GUI 컨피그레이션 예를 사용하여 로그인 인증을 위한 Aironet 액세스 포인트의 TACACS+

목차

소개

이 문서에서는 TACACS+ 서버를 사용하여 로그인 인증을 수행하기 위해 Cisco Aironet Access Point(AP)에서 TACACS+(TACACS Plus) 서비스를 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Aironet AP에서 기본 매개변수를 구성하는 방법에 대한 지식
- Cisco ACS(Secure Access Control Server)와 같은 TACACS+ 서버를 구성하는 방법에 대한 지식
- TACACS+ 개념 지식

TACACS+의 작동 방식에 대한 자세한 내용은 RADIUS 및 TACACS+ 서버 구성의 *Understanding TACACS+* 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Aironet Cisco Aironet 1240/1140 Series 액세스 포인트
- 소프트웨어 버전 4.1을 실행하는 ACS
- 소프트웨어 버전 5.2를 실행하는 ACS

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

이 섹션에서는 TACACS+ 기반 로그인 인증을 위해 Aironet AP와 TACACS+ 서버(ACS)를 구성하는 방법에 대해 설명합니다.

이 컨피그레이션 예에서는 다음 매개변수를 사용합니다.

- ACS의 IP 주소—172.16.1.1/255.255.0.0
- AP의 IP 주소—172.16.1.30/255.255.0.0
- AP 및 TACACS+ 서버에서 사용되는 공유 비밀 키 - **예**

다음은 이 예에서는 ACS에서 구성하는 사용자의 자격 증명입니다.

- 사용자 이름 - **User1**
- 비밀번호 - **Cisco**
- Group(그룹) - **AdminUsers**

웹 인터페이스를 통해 또는 CLI(Command-Line Interface)를 통해 AP에 연결하려는 사용자를 검증하려면 TACACS+ 기능을 구성해야 합니다. 이 구성을 수행하려면 다음 작업을 수행해야 합니다.

1. 로그인 인증을 위해 TACACS+ 서버를 구성합니다.
2. TACACS+ 인증을 위한 Aironet AP를 구성합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

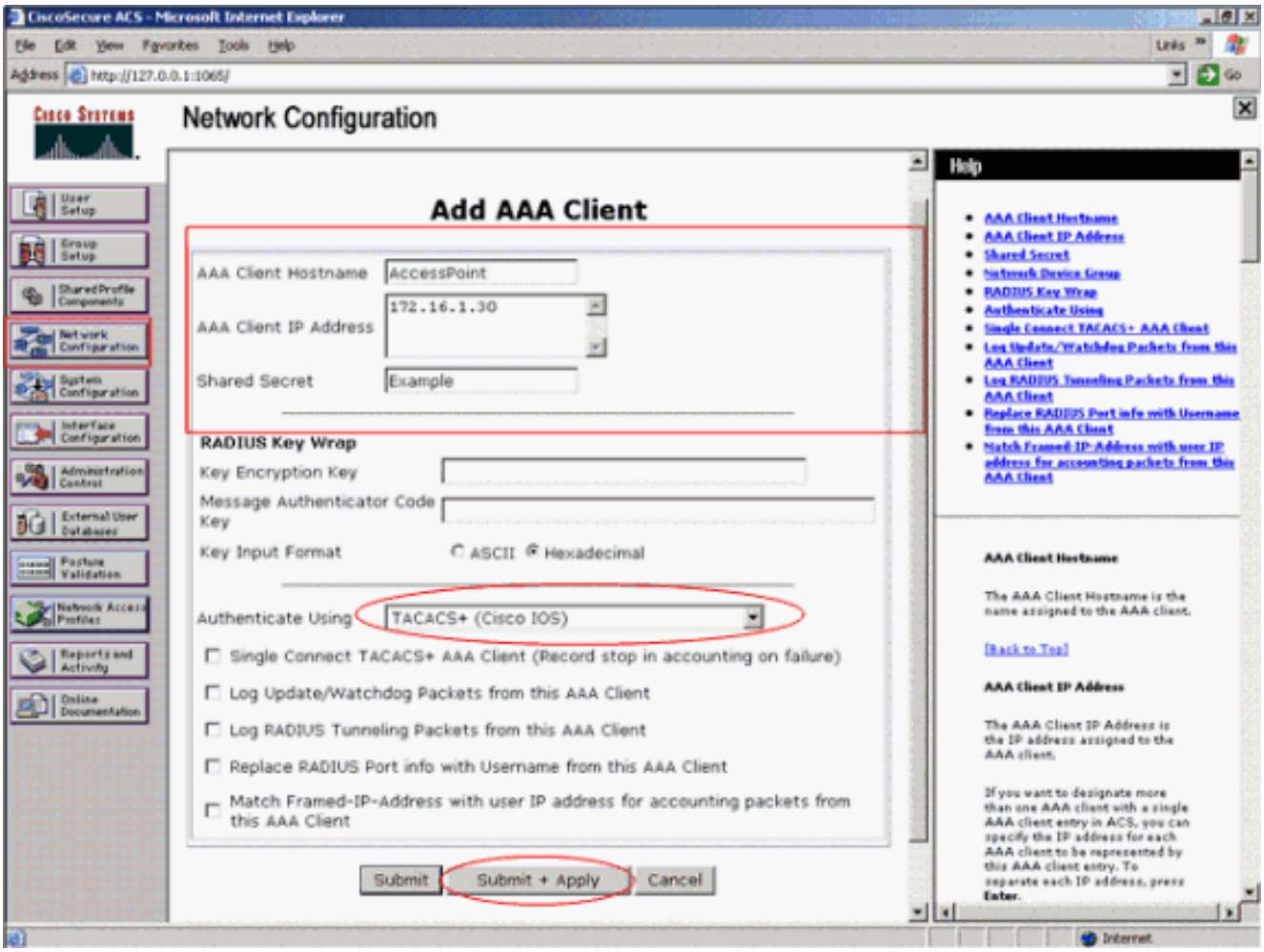
이 문서에서는 다음 네트워크 설정을 사용합니다.

로그인 인증을 위해 TACACS+ 서버 구성 - ACS 4.1 사용

첫 번째 단계는 AP에 액세스하려는 사용자를 검증하기 위해 TACACS+ 데몬을 설정하는 것입니다. TACACS+ 인증을 위한 ACS를 설정하고 사용자 데이터베이스를 생성해야 합니다. 모든 TACACS+ 서버를 사용할 수 있습니다. 이 예에서는 ACS를 TACACS+ 서버로 사용합니다. 다음 단계를 완료하십시오.

1. AP를 AAA(Authentication, Authorization, and Accounting) 클라이언트로 추가하려면 다음 단계를 완료합니다.ACS GUI에서 **Network Configuration** 탭을 클릭합니다.AAA Clients(AAA 클라이언트)에서 Add **Entry(항목 추가)를** 클릭합니다.Add AAA Client(AAA 클라이언트 추가) 창에서 AP 호스트 이름, AP의 IP 주소 및 공유 비밀 키를 입력합니다.이 공유 비밀 키는 AP에서 구성한 공유 비밀 키와 동일해야 합니다.Authenticate Using 드롭다운 메뉴에서 TACACS**+(Cisco IOS)를** 선택합니다.구성을 **저장하려면 Submit + Restart**를 클릭합니다.예를 들면 다음과 같습니다

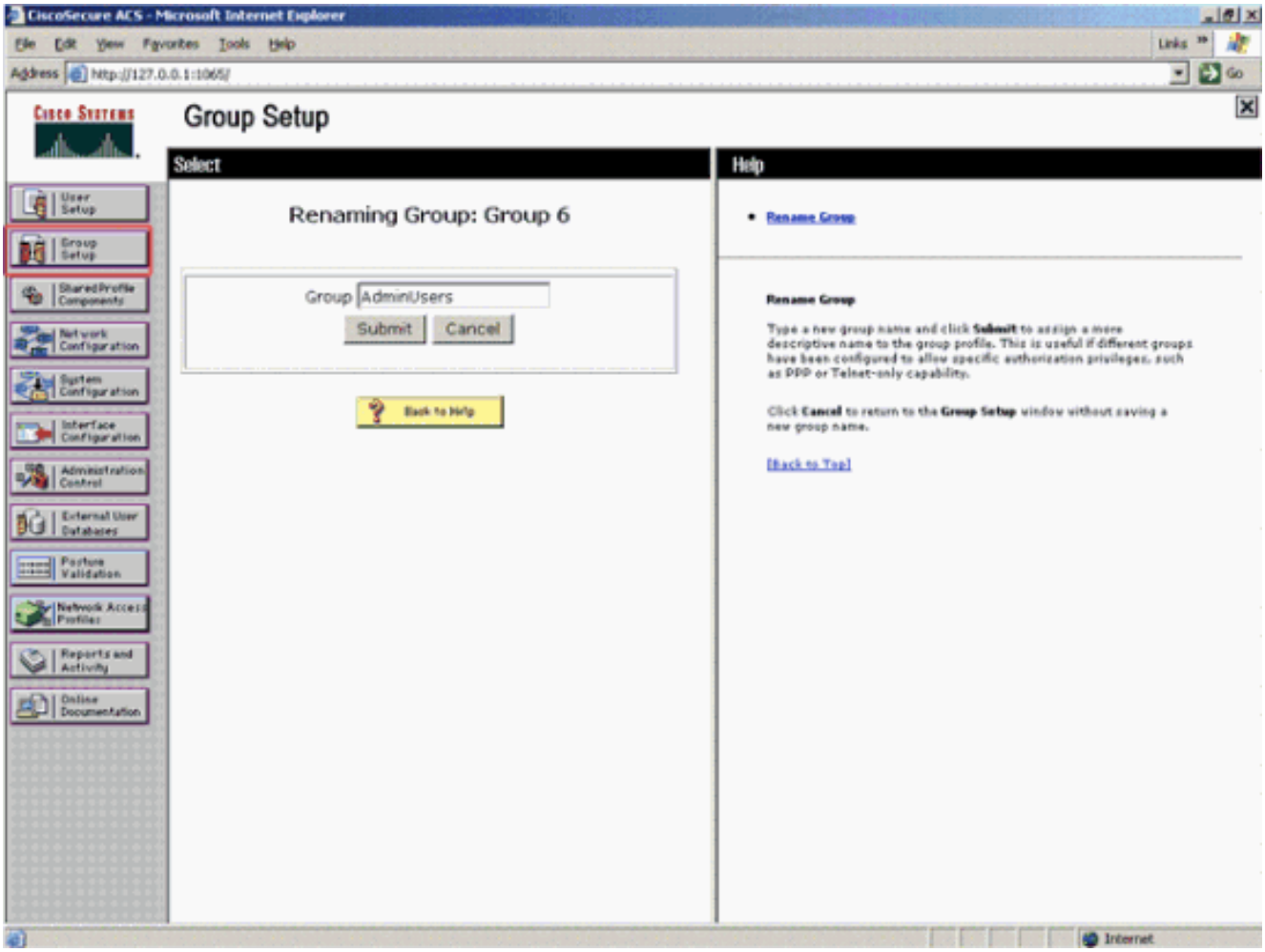
.



