

Konfigurieren der Duo Two-Factor-Authentifizierung für den ISE Management Access

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Duo-Konfiguration](#)

[ISE-Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration einer externen Zwei-Faktor-Authentifizierung für den ISE-Managementzugriff (Identity Services Engine) beschrieben. In diesem Beispiel authentifiziert sich der ISE-Administrator anhand des RADIUS-Token-Servers, und eine zusätzliche Authentifizierung in Form von Push-Benachrichtigung wird vom Duo Authentication Proxy-Server an das Mobilgerät des Administrators gesendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- RADIUS-Protokoll
- Konfigurieren des ISE RADIUS Token-Servers und der Identitäten

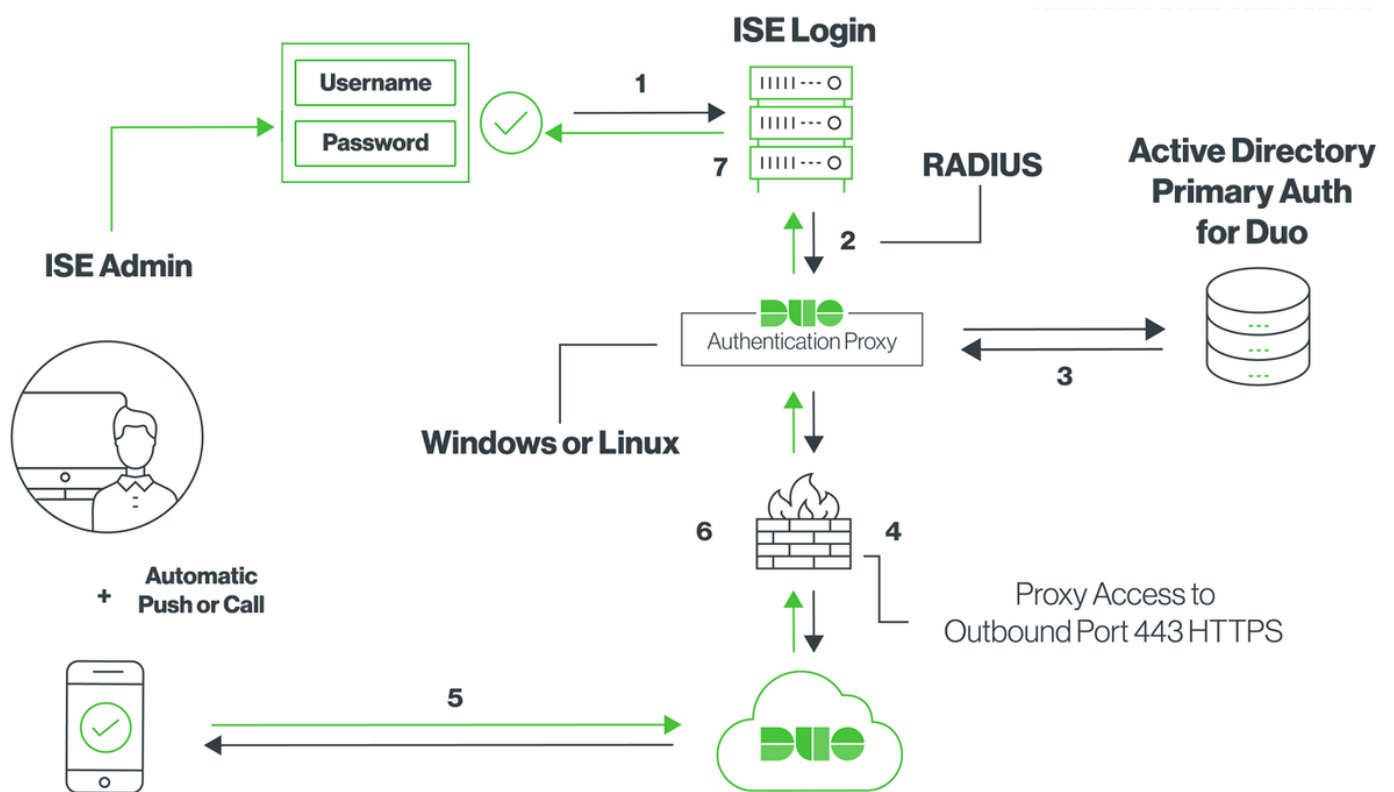
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo-Authentifizierungsproxyserver
- Duo Cloud-Service

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm



Konfiguration

Duo-Konfiguration

Schritt 1: Download und Installation des Duo Authentication Proxy Servers auf einem Windows- oder Linux-Computer: <https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy>

Hinweis: Dieser Computer muss Zugriff auf die ISE und die Duo Cloud (Internet) haben.

