさらにユーザを追加する場合は、この手順のステップ 2 ~ 4 を繰り返します。以上の手順を終了すると、TACACS+ サーバは AP にログインしようとするユーザを検証できる状態になります。次に、TACACS+ 認証用に AP を設定する必要があります。

[ACS 5.2 を使用したログイン認証用の TACACS+ サーバの設定](#)

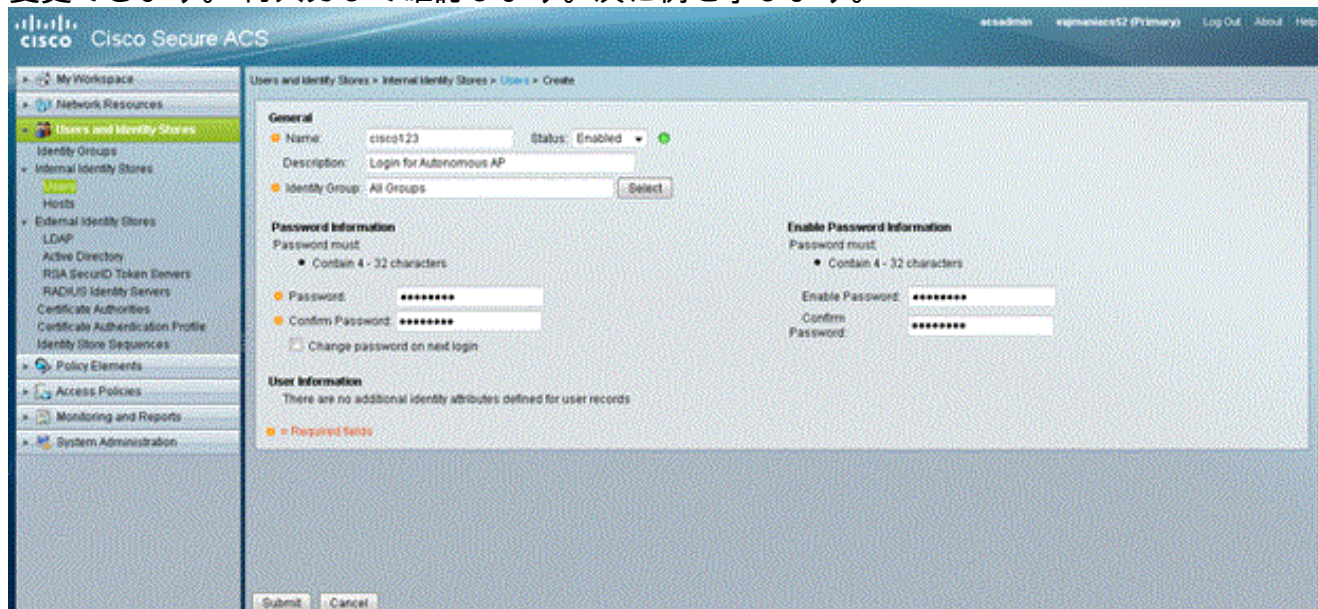
最初のステップは、AP を AAA クライアントとして ACS に追加し、ログイン用の TACACS ポリシーを作成することです。

1. AP を AAA クライアントとして追加するには、次の手順を実行します。ACS GUI で、[Network Resources] をクリックしてから、[Network Devices and AAA Clients] をクリックします。[Network Devices] で、[Create] をクリックします。[Name] に AP のホスト名を入力して、AP に関する説明を入力します。これらのカテゴリが定義されている場合は、[Location] と [Device Type] を選択します。1 つの AP しか設定しないため、[Single IP

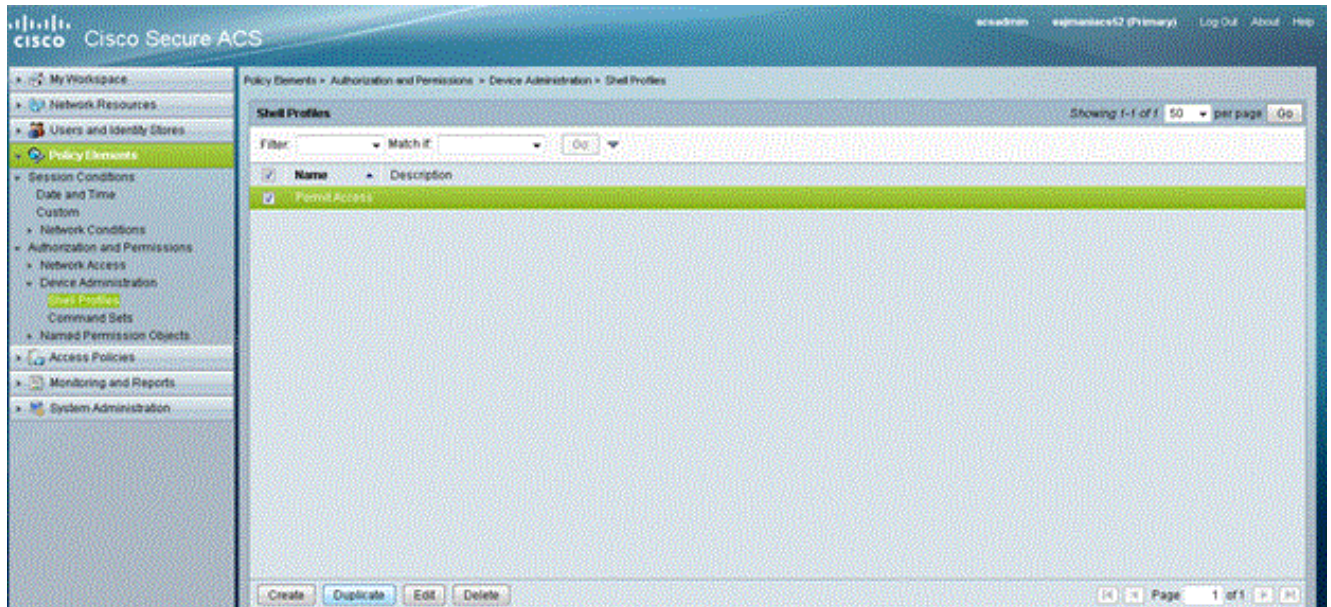
Address] をクリックします。 [IP Range(s)] をクリックすることによって、複数の AP の IP アドレスの範囲を追加できます。 次に、AP の IP アドレスを入力します。 [Authentication Options] で、 [TACACS+] ボックスをオンにして、 [Shared Secret] を入力します。 次に例を示します。



