

Cisco IOS 컨피그레이션의 ACS 5.x AAA 캐싱 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[Cisco IOS 라우터의 컨피그레이션](#)

[ACS의 구성](#)

[다음을 확인합니다.](#)

[텔넷 액세스 테스트](#)

[캐시 확인](#)

[ACS 실패 시뮬레이션](#)

[문제 해결](#)

소개

이 문서에서는 텔넷 및 VTY 라인 액세스를 위한 TACACS+ 관리자 사용자 자격 증명 캐싱을 구성하는 데 필요한 단계에 대해 설명합니다. Authorization and Authentication Caching은 Cisco IOS® Version 15.0(1)M에 통합되었습니다. 이 기능을 사용하면 라우터가 AAA 요청에 대한 TACACS+ 회신을 수신한 후 캐시에 AAA(Authentication, Authorization, and Accounting) 자격 증명을 저장할 수 있습니다. 캐시를 사용하여 성능을 높이고 AAA 서버로 전송되는 요청 수를 줄이거나 AAA 서버에 연결할 수 없는 경우 폴백 인증 방법으로 캐시를 사용합니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 권장 사항을 제공합니다.

- 라우터와 Cisco ACS(Secure Access Control Server) 버전 5.x 간의 IP 연결을 확인합니다.
- ACS의 라우터를 동일한 공유 암호를 가진 AAA 클라이언트(네트워크 디바이스)로 정의합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ACS 버전 5

- Cisco IOS 버전 15.1을 실행하는 라우터

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.

구성

Cisco IOS 라우터의 컨피그레이션

1. TACACS 서버 및 사전 공유 키를 정의하려면 다음 명령을 입력합니다.

```
Router(config)#tacacs-server host 192.168.159.41
Router(config)#tacacs-server timeout 4
Router(config)#tacacs-server key SECRET12345
```

2. 캐시 프로파일 그룹을 정의하려면 다음 명령을 입력합니다.

참고: 각 프로파일 이름은 AAA 사용자 이름과 일치해야 합니다.

```
Router(config)#aaa cache profile admin
Router(config-profile-map)# profile peteradmin
```

3. 인증 및 권한 부여 캐싱 규칙을 AAA 서버 그룹에 할당하려면 다음 명령을 입력합니다.

```
Router(config-profile-map)# aaa group server tacacs+ admin-tac
Router(config-sg-tacacs+)# server 192.168.159.41
Router(config-sg-tacacs+)# cache authentication profile admin
Router(config-sg-tacacs+)# cache authorization profile admin
```

4. 캐시 방법을 포함하는 인증 및 권한 부여 방법 목록을 정의합니다. 이 컨피그레이션 예에서는 AAA 서버가 응답하지 않는 경우에만 캐시가 사용됩니다. 주문이 **cache admin-tac group admin-tac**로 전환되면 캐시가 먼저 조회됩니다.

참고: TACACS의 enable 비밀번호는 캐시되지 않습니다.

```
aaa authentication login mtac group admin-tac cache admin-tac local
aaa authorization exec default group admin-tac cache admin-tac local
aaa accounting exec default start-stop group admin-tac
```

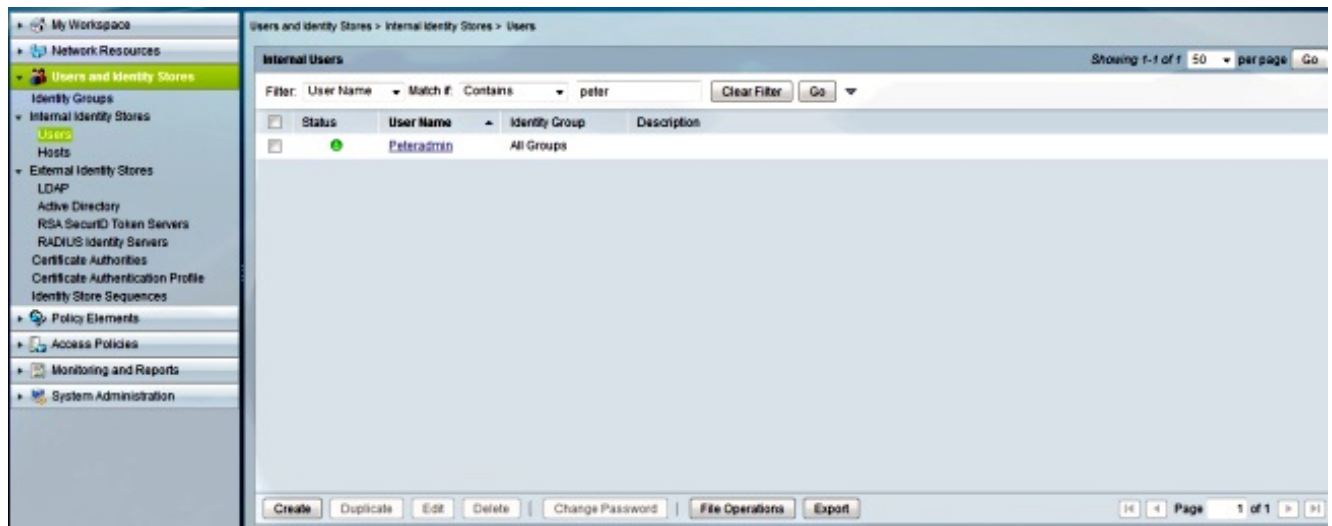
5. VTY 행에서 TACACS+를 구성하려면 다음 명령을 입력합니다.

```
Router(config)#line vty 0 4
Router(config-line)#login authentication mtac
```

