

ISE管理アクセス用のDuo Two Factor Authenticationの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[Duo設定](#)

[ISE の設定](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

このドキュメントでは、Identity Services Engine(ISE)管理アクセスの外部2要素認証を設定するために必要な手順について説明します。この例では、ISE管理者がRADIUSトークンサーバに対して認証を行い、プッシュ通知の形式の追加認証がDuo Authentication Proxyサーバによって管理者のモバイルデバイスに送信されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- RADIUS プロトコル
- ISE RADIUSトークンサーバとIDの設定

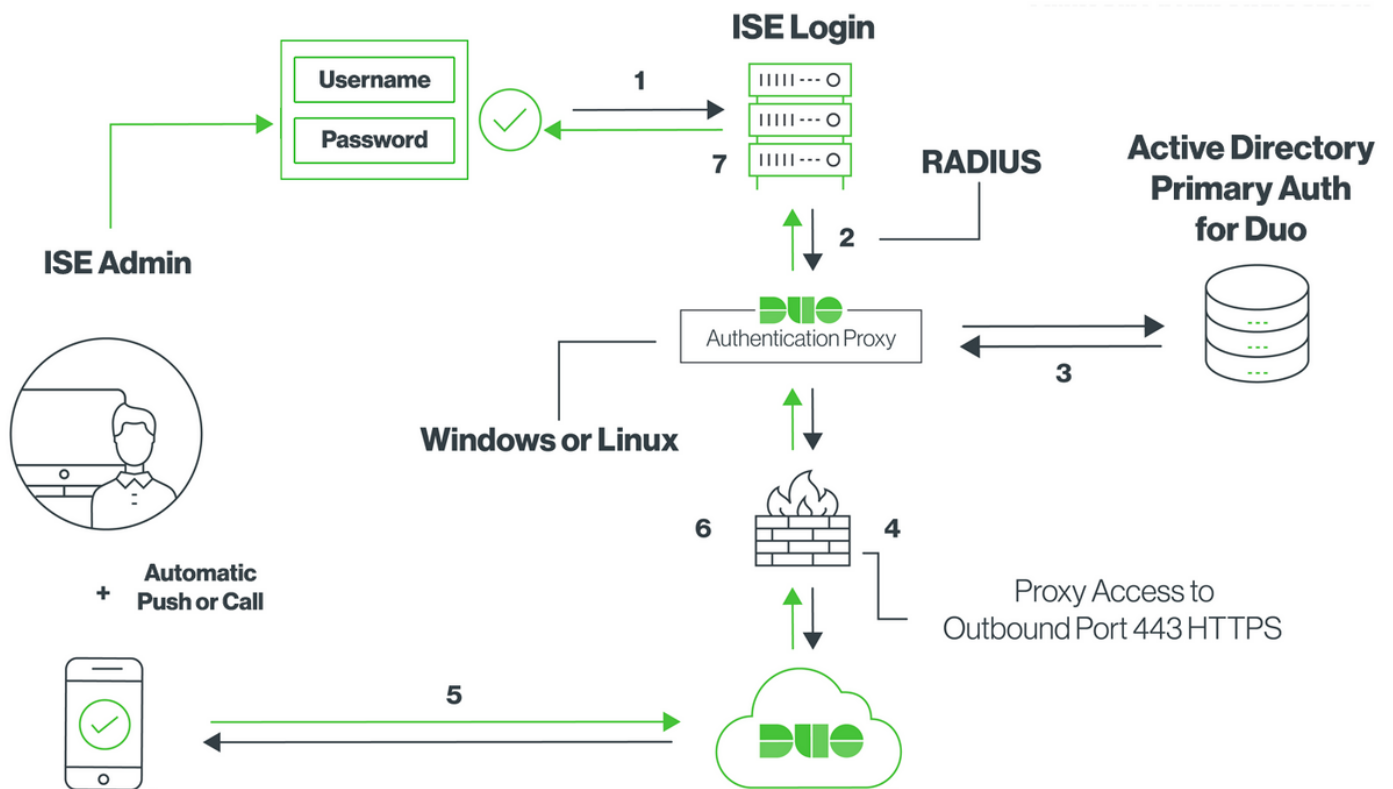
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo認証プロキシサーバ
- Duo Cloud Service