이 예에서는 다음을 사용합니다.AAA 클라이언트 호스트 이름 **액세스 포인트**주소 **172.16.1.30/16**를 AAA 클라이언트 IP 주소로공유 비밀 키 **예**

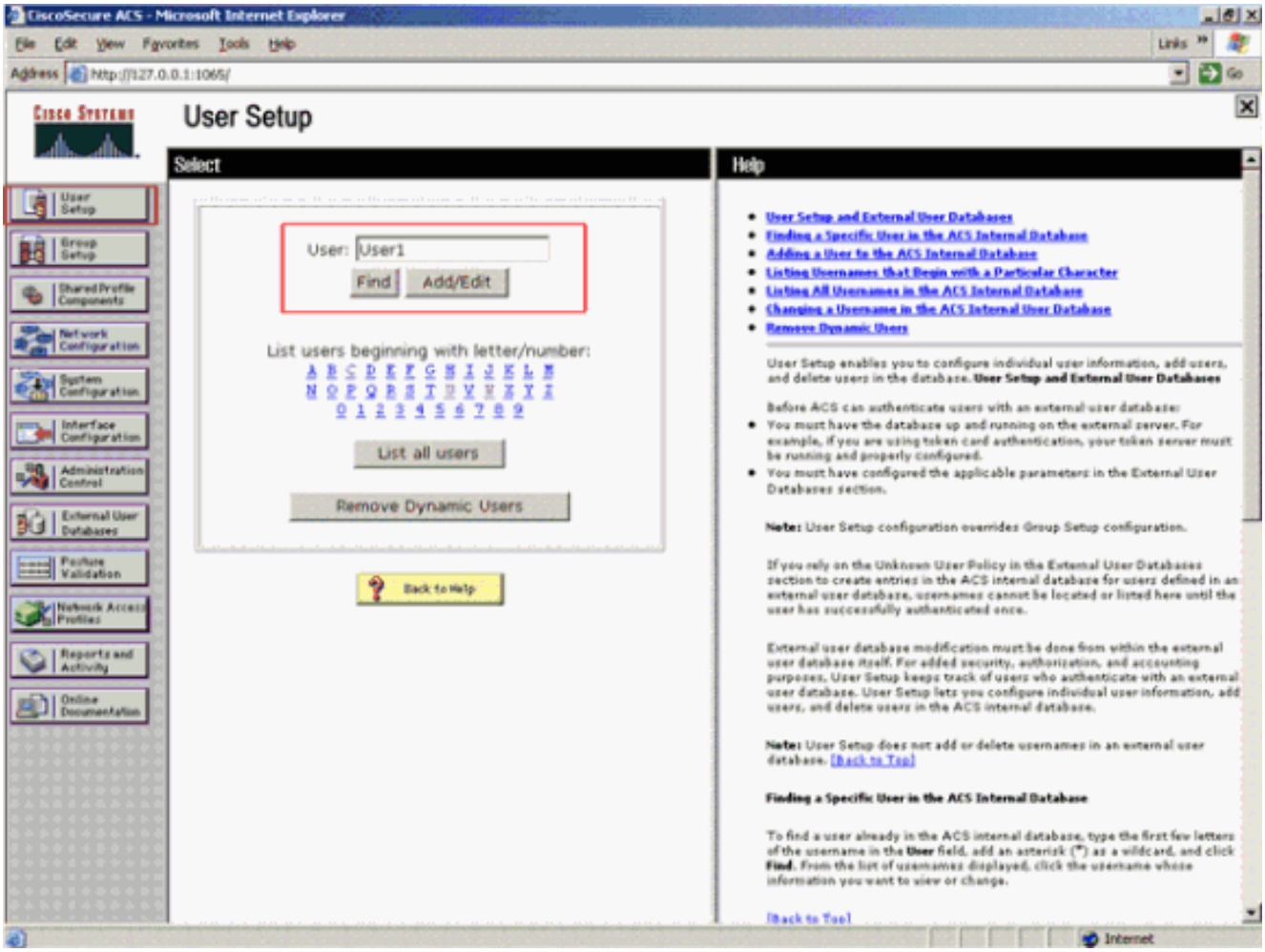
2. 모든 관리(admin) 사용자를 포함하는 그룹을 생성하려면 다음 단계를 완료합니다.왼쪽 메뉴에서 그룹 설정(Group Setup)을 클릭합니다.새 창이 나타납니다.Group Setup(그룹 설정) 창의 드롭다운 메뉴에서 구성할 그룹을 선택하고 Rename Group(그룹 이름 **바꾸기)을** 클릭합니다.이 예에서는 드롭다운 메뉴에서 그룹 6을 선택하고 그룹 AdminUsers의 이름을 변경합니다.Submit(제출**)을 클릭합니다**.예를 들면 다음과 같습니다

.



3. TACACS+ 데이터베이스에 사용자를 추가하려면 다음 단계를 완료합니다.**사용자 설정** 탭을 클릭합니다.새 사용자를 생성하려면 User 필드에 사용자 이름을 입력하고 Add/**Edit**를 클릭합니다.다음은 **User1**을 생성하는 예입니다

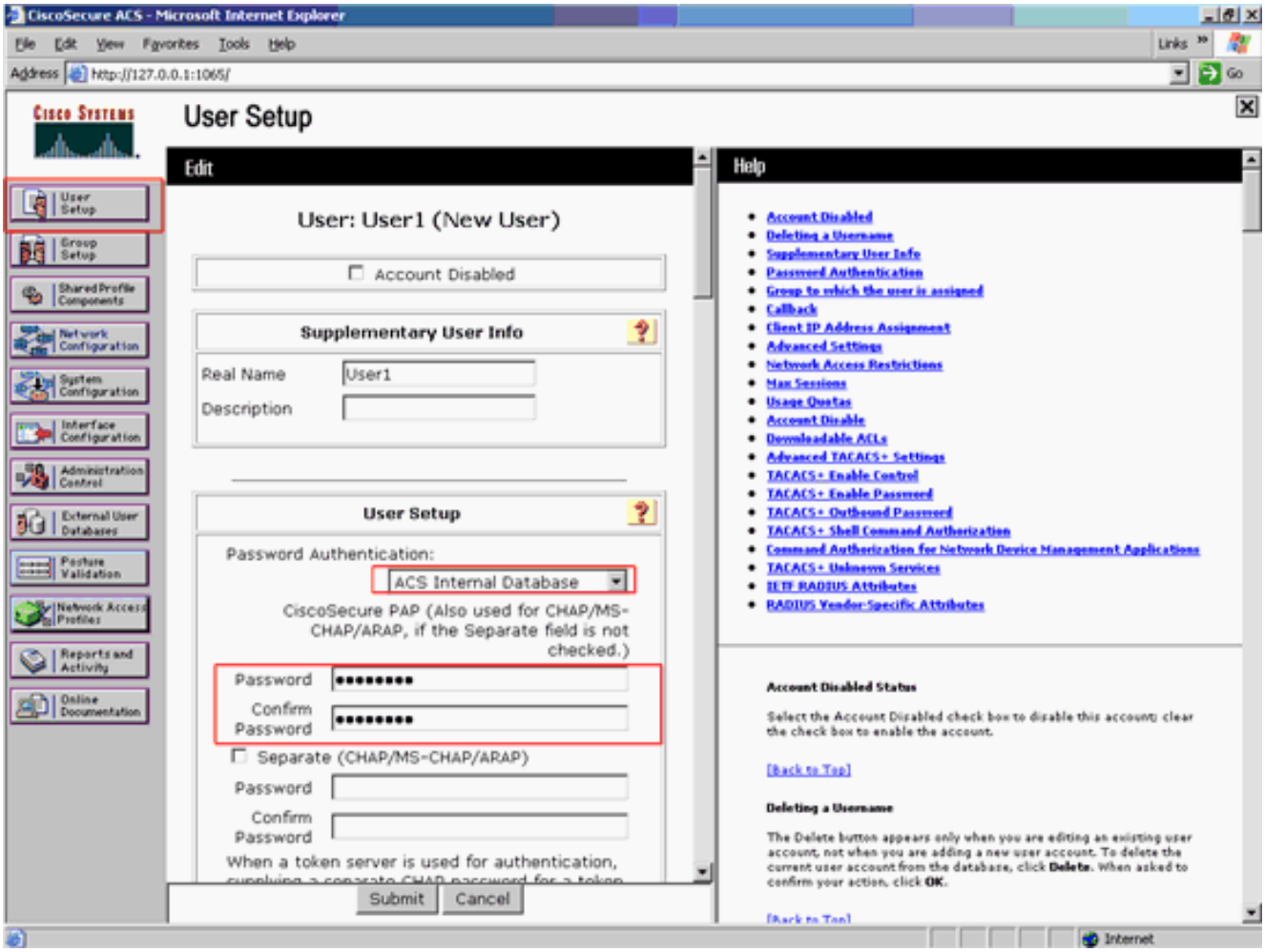
.