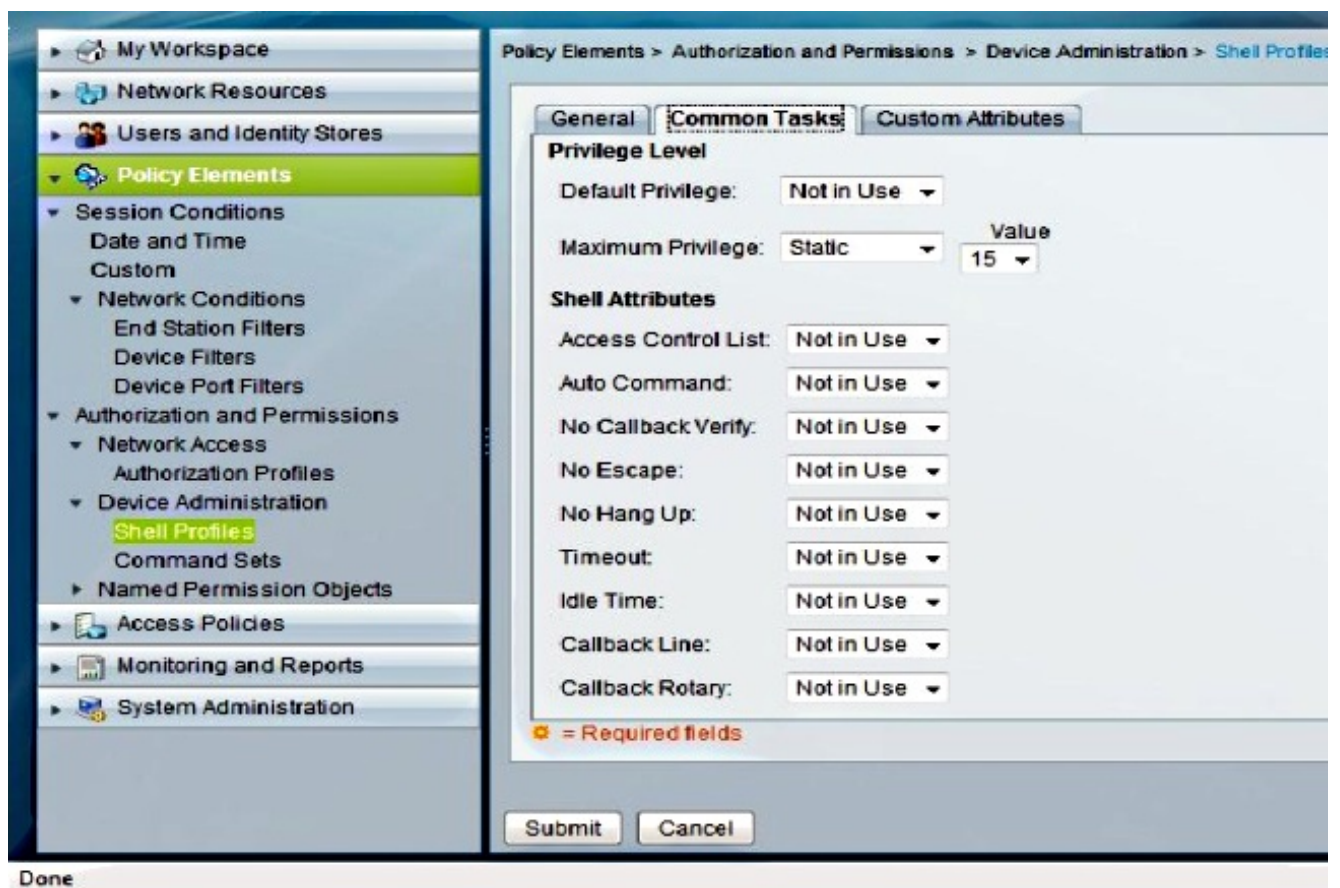
ACS의 구성

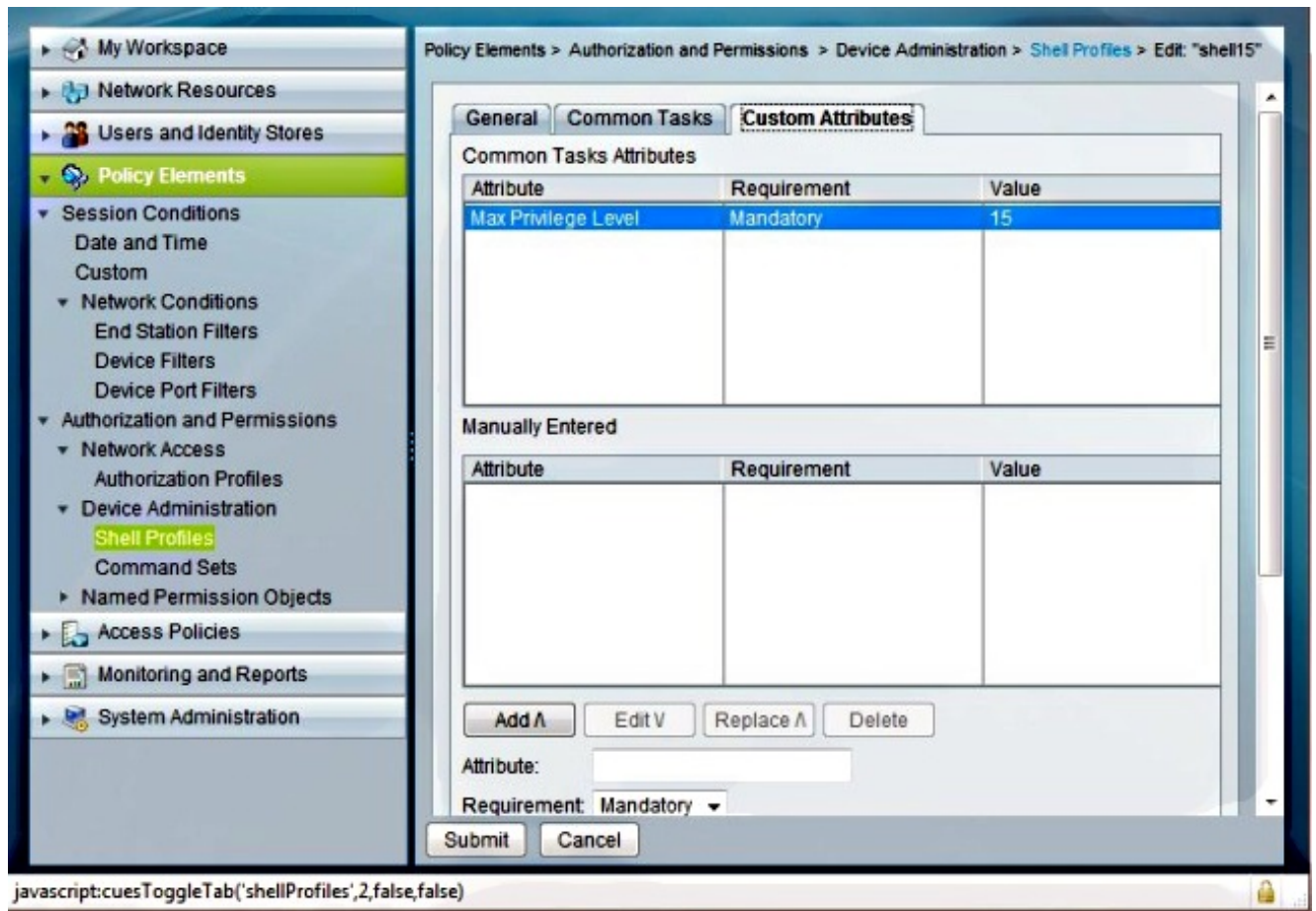
1. ACS에서 사용자를 생성합니다. Users and Identity Stores > Create User로 이동합니다. 이 예

에서는 테스트 사용자 Peteradmin을 사용합니다.