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図



コンフィギュレーション

Duo設定

ステップ1: WindowsまたはLinuxマシンでのDuo認証プロキシサーバのダウンロードとインストール : <https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy>

注：このマシンは、ISEおよびDuoクラウド（インターネット）にアクセスできる必要があります

ステップ2: authproxy.cfgファイルを設定します。

このファイルをメモ帳++やワードパッドなどのテキストエディタで開きます。

注：デフォルトの場所はC:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

ステップ3 Duo Admin Panelで「Cisco ISE RADIUS」アプリケーションを作成します。
<https://duo.com/docs/ciscoise-radius#first-steps>

ステップ4: authproxy.cfgファイルを編集し、この設定を追加します。

```
ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```


The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation links: Dashboard, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, Administrators, and Reports. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form field for "Username" containing the text "duoadmin". A note below the field says "Should match the primary authentication username." At the bottom of the form is a blue button labeled "Add User".

エンドユーザにDuoアプリが電話機にインストールされていることを確認します。

The screenshot shows the "Phones" section of the Duo Admin console. The heading is "Phones". Below it is the text "You may rearrange the phones by dragging and dropping in the table." In the top right corner is a blue button labeled "Add Phone". The main content area is a large empty box with the text "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous screenshot, but the "Users" section is expanded to show "Add User" (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, and 2FA Devices. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: Dashboard > Users > duoadmin > Add Phone. The main heading is "Add Phone". The "Type" section has two radio buttons: "Phone" (selected) and "Tablet". Below this is a form field for "Phone number" containing a dropdown menu with the US flag and the text "+1 201-555-5555". To the right of the field is a link "Show extension field". At the bottom of the form is a blue button labeled "Add Phone".

