EAP 및 DUO 인증을 사용하여 AnyConnect Flexvpn 구성

목차

소개

이 문서에서는 Cisco IOS® XE 라우터에 대한 AnyConnect IPSec 연결을 위해 외부 2단계 인증을 구성하는 방법에 대해 설명합니다.

기고자: Sadhana K S 및 Rishabh Aggarwal Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 라우터에서 RA VPN 구성 경험
- ISE(Identity Services Engine) 관리

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 17.10.01a를 실행하는 Cisco Catalyst 8000V(C8000V)
- Cisco AnyConnect Secure Mobility Client 버전 4.10.04071

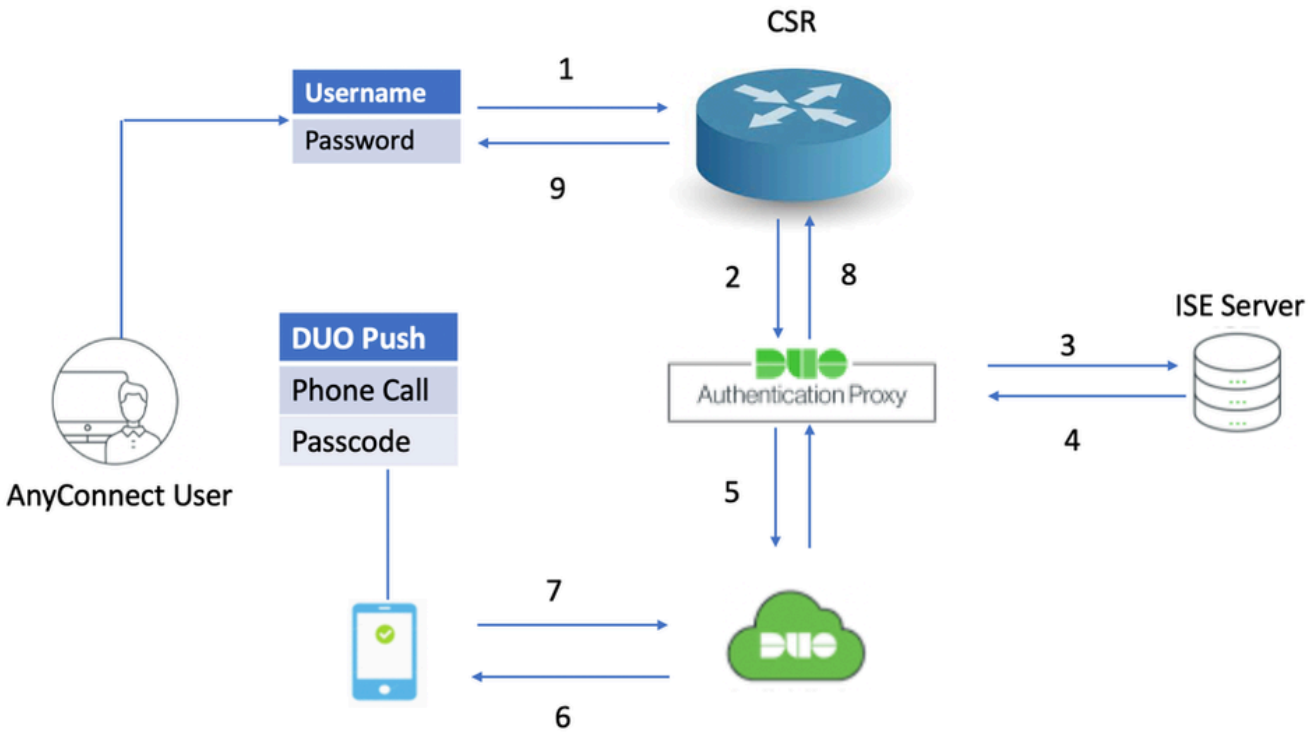
- 버전 3.1.0을 실행 중인 Cisco ISE
- Duo 인증 프록시 서버 (windows 10 또는 모든 Linux PC)
- Duo 웹 계정
- AnyConnect가 설치된 클라이언트 PC

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

인증 흐름

AnyConnect 사용자는 ISE 서버에서 사용자 이름 및 비밀번호로 인증합니다. Duo Authentication Proxy 서버는 또한 푸시 알림(push notification) 형태의 추가 인증을 사용자의 모바일 디바이스로 전송한다.

순서도



인증 흐름도

통신 과정

1. 사용자는 C8000V에 대한 RAVPN 연결을 시작하고 기본 인증을 위한 사용자 이름 및 비밀번호를 제공합니다.
2. C8000V는 Duo 인증 프록시에 인증 요청을 보냅니다.
3. 그런 다음 Duo 인증 프록시가 기본 요청을 Active Directory 또는 RADIUS 서버로 전송합니다.
4. 인증 응답은 인증 프록시로 다시 전송됩니다.

5. 1차 인증에 성공하면 Duo 인증 프록시가 Duo 서버를 통해 2차 인증을 요청합니다.
6. 그런 다음 Duo 서비스는 보조 인증 방법(푸시, 전화 통화, 암호)에 따라 사용자를 인증합니다.
7. Duo 인증 프록시가 인증 응답을 수신합니다.
8. 응답이 C8000V로 전송됩니다.
9. 성공하면 AnyConnect 연결이 설정됩니다.

구성

구성을 완료하려면 다음 섹션을 고려하십시오.

C8000V의 컨피그레이션 단계(VPN Headend)

1. RADIUS 서버를 구성합니다. RADIUS 서버의 IP 주소는 Duo 인증 프록시의 IP여야 합니다.

```
radius server rad_server
 address ipv4 10.197.243.97 auth-port 1812 acct-port 1813
 timeout 120
 key cisco
```

2. RADIUS 서버를 인증으로aaa구성하고 권한 부여를 로컬로 구성합니다.

```
aaa new-model
aaa group server radius FlexVPN_auth_server
 server name rad_server
aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network FlexVPN_authz local
```

3. 로컬 인증을 위해 ID 인증서가 없는 경우 ID 인증서를 설치하기 위해 신뢰 지점을 만듭니다. 인증서 생성에 대한 자세한 내용은 PKI의 Certificate Enrollment(인증서 등록)를 참조하십시오.

```
crypto pki trustpoint TP_AnyConnect
enrollment url http://x.x.x.x:80/certsrv/mscep/mscep.dll
usage ike
serial-number none
fqdn flexvpn-C8000V.cisco.com
ip-address none
subject-name cn=flexvpn-C8000V.cisco.com
revocation-check none
rsakeypair AnyConnect
```

4. (선택 사항) 스플릿 터널에 사용할 표준 액세스 목록을 구성합니다. 이 액세스 목록은 VPN 터널을 통해 액세스할 수 있는 대상 네트워크로 구성됩니다. 스플릿 터널이 구성되지 않은 경우 기본적으로 모든 트래픽이 VPN 터널을 통과합니다.

```
ip access-list standard split-tunnel-acl
 10 permit 192.168.11.0 0.0.0.255
 20 permit 192.168.12.0 0.0.0.255
```

5. IPv4 주소 풀을 생성합니다.

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

생성된 IP 주소 풀은 성공적인 AnyConnect 연결 중에 AnyConnect 클라이언트에 IPv4 주소를 할당합니다.

6. 권한 부여 정책을 구성합니다.

```
crypto ikev2 authorization policy ikev2-authz-policy
 pool SSLVPN_POOL
 dns 10.106.60.12
 route set access-list split-tunnel-acl
```

IP 풀, DNS, 스플릿 터널 목록 등은 권한 부여 정책에 지정됩니다.

참고: 사용자 지정 IKEv2 권한 부여 정책이 구성되지 않은 경우 'default'라는 기본 권한 부여 정책이 권한 부여에 사용됩니다. IKEv2 권한 부여 정책에 지정된 특성은 RADIUS 서버를 통해 푸시될 수도 있습니다.

