

Zwei-Faktor-Authentifizierung für FMC-Managementzugriff konfigurieren

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Authentifizierungsablauf](#)
- [Erläuterung des Authentifizierungsflusses](#)
- [Konfigurieren](#)
- [Konfigurationsschritte auf FMC](#)
- [Konfigurationsschritte auf der ISE](#)
- [Konfigurationsschritte im Duo Administrationsportal](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte beschrieben, die für die Konfiguration einer externen Zwei-Faktor-Authentifizierung für den Verwaltungszugriff in FirePOWER Management Center (FMC) erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Management Center (FMC)-Objektkonfiguration
- Identity Services Engine (ISE)-Administration

Verwendete Komponenten

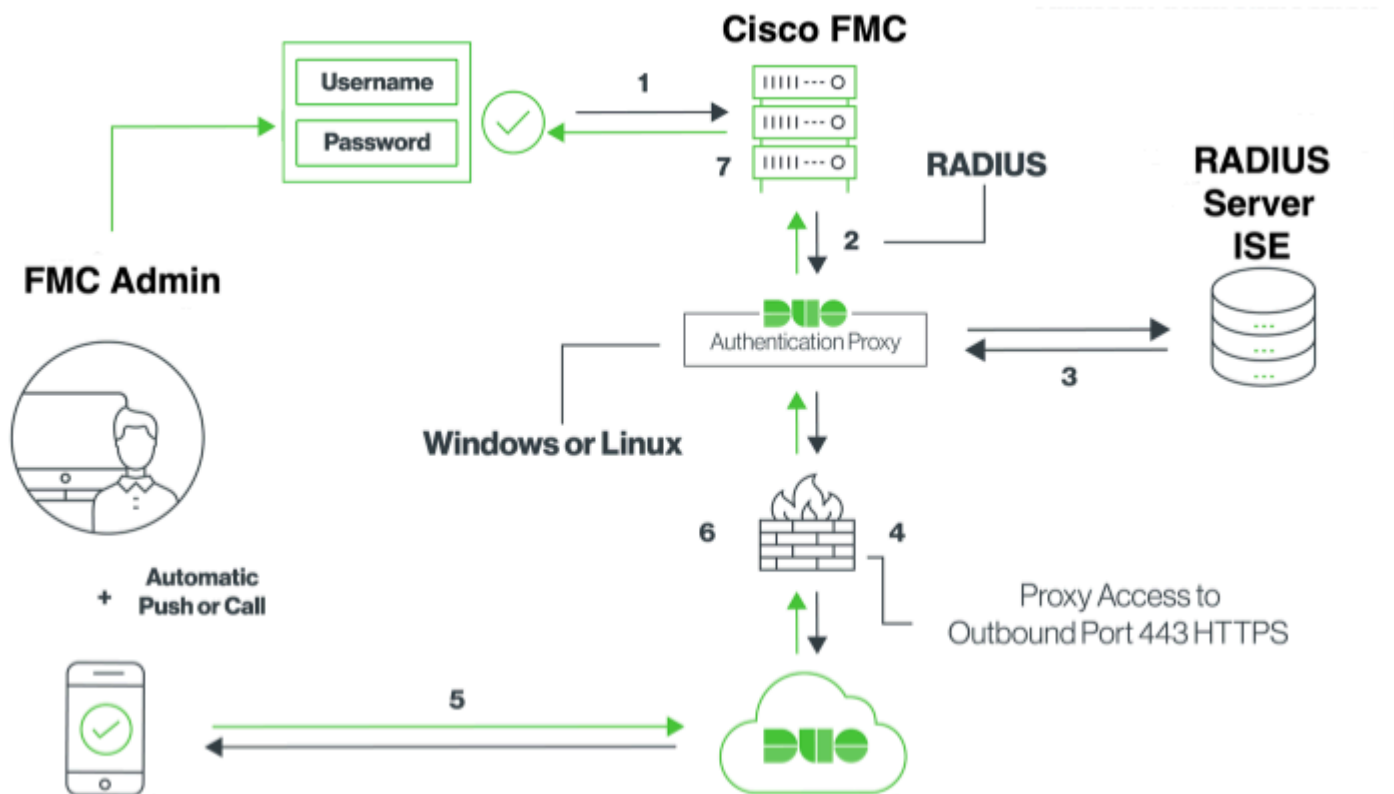
- Cisco FirePOWER Management Center (FMC) mit Version 6.3.0
- Cisco Identity Services Engine (ISE) mit Version 2.6.0.156
- Unterstützte Windows-Version (<https://duo.com/docs/authproxy-reference#new-proxy-install>) mit Verbindung zu FMC, ISE und Internet als Proxy-Server für die Duo-Authentifizierung
- Windows-Maschine für den Zugriff auf das FMC-, ISE- und Duo-Verwaltungsportal
- Duo Webkonto

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der FMC-Administrator authentifiziert sich über den ISE-Server, und eine zusätzliche Authentifizierung in Form einer Push-Benachrichtigung wird vom Duo Authentication Proxy-Server an das Mobilgerät des Administrators gesendet.

