TACACS+ auf einem Aironet Access Point für die Anmeldeauthentifizierung mithilfe des GUI-Konfigurationsbeispiels

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie TACACS Plus (TACACS+)-Dienste auf einem Cisco Aironet Access Point (AP) aktivieren, um die Anmeldeauthentifizierung mit einem TACACS+-Server durchzuführen.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von Aironet APs
- Kenntnisse zum Konfigurieren eines TACACS+-Servers wie des Cisco Secure Access Control Server (ACS)
- Kenntnisse der TACACS+-Konzepte

Weitere Informationen zur Funktionsweise von TACACS+ finden Sie im Abschnitt *Understanding TACACS+* of Configuring RADIUS and TACACS+ Servers.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Aironet Cisco Aironet Access Points der Serien 1240/1140
- ACS mit Softwareversion 4.1
- ACS mit Softwareversion 5.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt wird erläutert, wie der Aironet AP und der TACACS+-Server (ACS) für die TACACS+-basierte Anmeldeauthentifizierung konfiguriert werden.

In diesem Konfigurationsbeispiel werden folgende Parameter verwendet:

- IP-Adresse des ACS: 172.16.1.1/255.255.0.0
- IP-Adresse des AP: 172.16.1.30/255.255.0.0
- Gemeinsamer geheimer Schlüssel, der auf dem AP und dem TACACS+-Server verwendet wird - **Beispiel**

Dies sind die Anmeldeinformationen des Benutzers, der in diesem Beispiel für den ACS konfiguriert wird:

- Benutzername - **Benutzer1**
- Kennwort - **Cisco**
- Gruppe - **AdminUsers**

Sie müssen TACACS+-Funktionen konfigurieren, um Benutzer zu validieren, die versuchen, eine Verbindung zum Access Point herzustellen, entweder über die Webschnittstelle oder über die Befehlszeilenschnittstelle (CLI). Um diese Konfiguration auszuführen, müssen Sie folgende Aufgaben ausführen:

1. Konfigurieren Sie den TACACS+-Server für die Anmeldeauthentifizierung.
2. Konfigurieren Sie den Aironet AP für die TACACS+-Authentifizierung.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

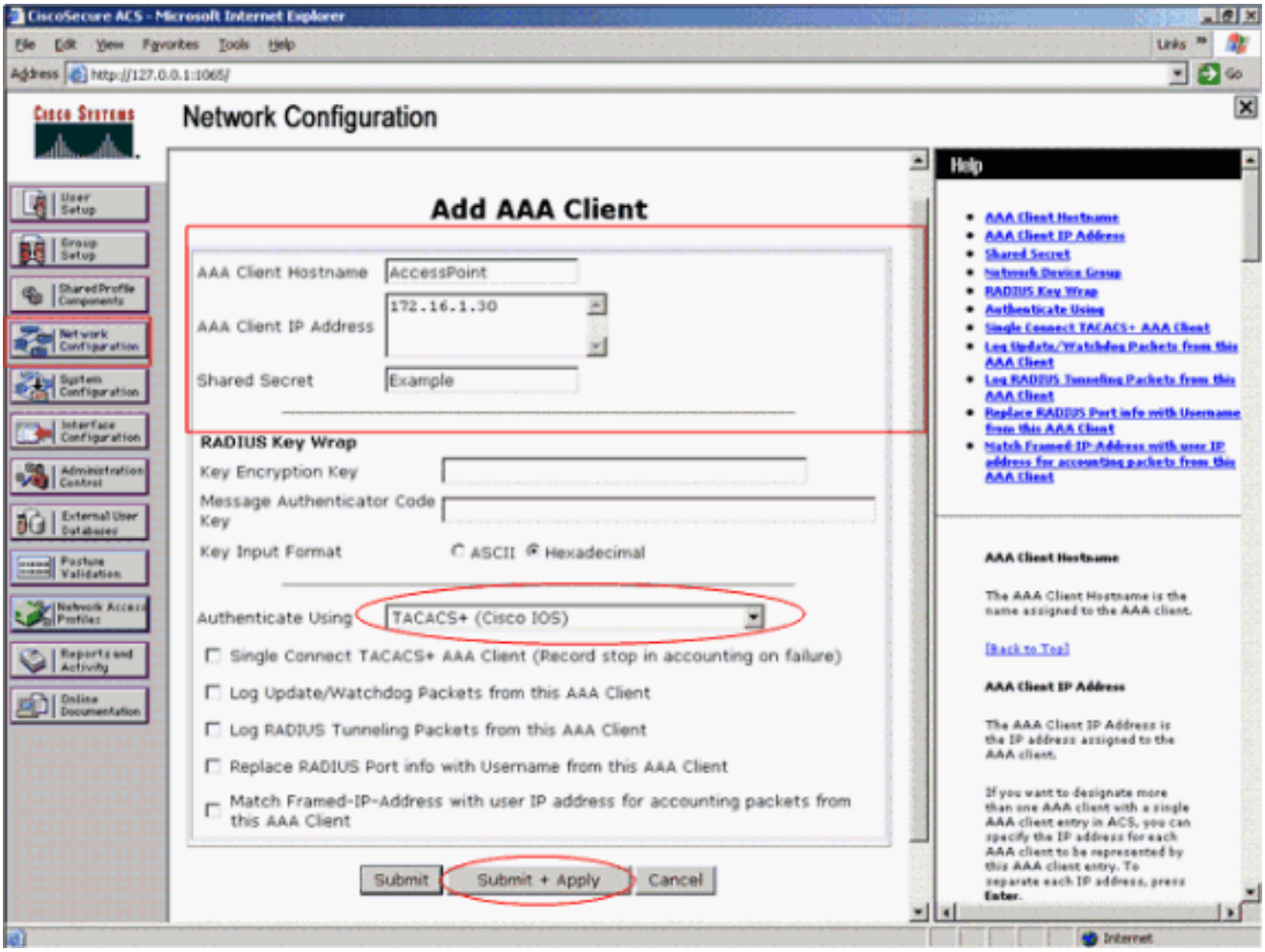
Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Konfigurieren des TACACS+-Servers für die Anmeldeauthentifizierung - Verwenden von ACS 4.1

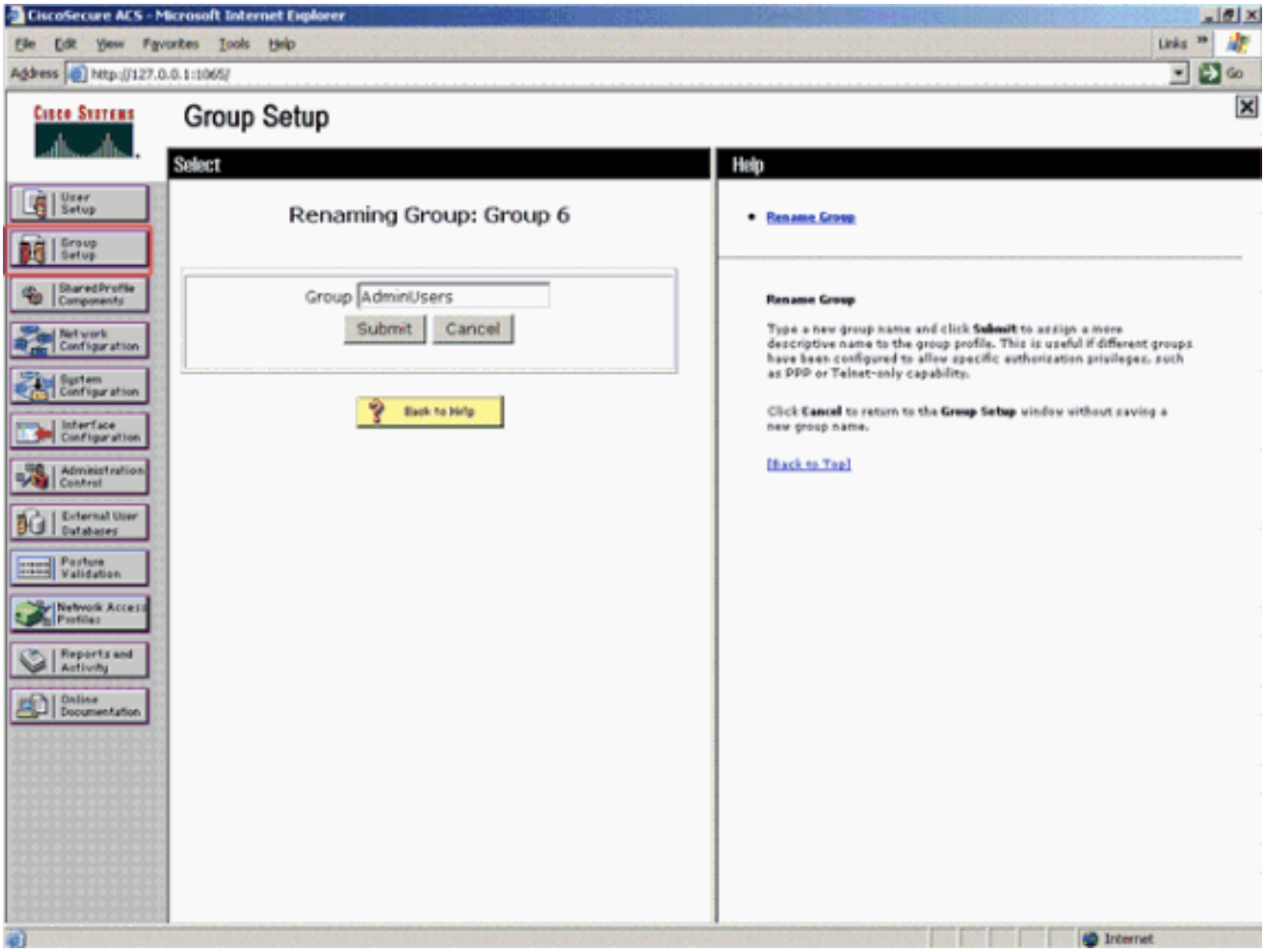
Der erste Schritt besteht darin, einen TACACS+-Daemon einzurichten, um die Benutzer zu validieren, die versuchen, auf den Access Point zuzugreifen. Sie müssen den ACS für die TACACS+-Authentifizierung einrichten und eine Benutzerdatenbank erstellen. Sie können jeden TACACS+-Server verwenden. In diesem Beispiel wird der ACS als TACACS+-Server verwendet. Gehen Sie wie folgt vor:

1. Gehen Sie wie folgt vor, um den Access Point als AAA-Client (Authentication, Authorization, Accounting) hinzuzufügen:Klicken Sie in der ACS-GUI auf die Registerkarte **Network Configuration (Netzwerkkonfiguration)**.Klicken Sie unter AAA-Clients auf **Eintrag hinzufügen**.Geben Sie im Fenster Add AAA Client (AAA-Client hinzufügen) den Hostnamen des Access Points, die IP-Adresse des Access Points und einen gemeinsamen geheimen Schlüssel ein.Dieser gemeinsam verwendete geheime Schlüssel muss mit dem gemeinsam genutzten geheimen Schlüssel identisch sein, den Sie auf dem Access Point konfigurieren.Wählen Sie im Dropdown-Menü Authenticate Using (Authentifizierung über Verwendung) die Option **TACACS+ (Cisco IOS)** aus.Klicken Sie auf **Senden + Neu starten**, um die Konfiguration zu speichern.Hier ein
   Beispiel:

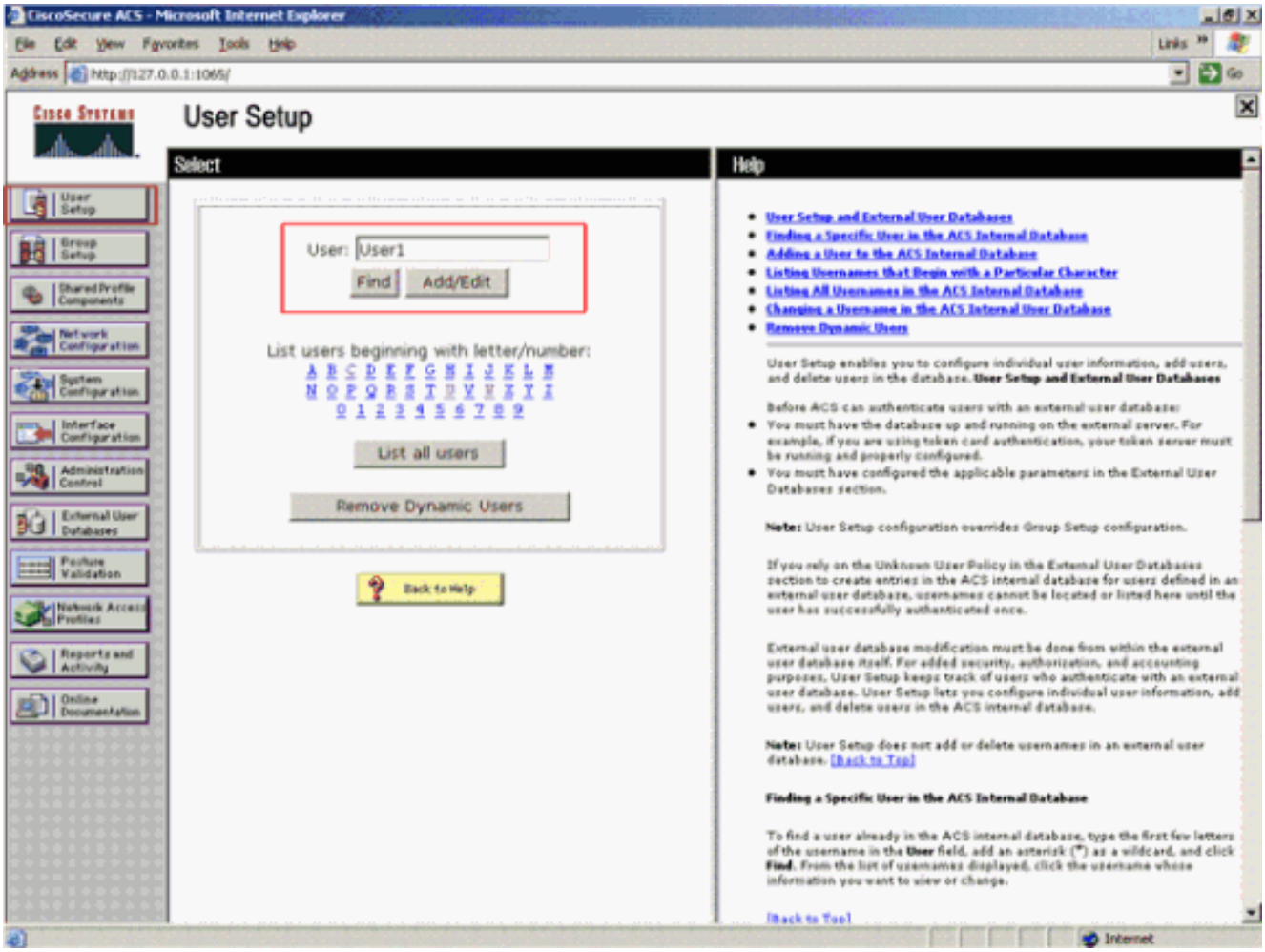


In diesem Beispiel wird Folgendes verwendet:Der AAA-Client-Hostname **AccessPoint**Die Adresse **172.16.1.30/16** als IP-Adresse des AAA-ClientsDas **Beispiel** eines gemeinsam genutzten geheimen Schlüssels

2. Gehen Sie wie folgt vor, um eine Gruppe zu erstellen, die alle administrativen (Administrator-)Benutzer enthält:Klicken Sie im Menü auf der linken Seite auf **Gruppeneinrichtung**.Ein neues Fenster wird angezeigt.Wählen Sie im Fenster Gruppeneinrichtung eine Gruppe aus dem Dropdown-Menü aus, die konfiguriert werden soll, und klicken Sie auf **Gruppe umbenennen**.In diesem Beispiel wird Gruppe 6 aus dem Dropdown-Menü ausgewählt und die Gruppe AdminUsers umbenannt.Klicken Sie auf **Senden**.Hier ein Beispiel:

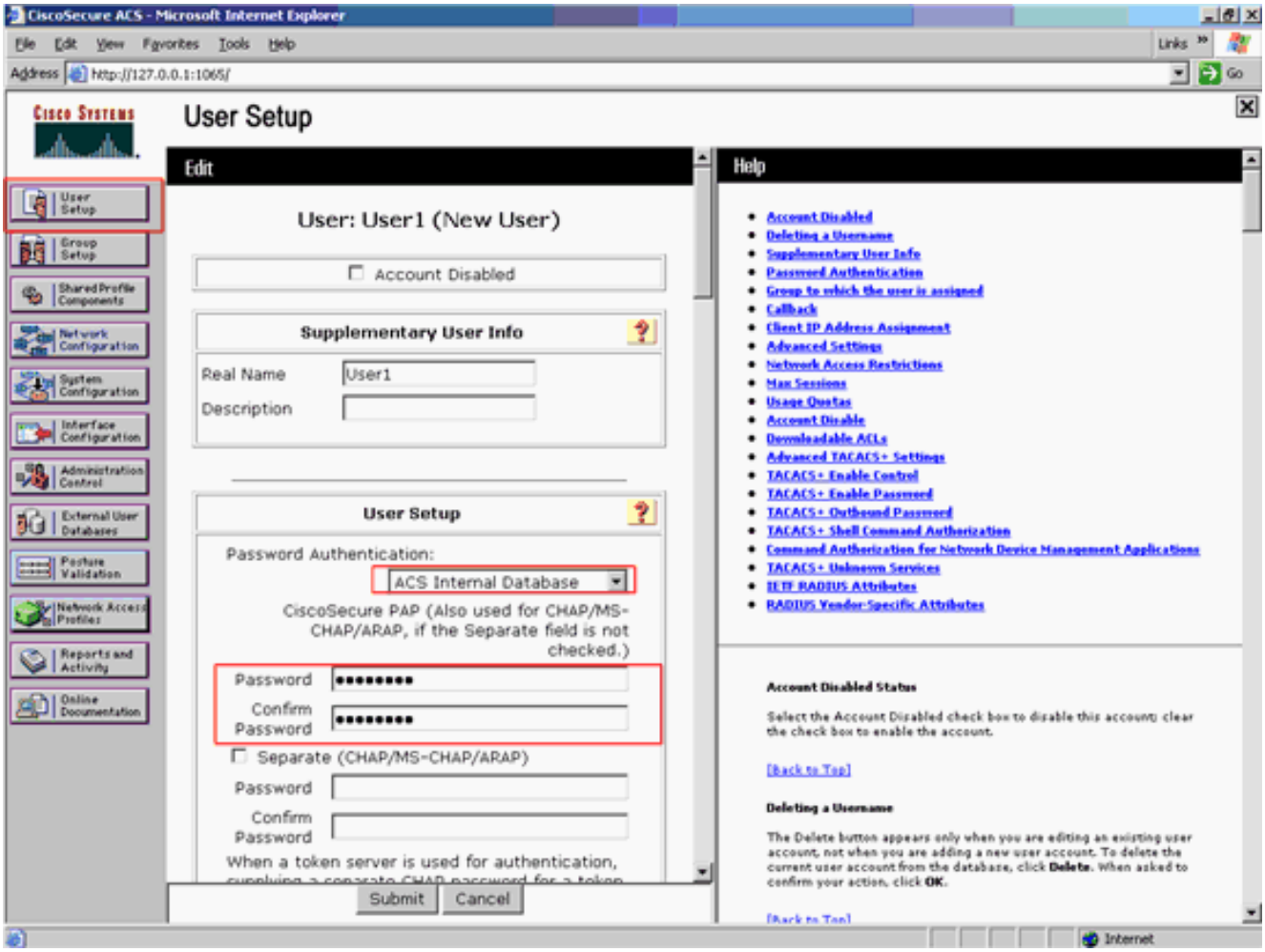


3. Gehen Sie wie folgt vor, um die Benutzer der TACACS+-Datenbank hinzuzufügen:Klicken Sie auf die Registerkarte **Benutzereinrichtung**.Um einen neuen Benutzer zu erstellen, geben Sie den Benutzernamen im Feld Benutzer ein, und klicken Sie auf **Hinzufügen/Bearbeiten**.Im folgenden Beispiel wird **User1**
erstellt:

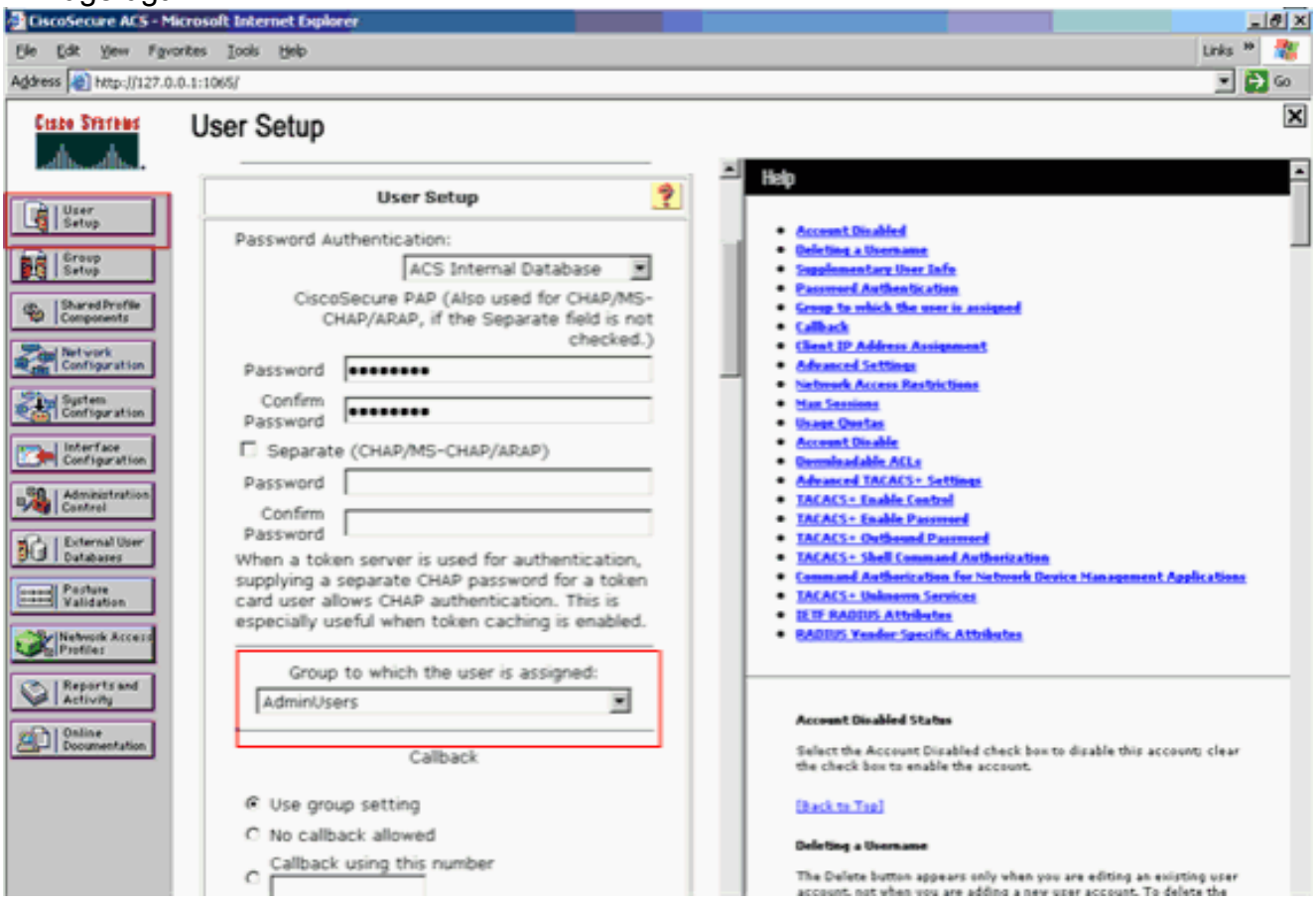


Wenn Sie auf Hinzufügen/Bearbeiten klicken, wird das Fenster Hinzufügen/Bearbeiten für diesen Benutzer angezeigt.

4. Geben Sie Anmeldeinformationen für diesen Benutzer ein, und klicken Sie auf **Senden**, um die Konfiguration zu speichern.Folgende Anmeldeinformationen können Sie eingeben:Zusätzliche BenutzerinformationenBenutzereinrichtungDie Gruppe, der der Benutzer zugewiesen istHier ein
Beispiel:



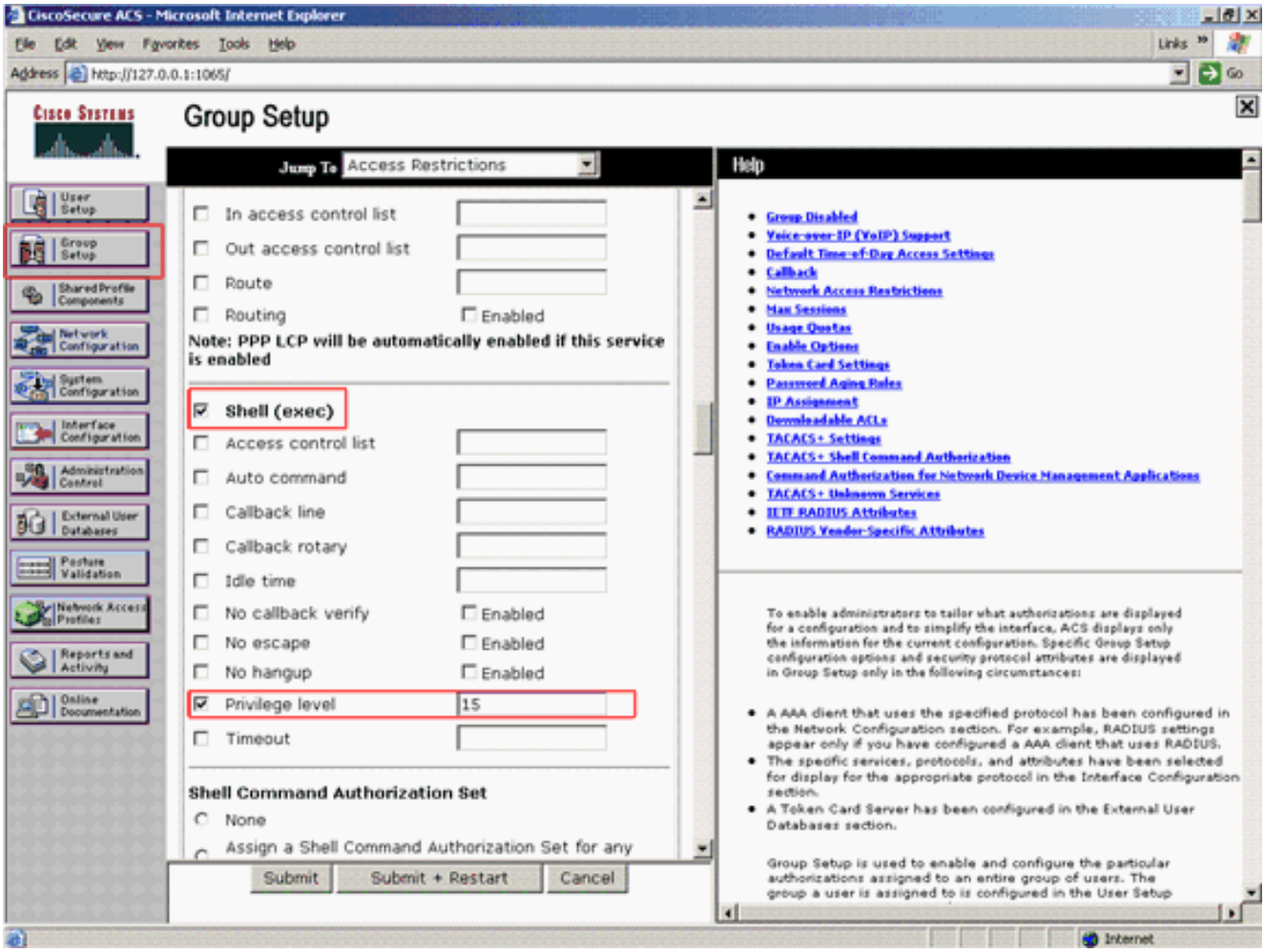
In diesem Beispiel wird der Benutzer User1 der Gruppe AdminUsers hinzugefügt.



Hinweis: Wenn Sie keine bestimmte Gruppe erstellen, werden die Benutzer der

Standardgruppe zugewiesen.

5. Führen Sie die folgenden Schritte aus, um die Berechtigungsebene zu definieren:Klicken Sie auf die Registerkarte **Gruppeneinrichtung**.Wählen Sie die Gruppe aus, die Sie diesem Benutzer zuvor zugewiesen haben, und klicken Sie auf **Einstellungen bearbeiten**.In diesem Beispiel wird die Gruppe AdminUsers verwendet.Aktivieren Sie unter TACACS+ Settings (TACACS+-Einstellungen) das Kontrollkästchen **Shell (exec)**, und aktivieren Sie das Kontrollkästchen **Privilege** (Berechtigungsebene) mit einem Wert von 15.Klicken Sie auf **Senden + Neu starten**.