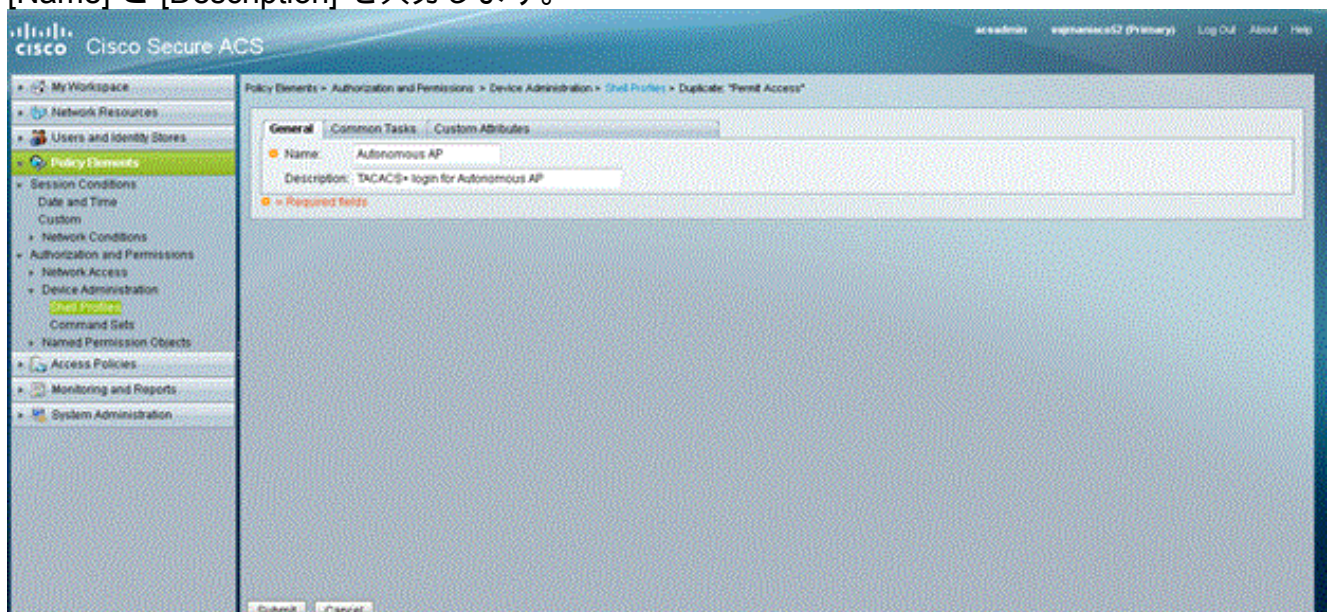
2. 次のステップは、ログイン ユーザ名とパスワードを作成することです。 [Users and Identity Stores] をクリックしてから、 [Users] をクリックします。 [Create] をクリックします。 [Name] にユーザ名を入力して、説明を入力します。 もしあれば、 [Identity Group] を選択します。 [Password] テキスト ボックスにパスワードを入力して、 [Confirm Password] に再入力します。 [Enable Password] にパスワードを入力することによって、有効なパスワードを変更できます。 再入力して確認します。 次に例を示します。



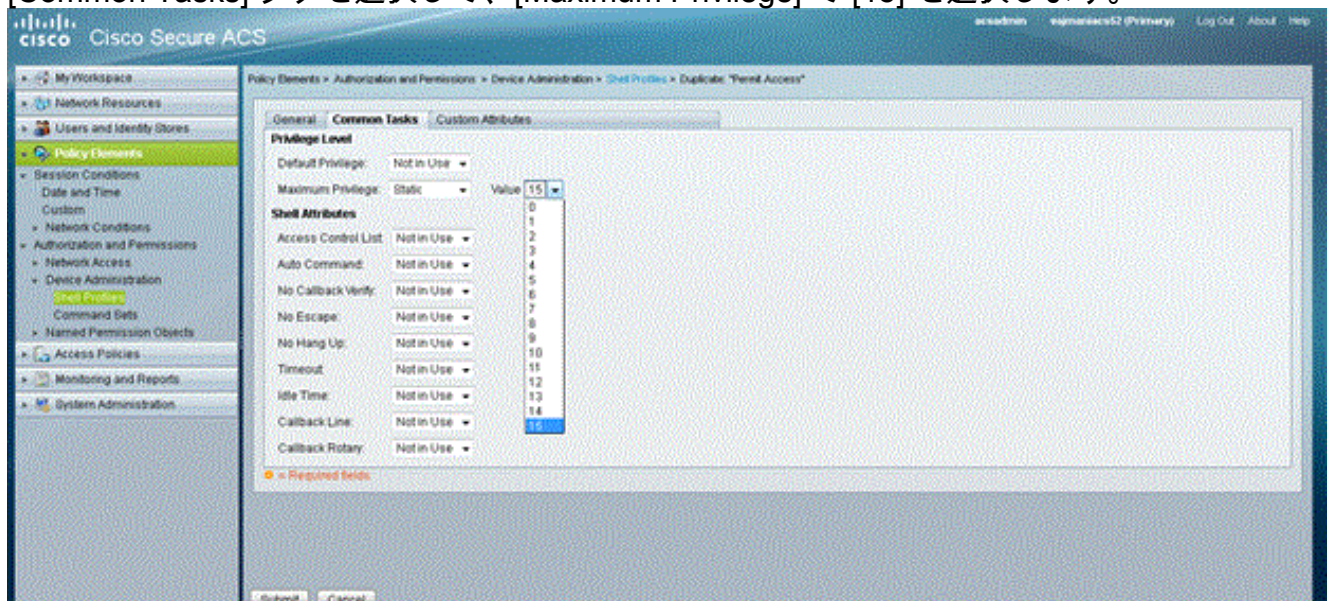
3. 次の手順を実行して、特権レベルを定義します。 [Policy Elements] > [Authorizations and Permissions] > [Device Administration] > [Shell Profiles] の順にクリックします。 [Permit Access] チェック ボックスをオンにして、 [Duplicate] をクリックします。



