

ISE 관리 액세스를 위한 Duo Two Factor Authentication 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[구성](#)

[Duo 구성](#)

[ISE 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 ISE(Identity Services Engine) 관리 액세스를 위한 외부 2단계 인증을 구성하는 데 필요한 단계에 대해 설명합니다. 이 예에서는 ISE 관리자가 RADIUS 토큰 서버에 대해 인증하고 푸시 알림 형태의 추가 인증이 Duo 인증 프록시 서버에서 관리자의 모바일 디바이스로 전송됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 프로토콜
- ISE RADIUS 토큰 서버 및 ID 구성

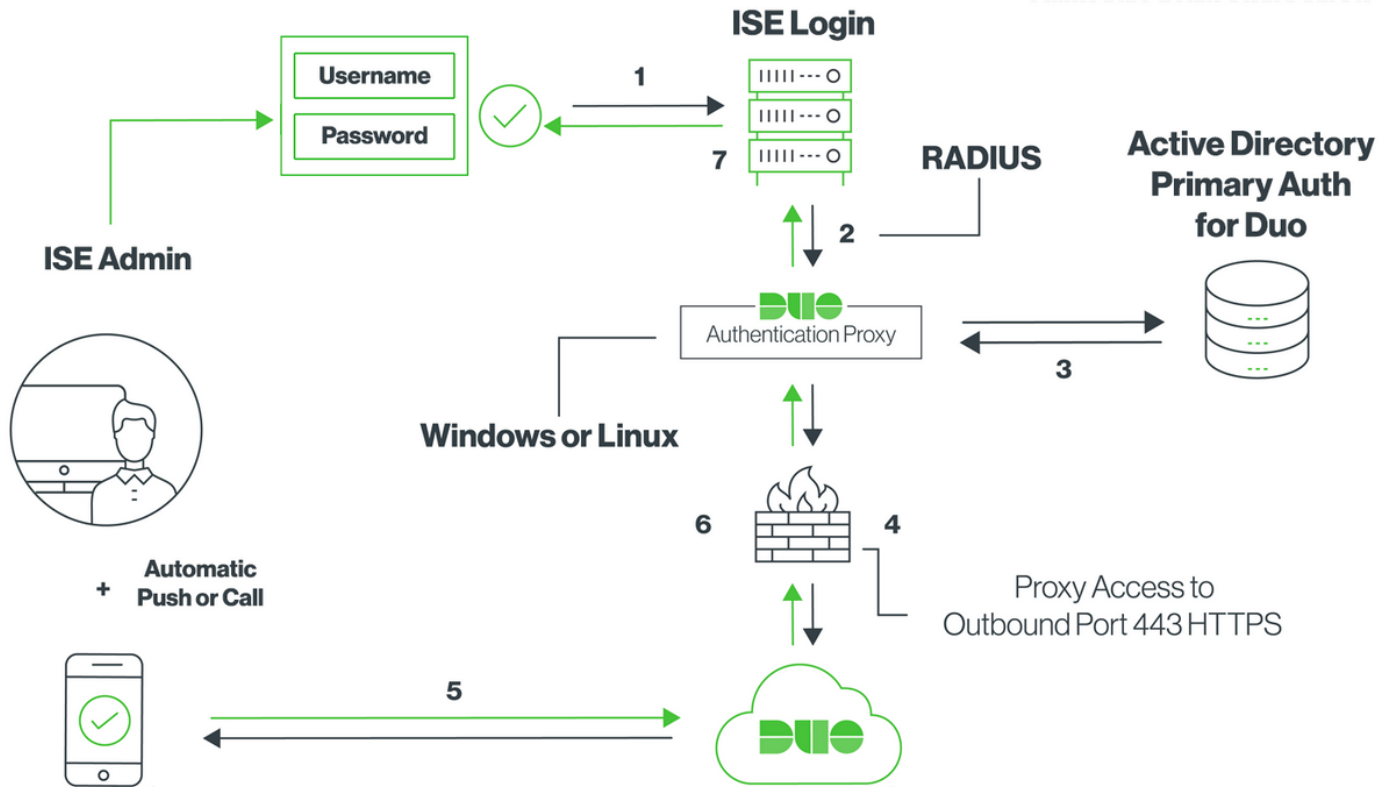
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine)
- AD(Active Directory)
- Duo 인증 프록시 서버
- Duo 클라우드 서비스

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.