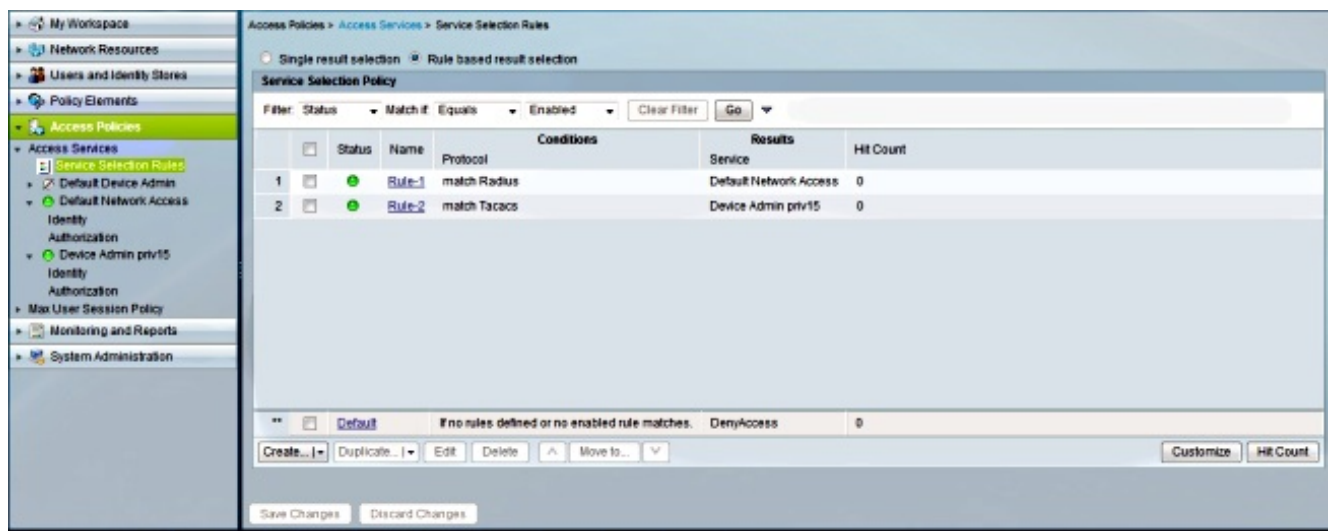


2. TACACS+ 관리자 사용자는 **활성화** 모드로 들어가도록 권한 레벨 **15**를 허용하는 셸 프로파일 이 필요합니다. 셸 프로필을 구성하려면 Policy Elements(정책 요소) > **Authorization and Permissions**(권한 부여 및 권한) > **Device Administration**(디바이스 관리) > **Shell Profiles**(셸 프로파일)로 이동합니다.