[Name] と [Description] を入力します。



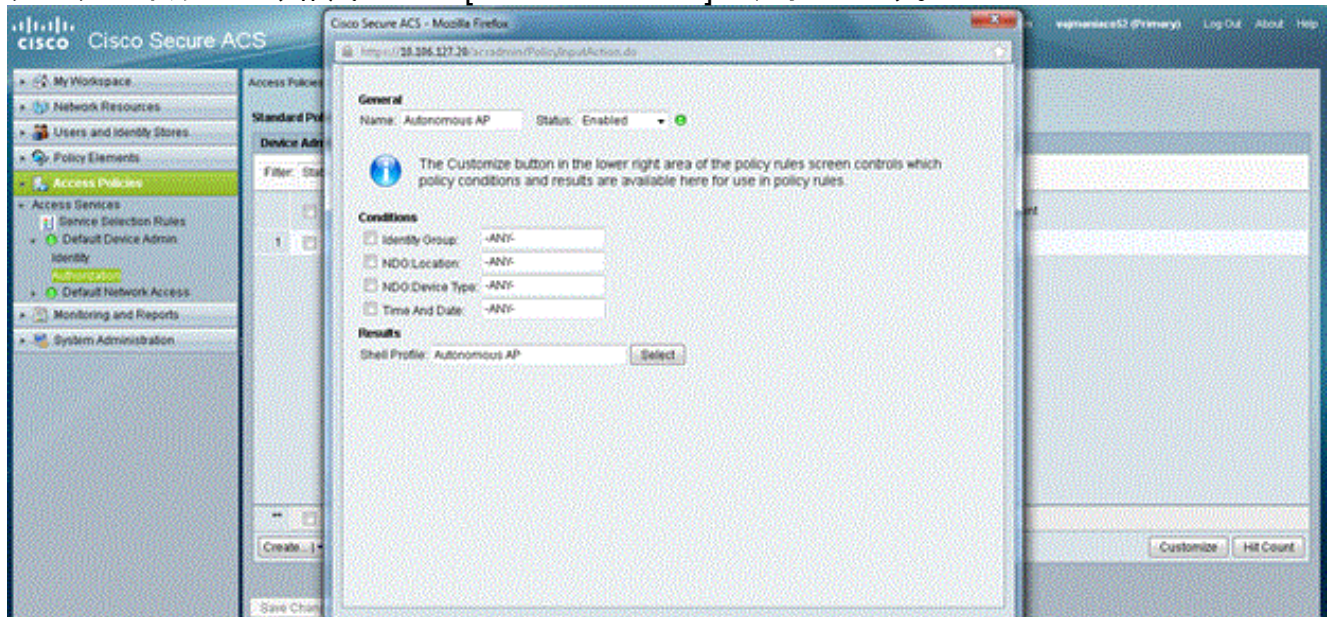
[Common Tasks] タブを選択して、[Maximum Privilege] で [15] を選択します。