---

7. IKEv2 제안서 및 정책을 구성합니다.

```
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-128
 integrity sha384
 group 19

crypto ikev2 policy FlexVPN_IKEv2_Policy
match fvrf any
```

```
proposal FlexVPN_IKEv2_Proposal
```

8. AnyConnect 클라이언트 프로파일을 라우터의 부트플래시에 업로드하고 지정된 대로 프로파일을 정의합니다.

```
crypto vpn anyconnect profile Client_Profile bootflash:/Client_Profile.xml
```

9. HTTP 보안 서버를 비활성화합니다.

```
no ip http secure-server
```

10. SSL 정책을 구성하고 라우터의 WAN IP를 프로파일 다운로드를 위한 로컬 주소로 지정합니다.

```
crypto ssl policy ssl-server
  pki trustpoint TP_AnyConnect sign
  ip address local

           port 443
```

11. virtual-access int가 시작되는 가상 템플릿을 구성합니다인터페이스가 복제됩니다.

```
interface Virtual-Template20 type tunnel
 ip unnumbered GigabitEthernet1
```

unnumbered 명령은 구성된 인터페이스(GigabitEthernet1)에서 IP 주소를 가져옵니다.

13. 모든 connection-relat를 포함하는 IKEv2 프로파일을 구성합니다ed 정보.

```
crypto ikev2 profile Flexvpn_ikev2_Profile
 match identity remote any
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint TP_AnyConnect
 dpd 60 2 on-demand
```

```
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list FlexVPN_authz ikev2-authz-policy
 aaa authorization user eap cached
 virtual-template 20 mode auto
 anyconnect profile Client_Profile
```

IKEv2 프로파일에서 사용됩니다.

- match identity remote any - 클라이언트의 ID를 나타냅니다. 여기서 'any'는 올바른 자격 증명을 가진 모든 클라이언트가 연결할 수 있도록 구성됩니다
- authentication remote - 클라이언트 인증에 EAP 프로토콜을 사용해야 한다는 점을 설명합니다.
- authentication local - 인증서를 로컬 인증에 사용해야 한다는 점을 언급합니다.
- aaa authentication eap - EAP 인증 중에 RADIUS 서버FlexVPN_auth사용
- aaa authorization group eap list - 권한 부여 과정에서 네트워크 목록 FlexVPN_authz권한 부여 정책과 함께 사용됩니다. ikev2-authz-policy
- aaa authorization user eap cached- 암시적 사용자 권한 부여 활성화
- virtual-template 20 mode auto - 복제할 가상 템플릿을 정의합니다.
- anyconnect profile Client_Profile - 8단계에서 정의한 클라이언트 프로파일이 여기에 이 IKEv2 프로파일에 적용됩니다.

14. 변형 집합 및 IPSec 프로필을 구성합니다.

```
crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto ipsec profile Flexvpn_IPsec_Profile
 set transform-set TS
 set ikev2-profile Flexvpn_ikev2_Profile
```

15. IPSec 프로필을 가상 템플릿에 추가합니다.

```
interface Virtual-Template20 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flexvpn_IPsec_Profile
```

클라이언트 프로필(XML 프로필) 코드 조각

Cisco IOS XE 16.9.1 이전에는 헤드엔드에서 자동 프로파일 다운로드를 사용할 수 없습니다.
16.9.1을 게시하면 헤드엔드에서 프로필을 다운로드할 수 있습니다.

<#root>

```
!
!
```

false

true

false

All

All

false

Native

false

30

false

true

false

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Automatic

false

```
false
```

```
 20
```

```
 4
```

```
false
```

false

true

```
<ServerList>
<HostEntry>
<HostName>FlexVPN</HostName>
<HostAddress>
```

flexvpn-csr.cisco.com

```
</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
```

EAP

-

MD5

```
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

DUO 인증 프록시의 컨피그레이션 단계

참고: Duo 인증 프록시는 RADIUS 인증에서만 MS-CHAPv2를 지원합니다.

1단계. Duo 인증 프록시 서버를 다운로드하고 설치합니다.

Windows 시스템에 로그인하고 Duo 인증 프록시 서버를 설치합니다.

최소 1개의 CPU, 200MB의 디스크 공간 및 4GB RAM이 있는 시스템을 사용하는 것이 좋습니다.

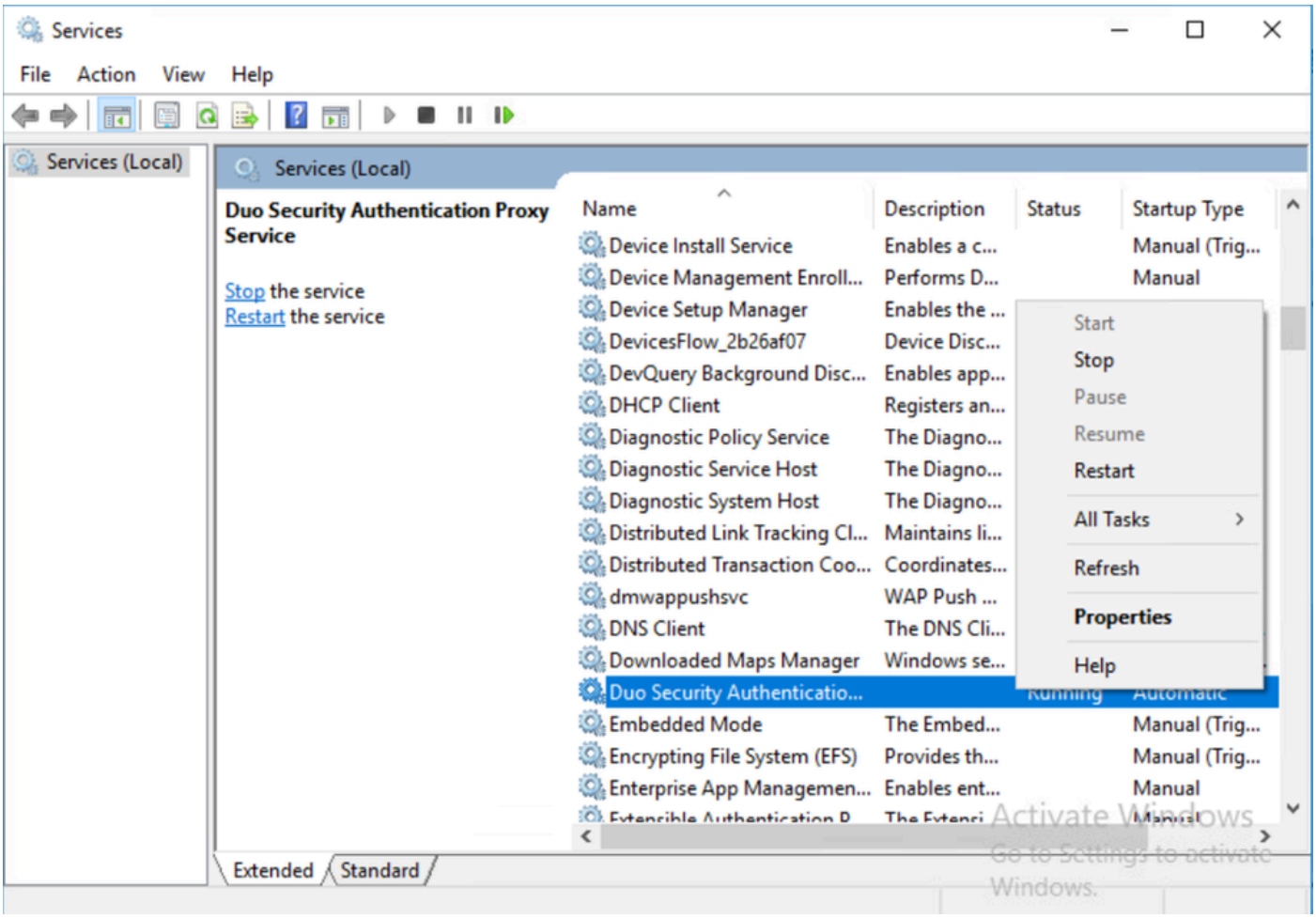
2단계. 적절한 세부사항으로 인증 프록시를 구성하려면 로C:\Program Files\Duo Security Authentication Proxy\conf\이동하여 엽니다authproxy.cfg.