네트워크 다이어그램



구성

Duo 구성

1단계. Windows 또는 Linux 시스템에 Duo Authentication Proxy Server 다운로드 및 설치:
<https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy>

참고: 이 시스템은 ISE 및 Duo 클라우드(인터넷)에 액세스할 수 있어야 합니다.

2단계. authproxy.cfg 파일을 구성합니다.

Notepad+ 또는 WordPad와 같은 텍스트 편집기에서 이 파일을 엽니다.

참고: 기본 위치는 C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg에 있습니다.

3단계. Duo Admin Panel에서 "Cisco ISE RADIUS" 애플리케이션을 생성합니다
<https://duo.com/docs/ciscoise-radius#first-steps>

4단계. authproxy.cfg 파일을 편집하고 이 구성을 추가합니다.

```

ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com
    
```

```
radius_ip_1=10.127.196.189
radius_secret_1=*****
failmode=secure
client=ad_client
port=1812
```

Sample IP address of the ISE server

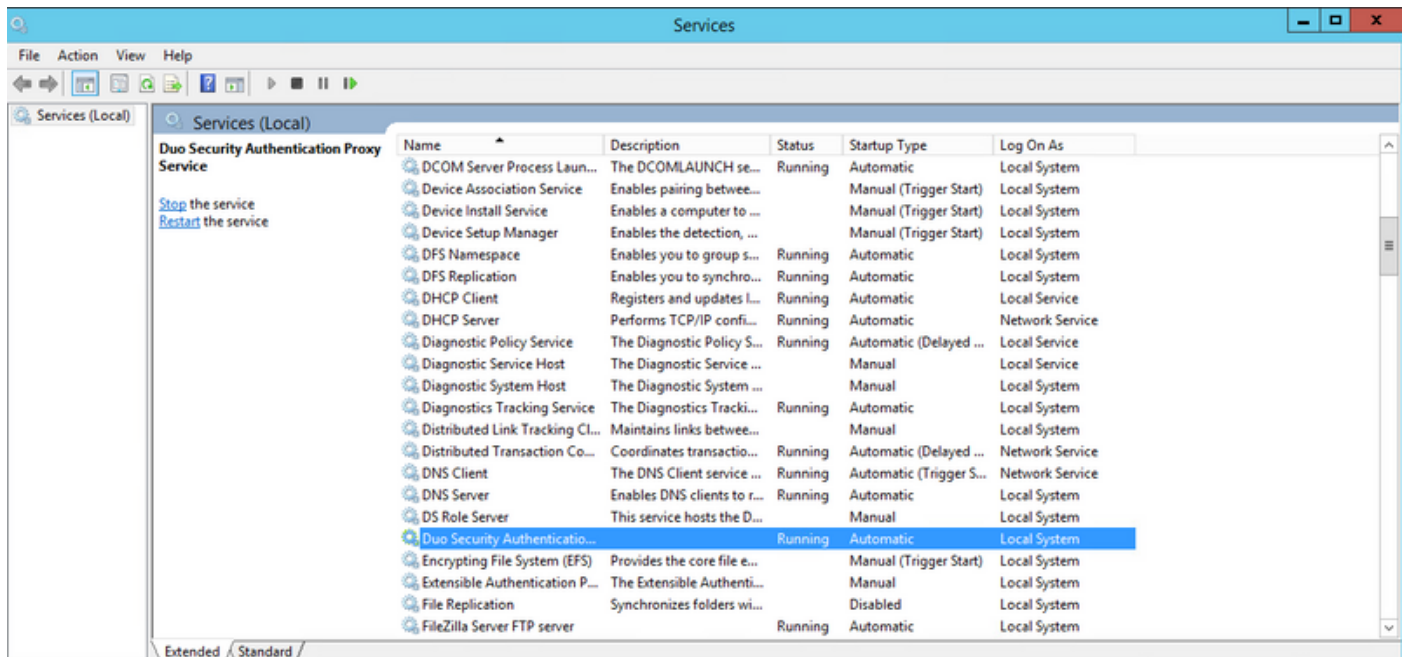
5단계. ad_client를 Active Directory 세부 정보로 구성합니다. Duo Auth Proxy는 기본 인증을 위해 아래 정보를 사용하여 AD에 대해 인증합니다.

```
[ad_client]
host=10.127.196.230
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

Sample IP address of the Active Directory


참고: 네트워크에 인터넷 액세스를 위해 HTTP 프록시 연결이 필요한 경우 authproxy.cfg에 http_proxy 세부 정보를 추가합니다.

6단계. Duo 보안 인증 프록시 서비스를 다시 시작합니다. 파일을 저장하고 Windows 시스템에서 Duo 서비스를 다시 시작합니다. Windows 서비스 콘솔(services.msc)을 열고 서비스 목록에서 Duo 보안 인증 프록시 서비스를 찾은 다음 이미지에 표시된 대로 다시 시작을 클릭합니다.



7단계. 사용자 이름을 생성하고 엔드 디바이스에서 Duo Mobile을 활성화합니다
<https://duo.com/docs/administration-users#creating-users-manually>

Duo Admin Panel에서 사용자를 추가합니다. 이미지에 표시된 대로 Users(사용자) > add users(사용자 추가)로 이동합니다.



- Dashboard
- Policies
- Applications
- Users**
- Add User
- Pending Enrollments
- Bulk Enroll Users
- Import Users
- Directory Sync
- Bypass Codes
- 2FA Devices
- Groups
- Administrators
- Reports

[Dashboard](#) > [Users](#) > Add User

Add User

Adding Users

Most applications allow users to enroll themselves after they complete primary authentication.

[Learn more about adding users](#) ↗

Username


Should match the primary authentication username.