Add/Edit를 클릭하면 이 사용자에 대한 Add/Edit 창이 나타납니다.

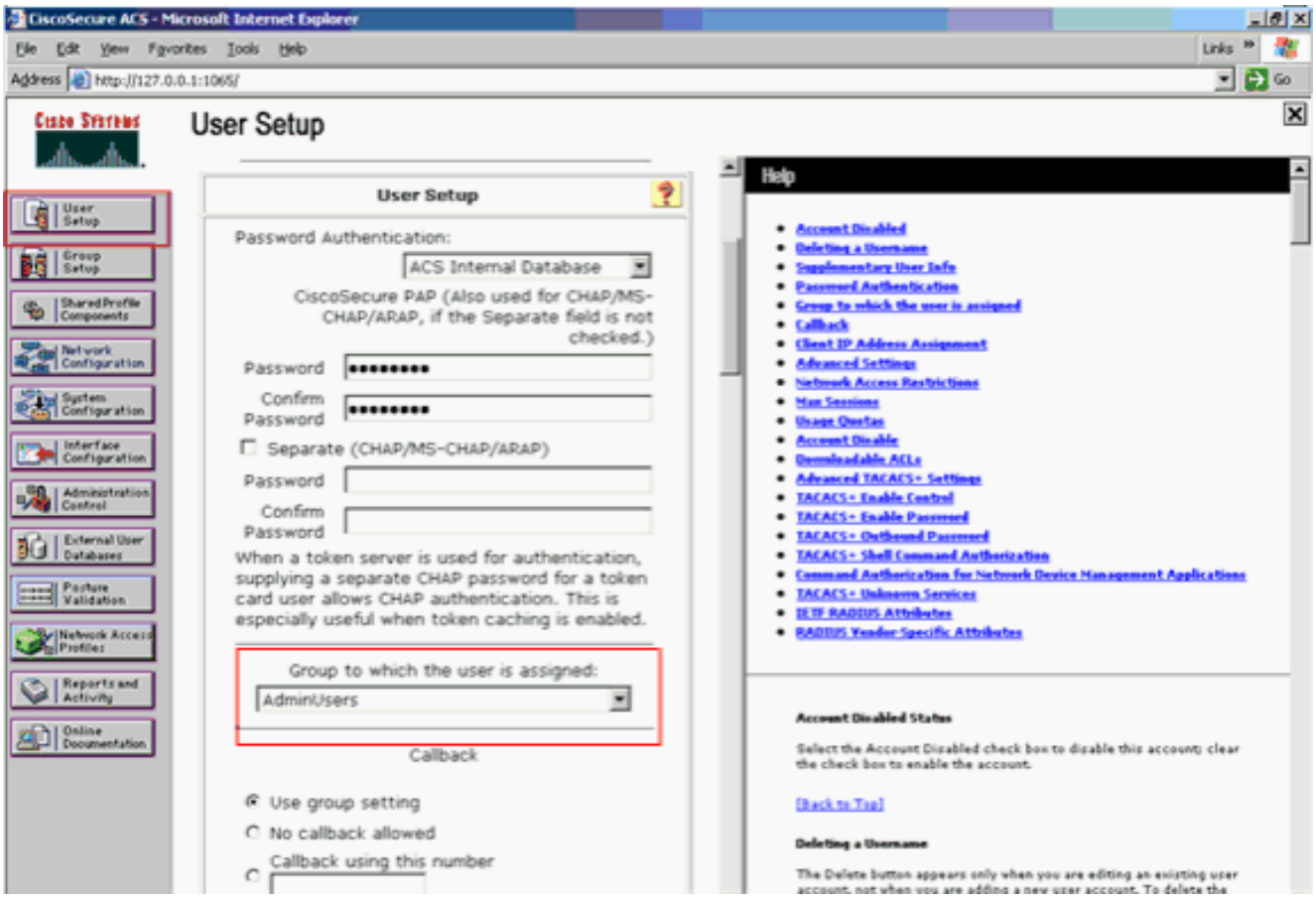
4. 이 사용자에 해당하는 자격 증명을 입력하고 **Submit**(제출)을 클릭하여 구성을 저장합니다.입력할 수 있는 자격 증명은 다음과 같습니다.추가 사용자 정보사용자 설정사용자가 할당된 그룹입니다.예를 들면 다음과 같습니다

.



이 예에서는 사용자 User1을 그룹 AdminUsers에 추가합니다

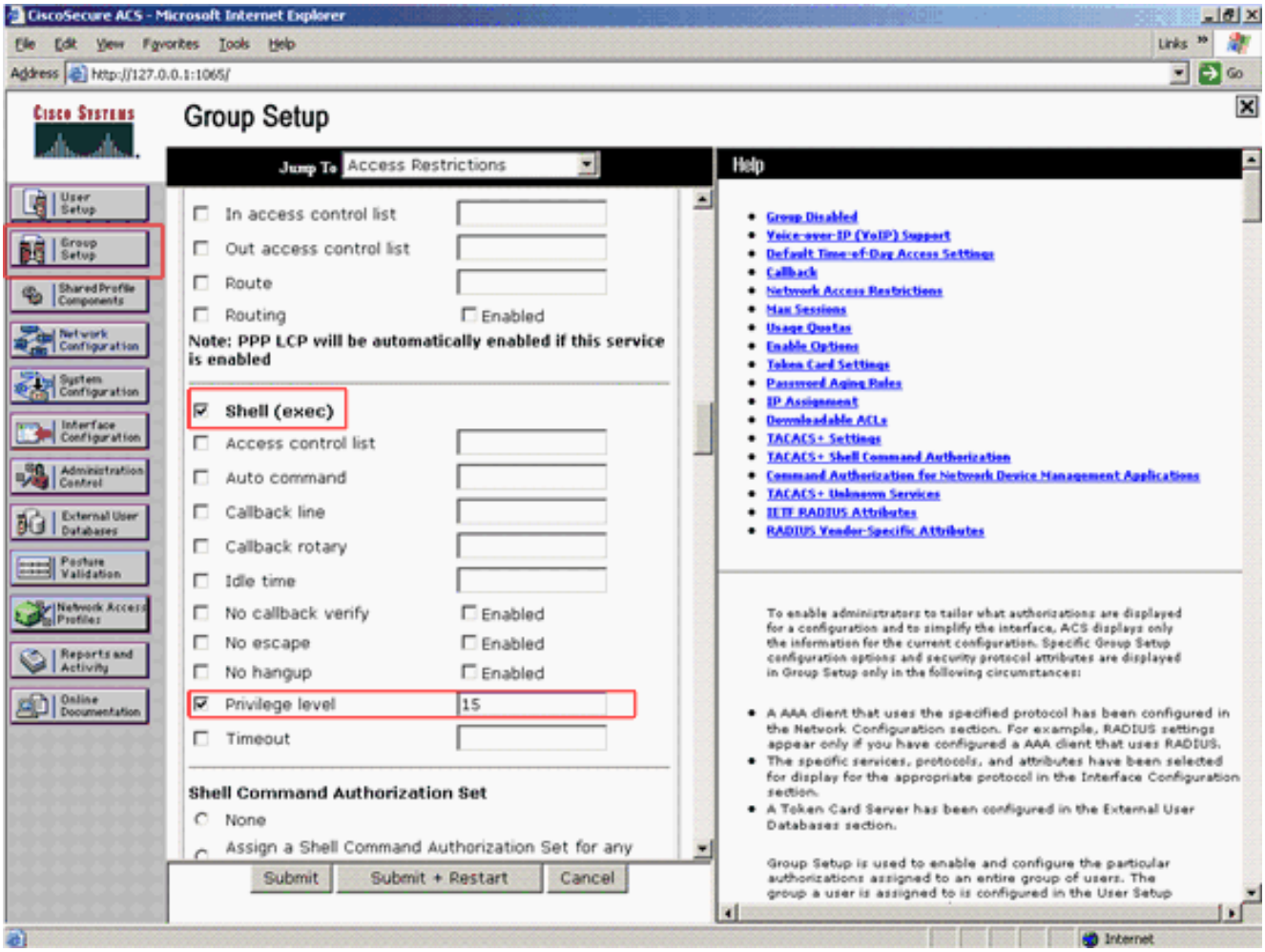
.



참고: 특정 그룹을 생성하지 않으면 사용자가 기본 그룹에 할당됩니다.

5. 권한 레벨을 정의하려면 다음 단계를 완료합니다.**그룹 설정** 탭을 클릭합니다.이전에 이 사용자에게 할당한 그룹을 선택하고 Edit **Settings**(설정 편집)를 클릭합니다.이 예에서는 AdminUsers 그룹을 사용합니다.TACACS+ Settings(TACACS+ 설정)에서 **Shell(exec)** 확인란을 선택하고 **Privilege level(권한 수준)** 확인란(값 15)을 선택합니다.Submit **+Restart를 클릭합니다**

.



주: 레벨 15로 액세스할 수 있으려면 GUI 및 텔넷에 대해 권한 레벨 15를 정의해야 합니다. 그렇지 않으면 기본적으로 사용자는 레벨 1로만 액세스할 수 있습니다. 권한 레벨이 정의되어 있지 않고 사용자가 CLI에서 enable 모드를 시작하려고 하면(텔넷 사용) AP에 다음 오류 메시지가 표시됩니다.

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

TACACS+ 데이터베이스에 사용자를 더 추가하려면 이 절차의 2~4단계를 반복합니다. 이러한 단계를 완료하면 TACACS+ 서버에서 AP에 로그인을 시도하는 사용자를 검증할 준비가 되었습니다. 이제 TACACS+ 인증을 위한 AP를 구성해야 합니다.