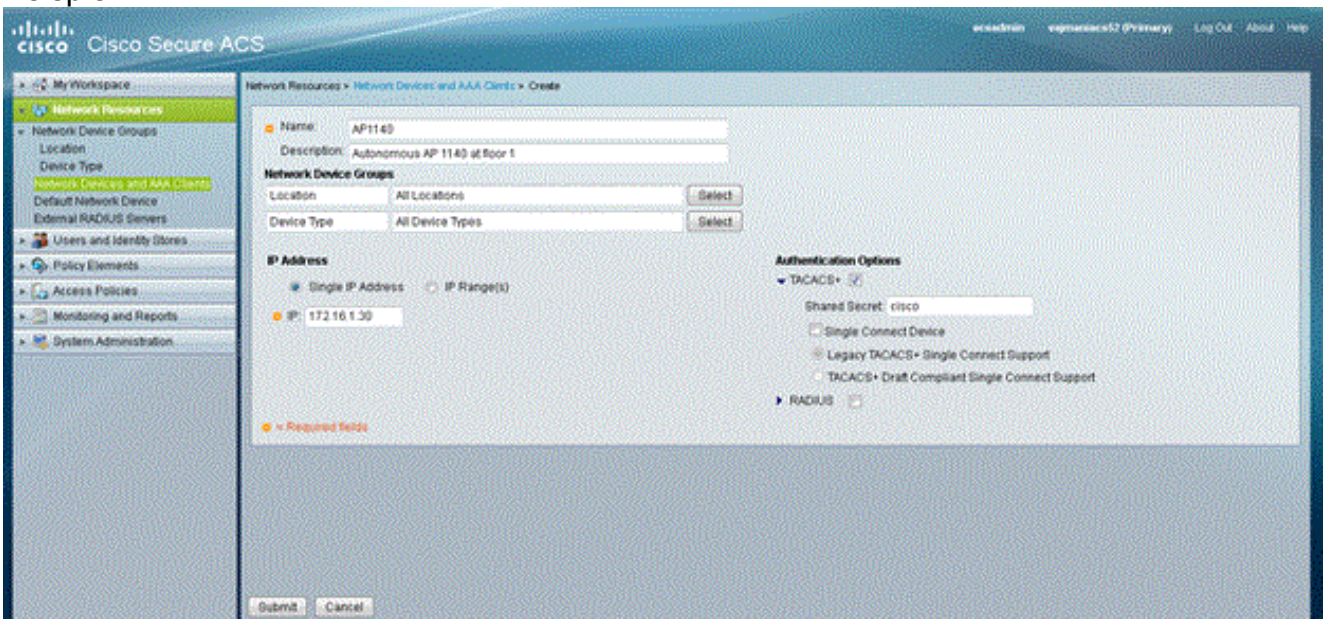
Hinweis: Die Berechtigungsstufe 15 muss für die GUI und Telnet definiert werden, damit der Zugriff auf Stufe 15 möglich ist. Andernfalls kann der Benutzer standardmäßig nur auf Ebene 1 zugreifen. Wenn die Berechtigungsebene nicht definiert ist und der Benutzer versucht, in der CLI (mit Telnet) in den Aktivierungsmodus zu wechseln, zeigt der Access Point folgende Fehlermeldung an:

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

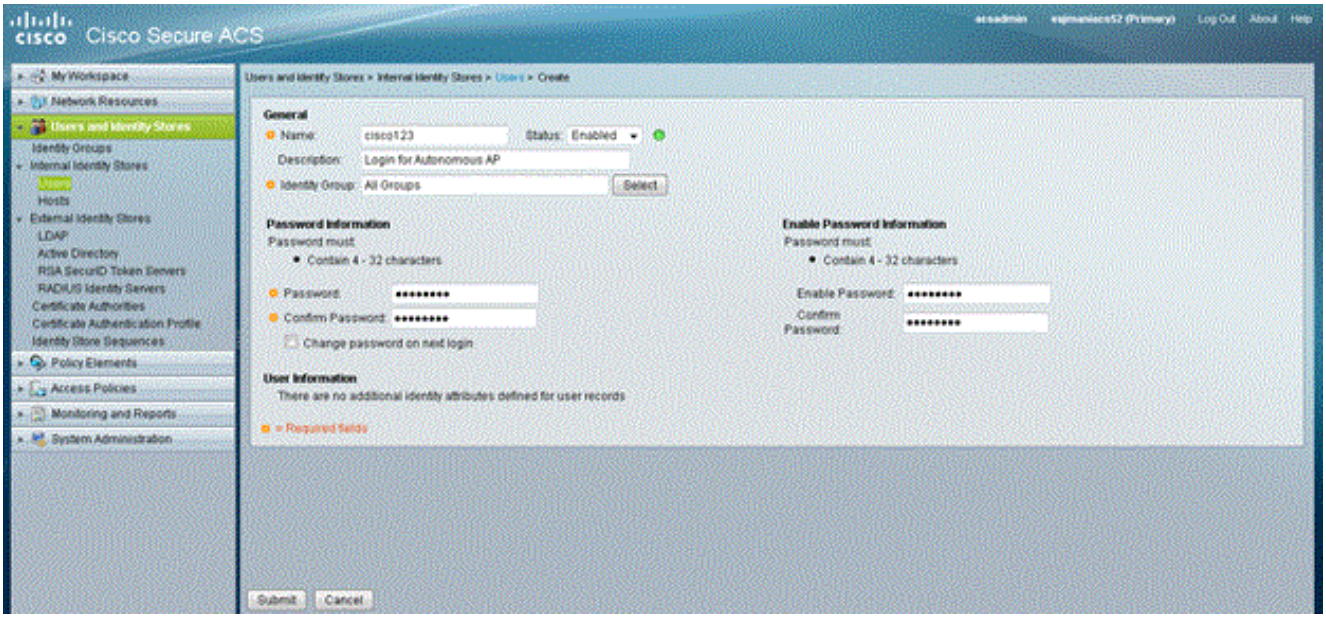
Wiederholen Sie die Schritte 2 bis 4 dieses Verfahrens, wenn Sie der TACACS+-Datenbank weitere Benutzer hinzufügen möchten. Nachdem Sie diese Schritte ausgeführt haben, kann der TACACS+-Server Benutzer validieren, die versuchen, sich beim Access Point anzumelden. Jetzt müssen Sie den Access Point für die TACACS+-Authentifizierung konfigurieren.

Konfigurieren des TACACS+-Servers für die Anmeldeauthentifizierung - Verwenden von ACS 5.2

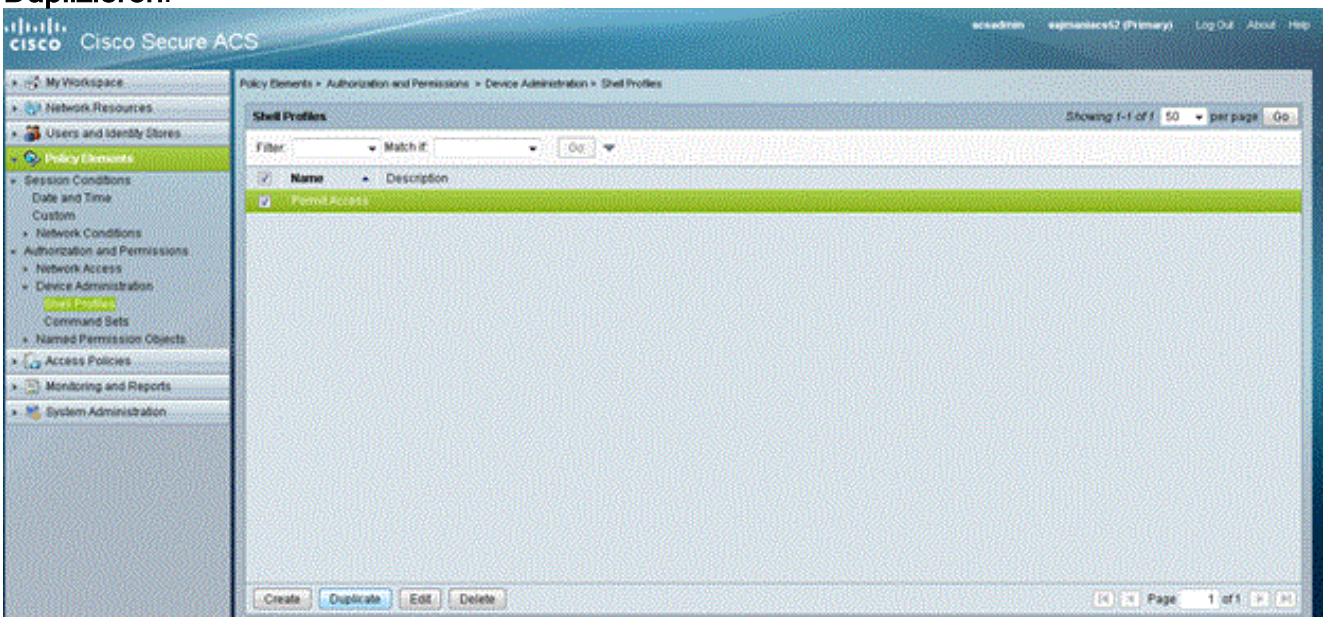
Der erste Schritt besteht darin, den Access Point dem ACS als AAA-Client hinzuzufügen und eine TACACS-Richtlinie für die Anmeldung zu erstellen.