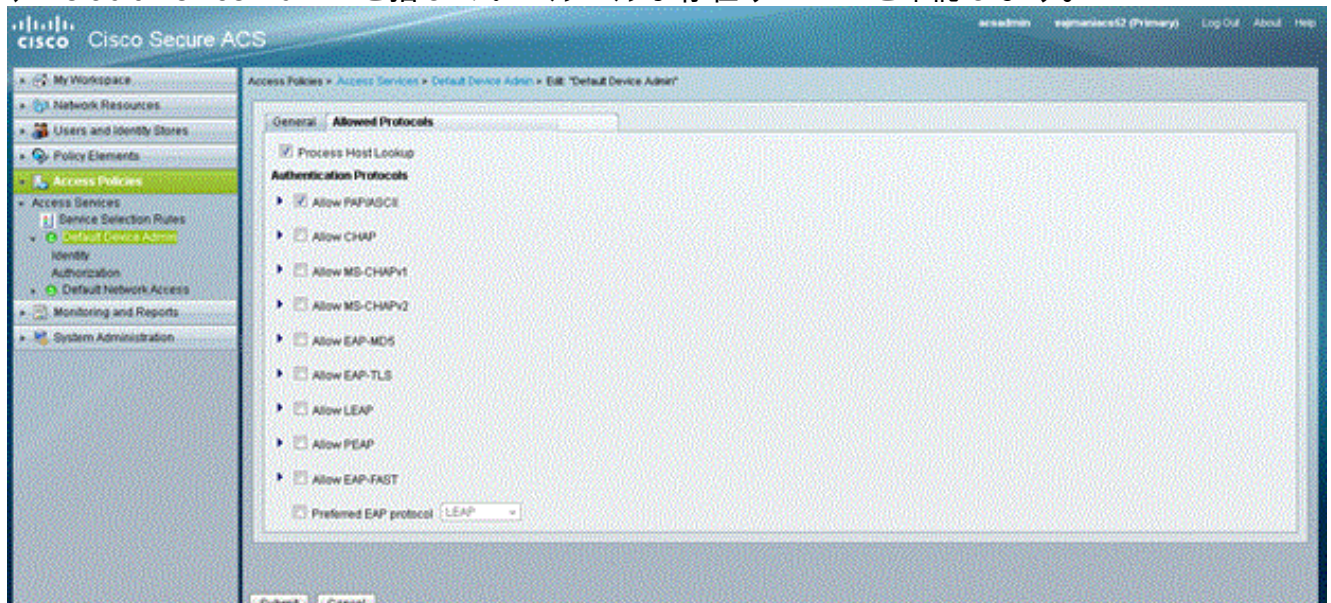
[Submit] をクリックします。

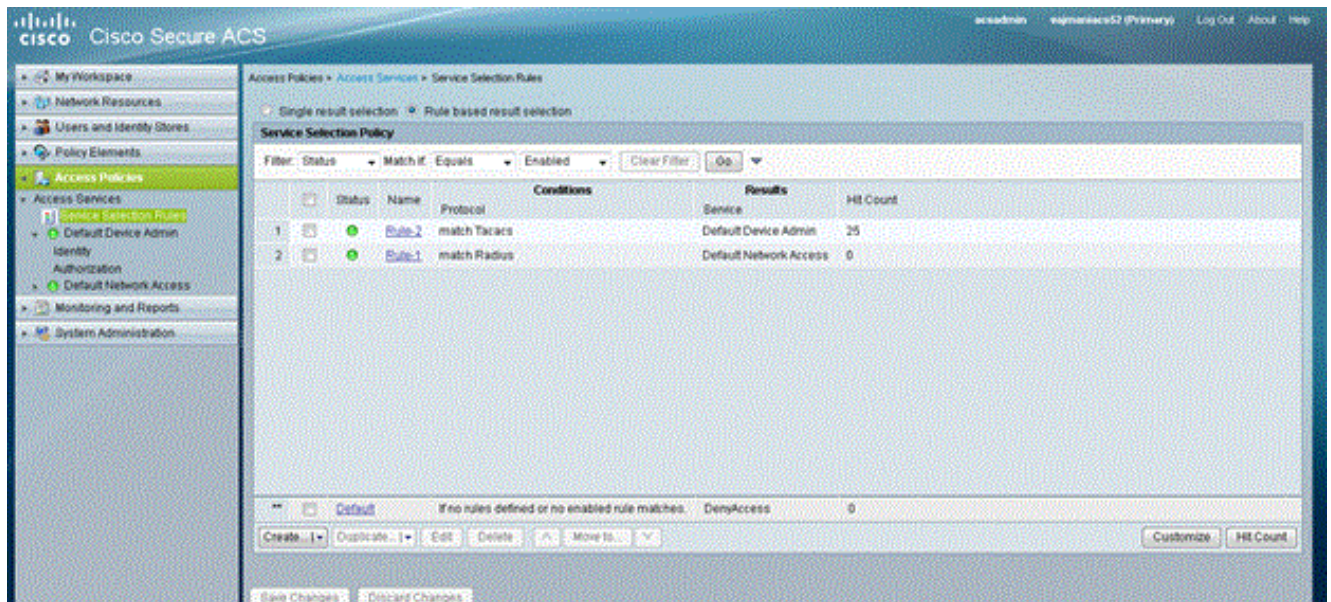
4. 次の手順を実行して、認可ポリシーを作成します。[Access Policies] > [Access Services] > [Default Device Admin] > [Authorization] の順にクリックします。[Create] をクリックして、

新しい認可ポリシーを作成します。認可ポリシーのルールを作成するための新しいポップアップが表示されます。もしあれば、特定のユーザ名と AAA クライアント (AP) の [Identity Group] や [Location] などを選択します。[Shell Profile] に対して [Select] をクリックして、プロファイルにより作成された [Autonomous AP] を選択します。



これが終わったら、[Save Changes] をクリックします。[Default Device Admin] をクリックしてから、[Allowed Protocols] をクリックします。[Allow PAP/ASCII] をオンにしてから、[Submit] をクリックします。[Service Selection Rules] をクリックして、TACACS を照合し、Default Device Admin を指しているルールが存在することを確認します。