```
[radius_client]
host=10.197.243.116
secret=cisco
```

참고: 여기서 '10.197.243.116'은 ISE 서버의 IP 주소이고 'cisco'는 기본 인증을 확인하기 위해 구성된 비밀번호입니다.

이러한 변경 사항을 적용한 후에는 파일을 저장합니다.

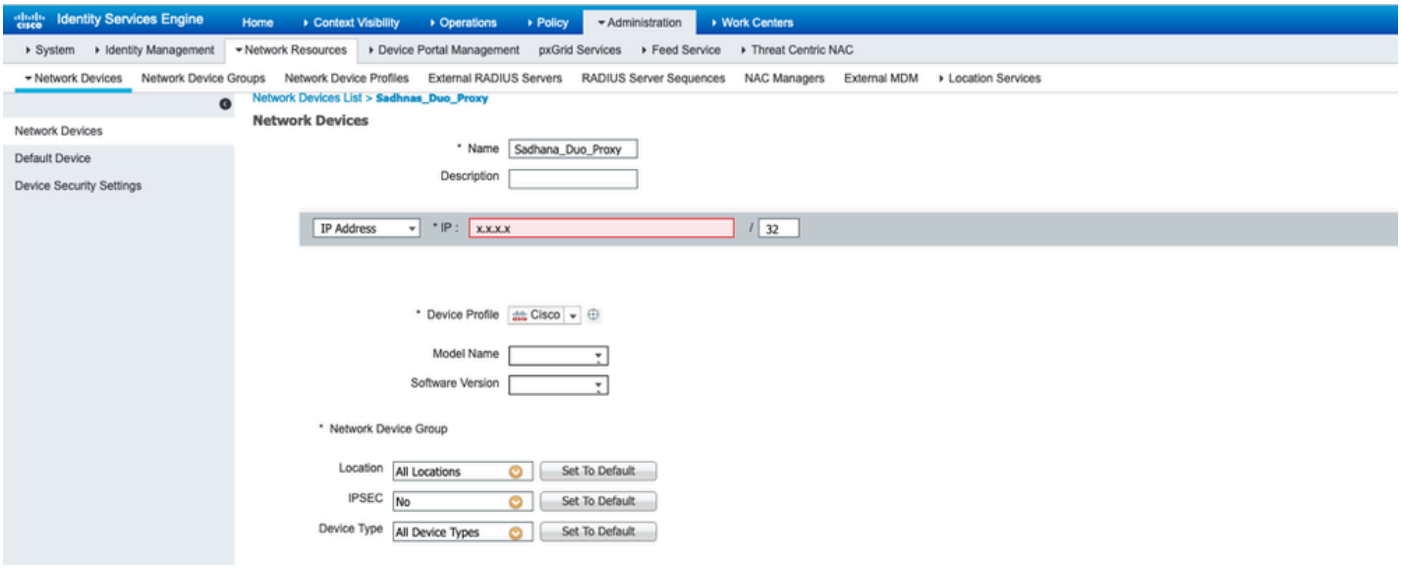
3단계. Windows 서비스 콘솔(services.msc)을 엽니다. 다시 시작합니다Duo Security Authentication Proxy Service.



ISE의 컨피그레이션 단계

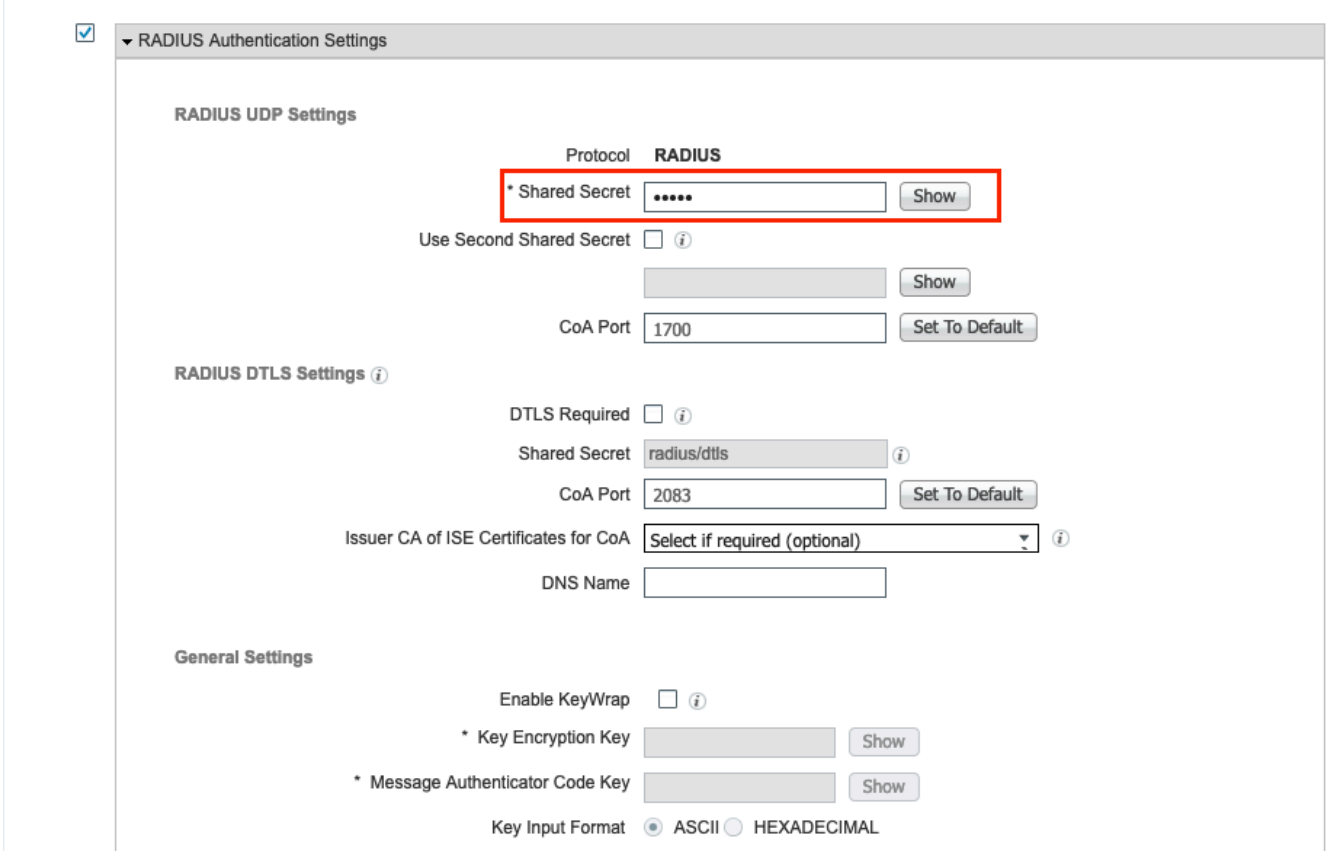
1단계. 로 **Administration** > **Network Devices**이동하여Add네트워크 디바이스를 구성합니다.

참고: Duox.x.x.xAuthentication Proxy 서버의 IP 주소로 대체합니다.



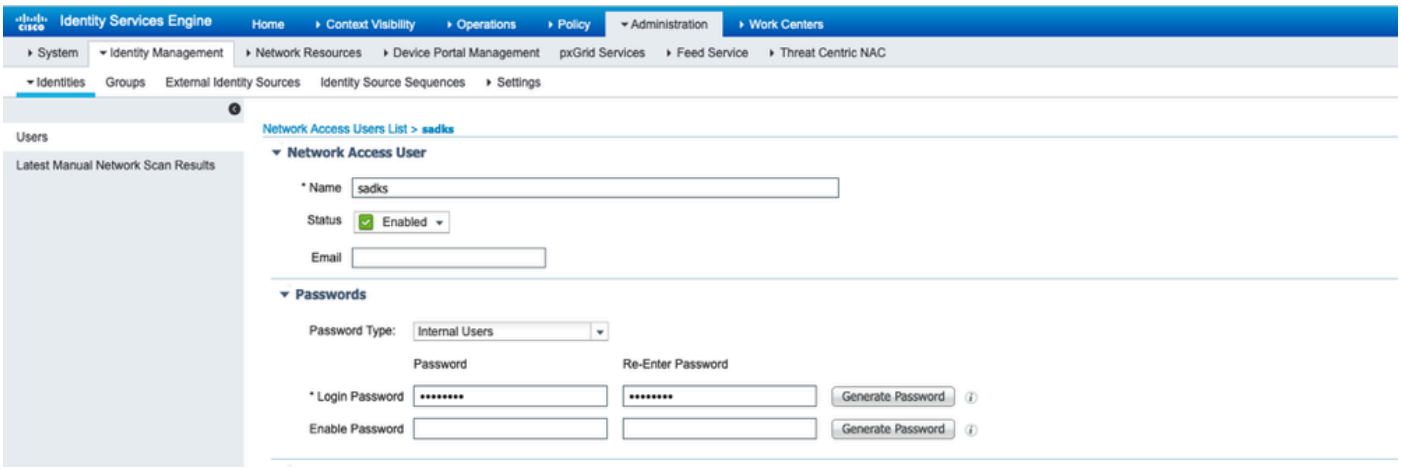
ISE - 네트워크 디바이스

2단계. 의Shared Secret설명에 따라 를authproxy.cfgsecret구성합니다.