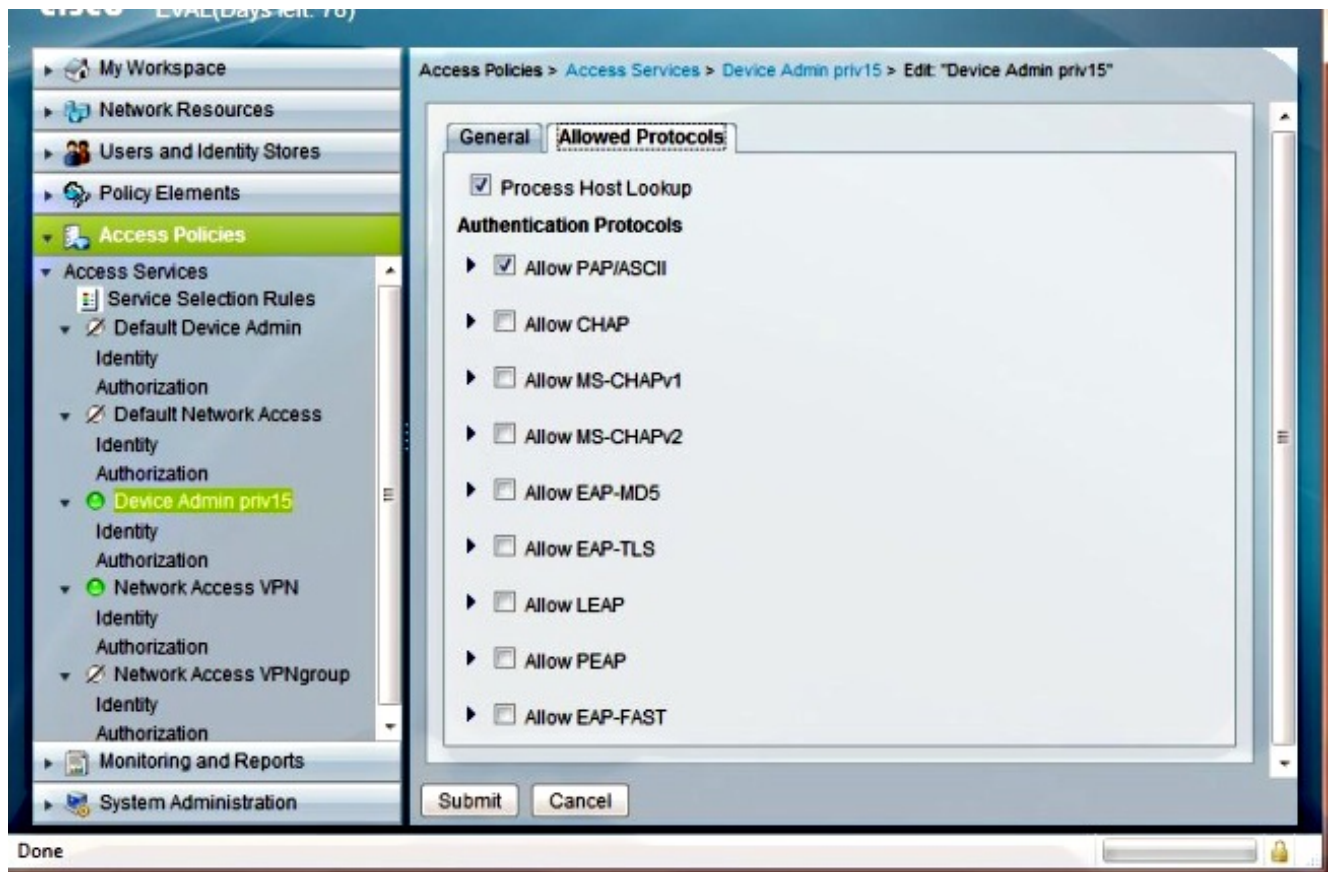




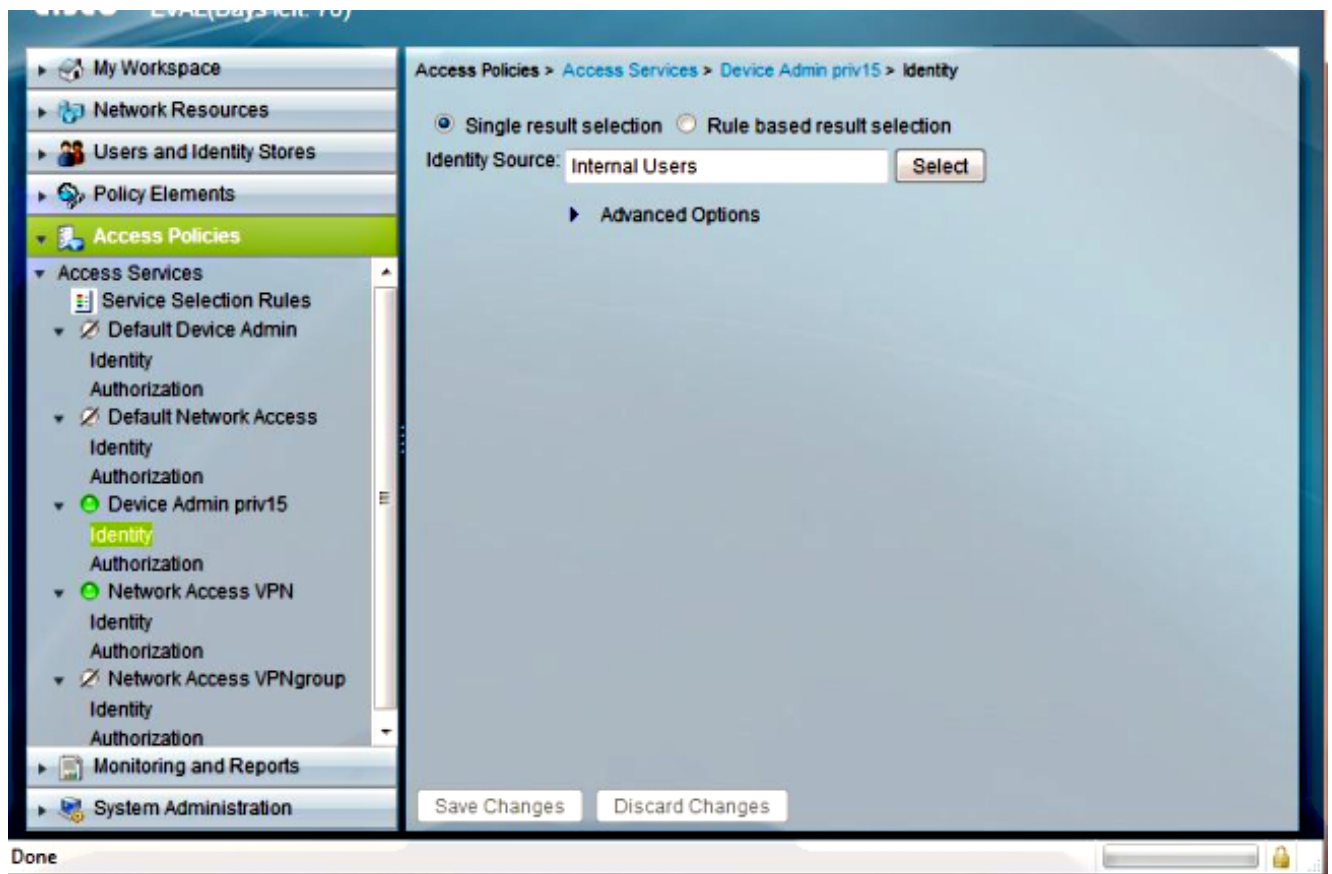
3. TACACS와 일치하도록 Access Policies(액세스 정책) > Access Services(액세스 서비스) 아래에 서비스 선택 규칙을 생성합니다.