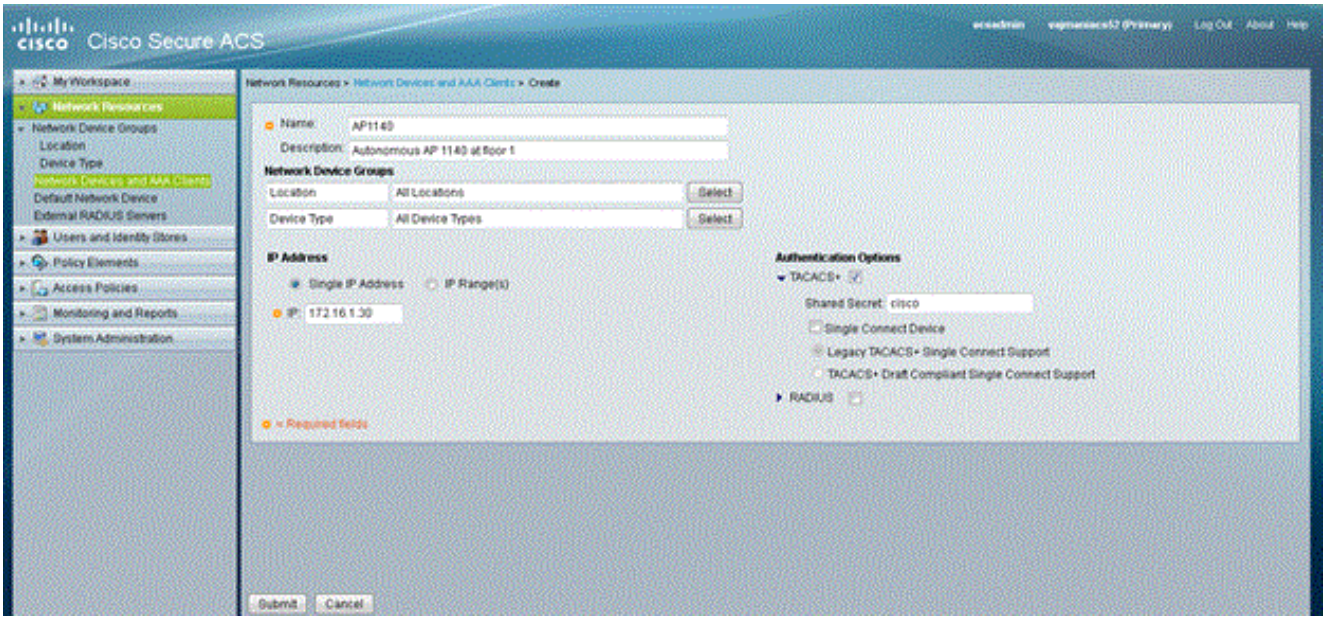
로그인 인증을 위해 TACACS+ 서버 구성 - ACS 5.2 사용

첫 번째 단계는 ACS에서 AP를 AAA 클라이언트로 추가하고 로그인에 대한 TACACS 정책을 생성하는 것입니다.

1. AP를 AAA 클라이언트로 추가하려면 다음 단계를 완료합니다.ACS GUI에서 **Network Resources(네트워크 리소스)**를 클릭한 다음 Network Devices and **AAA Clients(네트워크 디바이스 및 AAA 클라이언트)를 클릭합니다**.Network Devices(네트워크 디바이스)에서 Create(**생**

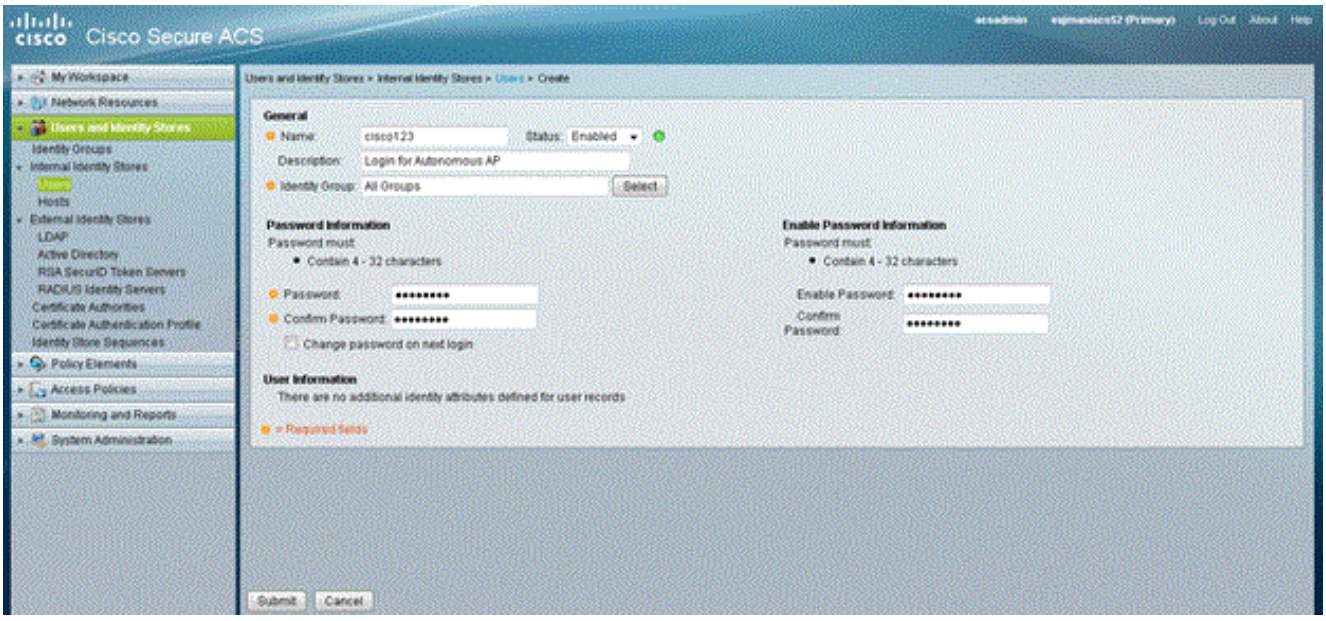
성)를 클릭합니다.AP의 호스트 이름을 Name(이름)에 입력하고 AP에 대한 설명을 입력합니다.이러한 카테고리가 정의된 경우 Location 및 Device Type을 선택합니다.단일 AP만 구성되고 있으므로 Single IP Address(단일 IP 주소)를 클릭합니다. IP Range(s)를 클릭하여 여러 AP에 대한 IP 주소 범위를 추가할 수 있습니다. 그런 다음 AP의 IP 주소를 입력합니다.Authentication Options(인증 옵션)에서 TACACS+ 상자를 선택하고 Shared Secret(공유 암호)을 입력합니다.예를 들면 다음과 같습니다

.



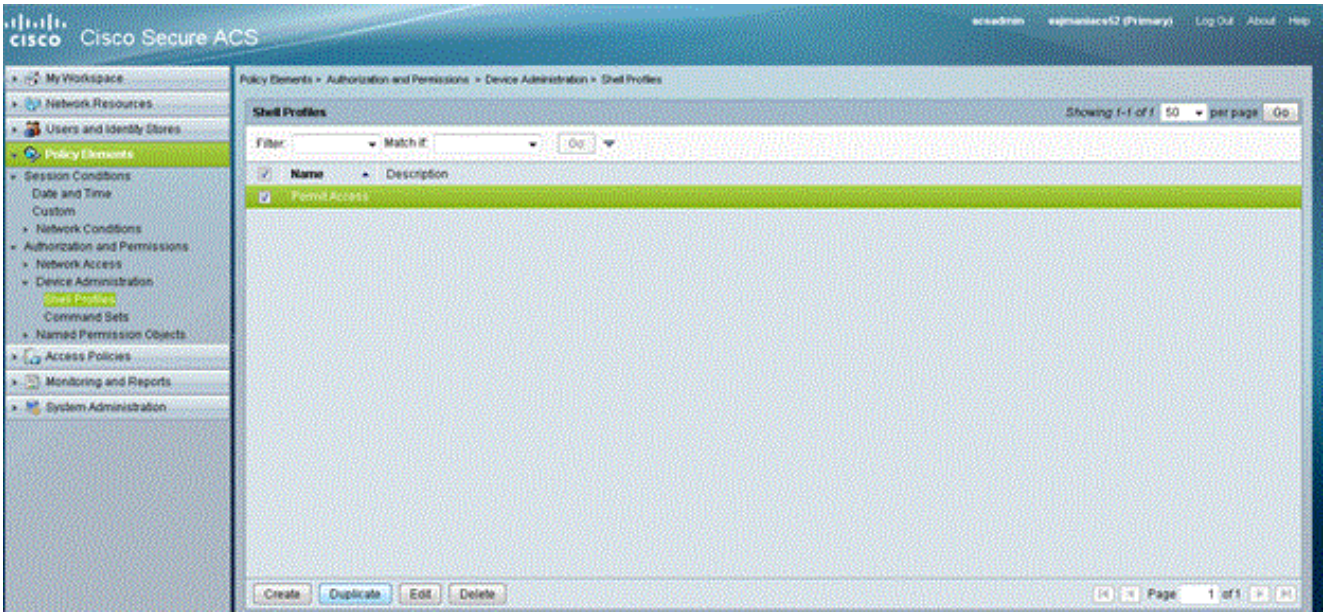
2. 다음 단계는 로그인 사용자 이름 및 비밀번호를 생성하는 것입니다.Users and Identity Stores(사용자 및 ID 저장소)를 클릭한 다음 Users(사용자)를 클릭합니다.Create를 클릭합니다.Name(이름) 아래에 사용자 이름을 지정하고 설명을 입력합니다.ID 그룹(있는 경우)을 선택합니다.암호 텍스트 상자에 암호를 입력하고 암호 확인 아래에 다시 입력합니다.Enable Password(비밀번호 활성화)에 비밀번호를 입력하여 enable 비밀번호를 수정할 수 있습니다. 확인을 위해 다시 입력합니다.예를 들면 다음과 같습니다

.