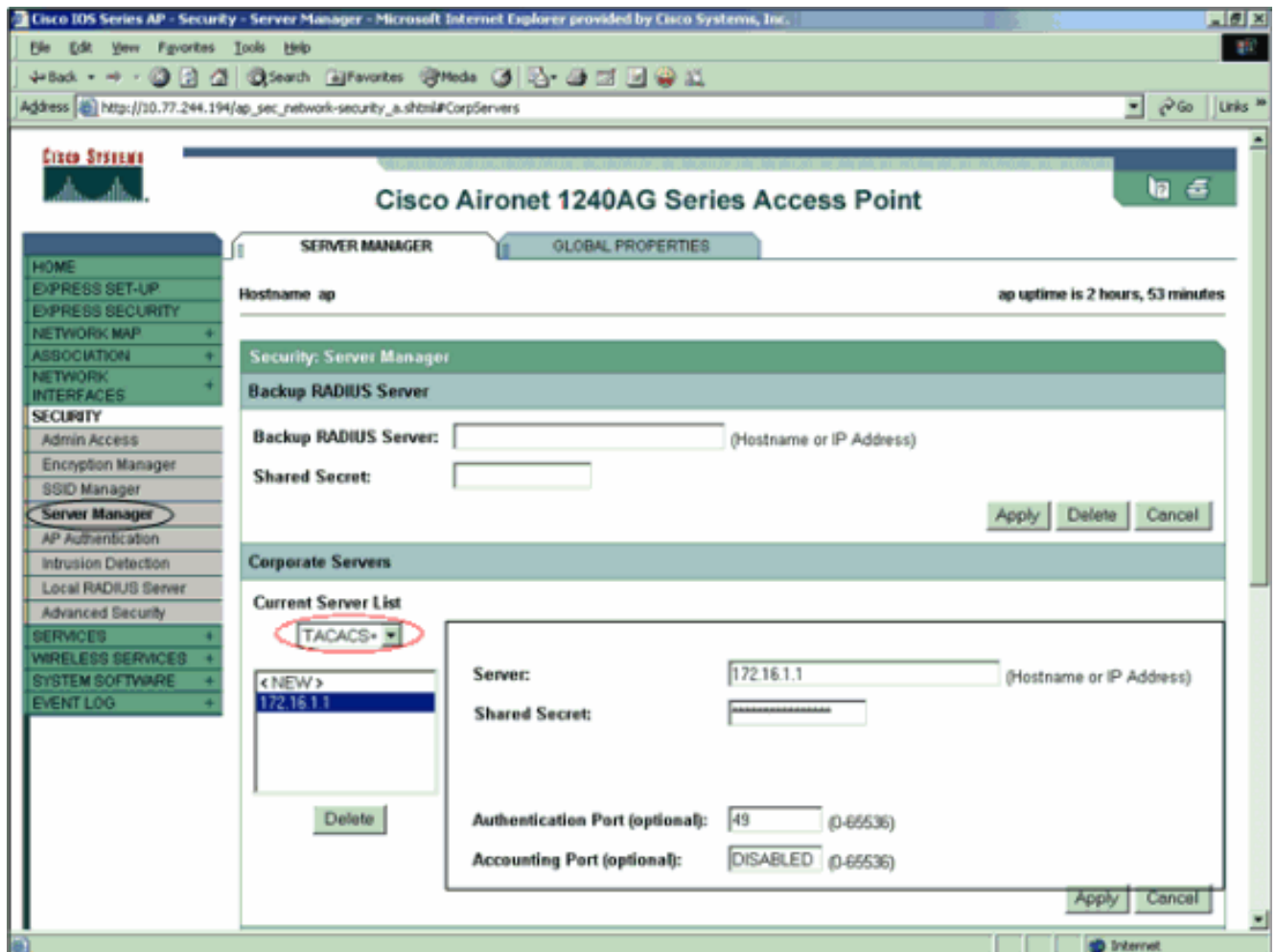


TACACS+ 認証用の Aironet AP の設定

Aironet AP で TACACS+ の機能を有効にするには、CLI または GUI が使用できます。このセクションでは、GUI を使用して TACACS+ ログイン認証用に AP を設定する方法について説明しています。

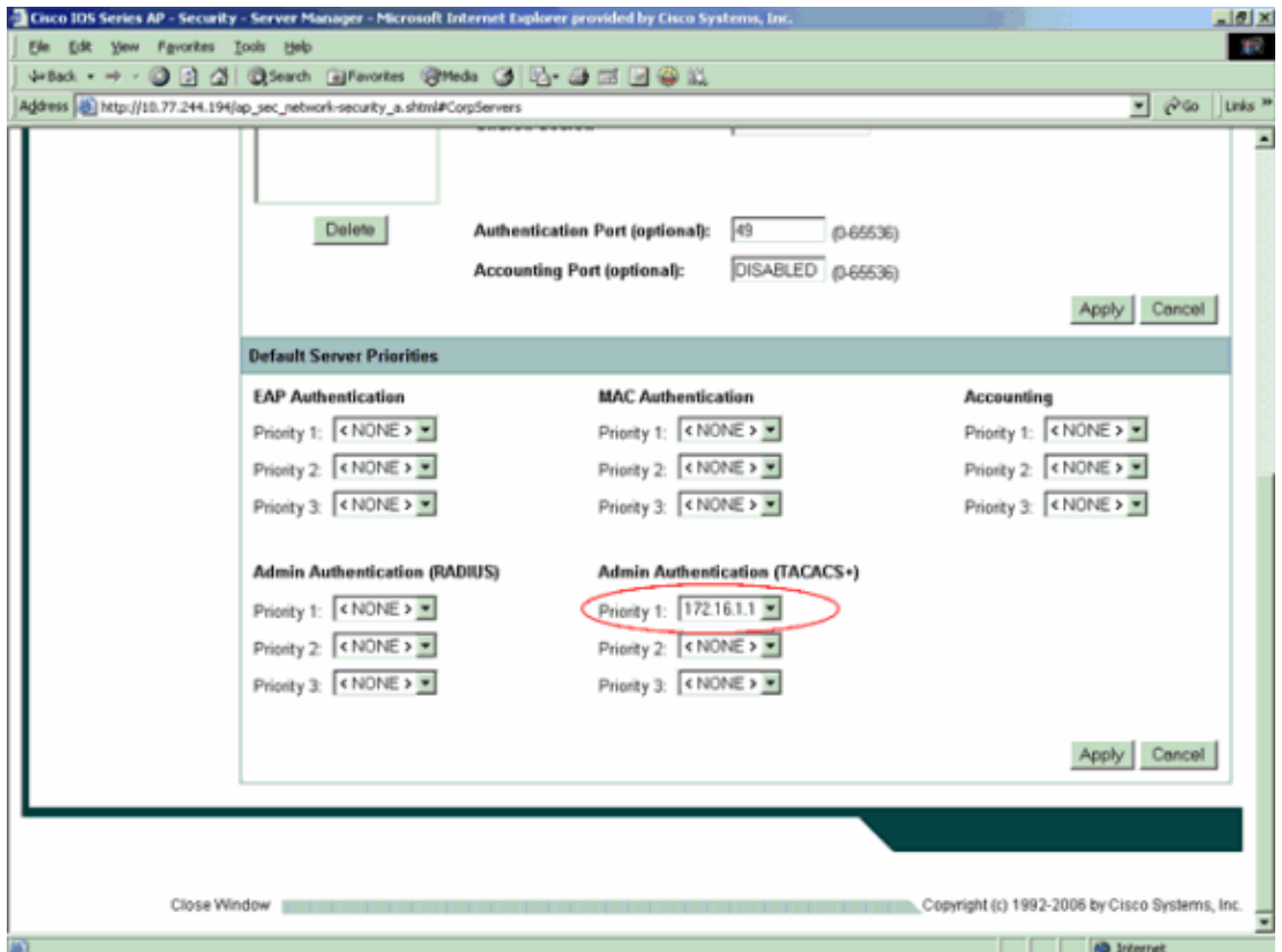
GUI を使用して AP に TACACS+ を設定するには、次の手順を実行します。