1. Gehen Sie wie folgt vor, um den Access Point als AAA-Client hinzuzufügen:Klicken Sie in der ACS-GUI auf **Netzwerkressourcen** und dann auf **Netzwerkgeräte und AAA-Clients**.Klicken Sie unter Netzwerkgeräte auf **Erstellen**.Geben Sie den Hostnamen des Access Points in **Name ein**, und geben Sie eine Beschreibung des Access Points an.Wählen Sie den **Standort** und **Gerätetyp aus**, wenn diese Kategorien definiert sind.Da nur ein einziger Access Point konfiguriert wird, klicken Sie auf **Single IP Address**. Sie können den IP-Adressbereich für mehrere APs hinzufügen, indem Sie auf **IP Range(s)** klicken. Geben Sie dann die IP-Adresse des Access Points ein.Aktivieren Sie unter **Authentifizierungsoptionen** das **Kontrollkästchen TACACS+**, und geben Sie den **Shared Secret ein**.Hier ein Beispiel:


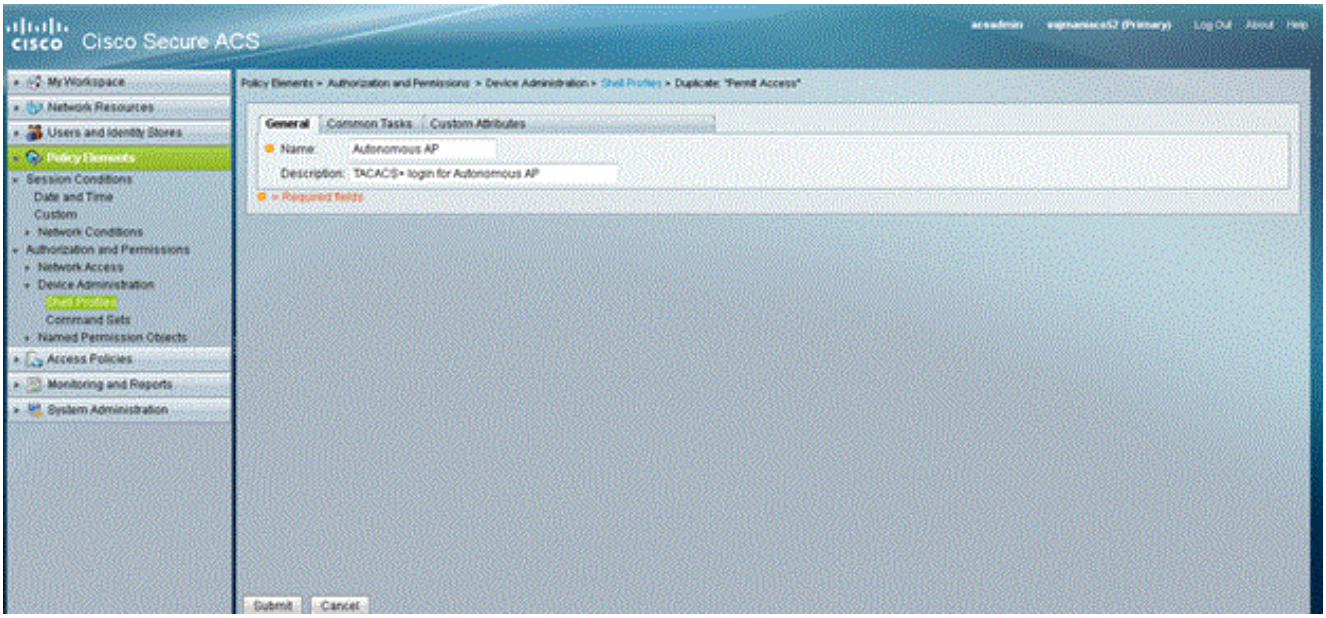
2. Im nächsten Schritt erstellen Sie einen Anmeldenamen und ein Kennwort:Klicken Sie auf **Benutzer und Identitätsdatenbanken** und anschließend auf **Benutzer**.Klicken Sie auf **Erstellen**.Geben Sie den Benutzernamen unter **Name** an, und geben Sie eine Beschreibung an.Wählen Sie die **Identitätsgruppe aus**, sofern vorhanden.Geben Sie das Kennwort unter das Textfeld **Kennwort ein**, und geben Sie es erneut unter **Kennwort bestätigen** ein.Sie können das enable-Kennwort ändern, indem Sie unter **Enable Password (Kennwort aktivieren)** ein Kennwort eingeben. Zur Bestätigung erneut eingeben.Hier ein Beispiel:



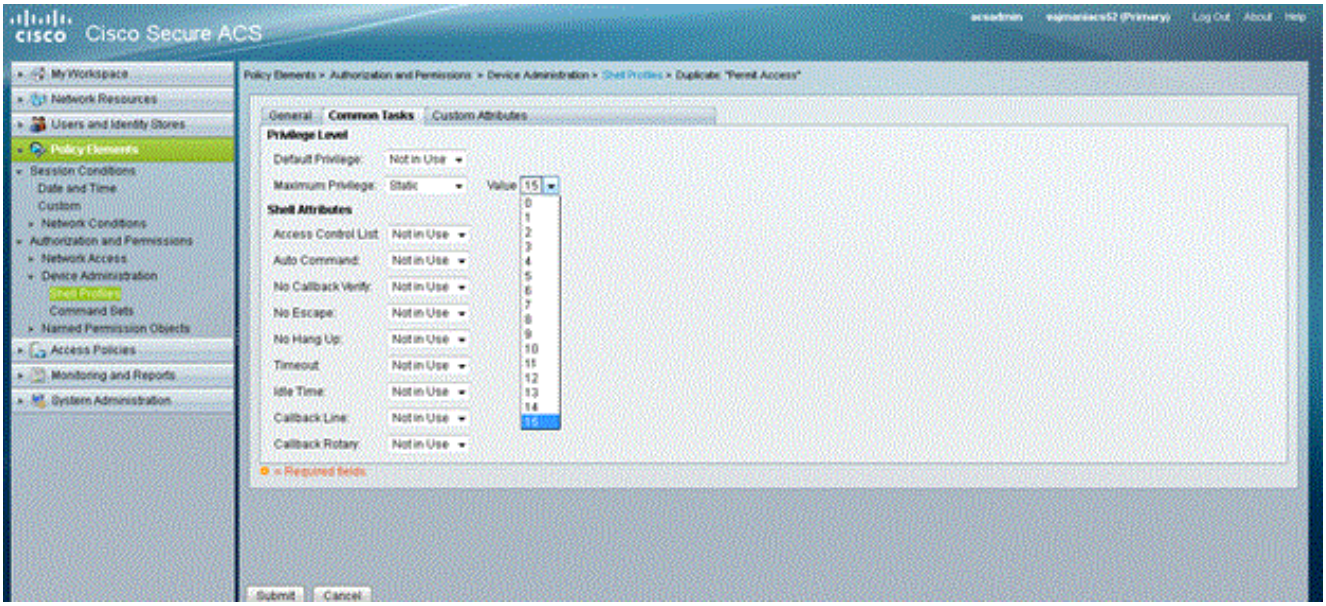
3. Führen Sie die folgenden Schritte aus, um die Berechtigungsebene zu definieren:Klicken Sie auf **Richtlinienelemente > Autorisierungen und Berechtigungen > Geräteverwaltung > Shell-Profile**.Aktivieren Sie das Kontrollkästchen **Zugriff zulassen**, und klicken Sie auf **Duplizieren**.



Geben Sie den **Namen** und die **Beschreibung ein**.

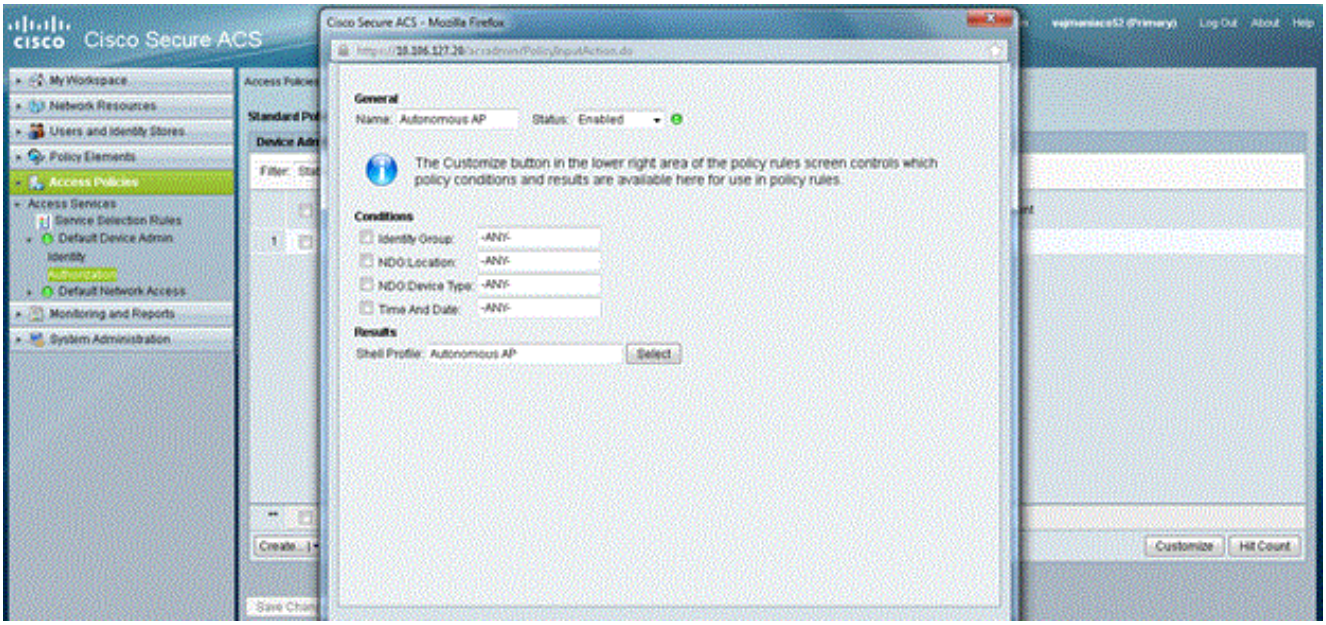


Wählen Sie die Registerkarte Allgemeine Aufgaben aus, und wählen Sie **15** für die maximale Berechtigung
aus.