ISE - 공유 암호

3단계. 로Administration > Identities > Users이동합니다.AnyConnectAdd기본 인증을 위해 ID 사용자를 구성하려면 다음을 선택합니다.

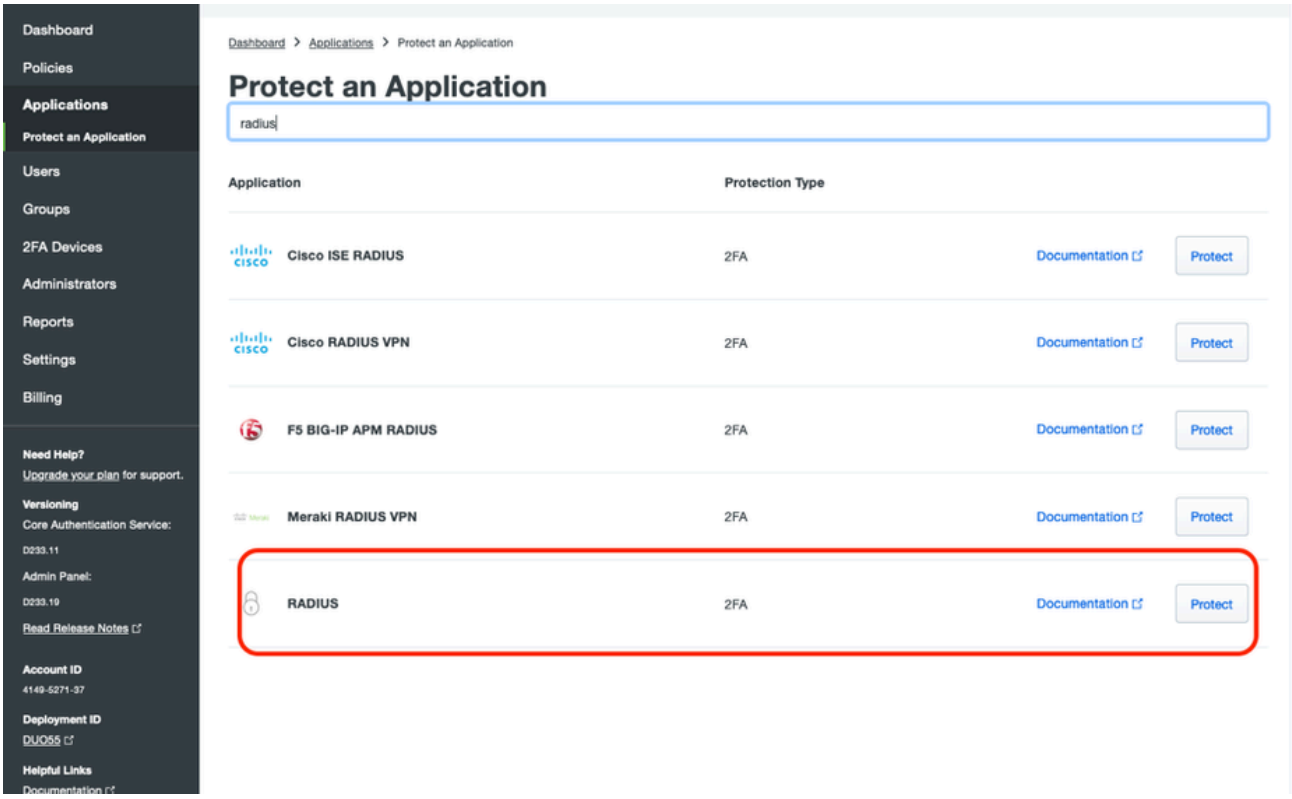


ISE - 사용자

DUO 관리 포털의 컨피그레이션 단계

1단계. Duo 계정에 로그인합니다.

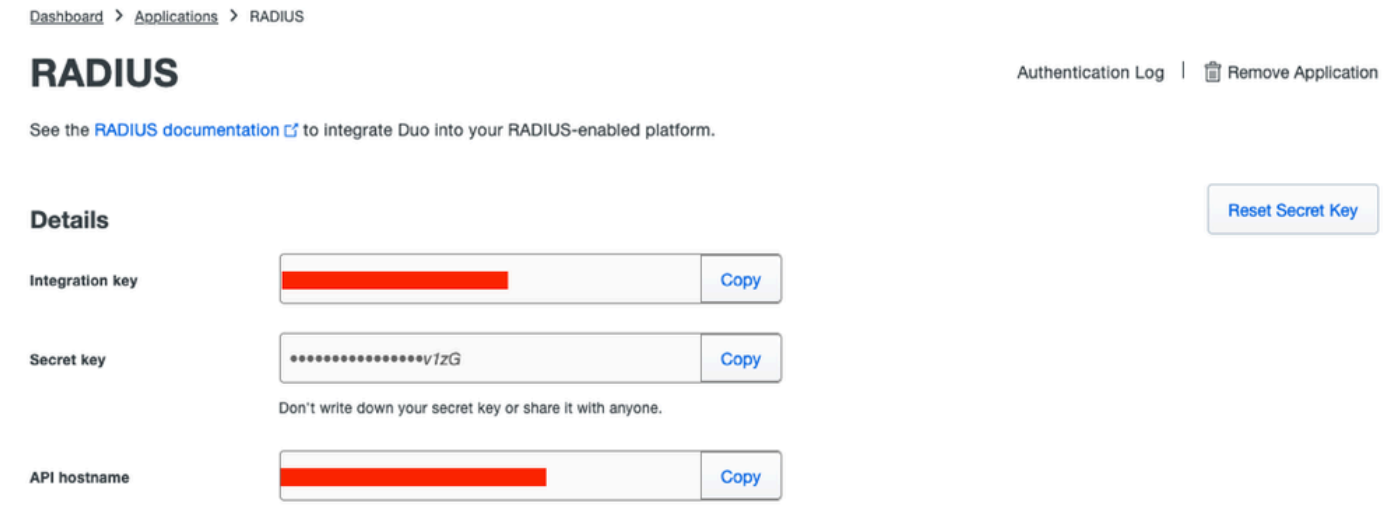
로Applications > Protect an Application이동합니다. 사용하려는 응용 프로그램을 클릭합니다Protect. (이 경우 RADIUS)



DUO - 애플리케이션

2단계. 사용할 애플리케이션에 대해 클릭합니다Protect. (이 경우 RADIUS)

통합 키, 비밀 키 및 API 호스트 이름을 복사하여 Duo 인증 프록시authproxy.cfg의 서버에 붙여넣습니다
.



듀오 - RADIUS

이 값을 복사하고 DUO 인증 프록시로 다시 이동하여 authproxy.cfg다음과 같이 값을 붙여 넣습니다.

통합 키 = ikey

비밀 키 = skey

API 호스트 이름 = api_host