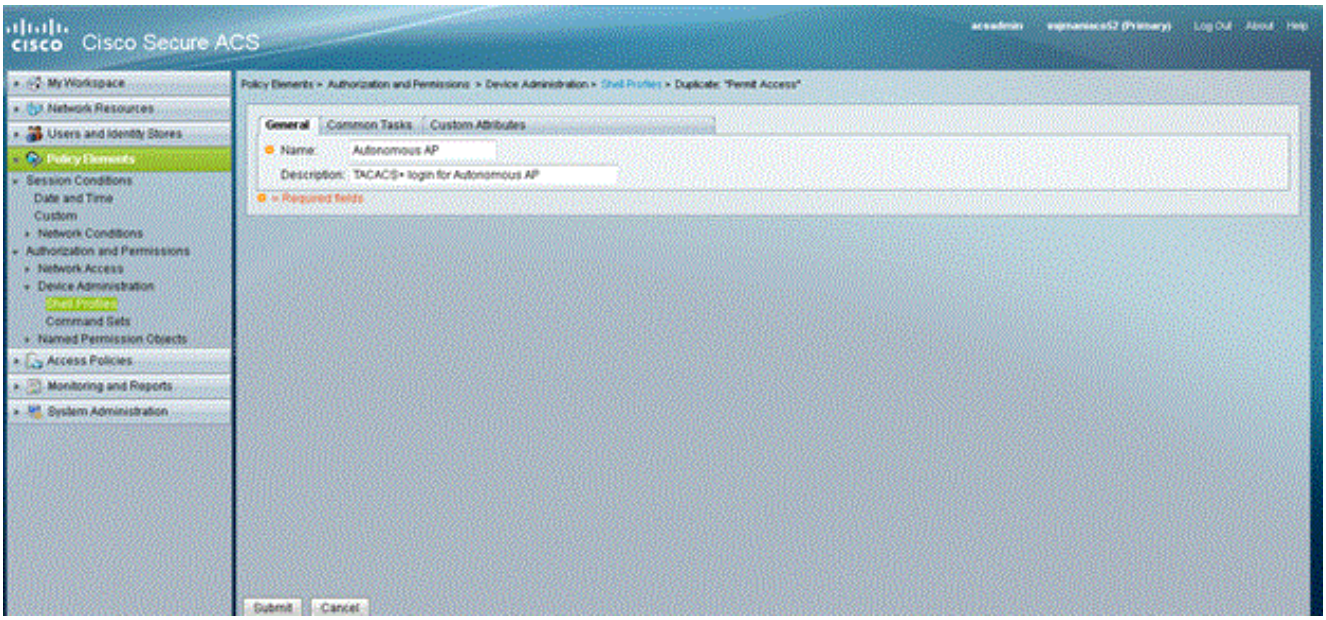
3. 권한 레벨을 정의하려면 다음 단계를 완료합니다.Policy Elements(정책 요소) > Authorizations and Permissions(권한 부여 및 권한) > Device Administration(디바이스 관리) > Shell Profiles(셸 프로파일)를 클릭합니다.Permit Access 확인란을 선택하고 Duplicate를 클릭합니다

.



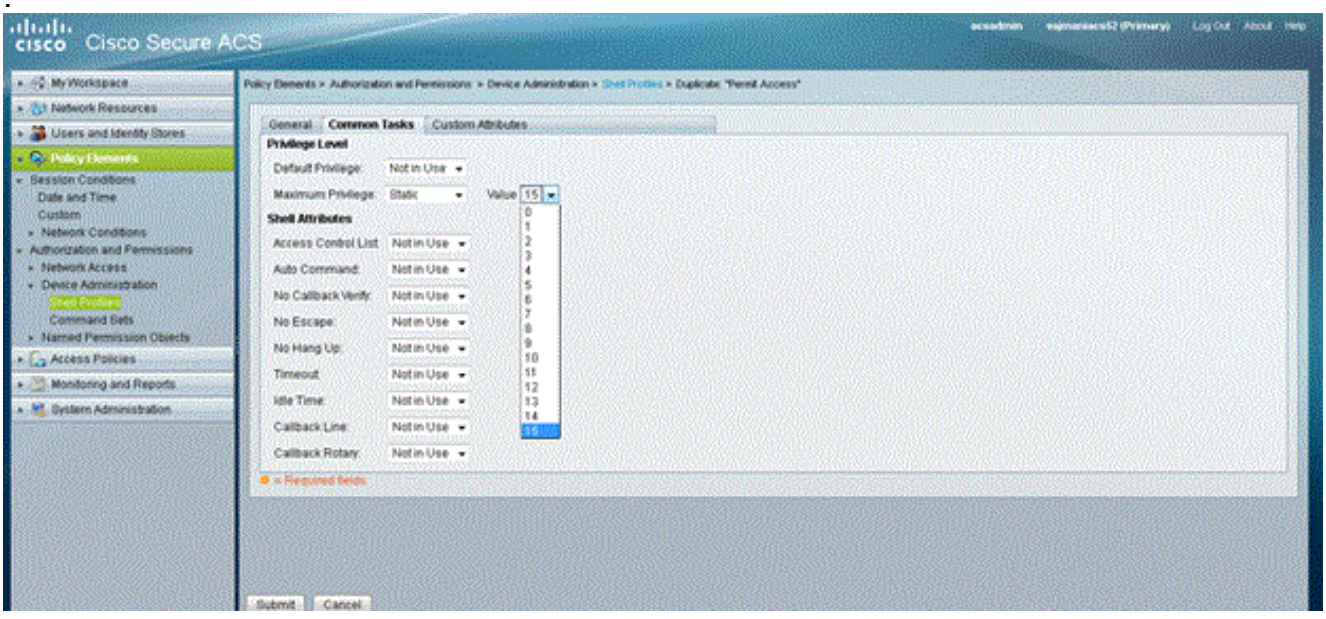
이름 및 **설명**을 **입력합니다**

.



Common Tasks(일반 작업) 탭을 선택하고 Maximum Privilege(최대 권한)에 대해 **15**를 선택합니다

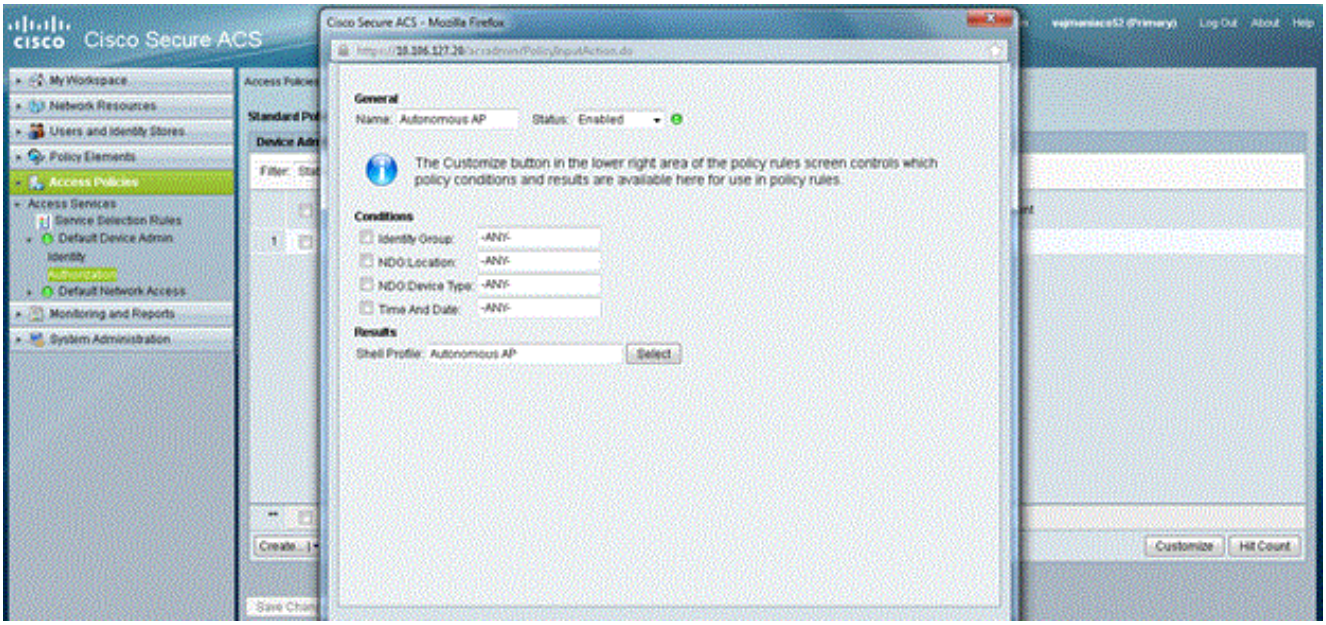
.



Submit(제출)**을 클릭합니다**.