Schritt 2: Konfigurieren Sie die Datei `authproxy.cfg`.

Öffnen Sie diese Datei in einem Texteditor wie Notepad++ oder WordPad.

Hinweis: Der Standardspeicherort finden Sie unter `C:\Program Files (x86)\Duo Security AuthenticationProxy\conf\authproxy.cfg`

Schritt 3: Erstellen Sie im Duo Admin Panel eine Cisco ISE RADIUS-Anwendung: <https://duo.com/docs/ciscoise-radius#first-steps>

Schritt 4: Bearbeiten Sie die Datei `authproxy.cfg`, und fügen Sie diese Konfiguration hinzu.

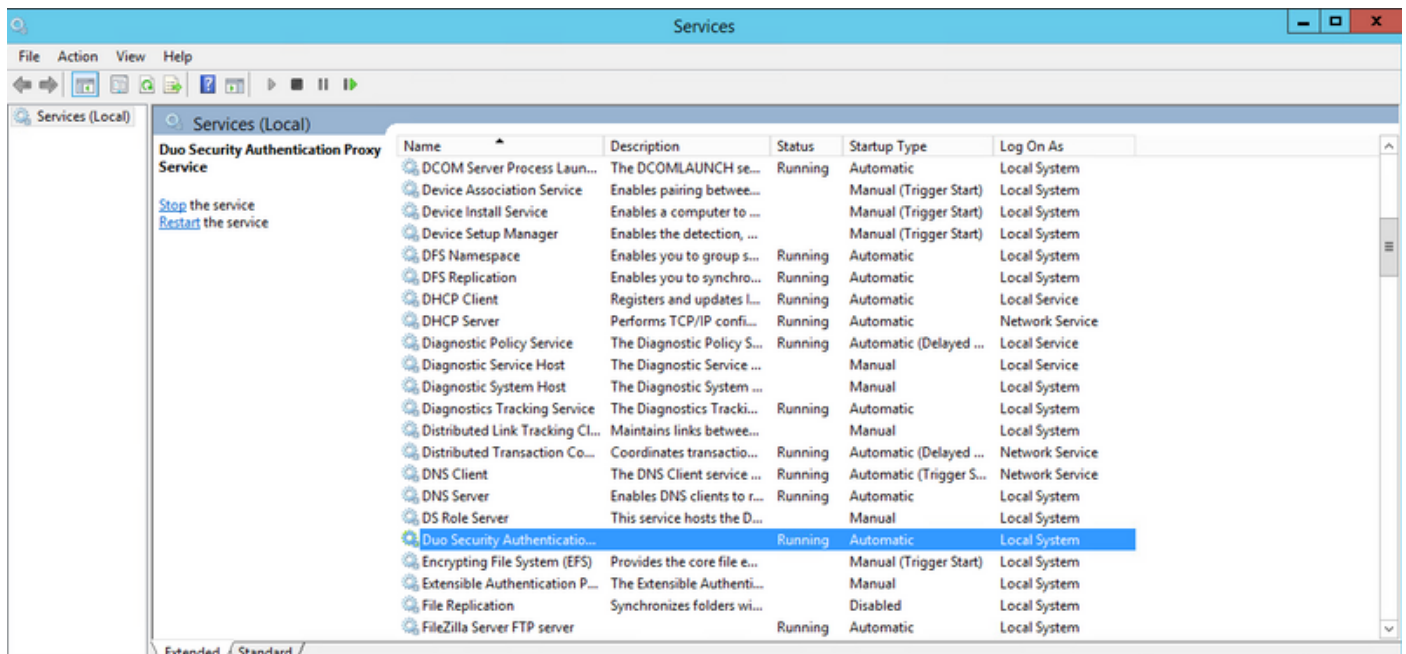
```
ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
skkey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189 Sample IP address of the ISE server
radius_secret_1=*****
failmode=secure
client=ad_client
port=1812
```