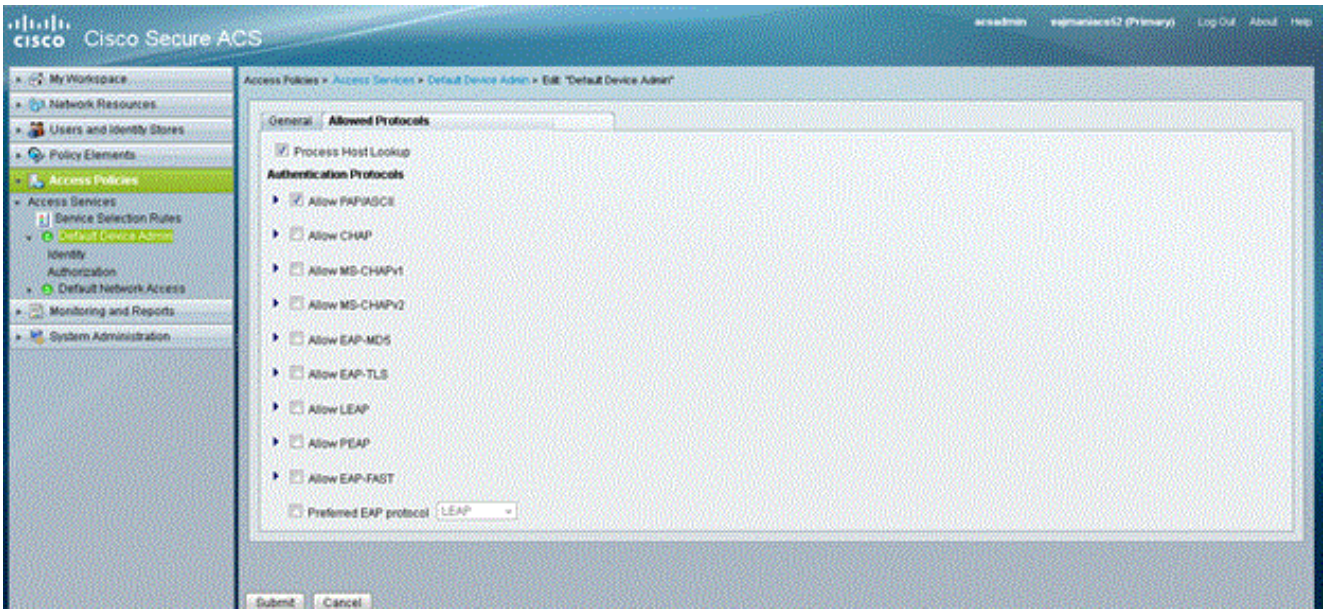


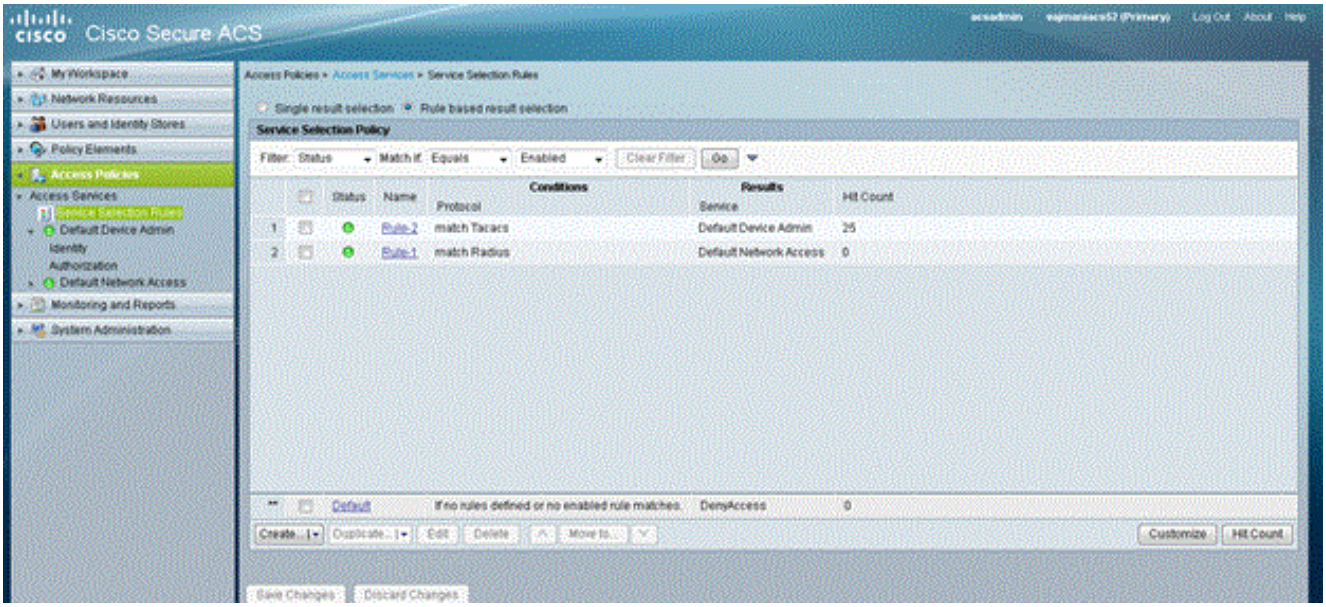
Klicken Sie auf **Senden**.

4. Gehen Sie wie folgt vor, um eine Autorisierungsrichtlinie zu erstellen:Klicken Sie auf **Zugriffsrichtlinien > Zugriffsdienste > Standardgeräteadministrator > Autorisierung**.Klicken Sie auf **Erstellen**, um eine neue Autorisierungsrichtlinie zu erstellen.Es wird ein neues Popup angezeigt, in dem die Regeln für die Autorisierungsrichtlinie erstellt werden.Wählen Sie die **Identitätsgruppe**, den **Standort** usw. für den spezifischen Benutzernamen und den AAA-Client (AP) aus, falls vorhanden.Klicken Sie für das Shell-Profil auf **Select (Auswählen)**, um das Profil zu wählen, das mit dem Autonomous Access Point erstellt
wurde.



Klicken Sie anschließend auf **Änderungen speichern**.Klicken Sie auf **Standard-Geräteadministrator** und anschließend auf **Zulässige Protokolle**.Aktivieren Sie **PAP/ASCII zulassen**, und klicken Sie dann auf **Senden**.Klicken Sie auf **Dienstauswahlregeln**, um sicherzustellen, dass eine Regel mit TACACS übereinstimmt und auf Default Device Admin (Standardgeräteadministrator)
verweist.



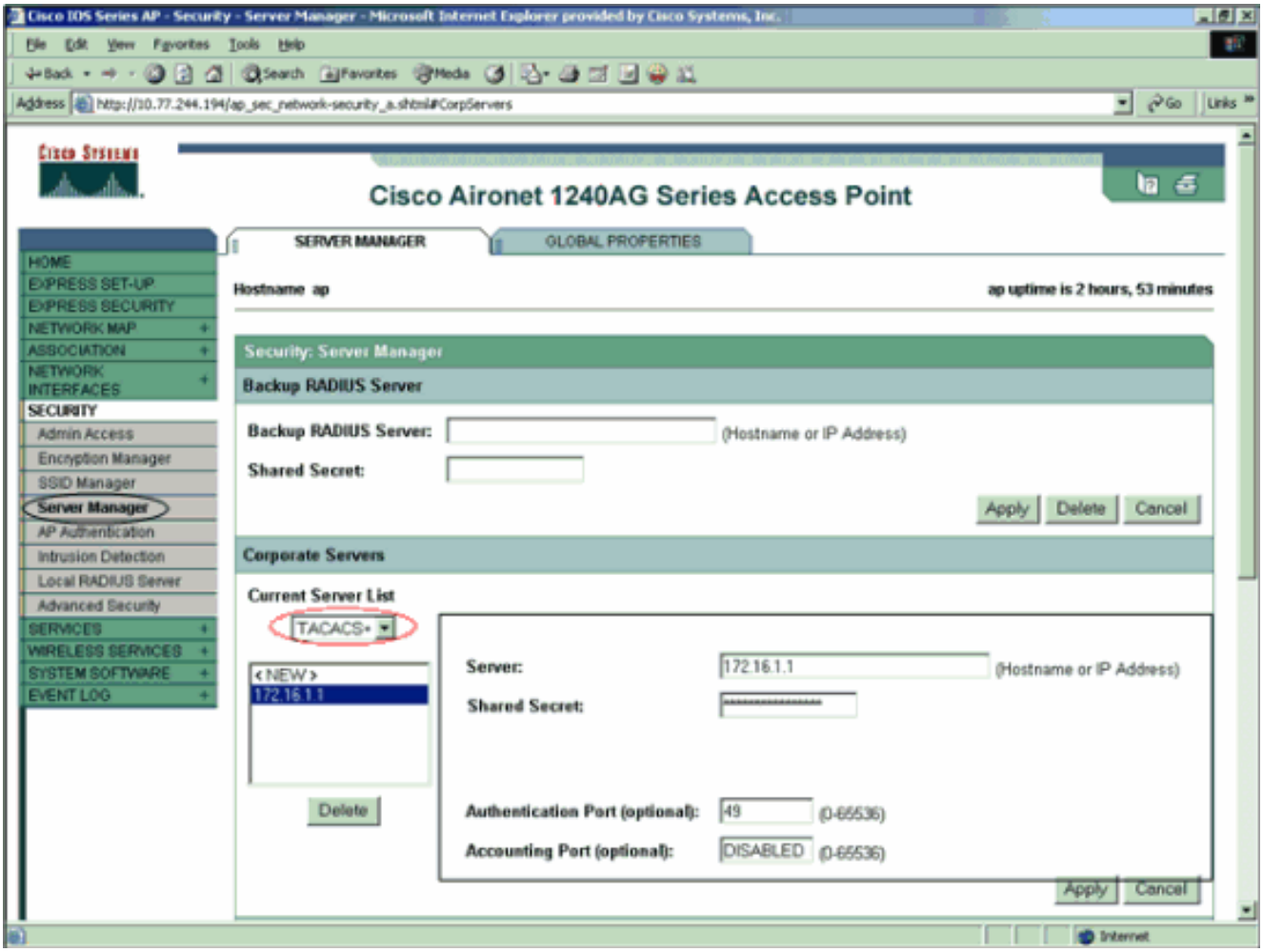


Konfigurieren des Aironet AP für die TACACS+-Authentifizierung

Sie können entweder CLI oder GUI verwenden, um die TACACS+-Funktionen des Aironet AP zu aktivieren. In diesem Abschnitt wird erläutert, wie der Access Point für die TACACS+-Anmeldeauthentifizierung mithilfe der GUI konfiguriert wird.