```
[radius_server_auto]
ikey=xxxxxxxx
skey=xxxxxxxv1zG
api_host=xxxxxxxx
radius_ip_1=10.106.54.143
radius_secret_1=cisco
failmode=safe
client=radius_client
port=1812
```

참고: 서버를 구성할 때 Duo 서버에서 ikey, skey 및 api_host를 복사해야 합니다. '10.106.54.143'은 C8000V 라우터의 IP 주소이고 'cisco'는 radius 서버 컨피그레이션의 라우터에 구성된 키입니다.

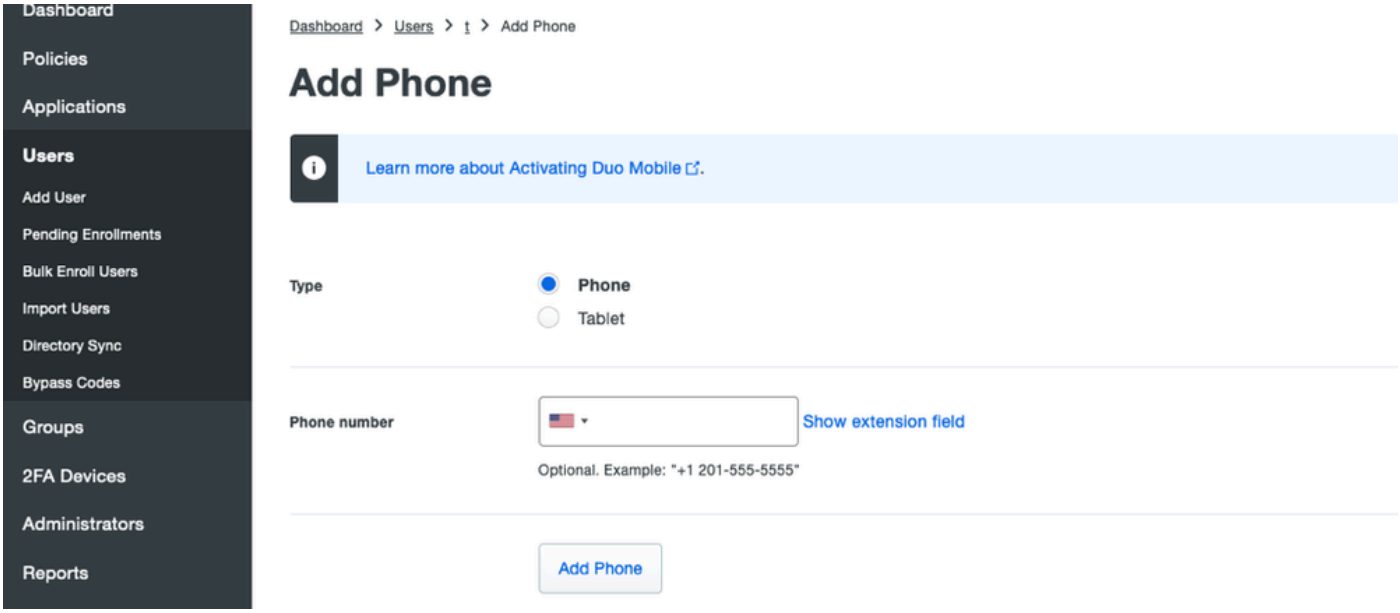
이러한 변경 사항을 적용한 후 파일을 다시 저장하고 Duo Security Authentication Proxy Service(Duo Security Authentication Proxy 서비스)를 다시services.msc시작합니다.

3단계. 2차 인증을 위해 DUO에서 사용자를 생성합니다.