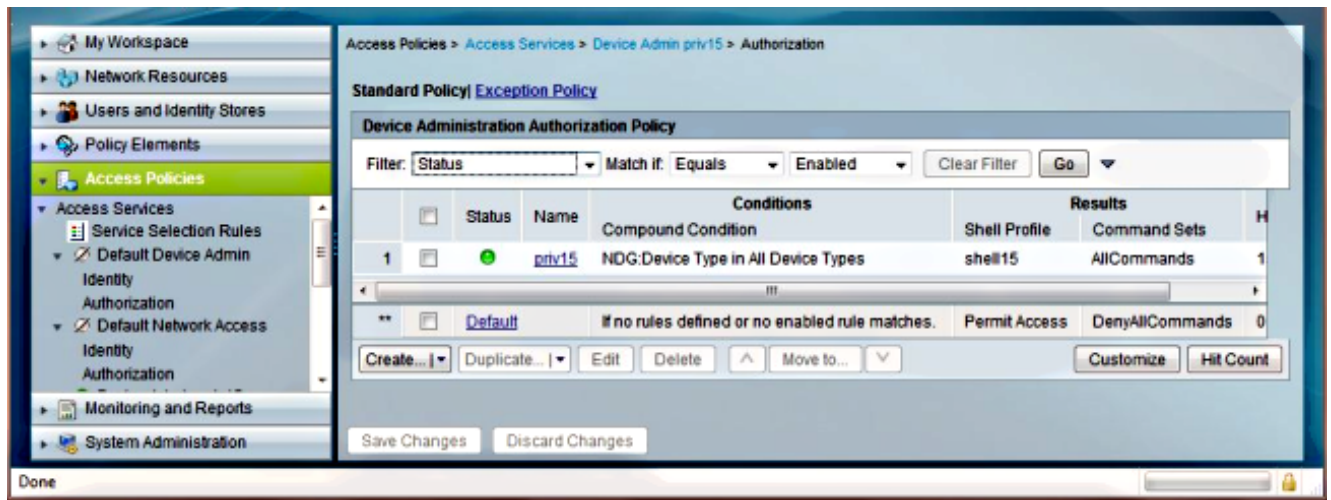
4. Device Admin priv15 > Allowed Protocols > Select Authentication Protocols로 이동하고 Allowed Protocols를 구성합니다. 이 예에서는 PAP/ASCII를 사용합니다.



5. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Device Admin priv15 > Identity(디바이스 관리자 priv15)로 이동하고 내부 사용자에게 대한 ID 소스를 구성합니다.



6. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Device Admin priv15 > Authorization(디바이스 관리자 권한)에서 권한 부여 정책을 구성합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

텔넷 액세스 테스트

이러한 디버그는 TACACS+에 대한 인증 및 권한 부여 캐시를 확인하기 위해 사용됩니다.

- tacacs 이벤트 디버그
- 디버그 aaa 캐시 그룹

TACACS 사용자 및 TACACS enable 비밀번호를 사용하여 라우터에 텔넷합니다.

```
username: peteradmin
password: peteradmin
```

```
R102>en
password: cpeter
R102#
```

```
R102#debug tacacs events
R102#debug aaa cache group
R102#
11:35:47.151: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:47.159: TPLUS: processing authentication start request id 16
11:35:47.163: TPLUS: Authentication start packet created for 16()
11:35:47.167: TPLUS: Using server 192.168.159.41
11:35:47.187: TPLUS(00000010)/0/NB_WAIT/69540BEC: Started 4 sec timeout
11:35:47.223: TPLUS(00000010)/0/NB_WAIT: wrote entire 37 bytes request
11:35:47.227: TPLUS: Would block while reading pak header
11:35:47.251: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:47.255: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:47.255: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:47.259: TPLUS: Received authen response status GET_USER (7)
11:35:47.263: AAA/AUTHEN/CACHE: No username in response
11:35:56.703: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:56.711: TPLUS: processing authentication continue request id 16
11:35:56.715: TPLUS: Authentication continue packet generated for 16
11:35:56.719: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
```