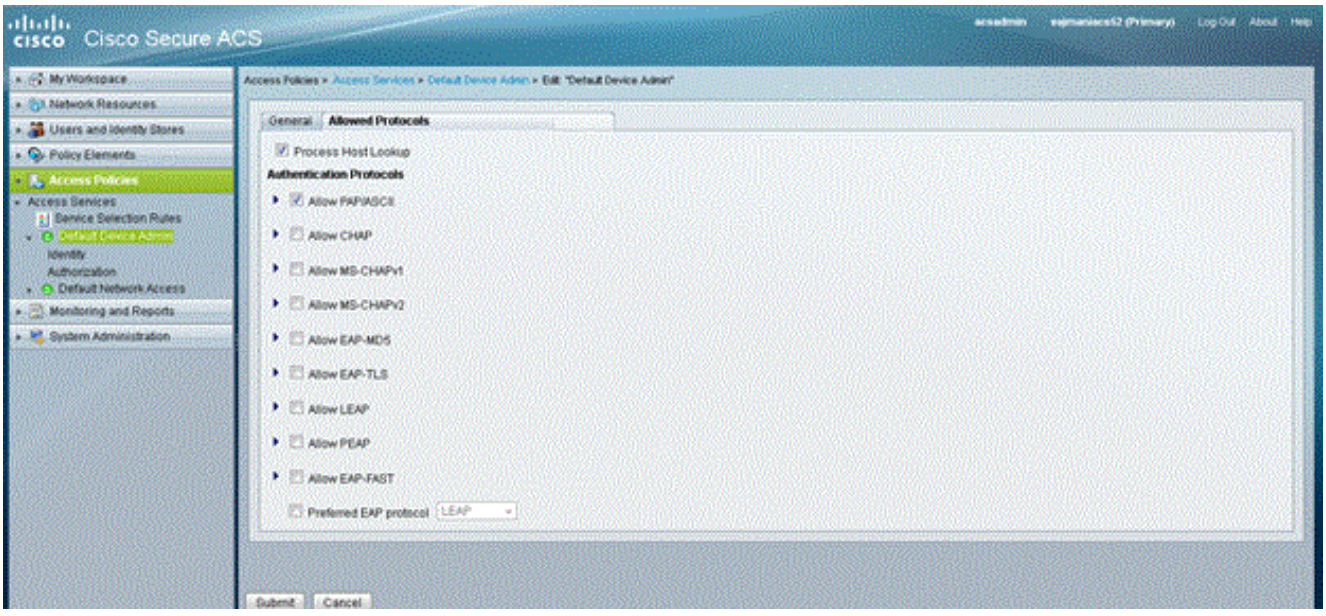
4. 권한 부여 정책을 생성하려면 다음 단계를 완료합니다.Access **Policies(액세스 정책)** > **Access Services(액세스 서비스)** > **Default Device Admin(기본 디바이스 관리자)** > Authorization(**권한 부여)을 클릭합니다**.새 권한 부여 정책을 생성하려면 Create(생성)를 클릭합니다.권한 부여 정책에 대한 규칙을 생성하는 새 팝업이 나타납니다.특정 사용자 이름 및 AAA 클라이언트(AP)에 대한 **Identity Group**, **Location** 등을 선택합니다(있는 경우).셸 프로파일에 대해 선택을 클릭하여 생성된 자동 AP를 선택합니다

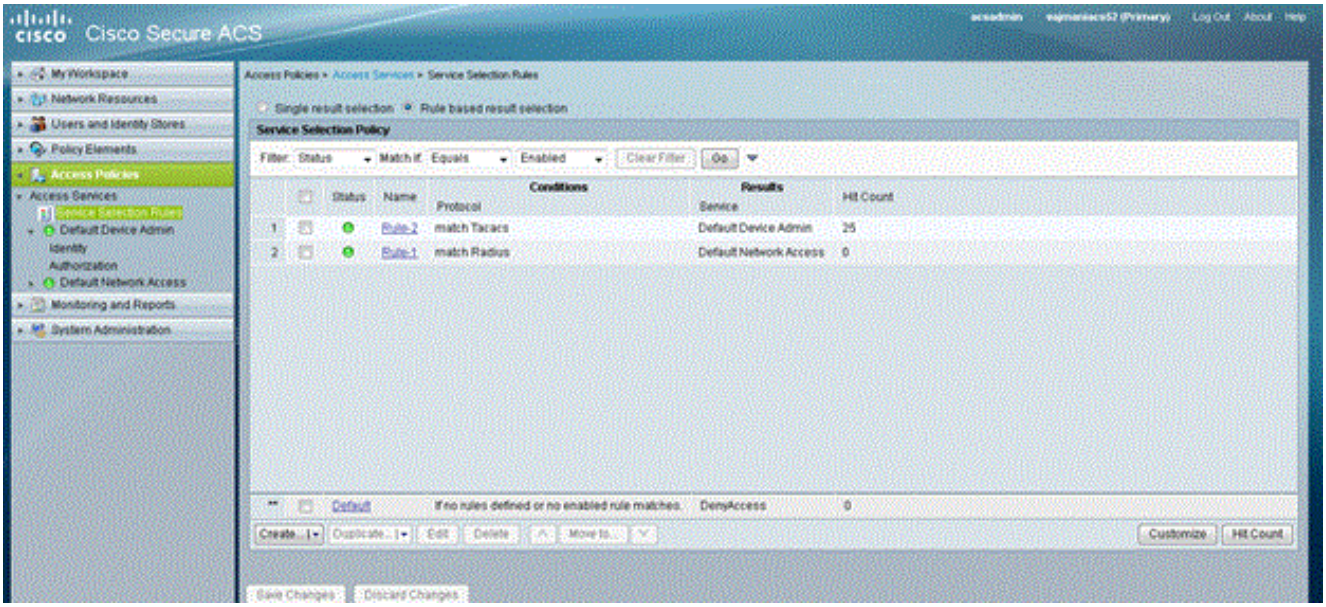
.



이 작업이 완료되면 Save **Changes(변경 사항 저장)를** 클릭합니다.Default **Device Admin(기본 디바이스 관리)**을 클릭한 다음 Allowed Protocols(허용된 프로토콜)**를 클릭합니다**.Allow **PAP/ASCII(PAP/ASCII 허용)**를 선택한 다음 Submit(제출)을 **클릭합니다**.Service **Selection Rules**(서비스 선택 규칙)를 클릭하여 TACACS와 일치하는 규칙이 있는지 확인하고 Default Device Admin(기본 디바이스 관리자)을 가리킵니다

.



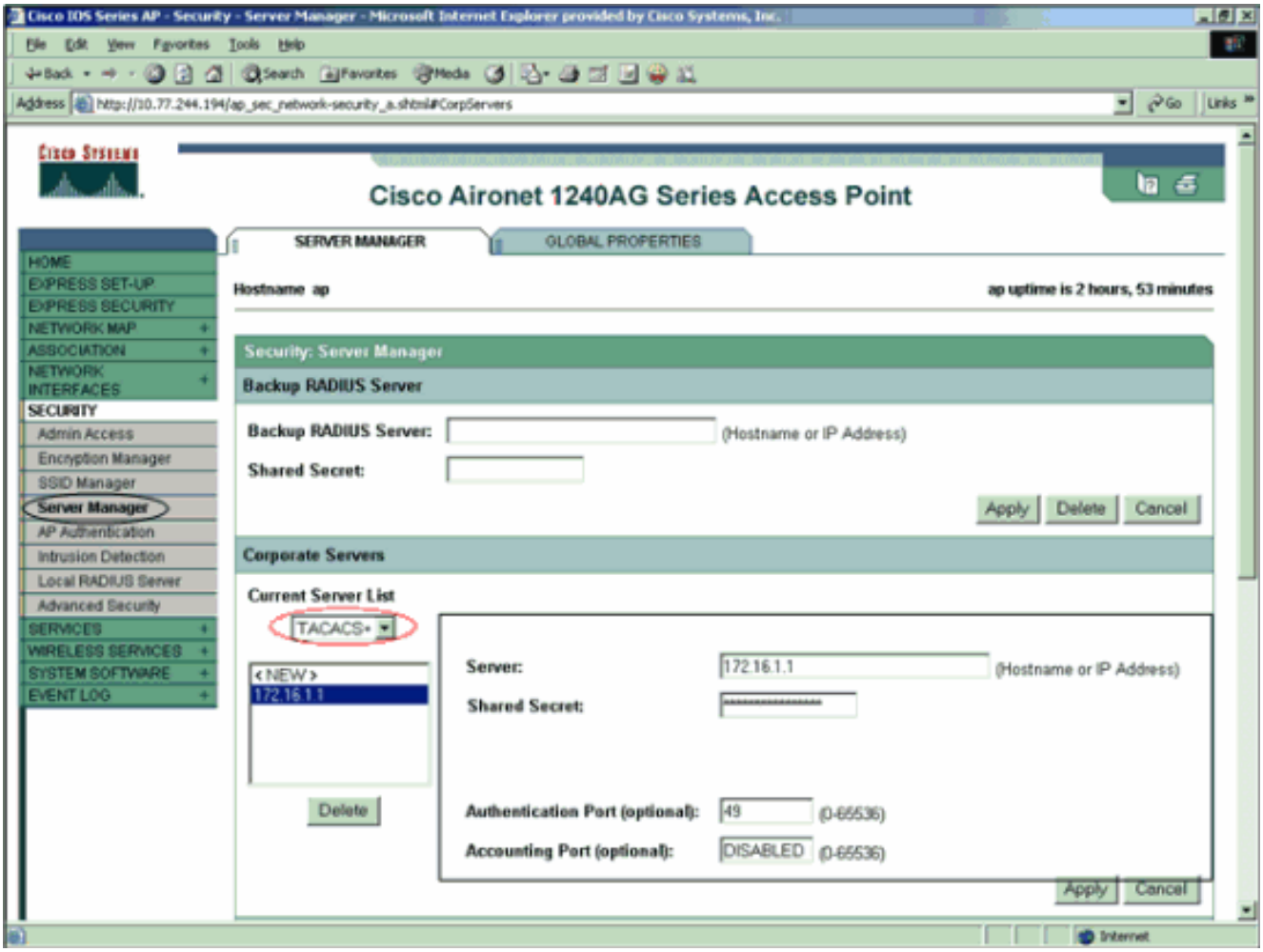


TACACS+ 인증을 위한 Aironet AP 구성

CLI 또는 GUI를 사용하여 Aironet AP에서 TACACS+ 기능을 활성화할 수 있습니다. 이 섹션에서는 GUI를 사용하여 TACACS+ 로그인 인증을 위한 AP를 구성하는 방법에 대해 설명합니다.