로Users > Add User이동하여 사용자 이름을 입력합니다.

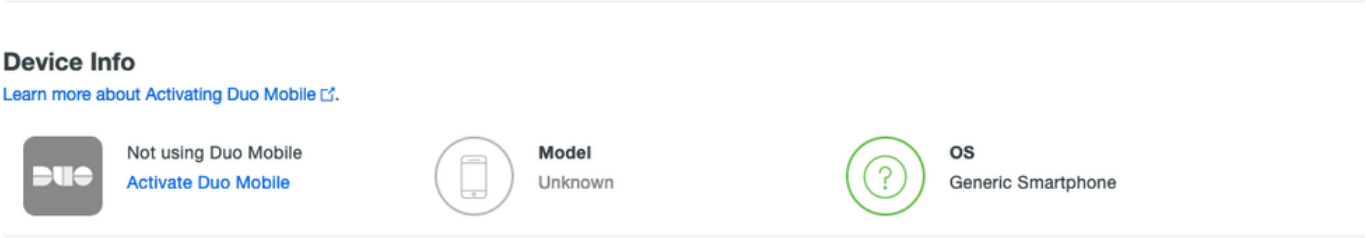
참고: 사용자 이름은 기본 인증 사용자 이름과 일치해야 합니다.

을 클릭합니다.Add User 생성되면PhonesAdd Phone아래에서 을 클릭하고 전화 번호를 입력한 다음 을 클릭합니다Add Phone.



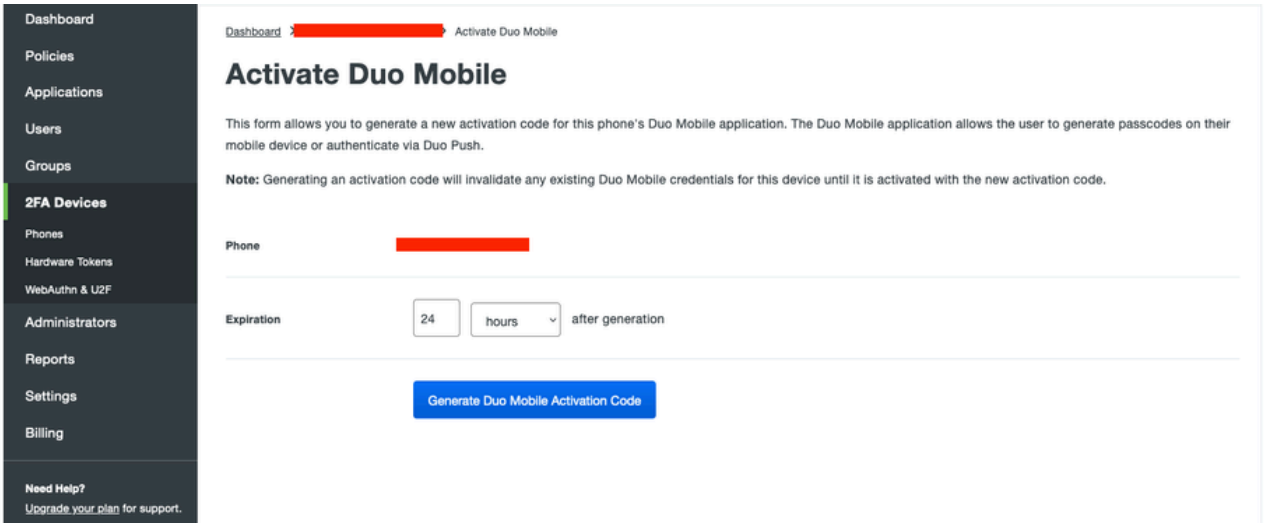
DUO - 전화기 추가

Type of authentication을 선택합니다.



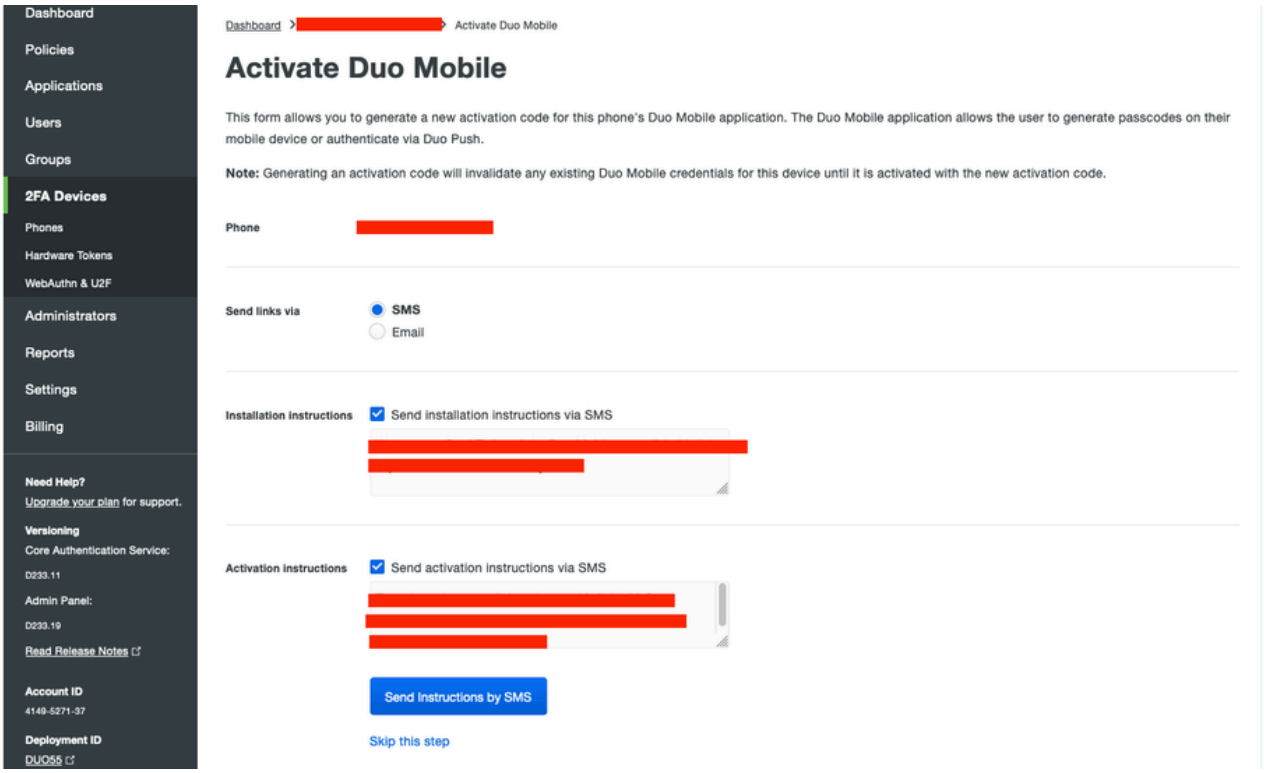
DUO - 장치 정보

선택합니다Generate Duo Mobile Activation Code.



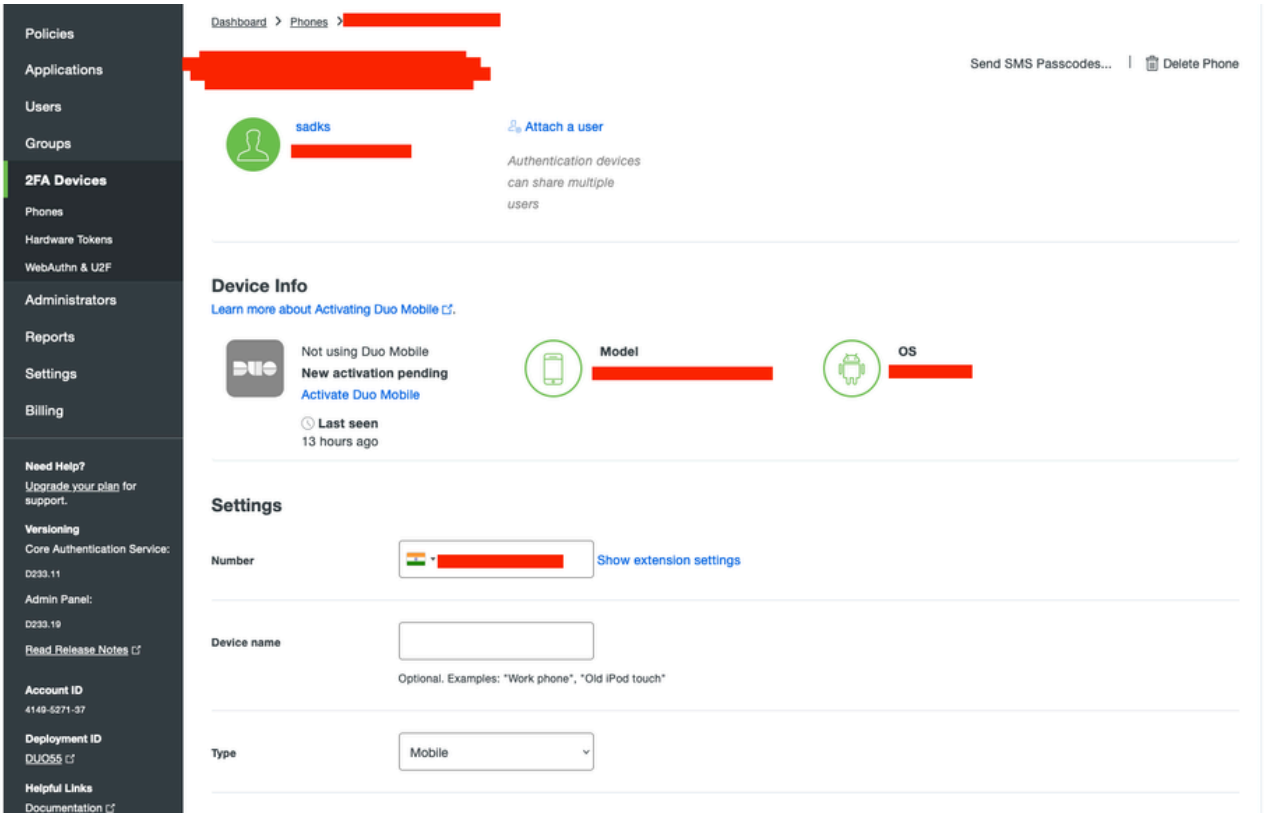
DUO - 전화 활성화

선택 Send Instructions by SMS.



DUO - SMS 전송

전화기로 전송된 링크를 클릭하면 DUO 앱이 그림과 같이 섹션의 사용자Device Info계정에 연결됩니다