Authentifizierungsablauf



Erläuterung des Authentifizierungsflusses

1. Primäre Authentifizierung an Cisco FMC initiiert.
2. Cisco FMC sendet eine Authentifizierungsanforderung an den Duo-Authentifizierungsproxy.
3. Für die primäre Authentifizierung muss Active Directory oder RADIUS verwendet werden.
4. Duo Authentication Proxy-Verbindung mit Duo Security über TCP-Port 443 hergestellt.
5. Sekundäre Authentifizierung über den Dienst von Duo Security.
6. Der Duo-Authentifizierungsproxy empfängt die Authentifizierungsantwort.
7. Der Zugriff auf die grafische Benutzeroberfläche von Cisco FMC wird gewährt.

Konfigurieren

Beachten Sie zum Abschließen der Konfiguration die folgenden Abschnitte:

Konfigurationsschritte auf FMC

Schritt 1: Navigieren Sie zu **System > Users > External Authentication**. Erstellen Sie ein externes Authentifizierungsobjekt, und legen Sie die Authentifizierungsmethode auf RADIUS fest. Vergewissern Sie

sich, dass Administrator unter "Standard-Benutzerrolle" ausgewählt ist, wie im Bild gezeigt:

Hinweis: 10.106.44.177 ist die IP-Beispieladresse des Duo Authentication Proxy-Servers.

The screenshot displays a web-based configuration interface for an External Authentication Object. The interface is organized into several sections:

- External Authentication Object:**
 - Authentication Method: RADIUS (dropdown menu)
 - Name: DuoAuthProxy (text input)
 - Description: (empty text input)
- Primary Server:**
 - Host Name/IP Address: 10.106.44.177 (text input, with "ex. IP or hostname" note)
 - Port: 1812 (text input)
 - RADIUS Secret Key: ***** (password field)
- Backup Server (Optional):**
 - Host Name/IP Address: (empty text input, with "ex. IP or hostname" note)
 - Port: 1812 (text input)
 - RADIUS Secret Key: (empty text input)
- RADIUS-Specific Parameters:**
 - Timeout (Seconds): 30 (text input)
 - Retries: 3 (text input)
 - Access Admin: (empty text input)
 - Administrator: (empty text input)

The interface includes a top navigation bar with "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence". Below this is a secondary navigation bar with "Configuration", "Users", "Domains", "Integration", and "Update". The "Users" section is active, and within it, "External Authentication" is selected.

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role
To specify the default user role if user is not found in any group

Shell Access Filter

Administrator Shell Access User List
ex. user1, user2, user3
(Mandatory for FTD devices)

► **Define Custom RADIUS Attributes**

Additional Test Parameters

User Name

Password

*Required Field

Klicken Sie auf **Speichern** und **Übernehmen**. Ignorieren Sie die Warnung, wie in der Abbildung dargestellt:

Overview Analysis Policies Devices Objects | AMP Intelligence

Configuration **Users** Domains Integration Updates Licenses

One or more enabled external authentication objects don't have defined user roles.

Users **User Roles** External Authentication

Default User Role: **None** Shell Authentication: Disabled

Name

1. DuoAuthProxy

Schritt 2: Navigieren Sie zu **System > Users > Users**. Erstellen Sie einen Benutzer, und aktivieren Sie die Authentifizierungsmethode als Extern, wie im Bild gezeigt:

The image shows two configuration windows from the Cisco Duo interface. The top window, titled "User Configuration", has a "User Name" field containing "cpiplani". Under "Authentication", the "Use External Authentication Method" checkbox is checked. Under "Options", the "Exempt from Browser Session Timeout" checkbox is unchecked. The bottom window, titled "User Role Configuration", lists "Default User Roles" with the following roles checked: Administrator, External Database User, Security Analyst, Security Approver, Intrusion Admin, Access Admin, Network Admin, Maintenance User, Discovery Admin, and Threat Intelligence Director (TID) User. The "Security Analyst (Read Only)" role is unchecked. At the bottom of this window are "Save" and "Cancel" buttons.

Schritt 1: Laden Sie den Duo Authentication Proxy Server herunter, und installieren Sie ihn.

Melden Sie sich beim Windows-Computer an, und installieren Sie den [Duo Authentication Proxy Server](#).

Es wird empfohlen, ein System mit mindestens 1 CPU, 200 MB Festplattenspeicher und 4 GB RAM zu verwenden.