최종 사용자에게 전화기에 Duo 앱이 설치되어 있는지 확인합니다.

Phones Add Phone

You may rearrange the phones by dragging and dropping in the table.

This user has no phones. [Add one.](#)



- Dashboard
- Policies
- Applications
- Users**
- Add User
- Pending Enrollments
- Bulk Enroll Users
- Import Users
- Directory Sync
- Bypass Codes
- 2FA Devices

[Dashboard](#) > [Users](#) > [duoadmin](#) > Add Phone

Add Phone

Type

Phone
 Tablet

Phone number [Show extension field](#)

이미지에 표시된 대로 Activate **Duo Mobile**을 선택합니다.

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone

이미지에 표시된 대로 **Generate Duo Mobile Activation Code**를 선택합니다.

Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: after generation

[Generate Duo Mobile Activation Code](#)

이미지에 표시된 대로 **Send Instructions by SMS(SMS로 지침 보내기)**를 선택합니다.

Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone: Generic Smartphone

Installation instructions Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile:

[Send Instructions by SMS](#) or [skip this step](#)

SMS에서 링크를 클릭하면 Duo 앱이 이미지에 표시된 대로 **Device Info** 섹션의 사용자 계정에 연결됩니다.

The screenshot shows the Cisco Duo Mobile interface. On the left is a navigation menu with options: Dashboard, Policies, Applications, Users, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Groups, Administrators, Reports, Settings, and Billing. The main content area shows a search bar at the top, a breadcrumb trail 'Dashboard > Phones > Phone: [redacted]', and a 'Send SMS' button. Below this is a user profile card for 'duoadmin (NANCY)' with a green profile icon and a link to 'Attach a user'. A note states 'Authentication devices can share multiple users'. The 'Device Info' section shows the device is using Duo Mobile 3.28.0, last seen 29 minutes ago, and is an Android 8.0.0 device.

ISE 컨피그레이션

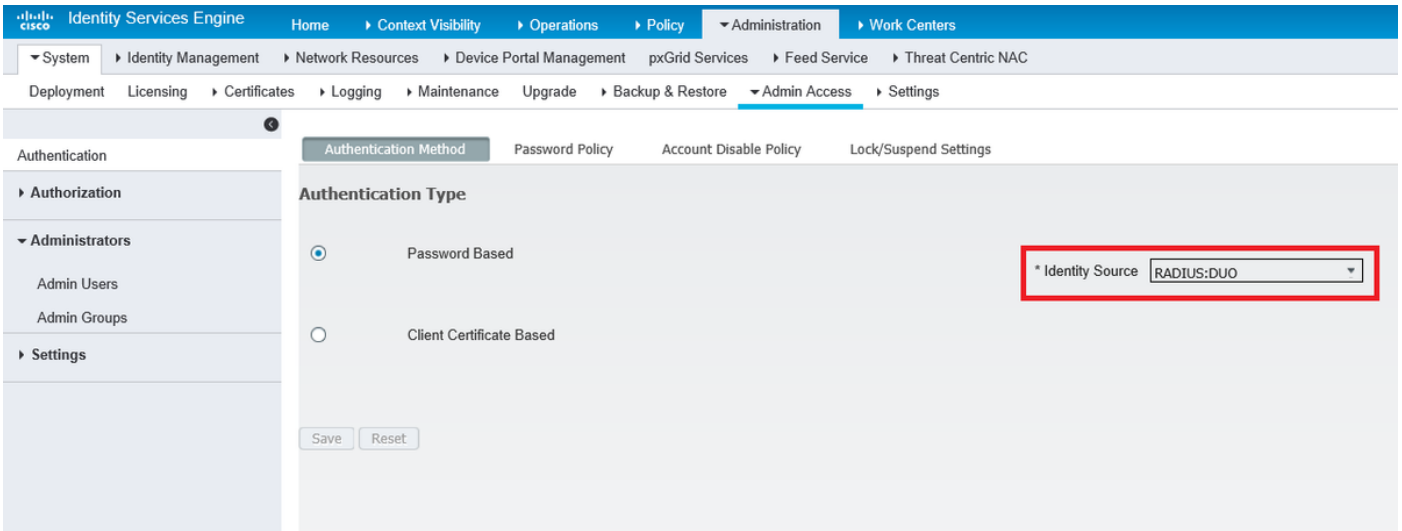
1단계. ISE를 Duo 인증 프록시와 통합합니다.

Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > RADIUS Token(RADIUS 토큰)으로 이동하여 Add(추가)를 클릭하여 새 RADIUS 토큰 서버를 추가합니다. 이미지에 표시된 대로 [일반] 탭, [연결] 탭의 [IP 주소] 및 [공유 키]에서 서버 이름을 정의합니다.

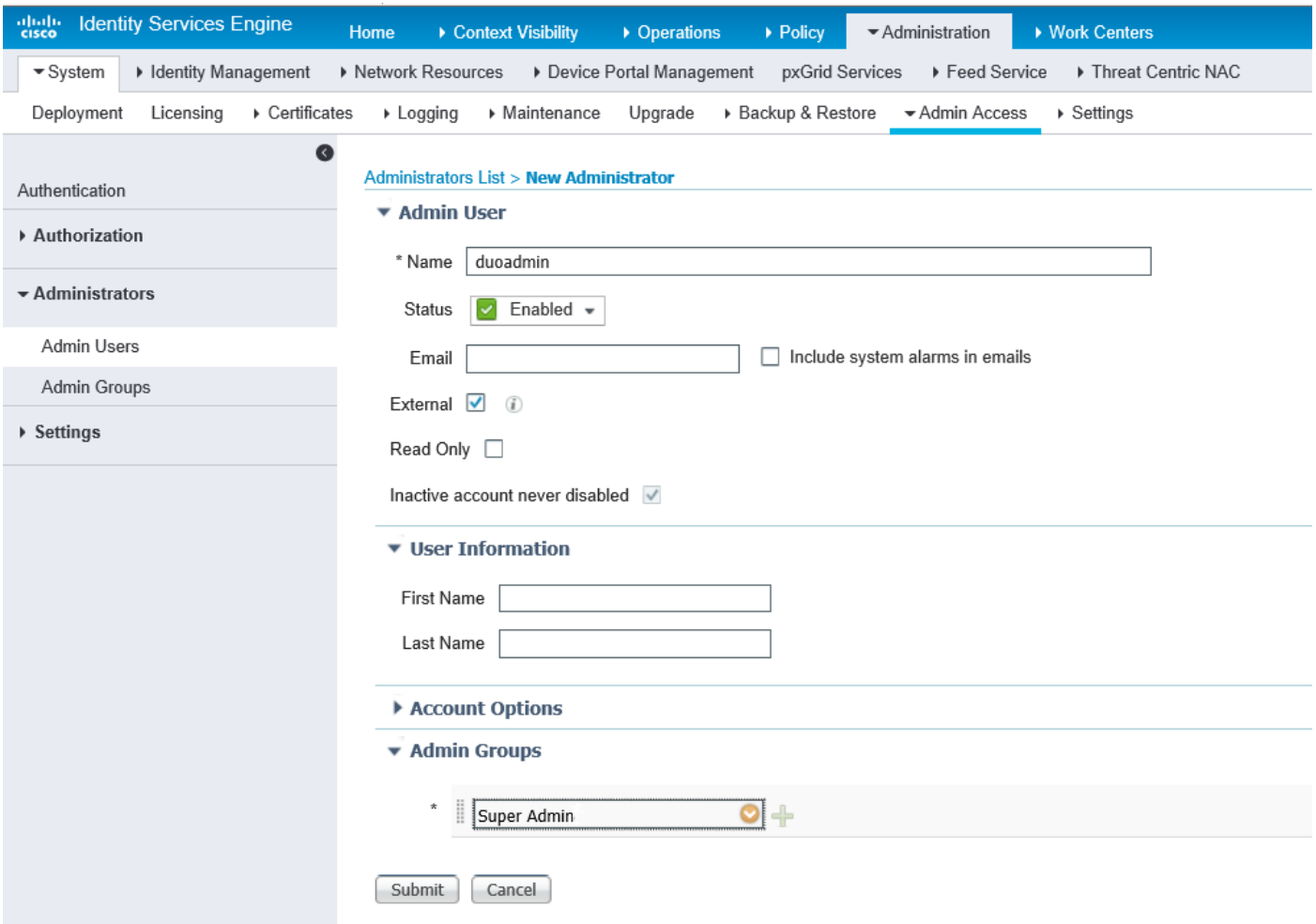
:Server Timeout() 60 .

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is 'Administration > Work Centers > External Identity Sources > Identity Source Sequences > Settings'. The left sidebar shows 'External Identity Sources' with a tree view including Certificate Authentication Profile, Active Directory, RADIUS Token (selected), and Social Login. The main content area is titled 'RADIUS Token List > DUO' and shows the configuration for a 'RADIUS Token Identity Source'. The 'Connection' tab is active, showing 'Server Connection' options (Safeword Server, Enable Secondary Server, Fallback to Primary Server after 5 minutes) and 'Primary Server' and 'Secondary Server' configuration fields. The Primary Server fields are: Host IP (10.127.196.230), Shared Secret (masked), Authentication Port (1812), Server Timeout (60 seconds), and Connection Attempts (3). The Secondary Server fields are: Host IP (empty), Shared Secret (masked), Authentication Port (1812), Server Timeout (5 seconds), and Connection Attempts (3). 'Save' and 'Reset' buttons are at the bottom.

2단계. 이미지에 표시된 대로 Administration(관리) > System(시스템) > Admin Access(관리 액세스) > Authentication(인증) > Authentication Method(인증 방법)로 이동하고 이전에 구성한 RADIUS 토큰 서버를 ID 소스로 선택합니다.



3단계. 다음 이미지에 표시된 대로 Administration(관리) > System(시스템) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Users(관리자 사용자)로 이동하고 관리자 사용자를 External(외부)로 생성하고 슈퍼 관리자 권한을 제공합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ISE GUI를 열고 RADIUS 토큰 서버를 ID 소스로 선택하고 관리자 사용자로 로그인합니다.



Identity Services Engine

Username

Password

Identity Source

[Problem logging in?](#)

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