1. 次の手順を実行して、TACACS+ サーバのパラメータを定義します。AP の GUI で、**Security > Server Manager** の順に選択します。[Security: Server Manager] ウィンドウが表示されます。**Corporate Servers** 領域で、**Current Server List** ドロップダウンメニューから **TACACS+** を選択します。同じ領域で、TACACS+ サーバの IP アドレス、共有秘密、および認証ポート番号を入力します。[Apply] をクリックします。次に例を示します。

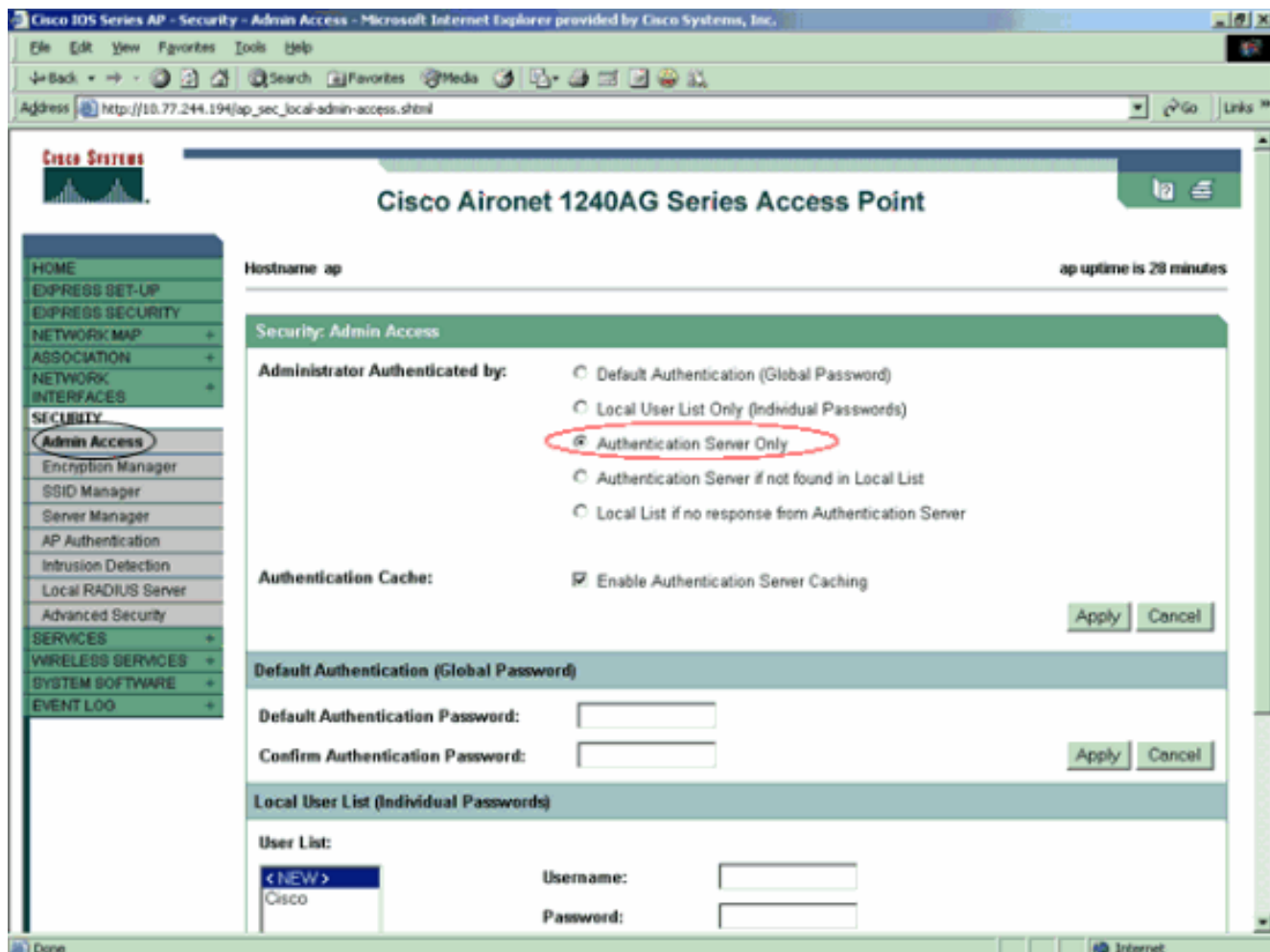


注: デフォルトでは、TACACS+ は TCP ポート 49 を使用します。注: ACS と AP で設定する共有秘密キーは、一致している必要があります。

2. **Default Server Priorities > Admin Authentication (TACACS+)** の順に選択し、**Priority 1** ドロップダウンメニューから先に設定した TACACS+ サーバの IP アドレスを選択して、**Apply** をクリックします。次に例を示します。