Schritt 5: Konfigurieren Sie `ad_client` mit Ihren Active Directory-Details. Duo Auth Proxy verwendet die folgenden Informationen, um sich für die primäre Authentifizierung gegen AD zu authentifizieren.

```
[ad_client]
host=10.127.196.230 Sample IP address of the Active Directory
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

Hinweis: Wenn Ihr Netzwerk HTTP-Proxyverbindungen für den Internetzugriff benötigt, fügen Sie `http_proxy`-Details in `authproxy.cfg` hinzu.

Schritt 6: Starten Sie den Duo Security Authentication Proxy Service neu. Speichern Sie die Datei, und **starten Sie den Duo-Dienst** auf dem Windows-Computer neu. Öffnen Sie die Windows Services-Konsole (`services.msc`), suchen Sie in der Liste der Dienste den **Duo Security Authentication Proxy Service**, und klicken Sie auf **Neu starten**, wie im Bild gezeigt:



Schritt 7: Erstellen Sie einen Benutzernamen, und aktivieren Sie Duo Mobile auf dem Endgerät: <https://duo.com/docs/administration-users#creating-users-manually>

Fügen Sie Benutzer in der Duo-Administrationskonsole hinzu. Navigieren Sie zu **Benutzer > Benutzer hinzufügen**, wie im Bild gezeigt:

The screenshot shows the Duo Admin interface. On the left is a dark sidebar with the Duo logo and navigation items: 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 it 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 with a "Username" label and a text input field containing "duoadmin". A note below the field says "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

Stellen Sie sicher, dass die Duo-App auf dem Telefon installiert ist.

The screenshot shows the "Phones" section of the Duo Admin interface. It has a heading "Phones" and a sub-heading "You may rearrange the phones by dragging and dropping in the table." On the right is a blue "Add Phone" button. Below this is a large empty box with the text "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin interface for adding a phone. The sidebar is the same as in the previous screenshot, but "Users" is highlighted and "Add User" is selected. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: "Dashboard > Users > duoadmin > Add Phone". The main heading is "Add Phone". Under "Type", there are two radio buttons: "Phone" (selected) and "Tablet". Below this is a form with a "Phone number" label and a text input field containing "+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 "Add Phone" button.