11:35:56.727: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:35:56.751: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16 bytes)
11:35:56.751: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:56.755: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:56.759: TPLUS: Received authen response status GET_PASSWORD (8)
11:35:56.763: AAA/AUTHEN/CACHE: Request status = 8, cannot add to cache
11:36:02.943: TPLUS: Queuing AAA Authentication request 16 for processing
11:36:02.955: TPLUS: processing authentication continue request id 16
11:36:02.959: TPLUS: Authentication continue packet generated for 16
11:36:02.963: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:36:02.967: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:36:03.971: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6 bytes)
11:36:03.975: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:03.975: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:36:03.979: TPLUS: Received authen response status PASS (2)
11:36:03.983: AAA/AUTHEN/CACHE: SG profile admin
11:36:03.987: AAA/AUTHEN/CACHE: SG block for admin found
11:36:03.987: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:03.991: AAA/AUTHEN/CACHE: Dealing with authen_type = 1
11:36:03.995: TPLUS: Error occurs in reading packet header, shutdown the single connection
11:36:04.047: TPLUS: Queuing AAA Authorization request 16 for processing
11:36:04.055: TPLUS: processing authorization request id 16
11:36:04.059: TPLUS: Protocol set to NoneSkipping
11:36:04.063: TPLUS: Sending AV service=shell
11:36:04.067: TPLUS: Sending AV cmd*
11:36:04.067: TPLUS: Authorization request created for 16(peteradmin)
11:36:04.071: TPLUS: using previously set server 192.168.159.41 from group admin-tac
11:36:04.091: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:04.127: TPLUS(00000010)/0/NB_WAIT: wrote entire 66 bytes request
11:36:04.131: TPLUS: Would block while reading pak header
11:36:05.319: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6 bytes)
11:36:05.323: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:05.327: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.327: TPLUS: received authorization response for 16: PASS
11:36:05.335: AAA/AUTHEN/CACHE: SG profile admin
11:36:05.335: AAA/AUTHEN/CACHE: SG block for admin found
11:36:05.339: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:05.339: AAA/AUTHOR/CACHE(00000010): Existing entry no set for authorization
11:36:05.347: TPLUS: Error occurs in reading packet header, shutdown the single connection
11:36:05.419: TPLUS: Queuing AAA Accounting request 16 for processing
11:36:05.431: TPLUS: processing accounting request id 16
11:36:05.439: TPLUS: Sending AV task_id=6
11:36:05.439: TPLUS: Sending AV timezone=UTC
11:36:05.443: TPLUS: Sending AV service=shell
11:36:05.443: TPLUS: Accounting request created for 16(peteradmin)
11:36:05.447: TPLUS: using previously set server 192.168.159.41 from group admin-tac
11:36:05.471: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:05.523: TPLUS(00000010)/0/NB_WAIT: wrote entire 85 bytes request
11:36:05.523: TPLUS: Would block while reading pak header
11:36:05.587: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 5 bytes)
11:36:05.591: TPLUS(00000010)/0/READ: read entire 17 bytes response
11:36:05.591: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.595: TPLUS: Received accounting response with status PASS
11:36:05.603: TPLUS: Error occurs in reading packet header, shutdown the single connection
R102#

캐시 확인

캐시 정보를 검토하고 지우려면 다음 명령을 입력합니다.

- **show aaa cache group [cache group name] all**
- **aaa 캐시 그룹 [캐시 그룹 이름] 모두 지우기**

```
R102#show aaa cache group admin-tac all
-----
Entries in Profile dB admin-tac for exact match
-----
Profile: peteradmin
Updated: 00:00:42
Parse User: N
Authen User: Y
Query Count: 2
6731AF7C 0 00000009 username(422) 10 peteradmin, service shell, protocol none
6731AF8C 0 0000000A cmd(73) 0 , service shell, protocol none
-----
Entries in Profile dB admin-tac for regexp match
-----
No entries found for regexp match
```

ACS 실패 시뮬레이션

실패를 시뮬레이션하고 캐시 확인을 호출하려면 네트워크에서 ACS 서버 연결을 끊습니다.