GUI를 사용하여 AP에서 TACACS+를 구성하려면 다음 단계를 완료합니다.

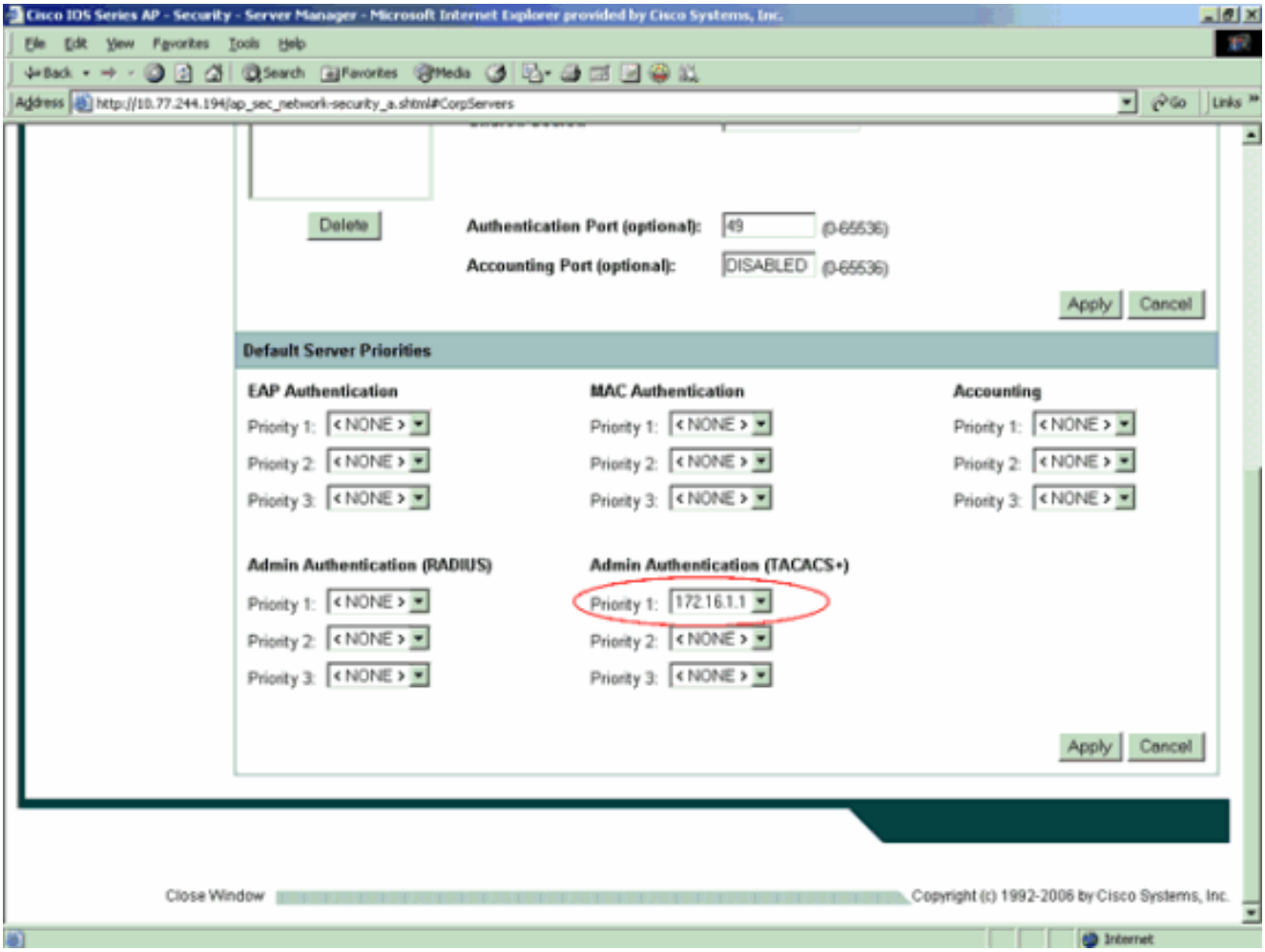
1. TACACS+ 서버 매개변수를 정의하려면 다음 단계를 완료합니다.AP GUI에서 Security(보안) **> Server Manager(서버 관리자)를** 선택합니다.보안: 서버 관리자 창이 나타납니다.Corporate Servers(회사 서버) 영역의 Current **Server List(현재 서버 목록)** 드롭다운 메뉴에서 TACACS+를 선택합니다.같은 영역에서 TACACS+ 서버의 IP 주소, 공유 암호 및 인증 포트 번호를 입력합니다.Apply를 **클릭합니다**.예를 들면 다음과 같습니다
   .



참고: 기본적으로 TACACS+는 TCP 포트 49를 사용합니다.**참고:** ACS와 AP에서 구성하는 공유 비밀 키가 일치해야 합니다.

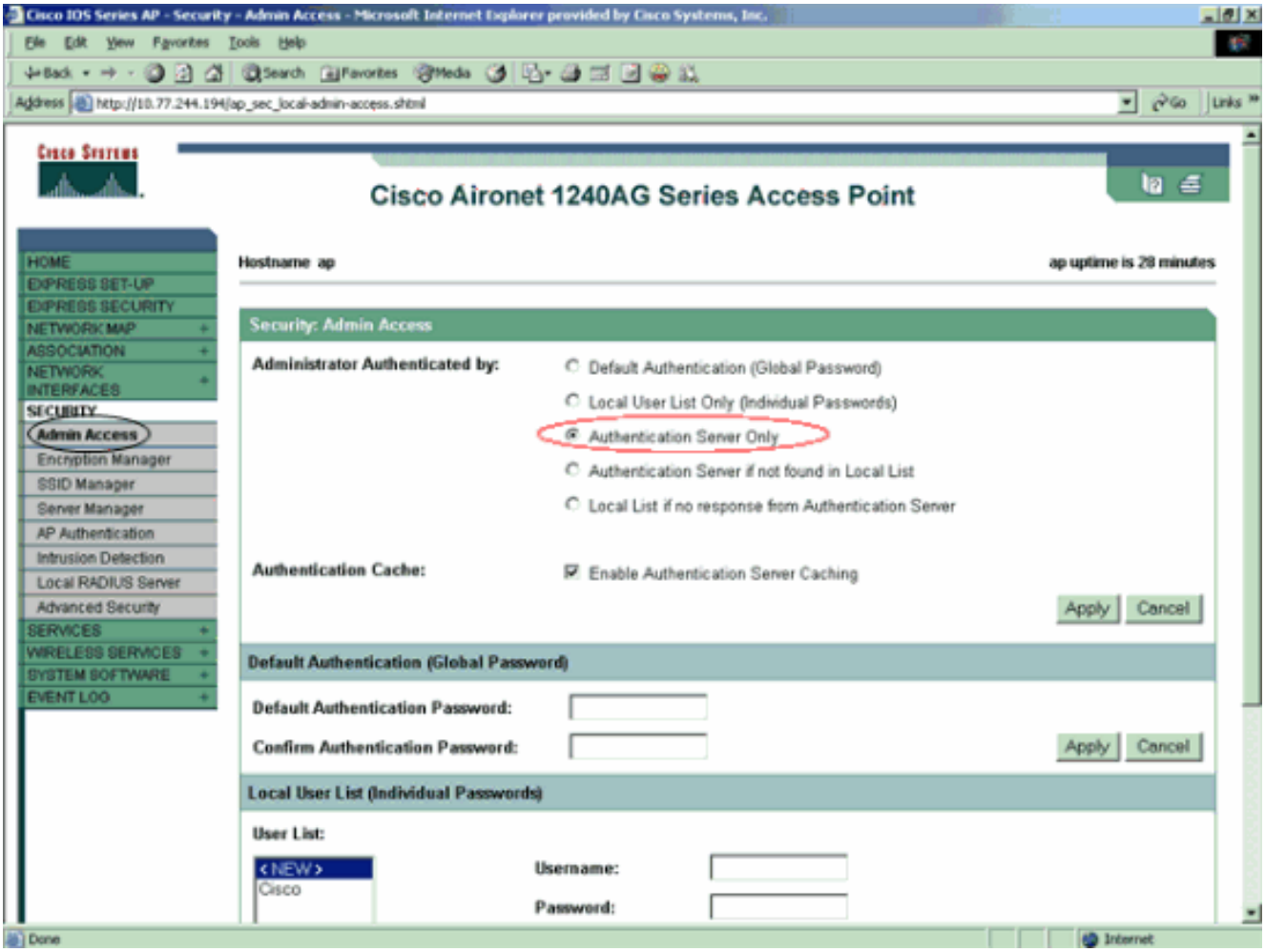
2. Default **Server Priorities(기본 서버 우선순위) > Admin Authentication(TACACS+)**을 선택하고 Priority 1 드롭다운 메뉴에서 구성한 TACACS+ 서버 IP 주소를 선택하고 **Apply**(적용)를 클릭합니다.예를 들면 다음과 같습니다

.



3. Security(**보안) > Admin Access(관리 액세스)**를 선택하고 Administrator Authenticated by(관리자 인증 기준)의 경우 Authentication Server Only(**인증 서버만)를** 선택하고 Apply(적용)를 **클릭합니다**.이렇게 선택하면 AP에 로그인하려는 사용자가 인증 서버에서 인증됩니다.예를 들면 다음과 같습니다

.



컨피그레이션 예제의 CLI 컨피그레이션입니다.