클라우드 또는 Active Directory의 Duo 프록시 연결과 관련된 문제를 해결하려면 authproxy.cfg의 주 섹션 아래에 "debug=true"를 추가하여 Duo Auth Proxy에서 디버깅을 활성화합니다.

로그는 다음 위치에 있습니다.

C:\Program Files (x86)\Duo 보안 인증 프록시\log

Notepad++ 또는 WordPad와 같은 텍스트 편집기에서 **authproxy.log** 파일을 엽니다.

ISE에서 요청을 수신하고 Duo Cloud로 전송하는 Duo Auth Proxy의 코드 조각을 기록합니다.

```
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending request from 10.127.196.189 to radius_server_auto
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Received new request id 2 from ('10.127.196.189', 62001)
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] (('10.127.196.189', 62001), duoadmin, 2): login attempt for username u'duoadmin'
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending AD authentication request for 'duoadmin' to '10.127.196.230'
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory
```


Duo 인증 프록시의 로그 조각이 Duo 클라우드에 연결할 수 없습니다.

```
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping
factory
2019-08-19T04:59:37-0700 [-] Duo preauth call failed
Traceback (most recent call last):
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "twisted\internet\defer.pyc", line 1475, in getResult
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\radius\duo_server.pyc", line 111, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 246, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 202, in call
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "duoauthproxy\lib\duo_async.pyc", line 186, in err_func
duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: DNSLookupError('api-
xxxxxxxxx.duosecurity.com',)

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied
Duo login on preauth failure
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Returning response code
3: AccessReject
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Sending response
```

관련 정보

- [DUO를 사용한 RA VPN 인증](#)
- [기술 지원 및 문서 - Cisco Systems](#)