TACACS 사용자 및 로컬 enable 비밀번호를 사용하여 라우터에 텔넷(TACACS에서 비밀번호를 활성화할 수 없음):

```
username: peteradmin
password: peteradmin
```

```
R102>en
password:
R102#
11:39:10.723: TPLUS: Queuing AAA Authentication request 17 for processing
11:39:10.735: TPLUS: processing authentication start request id 17
11:39:10.739: TPLUS: Authentication start packet created for 17()
11:39:10.743: TPLUS: Using server 192.168.159.41
11:39:10.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: Started 4 sec timeout
11:39:14.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out
11:39:14.763: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out, clean up
11:39:14.767: TPLUS(00000011)/0/68A4A820: Processing the reply packet
11:39:14.771: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:14.779: AAA/AUTHEN/CACHE(00000011): GET_USER for username NULL
11:39:23.315: AAA/AUTHEN/CACHE(00000011): GET_PASSWORD for username peteradmin
11:39:25.191: AAA/AUTHEN/CACHE(00000011): Found a match
11:39:25.195: AAA/AUTHEN/CACHE(00000011): PASS for username peteradmin
11:39:25.215: TPLUS: Queuing AAA Authorization request 17 for processing
11:39:25.223: TPLUS: processing authorization request id 17
11:39:25.227: TPLUS: Protocol set to None .....Skipping
11:39:25.231: TPLUS: Sending AV service=shell
11:39:25.235: TPLUS: Sending AV cmd*
11:39:25.239: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.239: TPLUS: Using server 192.168.159.41
11:39:25.243: TPLUS(00000011)/0/IDLE/689C3A0C: got immediate connect on new 0
```

11:39:25.247: TPLUS(00000011)/0/WRITE/689C3A0C: Started 4 sec timeout
11:39:25.251: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno 257((ENOTCONN))
11:39:25.255: TPLUS: Protocol set to NoneSkipping
11:39:25.259: TPLUS: Sending AV service=shell
11:39:25.259: TPLUS: Sending AV cmd*
11:39:25.263: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.263: TPLUS(00000011): Start write failed
11:39:29.247: TPLUS(00000011)/0/WRITE/689C3A0C: timed out
11:39:29.251: TPLUS: Protocol set to NoneSkipping
11:39:29.255: TPLUS: Sending AV service=shell
11:39:29.255: TPLUS: Sending AV cmd*
11:39:29.259: TPLUS: Authorization request created for 17(peteradmin)
11:39:29.263: TPLUS(00000011)/0/WRITE/689C3A0C: timed out, clean up
11:39:29.267: TPLUS: Error occurred while writing, shutdown the single connection
11:39:29.267: TPLUS(00000011)/0/689C3A0C: Processing the reply packet
11:39:29.271: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:29.331: TPLUS: Queuing AAA Accounting request 17 for processing
11:39:29.343: TPLUS: processing accounting request id 17
11:39:29.351: TPLUS: Sending AV task_id=7
11:39:29.351: TPLUS: Sending AV timezone=UTC
11:39:29.355: TPLUS: Sending AV service=shell
11:39:29.359: TPLUS: Accounting request created for 17(peteradmin)
11:39:29.359: TPLUS: using previously set server 192.168.159.41 from group admin-tac
11:39:29.379: TPLUS(00000011)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:39:33.375: TPLUS(00000011)/0/NB_WAIT/689C0FDC: timed out
11:39:33.379: TPLUS: Choosing next server 192.168.159.41
11:39:33.383: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:33.387: TPLUS(00000011)/0/NB_WAIT/689C0FDC: got immediate connect on new 0
11:39:33.387: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:33.391: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno 257((ENOTCONN))
11:39:33.399: TPLUS: Sending AV task_id=7
11:39:33.399: TPLUS: Sending AV timezone=UTC
11:39:33.403: TPLUS: Sending AV service=shell
11:39:33.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:33.407: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request will be cleaned up after timeout
11:39:37.387: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:37.395: TPLUS: Sending AV task_id=7
11:39:37.395: TPLUS: Sending AV timezone=UTC
11:39:37.399: TPLUS: Sending AV service=shell
11:39:37.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.407: TPLUS: Choosing next server 192.168.159.41
11:39:37.407: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:37.411: TPLUS(00000011)/0/WRITE/689C0FDC: got immediate connect on new 0
11:39:37.415: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:37.415: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno 257((ENOTCONN))
11:39:37.423: TPLUS: Sending AV task_id=7
11:39:37.427: TPLUS: Sending AV timezone=UTC
11:39:37.427: TPLUS: Sending AV service=shell
11:39:37.431: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.431: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request will be cleaned up after timeout
11:39:41.411: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:41.419: TPLUS: Sending AV task_id=7
11:39:41.423: TPLUS: Sending AV timezone=UTC
11:39:41.423: TPLUS: Sending AV service=shell
11:39:41.427: TPLUS: Accounting request created for 17(peteradmin)

```
11:39:41.431: TPLUS(00000011)/0/WRITE/689C0FDC: timed out, clean up
11:39:41.431: TPLUS: Error occurred while writing, shutdown the single
connection
11:39:41.435: TPLUS(00000011)/0/689C0FDC: Processing the reply packet
```

Cached username and password works.

```
R102#clear aaa cache group admin-tac all
R102#show aaa cache group admin-tac all
```

```
-----
Entries in Profile dB admin-tac for exact match
-----
```

```
No entries found in Profile dB
```

문제 해결

Output [Interpreter 도구\(등록된 고객만 해당\)](#)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.