Wählen Sie **ActivateDuo Mobile** aus, wie im Bild gezeigt:

Device Info



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



Model
Unknown



OS
Generic Smartphone

Wählen Sie Duo Mobile Activation Code generieren, wie im Bild gezeigt:

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](#)

Wählen Sie Anweisungen per SMS senden aus, wie im Bild gezeigt:

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](#)

Klicken Sie auf den Link in der SMS, und die Duo-App wird mit dem Benutzerkonto im Bereich Device Info verknüpft, wie im Bild gezeigt:

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications, Users, **2FA Devices** (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Groups, Administrators, Reports, Settings, and Billing. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices" and "Cisco Systems | ID:". Below the search bar is a breadcrumb trail: "Dashboard > Phones > Phone: [redacted]". A "Send SMS" button is visible on the right. The main content area displays a user profile for "duoadmin (NANCY)" with a green profile icon, a "Attach a user" link, and a note: "Authentication devices can share multiple users". Below this is a "Device Info" section with three cards: "Using Duo Mobile 3.28.0" with a "Reactivate Duo Mobile" link and "Last Seen 29 minutes ago"; "Model [redacted]"; and "OS Android 8.0.0".

ISE-Konfiguration

Schritt 1: Integrieren Sie die ISE in Duo Auth Proxy.

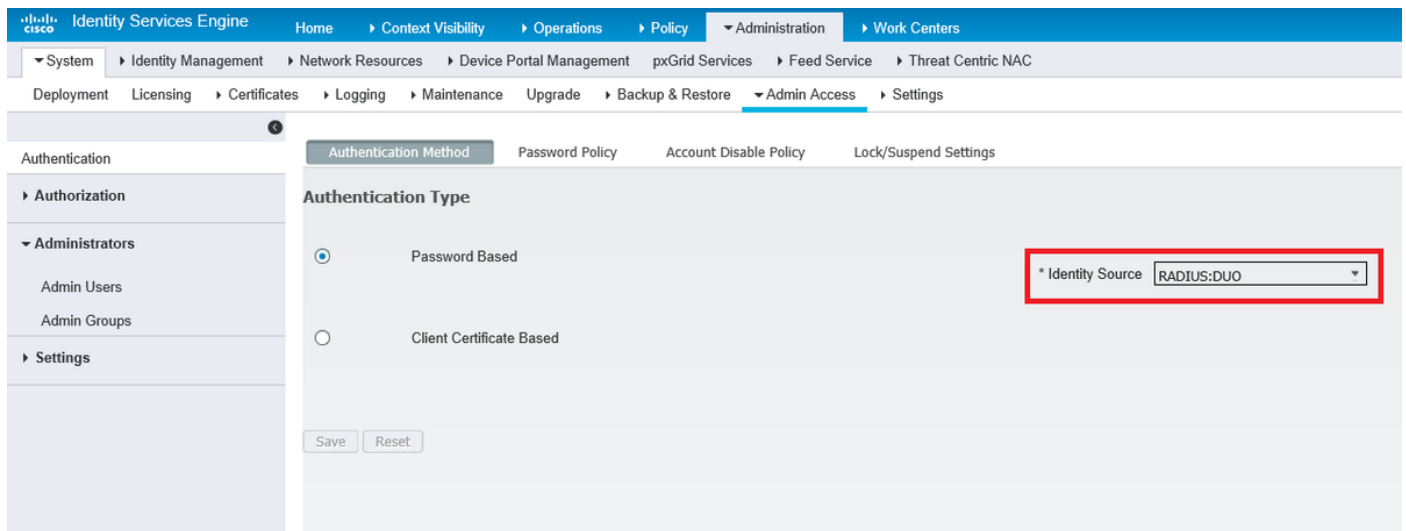
Navigieren Sie zu **Administration > Identity Management > External Identity Sources > RADIUS Token**, und klicken Sie auf **Add**, um einen neuen RADIUS Token-Server hinzuzufügen. Definieren Sie den Servernamen in der Registerkarte "Allgemein", die IP-Adresse und den gemeinsamen Schlüssel in der Registerkarte "Verbindung", wie im Bild gezeigt:

Hinweis: Legen Sie die Server-Timeout-Einstellung auf 60 Sekunden fest, sodass die Benutzer genügend Zeit haben, auf den Push zu reagieren.

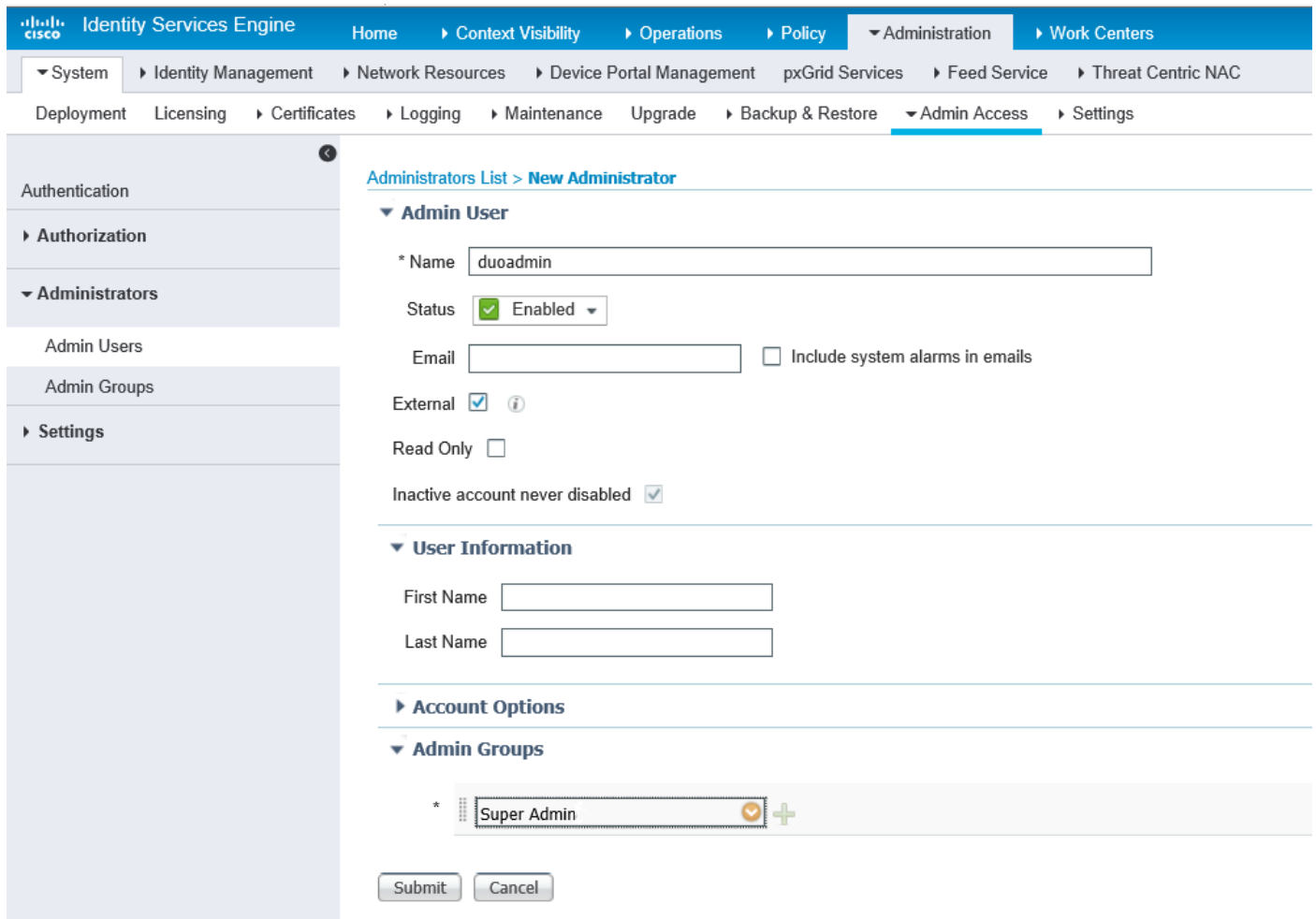
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes "Identity Services Engine" and various menu items like "Home", "Context Visibility", "Operations", "Policy", "Administration", and "Work Centers". Below this is a breadcrumb trail: "System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC". The main content area is titled "External Identity Sources" and shows a tree view on the left with "RADIUS Token" selected. The right pane shows the "RADIUS Token List > DUO" configuration