3. [Security] > [Admin Access] の順に選択して、[Administrator Authenticated by:] に対して、[Authentication Server Only] を選択して、[Apply] をクリックします。この選択により、AP にログインしようとするユーザは、認証サーバで認証されるようになります。次に例を示します。



CLI による設定の例を次に示します。

AccessPoint

```

AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. !! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1

```

```

!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
  cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BV11 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BV11 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end

```

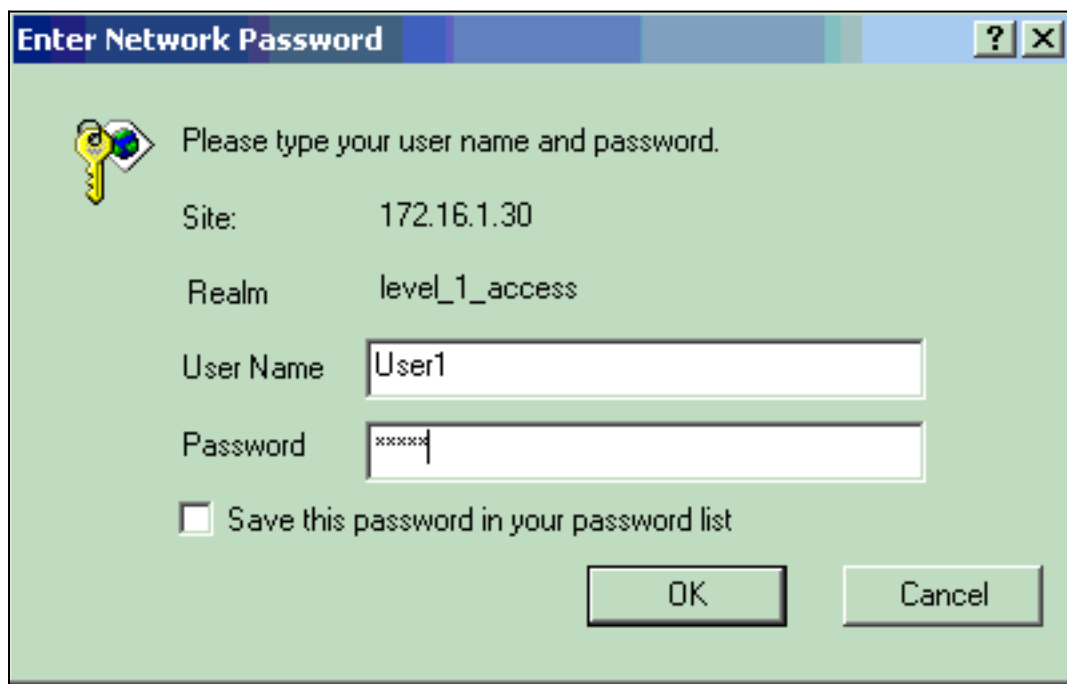
注: この設定のすべてのコマンドが正しく機能するには、Cisco IOS ソフトウェア リリース 12.3(7)JA 以降を使用する必要があります。古い Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。

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。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

設定を確認するには、GUI または CLI を使用して AP にログインしてみます。AP にアクセスを試みると、ユーザ名とパスワードの入力を求められます。



Enter Network Password

Please type your user name and password.