図に示すように[Activate Duo Mobile]を選択します。

Device Info



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

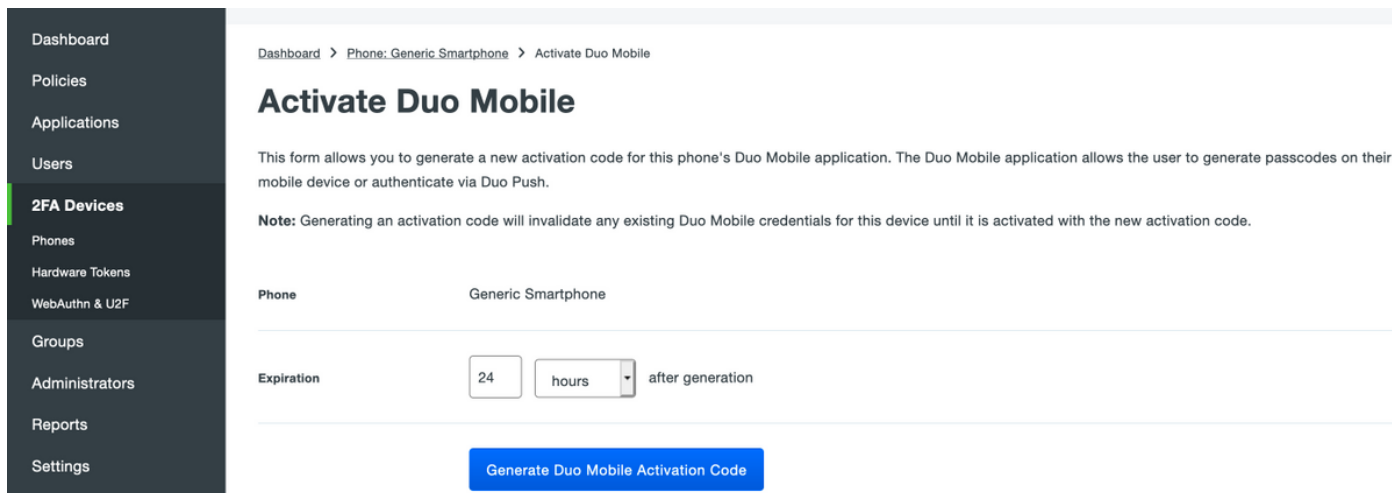


Model
Unknown



OS
Generic Smartphone

図に示すように、[Generate Duo Mobile Activation Code]を選択します。



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.

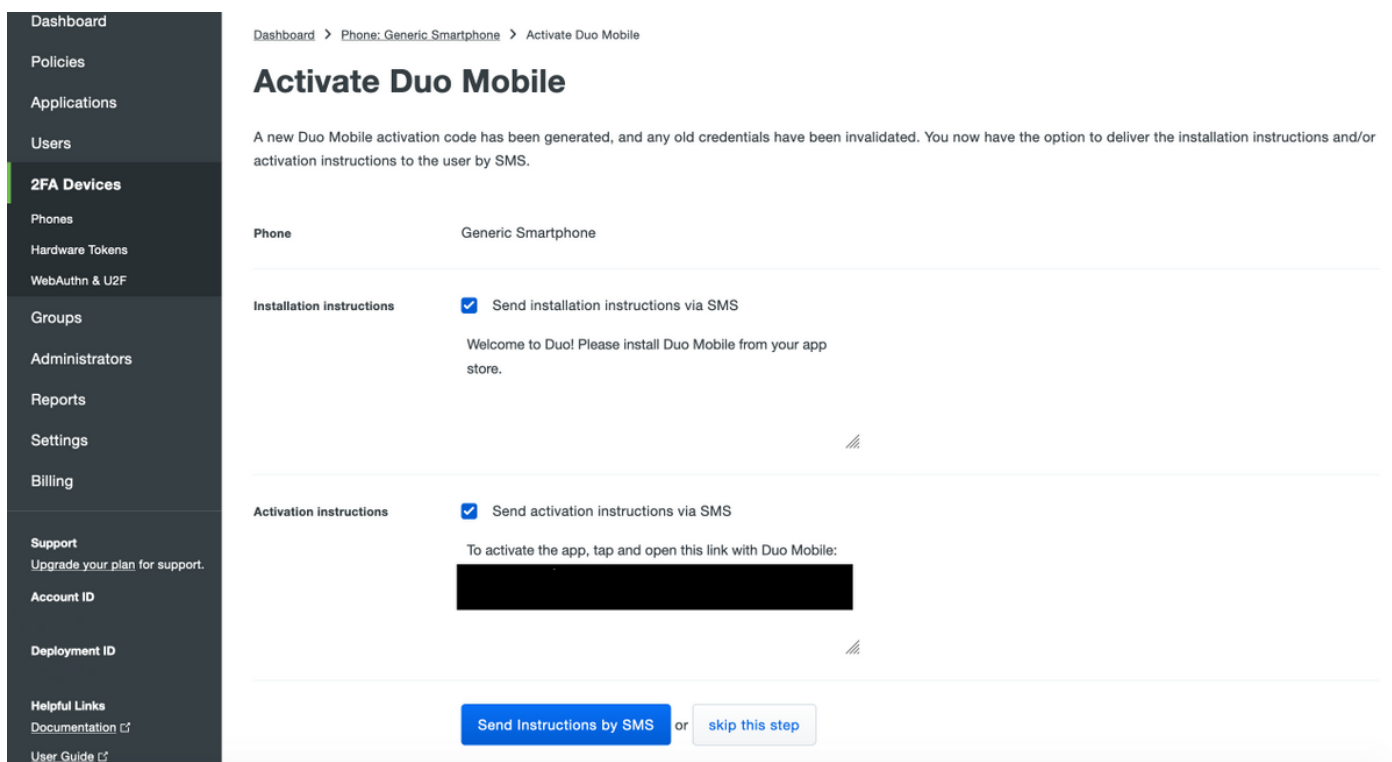
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

図に示すように、[Send Instructions by SMS]を選択します。



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](#)

SMS内のリンクをクリックすると、Duoアプリは次の図に示すように、[Device Info]セクションのユーザアカウントにリンクされます。

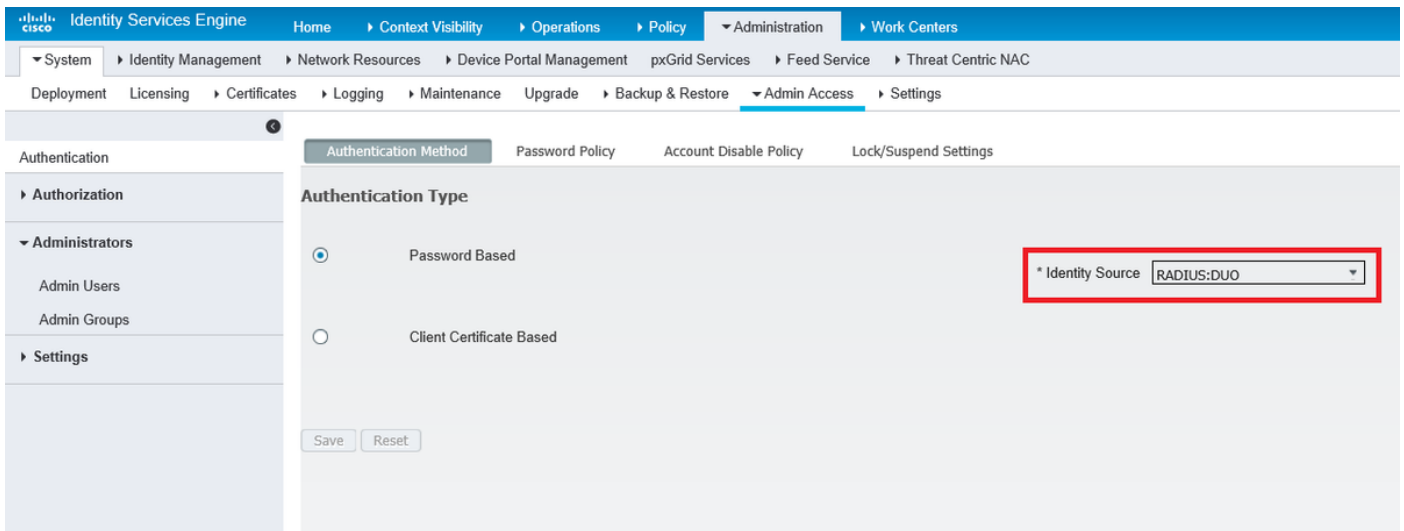
ISE の設定

ステップ1: ISEとDuo認証プロキシを統合します。

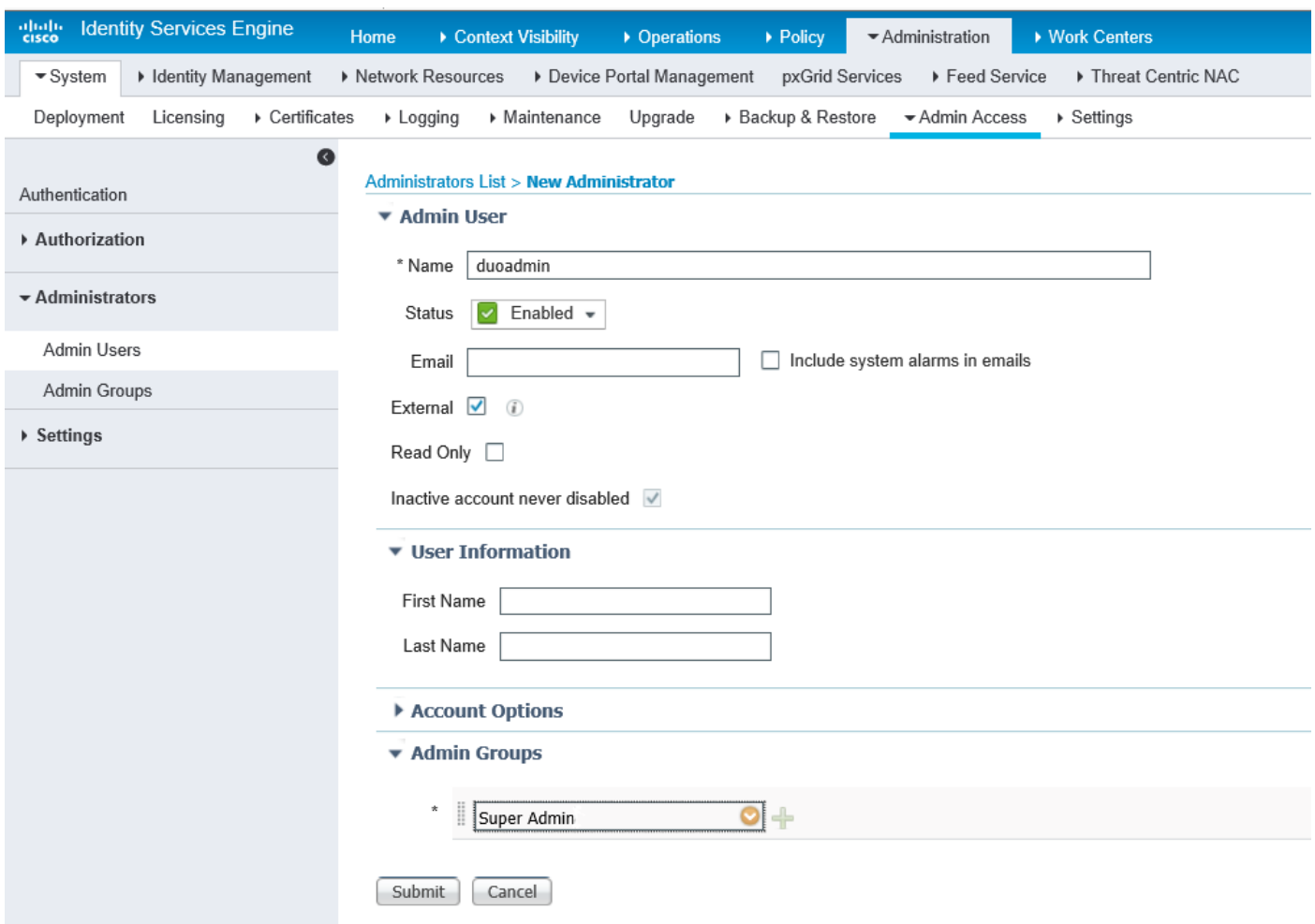
[Administration] > [Identity Management] > [External Identity Sources] > [RADIUS Token]に移動し、[Add]をクリックして新しいRADIUSトークンサーバを追加します。図に示すように、[general]タブでサーバ名、[IP address]タブで共有キーを定義します。

[Server Timeout]60

ステップ2 : 図に示すように、[Administration] > [System] > [Admin Access] > [Authentication] > [Authentication Method]に移動し、以前に設定したRADIUSトークンサーバを[Identity Source]として選択します。



ステップ3 : 図に示すように、[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Users]に移動し、管理ユーザを[External]として作成し、スーパー管理者権限を付与します。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

ISE GUIを開き、[ID Source]として[RADIUS Token Server]を選択し、adminユーザでログインします。



Identity Services Engine

Username

Password

Identity Source

[Problem logging in?](#)

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

クラウドまたはActive DirectoryとのDuoプロキシ接続に関連する問題をトラブルシューティングするには、authproxy.cfgのメインセクションに「debug=true」を追加して、Duo認証プロキシのデバッグを有効にします。

ログは次の場所にあります。

C:\Program Files (x86)\Duo Security Authentication Proxy\log

メモ帳++やWordPadなど、テキストエディタでauthproxy.logファイルを開きます。

ISEから要求を受信してDuo Cloudに送信するDuo Auth Proxyのログスニペット。

```
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 Auth ProxyのログスニペットがDuo Cloudに到達できません。

```
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
```

関連情報

- [DUOを使用したRA VPN認証](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)