page for a "RADIUS Token Identity Source". The "Connection" tab is active, showing settings for "Server Connection", "Primary Server", and "Secondary Server". The "Server Connection" section has checkboxes for "Safeword Server" and "Enable Secondary Server", and a radio button for "Always Access Primary Server First" with a "Fallback to Primary Server after" field set to 5 minutes. The "Primary Server" section has fields for "Host IP" (10.127.196.230), "Shared Secret" (masked), "Authentication Port" (1812), "Server Timeout" (60 seconds), and "Connection Attempts" (3). The "Secondary Server" section has fields for "Host IP", "Shared Secret" (masked), "Authentication Port" (1812), "Server Timeout" (5 seconds), and "Connection Attempts" (3). "Save" and "Reset" buttons are at the bottom.

Schritt 2: Navigieren Sie zu **Administration > System > Admin Access > Authentication > Authentication Method** und **Wählen Sie** zuvor konfigurierten RADIUS-Token-Server als

Identitätsquelle aus, wie im Bild gezeigt:



Schritt 3: Navigieren Sie zu **Administration > System > Admin Access > Administrator Users** und Create an admin user as External, und stellen Sie die Superadministratorberechtigung bereit, wie im Bild gezeigt:



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Öffnen Sie die ISE-GUI, wählen Sie RADIUS Token Server als Identitätsquelle aus, und melden

Sie sich bei einem Administrator-Benutzer an.



Identity Services Engine

Username

Password

Identity Source



[Problem logging in?](#)

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Um Probleme im Zusammenhang mit der Duo-Proxy-Konnektivität mit der Cloud oder Active Directory zu beheben, aktivieren Sie das Debuggen auf Duo Auth Proxy, indem Sie "debug=true" im Hauptbereich von authproxy.cfg hinzufügen.

Die Protokolle befinden sich unter dem folgenden Speicherort:

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

Öffnen Sie die Datei **authproxy.log** in einem Texteditor wie Notepad++ oder WordPad.

Protokollieren Sie Ausschnitte von Duo Auth Proxy, die Anfragen von der ISE empfangen und an die Duo Cloud senden.

```
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
```

Protokoll-Ausschnitte von Duo Auth Proxy können die Duo Cloud nicht erreichen.

```
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
```

Zugehörige Informationen

- [RA VPN-Authentifizierung mithilfe von DUO](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)