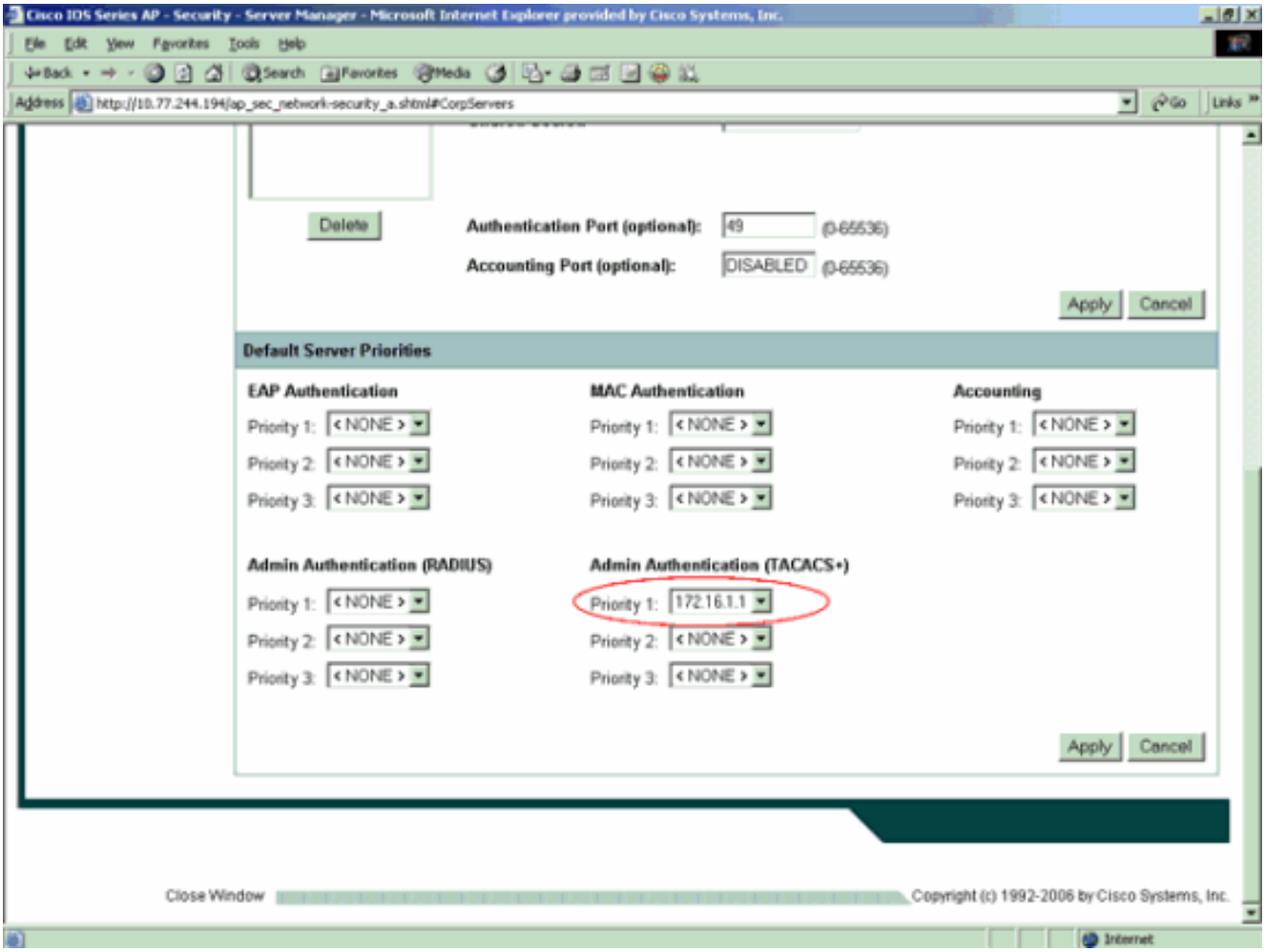
Gehen Sie wie folgt vor, um TACACS+ auf dem Access Point mithilfe der GUI zu konfigurieren:

1. Gehen Sie wie folgt vor, um die TACACS+-Serverparameter zu definieren:Wählen Sie in der AP-GUI **Security > Server Manager aus**.Sicherheit: Das Fenster Server Manager wird angezeigt.Wählen Sie im Bereich Firmenserver im Dropdown-Menü Aktuelle Serverliste die Option **TACACS+** aus.Geben Sie in diesem Bereich die IP-Adresse, den gemeinsamen geheimen Schlüssel und die Authentifizierungsportnummer des TACACS+-Servers ein.Klicken Sie auf **Übernehmen**.Hier ein
   Beispiel:

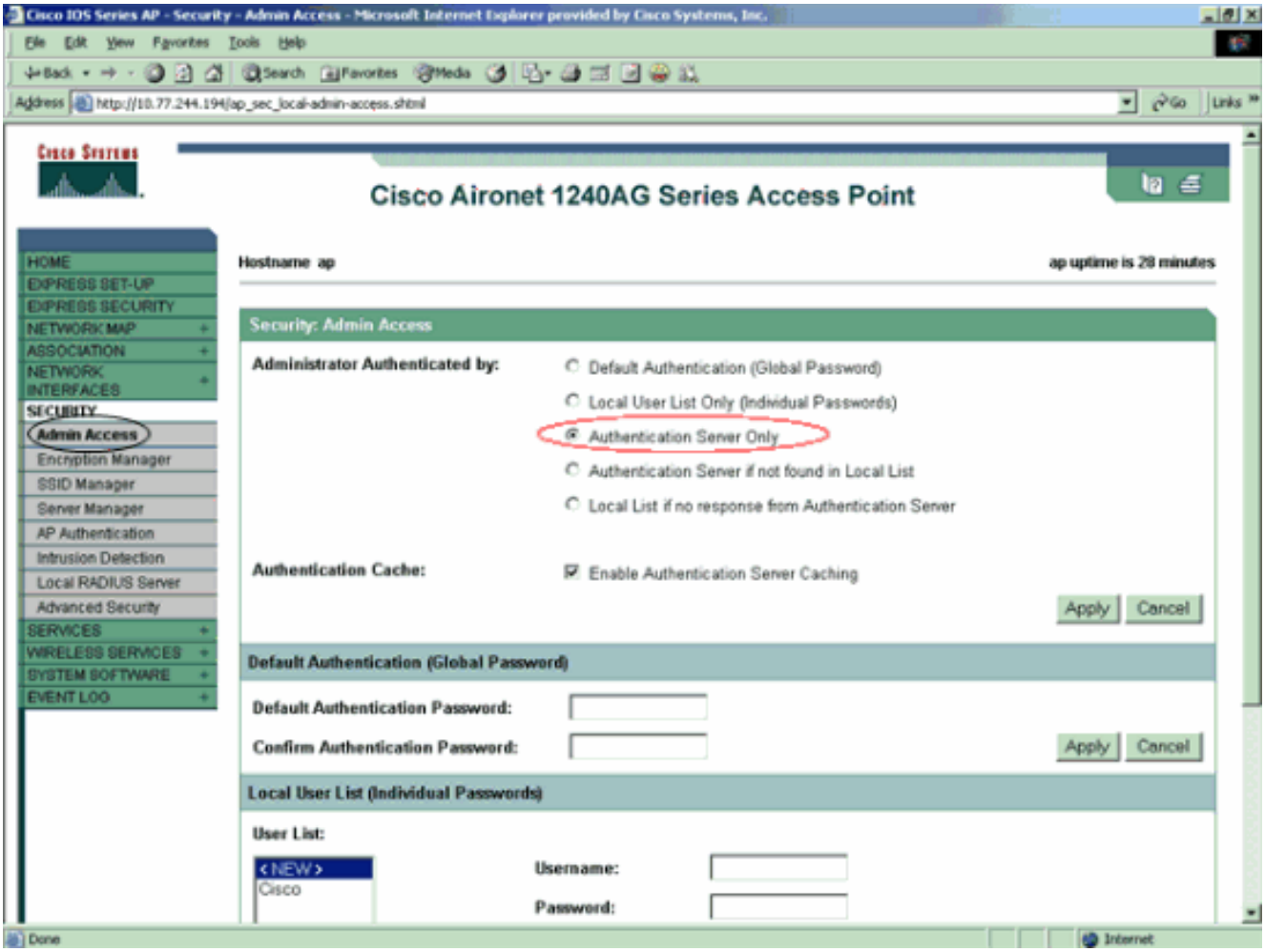


Hinweis: TACACS+ verwendet standardmäßig den TCP-Port 49.**Hinweis:** Der gemeinsam verwendete geheime Schlüssel, den Sie auf dem ACS und dem Access Point konfigurieren, muss übereinstimmen.

2. Wählen Sie **Standardserverprioritäten > Admin Authentication (TACACS+)**, wählen Sie im Dropdown-Menü Priority 1 (Priorität 1) die von Ihnen konfigurierte TACACS+-Server-IP-Adresse aus, und klicken Sie auf **Apply**.Hier ein
   Beispiel:



3. Wählen Sie **Security > Admin Access (Sicherheit > Administratorzugriff) aus**, und wählen Sie als Administrator Authenticated by: (Administrator Authenticated by:) die Option **Authentication Server Only (Nur Authentifizierungsserver)** aus, und klicken Sie auf **Apply (Übernehmen)**.Diese Auswahl stellt sicher, dass Benutzer, die sich am Access Point anmelden, von einem Authentifizierungsserver authentifiziert werden.Hier ein Beispiel:



Dies ist die CLI-Konfiguration für das Konfigurationsbeispiel:

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
BVI1 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 BVI1 ! 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
```

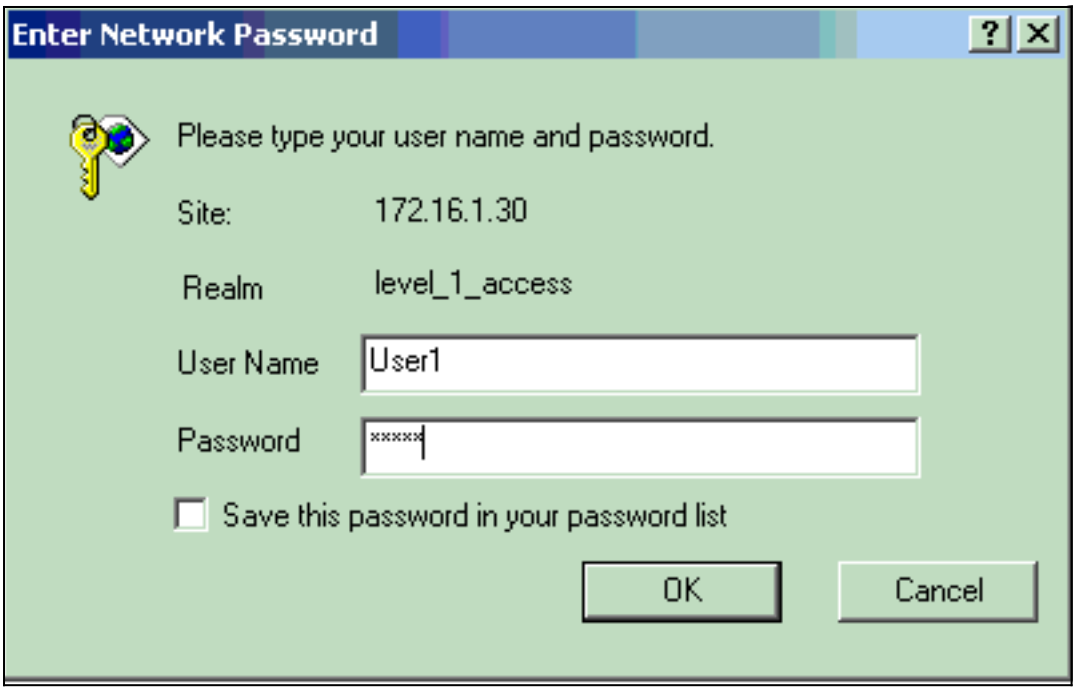
Hinweis: Damit alle Befehle in dieser Konfiguration ordnungsgemäß funktionieren, müssen Sie über Cisco IOS Software Release 12.3(7)JA oder höher verfügen. In einer früheren Version der Cisco IOS-Software sind möglicherweise nicht alle diese Befehle verfügbar.

Überprüfen

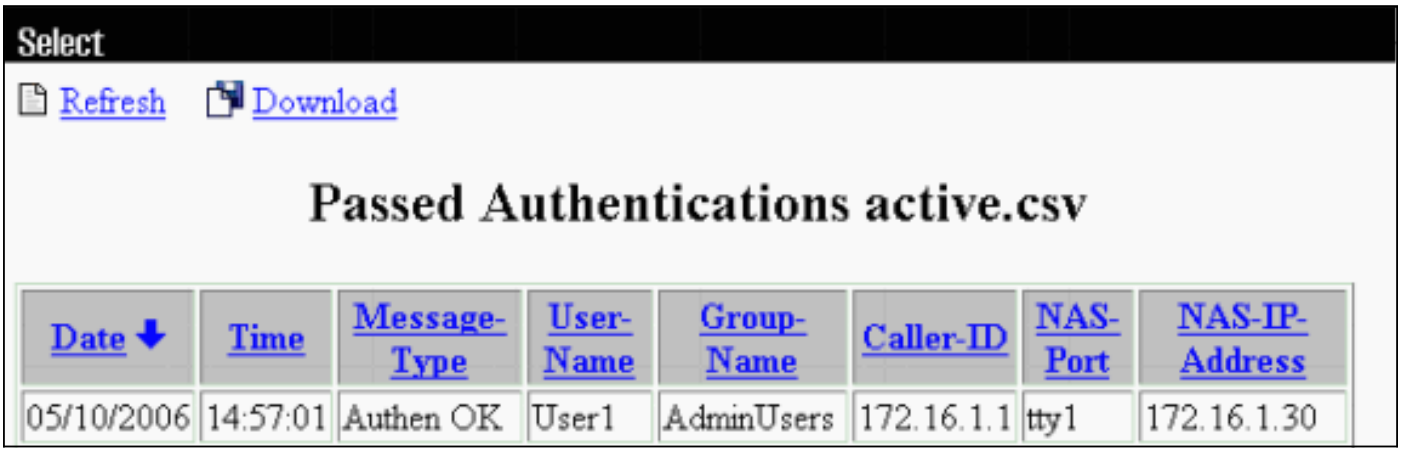
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Um die Konfiguration zu überprüfen, versuchen Sie, sich mit der GUI oder der CLI am Access Point anzumelden. Wenn Sie versuchen, auf den Access Point zuzugreifen, werden Sie vom Access Point aufgefordert, einen Benutzernamen und ein Kennwort einzugeben.



Wenn Sie die Benutzeranmeldeinformationen angeben, leitet der Access Point die Anmeldeinformationen an den TACACS+-Server weiter. Der TACACS+-Server validiert die Anmeldeinformationen anhand der in seiner Datenbank verfügbaren Informationen und ermöglicht nach erfolgreicher Authentifizierung Zugriff auf den Access Point. Sie können im ACS **Reports and Activity > Passed Authentication** (Berichte und Aktivität > Passed Authentication) und den Bericht Passed Authentication (Passed Authentication) verwenden, um die erfolgreiche Authentifizierung dieses Benutzers zu überprüfen. Hier ein Beispiel:



Sie können auch den Befehl **show tacacs** verwenden, um die richtige Konfiguration des TACACS+-Servers zu überprüfen. Hier ein Beispiel:

```
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
```

Überprüfung für ACS 5.2

Sie können die fehlgeschlagenen/vergebenen Anmeldeversuche für Anmeldeberechtigungen mit ACS 5.2 überprüfen:

1. Klicken Sie auf **Überwachung und Berichte > Überwachung und Berichtsanzeige starten**.Mit dem Dashboard wird ein neues Popup-Fenster geöffnet.
2. Klicken Sie auf **Authentications-TACACS-Today**. Hier werden die Details der fehlgeschlagenen/vergebenen Versuche angezeigt.

Fehlerbehebung

Sie können diese Debugbefehle auf dem Access Point verwenden, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen:

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug tacacs events** - Dieser Befehl zeigt die Ereignissequenz an, die während der TACACS-Authentifizierung vorkommt. Hier ein Beispiel für die Ausgabe dieses Befehls:

```
*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**: Verwenden Sie diesen Befehl, um HTTP-Authentifizierungsprobleme zu beheben. Der Befehl zeigt die Authentifizierungsmethode, mit

der der Router versucht hat, und authentifizierungsspezifische Statusmeldungen an.
- **debug aaa authentication**: Dieser Befehl zeigt Informationen zur AAA TACACS+-Authentifizierung an.

Wenn der Benutzer einen Benutzernamen eingibt, der auf dem TACACS+-Server nicht vorhanden ist, schlägt die Authentifizierung fehl. Im Folgenden finden Sie die Ausgabe des Befehls **debug tacacs zur Authentifizierung** für eine fehlgeschlagene Authentifizierung:

```
*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)
```

Sie können **Berichte und Aktivität > Fehlgeschlagene Authentifizierung** auswählen, um den fehlgeschlagenen Authentifizierungsversuch für den ACS anzuzeigen. Hier ein Beispiel:

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	..	..	..

Wenn Sie eine Cisco IOS Software-Version auf dem Access Point verwenden, die älter ist als die Cisco IOS-Softwareversion 12.3(7)JA, können Sie bei jedem Versuch, sich mit HTTP am Access Point anzumelden, einen Fehler auslösen. Die Cisco Bug-ID lautet CSCeb52431 (nur registrierte Kunden).

Die HTTP/AAA-Implementierung der Cisco IOS-Software erfordert die unabhängige Authentifizierung jeder separaten HTTP-Verbindung. Die drahtlose Cisco IOS Software-GUI umfasst die Verweise auf viele Dutzende separater Dateien auf einer Webseite (z. B. Javascript und GIF). Wenn Sie also eine Seite in die Wireless-Benutzeroberfläche der Cisco IOS Software laden, können Dutzende und Dutzende von separaten Authentifizierungs-/Autorisierungsanfragen auf den AAA-Server zugreifen.

Verwenden Sie für die HTTP-Authentifizierung RADIUS oder die lokale Authentifizierung. Der RADIUS-Server ist weiterhin mehreren Authentifizierungsanforderungen unterworfen. RADIUS ist jedoch skalierbarer als TACACS+ und bietet daher wahrscheinlich geringere Leistungseinbußen.

Wenn Sie TACACS+ verwenden müssen und über einen Cisco ACS verfügen, verwenden Sie das **Schlüsselwort Single-connection** mit dem Befehl **tacacs-server**. Die Verwendung dieses Schlüsselworts mit dem Befehl erspart den ACS-Großteil des TCP-Verbindungs-Setup/Teardown-Overheads und verringert wahrscheinlich die Last auf dem Server in einem gewissen Maße.

Für die Cisco IOS Software Releases 12.3(7) JA und höher auf dem AP enthält die Software einen Fix. Der Rest dieses Abschnitts beschreibt die Behebung.

Verwenden Sie die Funktion für den AAA-Authentifizierungscache, um die vom TACACS+-Server zurückgegebenen Informationen im Cache zu speichern. Der Authentifizierungs-Cache und die Profilfunktion ermöglichen dem Access Point, die Authentifizierungs-/Autorisierungsantworten eines Benutzers im Cache zu speichern, sodass nachfolgende Authentifizierungs-/Autorisierungsanforderungen nicht an den AAA-Server gesendet werden müssen. Verwenden Sie die folgenden Befehle, um diese Funktion mit der CLI zu aktivieren:

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

Weitere Informationen zu diesem Feature und den Befehlen finden Sie im Abschnitt *Konfigurieren des Authentifizierungscaches und* des *Profils* unter Verwalten des Access Points.

Um diese Funktion in der GUI zu aktivieren, wählen Sie **Security > Admin Access (Sicherheit > Admin-Zugriff) aus,** und aktivieren Sie das Kontrollkästchen **Enable Authentication Server Caching (Authentifizierungsserver-Caching aktivieren)**. Da in diesem Dokument die Cisco IOS Softwareversion 12.3(7)JA verwendet wird, wird das Fix wie die Konfigurationen veranschaulicht.

Zugehörige Informationen

- Konfigurieren von RADIUS- und TACACS+-Servern
- Problemhinweis: IOS Access Point Bombards TACACS+-Server mit Anforderungen
- EAP-Authentifizierung mit RADIUS-Server
- Wireless-Produktunterstützung
- Technischer Support und Dokumentation - Cisco Systems