Site: 172.16.1.30

Realm: level_1_access

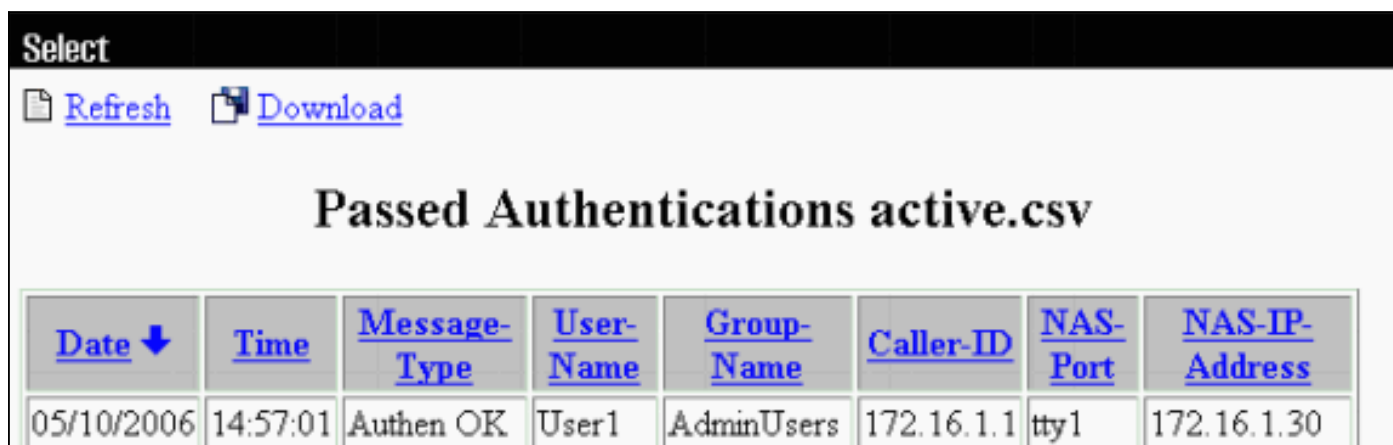
User Name: User1

Password: *****

Save this password in your password list

OK Cancel

ユーザ クレデンシャルを入力すると、AP はクレデンシャルを TACACS+ サーバに転送します。TACACS+ サーバは、データベースの情報に基づいてクレデンシャルを検証し、認証が成功すると AP へのアクセスを許可します。このユーザの認証が成功したことを確認するには、ACS で **Reports and Activity > Passed Authentication** の順に選択し、Passed Authentication レポートを使用します。次に例を示します。



Select

[Refresh](#) [Download](#)

Passed Authentications active.csv

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty1	172.16.1.30

show tacacs コマンドを使用して、TACACS+ サーバの設定が正しいことを確認することもできます。次に例を示します。

```
AccessPoint#show tacacs
```

```
Tacacs+ Server      : 172.16.1.1/49
  Socket opens:      348
  Socket closes:     348
  Socket aborts:     0
  Socket errors:     0
  Socket Timeouts:   0
  Failed Connect Attempts: 0
  Total Packets Sent: 525
  Total Packets Recv: 525
```


ACS 5.2 の検証

ACS 5.2 から、ログイン クレデンシャルの試みが失敗したか成功したかを確認できます。

1. [Monitoring Reports] > [Launch Monitoring and Report Viewer] の順にクリックします。ダッシュボード付きの新しいポップアップが表示されます。
2. [Authentications-TACACS-Today] をクリックします。これにより、失敗/成功した試みの詳細が表示されます。

トラブルシューティング

設定のトラブルシューティングを行うには、AP で次の debug コマンドが使用できます。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **debug tacacs events** : このコマンドは、TACACS 認証中に発生したイベントのシーケンスを表示します。このコマンドの出力例を次に示します。

```
*Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar 1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar 1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **debug ip http authentication** : HTTP 認証の問題をトラブルシューティングするためのコマンドです。ルータが使用した認証方式と認証特有の状況メッセージを表示します。
- **debug aaa authentication** : AAA TACACS+ 認証に関する情報を表示します。

TACACS+ サーバに存在しないユーザ名をユーザが入力すると、認証は失敗します。ここで、失敗した認証に対する **debug tacacs authentication** コマンドの出力を示します。

```
*Mar 1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
```

```

*Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar 1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.689: TPLUS: Received authen response status FAIL (3)

```

Reports and Activity > Failed Authentication の順に選択すると、ACS で失敗した認証の試行を確認できます。次に例を示します。

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	CS user unknown

Cisco IOS ソフトウェア リリース 12.3(7)JA より前のリリースを AP で使用している場合は、HTTP を使用して AP へのログインを試みるたびに不具合に遭遇する可能性があります。Cisco Bug ID は、[CSCeb52431](#) ([登録ユーザ専用](#)) です。

Cisco IOS ソフトウェアの HTTP/AAA の実装では、異なる HTTP 接続ごとに独立した認証が必要です。ワイヤレス Cisco IOS ソフトウェア GUI には、単一の Web ページ内に多数の異なるファイル (Javascript や GIF など) の参照が含まれます。そのため、ワイヤレス Cisco IOS ソフトウェア GUI で単一のページをロードする場合、個別の認証/認可要求が大量に AAA サーバに送られる可能性があります。

HTTP 認証の場合は、RADIUS またはローカル認証を使用してください。RADIUS サーバでも、やはり複数の認証要求を受け取ります。ただし、RADIUS は TACACS+ よりスケーラビリティが優れているので、パフォーマンスの低下は小さくて済みます。

TACACS+ を使用する必要があり、Cisco ACS がある場合は、**single-connection** キーワードを **tacacs-server** コマンドとともに使用します。コマンドでこのキーワードを使用すると、ACS での TCP 接続のセットアップ/ティアダウンのオーバーヘッドの大部分がなくなり、サーバの負荷がある程度まで軽減される可能性があります。

Cisco IOS ソフトウェア リリース 12.3(7) JA 以降を AP で使用している場合は、ソフトウェアに

修正が含まれています。次にこの修正について説明します。

TACACS+ サーバが返す情報をキャッシュするには、AAA の認証キャッシュ機能を使用します。認証キャッシュおよびプロファイル機能を使用すると、AP は、ユーザに対する認証/認可応答をキャッシュでき、以降の認証/認可要求を AAA サーバに送信する必要がなくなります。CLI でこの機能を有効にするには、次のコマンドを使用します。

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

この機能とコマンドについての詳細は、『[アクセスポイントの管理](#)』の「[認証キャッシュおよびプロファイルの設定](#)」の項を参照してください。

この機能を GUI で有効にするには、**Security > Admin Access** の順に選択し、**Enable Authentication Server Caching** チェックボックスにチェックマークを付けます。このドキュメントでは Cisco IOS ソフトウェア リリース 12.3(7)JA を使用しているため、この修正を「[設定](#)」の説明に従って使用しています。

[関連情報](#)

- [RADIUS サーバと TACACS+ サーバの設定](#)
- [Field Notice : IOS アクセスポイントから TACACS+ サーバに要求が殺到する](#)
- [RADIUS サーバとの EAP 認証](#)
- [ワイヤレス製品に関するサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)