.

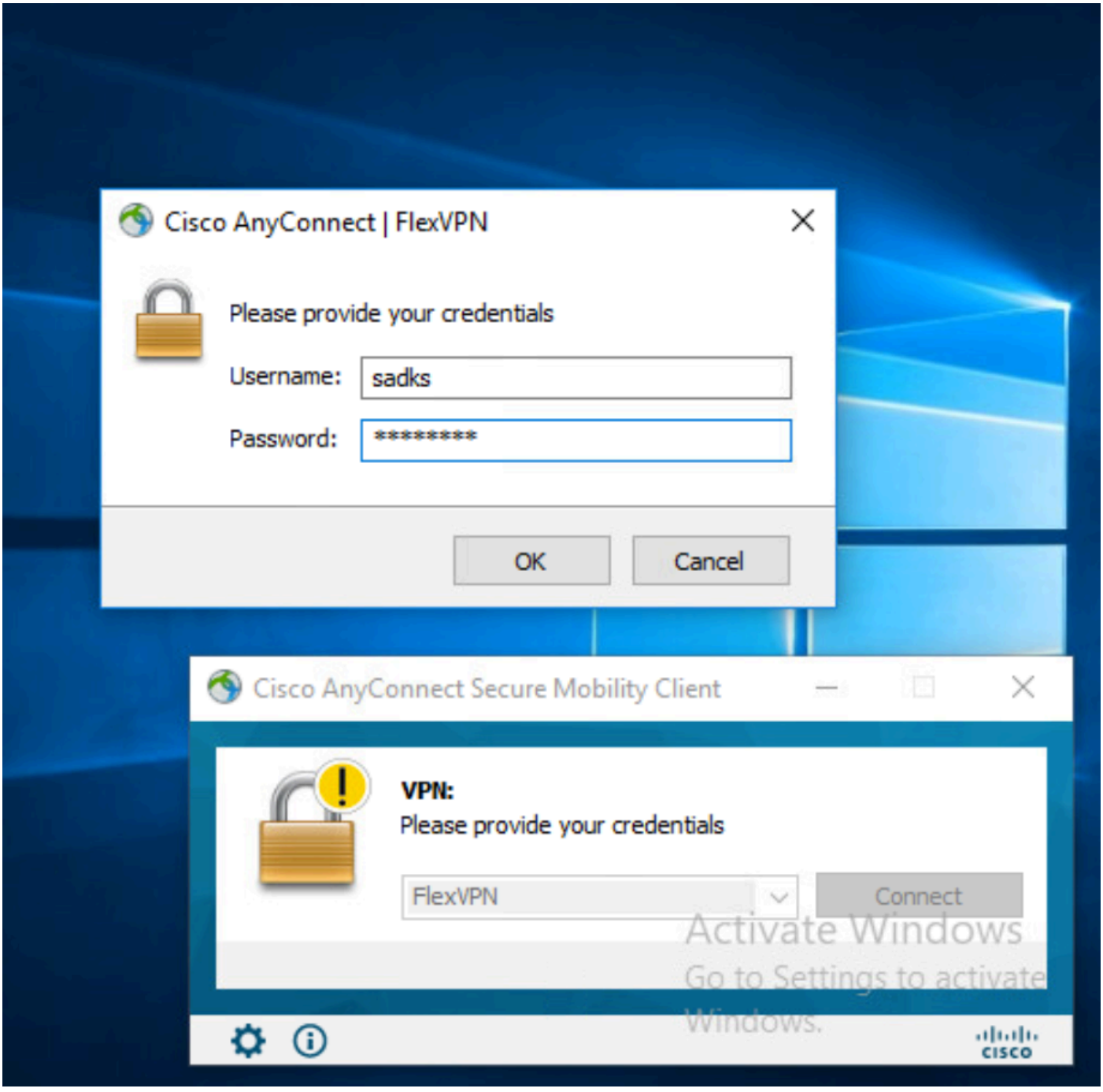


DUO - 장치 연결

다음을 확인합니다.

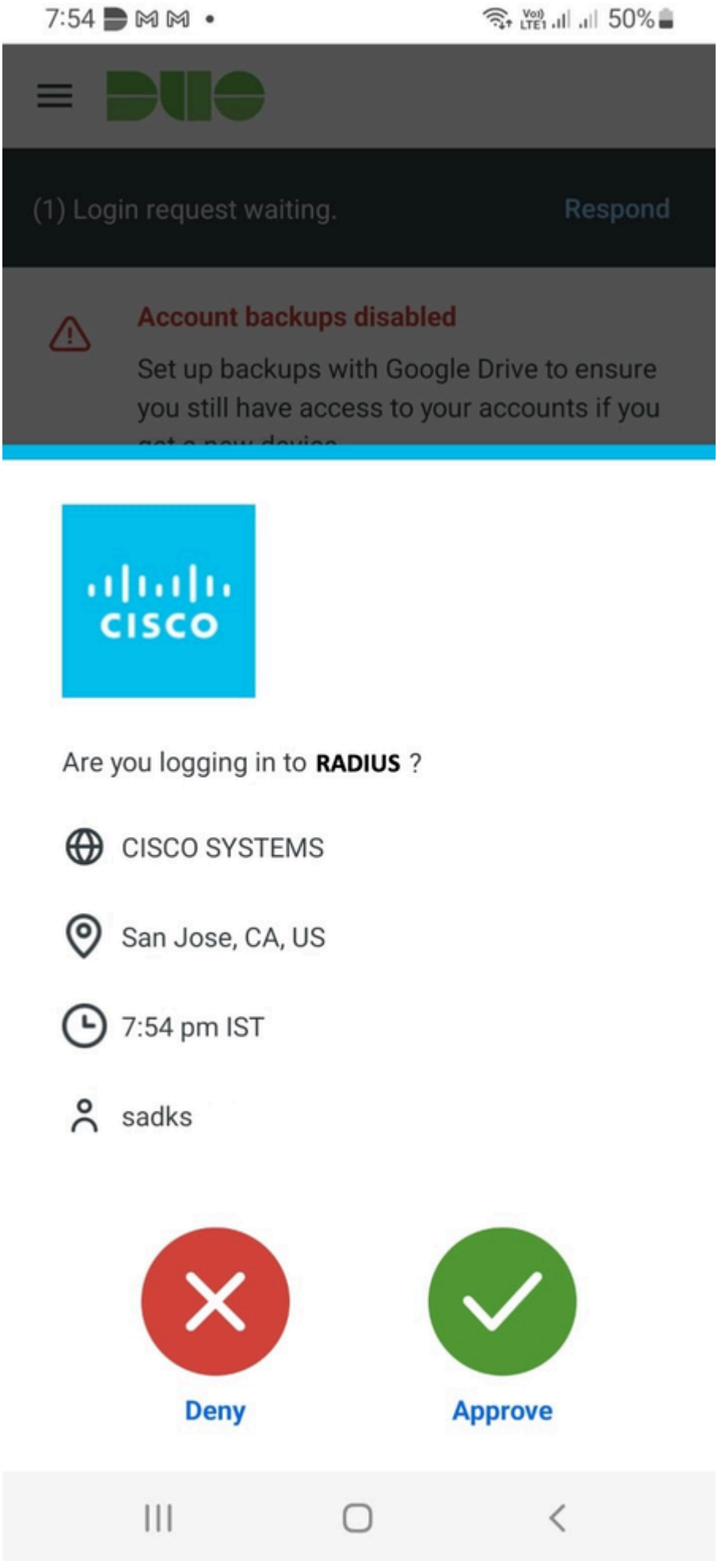
인증을 테스트하려면 AnyConnect를 통해 사용자의 PC에서 C8000V에 연결합니다.

기본 인증을 위한 사용자 이름 및 비밀번호를 입력합니다.



AnyConnect 연결

그런 다음 DUO가 모바일에 푸시하는 것을 수락합니다.


7:54
50%
(1) Login request waiting.
Respond
Account backups disabled
Set up backups with Google Drive to ensure you still have access to your accounts if you
CISCO
Are you logging in to RADIUS ?
CISCO SYSTEMS
San Jose, CA, US
7:54 pm IST
sadks
Deny
Approve

듀오 푸시

<#root>