액세스 포인트

```
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
```

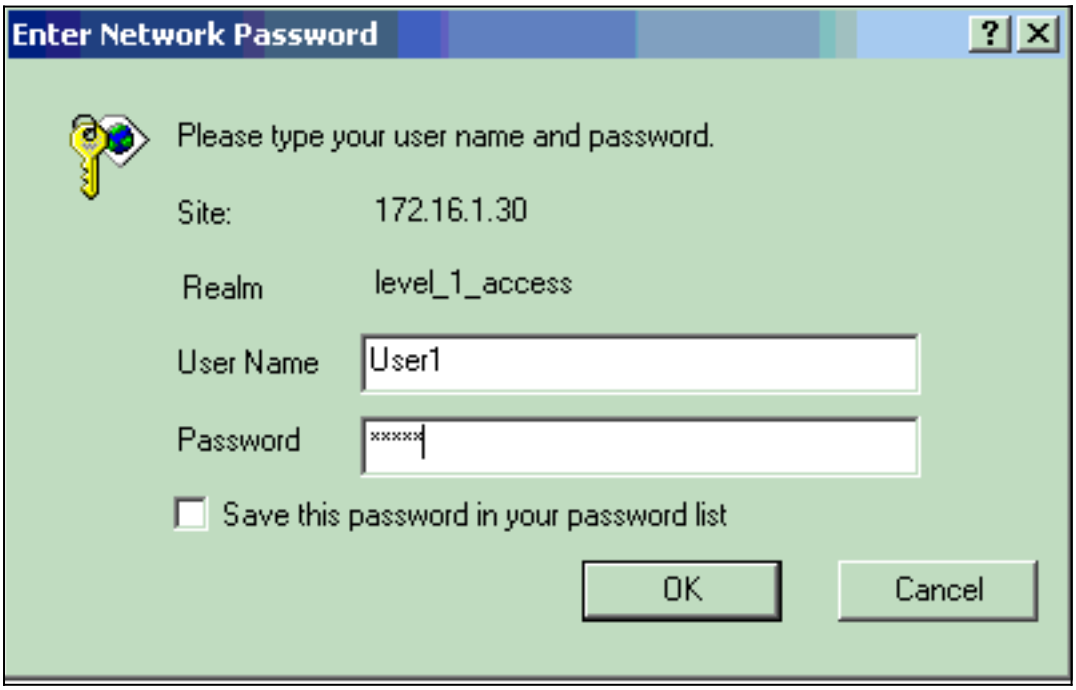
참고: 이 컨피그레이션의 모든 명령이 제대로 작동하려면 Cisco IOS Software Release 12.3(7)JA 이상이 있어야 합니다. 이전 버전의 Cisco IOS Software 릴리스에서는 이러한 명령을 모두 사용할 수 없을 수도 있습니다.

다음을 확인합니다.

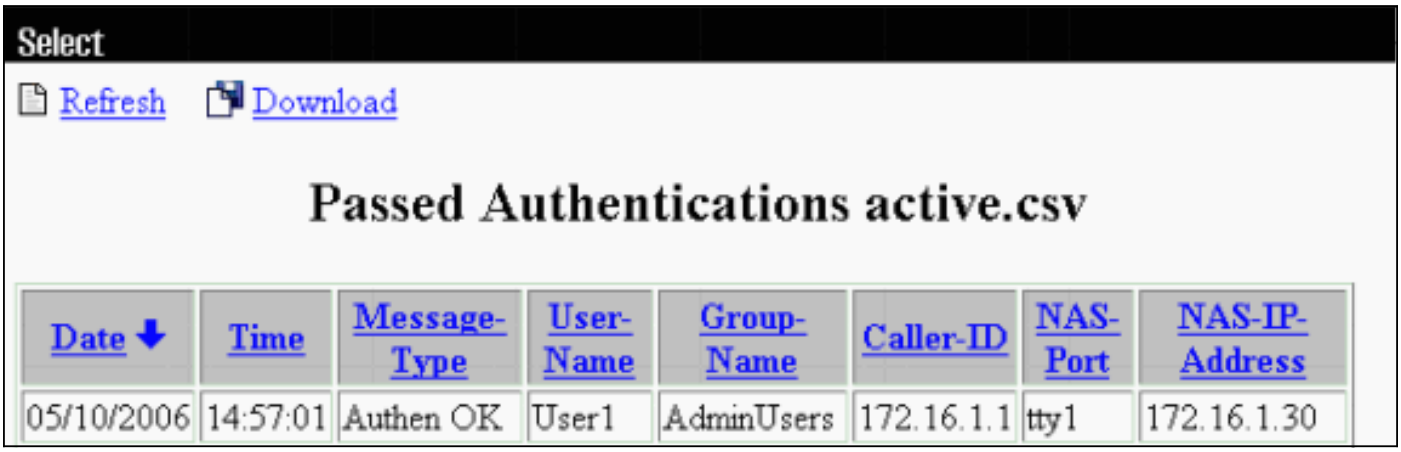
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

컨피그레이션을 확인하려면 GUI 또는 CLI를 사용하여 AP에 로그인하십시오. AP에 액세스하려고 하면 AP에서 사용자 이름과 비밀번호를 입력하라는 메시지를 표시합니다.



사용자 자격 증명을 제공할 때 AP는 자격 증명을 TACACS+ 서버에 전달합니다. TACACS+ 서버는 데이터베이스에서 사용 가능한 정보를 기반으로 자격 증명을 검증하고 인증에 성공하면 AP에 대한 액세스를 제공합니다. ACS에서 **Reports and Activity > Passed Authentication**을 선택하고 Passed Authentication 보고서를 사용하여 이 사용자에 대한 성공적인 인증을 확인할 수 있습니다. 예를 들면 다음과 같습니다.



또한 **show tacacs** 명령을 사용하여 TACACS+ 서버의 올바른 컨피그레이션을 확인할 수도 있습니다. 예를 들면 다음과 같습니다.

```
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 확인

ACS 5.2:

1. Monitoring **and Reports > Launch Monitoring and Report Viewer를 클릭합니다**.대시보드와 함께 새 팝업이 열립니다.
2. Authentications-**TACACS-Today를 클릭합니다**. 실패/통과 시도 세부 정보를 표시합니다.

문제 해결

컨피그레이션을 트러블슈팅하기 위해 AP에서 다음 debug 명령을 사용할 수 있습니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug tacacs events**—이 명령은 TACACS 인증 중에 발생하는 이벤트의 시퀀스를 표시합니다. 다음은 이 명령의 출력의 예입니다.

```
*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 인증 문제를 해결하려면 이 명령을 사용합니다. 이 명령은 라우터가 시도한 인증 방법 및 인증별 상태 메시지를 표시합니다.
- **debug aaa authentication**—이 명령은 AAA TACACS+ 인증에 대한 정보를 표시합니다.

사용자가 TACACS+ 서버에 없는 사용자 이름을 입력하면 인증이 실패합니다. 다음은 실패한 인증에 대한 **debug tacacs authentication** 명령 출력입니다.

```
*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)
```

ACS에서 실패한 인증 시도를 보려면 Reports and Activity > **Failed Authentication**을 선택할 수 있습니다. 예를 들면 다음과 같습니다.

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 Software Release 12.3(7)JA 이전의 AP에서 Cisco IOS Software 릴리스를 사용하는 경우 HTTP를 사용하여 AP에 로그인하려고 시도할 때마다 버그가 발생할 수 있습니다. Cisco 버그 ID는 CSCeb52431입니다(등록된 고객만 해당).

Cisco IOS Software HTTP/AAA 구현에는 각 개별 HTTP 연결에 대한 독립 인증이 필요합니다. 무선 Cisco IOS 소프트웨어 GUI는 단일 웹 페이지(예: Javascript 및 GIF)에서 수십 개의 개별 파일을 참조합니다. 따라서 무선 Cisco IOS 소프트웨어 GUI에서 단일 페이지를 로드하면 수십 개의 개별 인증/권한 부여 요청이 AAA 서버에 도달할 수 있습니다.

HTTP 인증의 경우 RADIUS 또는 로컬 인증을 사용합니다. RADIUS 서버는 여전히 여러 인증 요청을 받습니다. 그러나 RADIUS는 TACACS+보다 확장성이 뛰어나기 때문에 성능이 저하되지 않을 가능성이 높습니다.

TACACS+를 사용해야 하고 Cisco ACS가 있는 경우 **single-connection** 키워드를 tacacs-**server** 명령과 함께 사용합니다. 이 키워드를 명령과 함께 사용하면 대부분의 TCP 연결 설정/해제 오버헤드가 ACS에 남아 있으므로 서버의 부하를 일정 범위로 줄일 수 있습니다.

AP의 Cisco IOS Software 릴리스 12.3(7) JA 이상에는 수정 사항이 포함되어 있습니다. 이 섹션의 나머지 부분에서는 수정에 대해 설명합니다.

TACACS+ 서버에서 반환하는 정보를 캐시하려면 AAA 인증 캐시 기능을 사용합니다. 인증 캐시 및 프로필 기능을 사용하면 AP가 사용자에 대한 인증/권한 부여 응답을 캐시하여 후속 인증/권한 부여

요청을 AAA 서버로 보낼 필요가 없습니다. CLI에서 이 기능을 활성화하려면 다음 명령을 사용합니다.

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

이 기능 및 명령에 대한 자세한 내용은 액세스 포인트 관리*의 인증 캐시 및 프로파일* 구성 섹션을 참조하십시오.

GUI에서 이 기능을 활성화하려면 **Security(보안) > Admin Access(관리 액세스)**를 선택하고 **Enable Authentication Server Caching(인증 서버 캐싱 활성화)** 확인란을 선택합니다. 이 문서에서는 Cisco IOS Software Release 12.3(7)JA를 사용하므로 구성에 설명된 대로 수정 사항을 사용합니다.

관련 정보

- RADIUS 및 TACACS+ 서버 구성
- 필드 알림: IOS Access Point Bomds TACACS+ Server with Requests
- RADIUS 서버를 사용한 EAP 인증
- 무선 제품 지원
- 기술 지원 및 문서 – Cisco Systems