```
R1#sh crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.54.143/4500    10.197.243.98/54198   none/none
```

READY

```
      Encr: AES-CBC, keysize: 256, PRF: SHA384, Hash: SHA384, DH Grp:19, Auth sign: RSA, Auth verify: Fle
      Life/Active Time: 86400/147 sec
      CE id: 1108, Session-id: 15
      Status Description: Negotiation done
      Local spi: 81094D322A295C92       Remote spi: 802F3CC9E1C33C2F
      Local id: 10.106.54.143
      Remote id: cisco.com
      Remote EAP id:
```

sadks

//

AnyConnect username

```
      Local req msg id:  0              Remote req msg id:  10
      Local next msg id: 0              Remote next msg id: 10
      Local req queued:  0              Remote req queued:  10
      Local window:      5              Remote window:      1
      DPD configured for 60 seconds, retry 2
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
```

Assigned host addr: 192.168.13.5

//Assigned IP address from t

```
      Initiator of SA : No
```

2 . Crypto session detail for the vpn session

<#root>

```
R1#sh crypto session  detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access2
Profile:
```

FlexVPN

-

ikev2_Profile

Uptime: 00:01:07

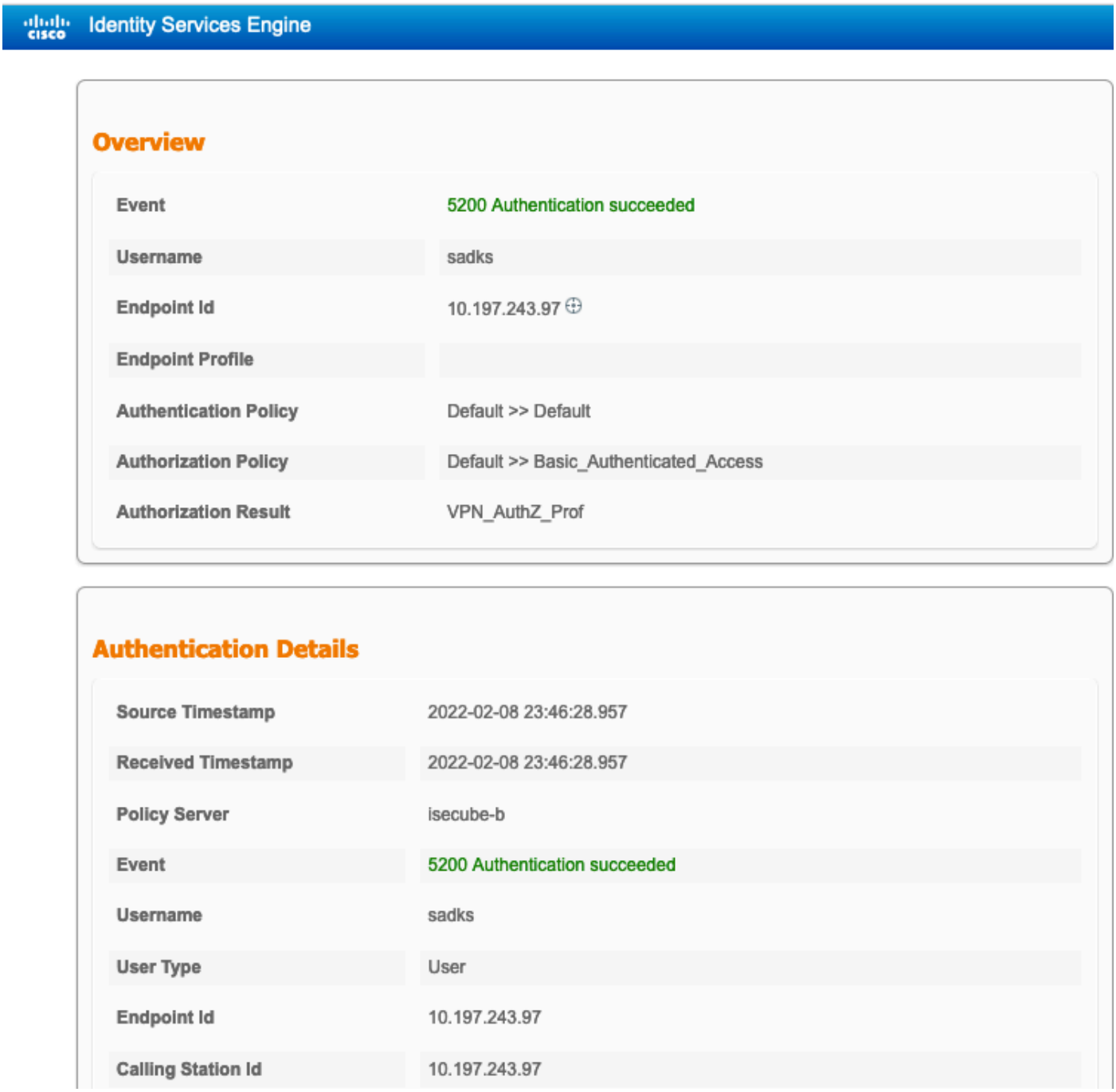
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host
```

192.168.13.5

```
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 3 drop 0 life (KB/Sec) 4607998/3532
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/3532
```

3 .Verification on ISE live logs

ISE에서 로Operations > Live Logs이동합니다. 기본 인증에 대한 인증 보고서를 볼 수 있습니다.



ISE - 라이브 로그

4. Verification on DUO authentication proxy

DUO Authentication Proxy(DUO 인증 프록시)에서 이 파일로 이동합니다. C:\Program Files\Duo Security Authentication Proxy\log

<#root>

```
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info]
 Sending request from 10.106.54.143
 to radius_server_auto
                                                                    //10.106.5
```

```
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info] Received new request id 163 from ('10.106.54
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
login attempt for username 'sadks'

2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info]
Sending request for user 'sadks' to ('10.197.243.116', 1812)

with id 191                                                                    //Primary auth sent t

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.log#info]
Got response for id 191 from ('10.197.243.116', 1812); code 2

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.log#info] http POST to
https://api
-
xxxx[.]duosecurity[.]com:443/rest/v1/preauth

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_Du
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163): Got
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.log#info]
http POST to
https://api
-
xxxx[.]duosecurity[.]com:443/rest/v1/auth

2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_Du
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_Du
2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
Duo authentication returned 'allow': 'Success. Logging you in...'

2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
Returning response code 2: AccessAccept

2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163): Send
2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_Du
```

문제 해결

1. C8000V에서 디버깅

IKEv2의 경우

- debug crypto ikev2
- debug crypto ikev2 client flexvpn
- debug crypto ikev2 internal
- debug crypto ikev2 packet
- debug crypto ikev2 error

IPSec의 경우:

- debug crypto ipsec
- debug crypto ipsec error

2. DUO 인증 프록시의 경우 로그 파일 프록시 관련 로그를 확인합니다. (C:\Program Files\Duo Security Authentication Proxy\log)

ISE가 기본 인증을 거부하는 오류 로그용 코드 조각이 표시됩니다.

<#root>

```
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info]

Sending proxied request

 for id 26 to ('10.197.243.116', 1812) with id 18
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info]

Got response

 for id 18 from ('10.197.243.116', 1812); code 3
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 26):

Primary credentials rejected - No reply message in packet


2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 26): Retur

AccessReject
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.