Hinweis: Dieser Computer muss Zugriff auf FMC, RADIUS-Server (in unserem Fall ISE) und 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 befindet sich unter C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

Bearbeiten Sie die Datei **authproxy.cfg**, und fügen Sie die folgende Konfiguration hinzu:

```
<#root>

[radius_client]

host=10.197.223.23                Sample IP Address of the ISE server

secret=cisco
```

Password configured on the ISE server in order to register the network device

Die IP-Adresse des FMC muss zusammen mit dem geheimen RADIUS-Schlüssel konfiguriert werden.

```
<#root>
```

```
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com

radius_ip_1=10.197.223.76
```

IP of FMC

```
radius_secret_1=cisco
```

Radius secret key used on the FMC

```
failmode=safe
client=radius_client
port=1812
api_timeout=
```

Stellen Sie sicher, dass Sie die ikey-, skey- und api_host-Parameter konfigurieren. Um diese Werte zu erhalten, melden Sie sich bei Ihrem Duo-Konto an ([Duo Admin Login](#)), und navigieren Sie zu **Applications > Protect an Application**. Wählen Sie anschließend die RADIUS-Authentifizierungsanwendung aus, wie im Bild gezeigt:

RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

Integration key	<input type="text"/>	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text"/>	select

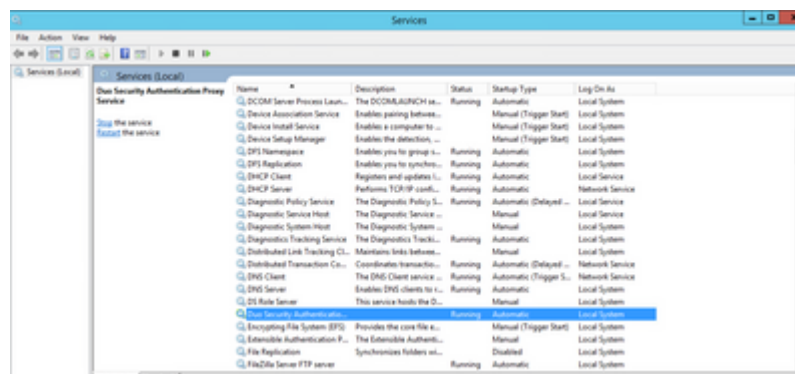
Integrationsschlüssel = Schlüssel

Geheimschlüssel = skey

API-Hostname = api_host

Schritt 3: Starten Sie den Duo Security Authentication Proxy-Dienst neu. **Speichern Sie** die Datei, und **starten Sie** den Duo-Dienst auf dem Windows-Computer neu.

Öffnen Sie die Konsole Windows-Dienste (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:



Konfigurationsschritte auf der ISE

Schritt 1: Navigieren Sie zu **Administration > Network Devices**, und klicken Sie auf **Add**, um das Network-Gerät wie in der Abbildung dargestellt zu konfigurieren:

Hinweis: 10.106.44.177 ist die IP-Beispieladresse des Duo Authentication Proxy-Servers.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices List > DuoAuthproxy' and 'Network Devices'. The configuration form includes: Name: DuoAuthproxy; Description: (empty); IP Address: (dropdown menu); * IP: 10.106.44.177; * Device Profile: Cisco; Model Name: (dropdown menu); Software Version: (dropdown menu).

Konfigurieren Sie den **gemeinsamen geheimen Schlüssel**, wie in der Datei **authproxy.cfg** im **geheimen** beschrieben, wie im Bild gezeigt:

The screenshot shows the RADIUS Authentication Settings configuration page in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices > RADIUS Authentication Settings. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'RADIUS Authentication Settings' and 'RADIUS UDP Settings'. The configuration form includes: Protocol: RADIUS; * Shared Secret: (masked with dots); Use Second Shared Secret: (checkbox); CoA Port: 1700.

Schritt 2: Navigieren Sie zu **Administration > Identities**. Klicken Sie auf **Hinzufügen**, um den Identity-

Benutzer wie im Bild dargestellt zu konfigurieren:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, and Feed Services. Under Identity Management, the 'Identities' section is selected, showing options for Groups, External Identity Sources, Identity Source Sequences, and Settings. The main content area displays the configuration for a 'Network Access User' named 'cpiplani'. The user's status is 'Enabled'. The 'Passwords' section is expanded, showing 'Password Type' set to 'Internal Users'. The 'Login Password' and 'Re-Enter Password' fields are visible, both containing masked characters. The 'Enable Password' checkbox is also present.

Konfigurationsschritte im Duo Administrationsportal

Schritt 1: Erstellen Sie einen Benutzernamen und aktivieren Sie Duo Mobile auf dem Endgerät.

Fügen Sie den Benutzer auf der Duo Cloud-Administrations-Webseite hinzu. Navigieren Sie zu **Benutzer > Benutzer hinzufügen**, wie in der Abbildung dargestellt:

The screenshot shows the Duo Cloud Administration portal. The left sidebar contains navigation options: Dashboard, Policies, Applications, Users, Add User, Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, and Administrators. The main content area is titled 'Add User' and includes a search bar for users, groups, applications, or devices. Below the search bar, there is a breadcrumb trail: Dashboard > Users > Add User. The 'Adding Users' section contains the text: 'Most applications allow users to enroll themselves after they complete primary authentication. Learn more about adding users'. The 'Username' field is populated with 'cpiplani' and has a note: 'Should match the primary authentication username.' A blue 'Add User' button is located at the bottom of the form.

Hinweis: Stellen Sie sicher, dass die Duo-App auf dem Endbenutzer installiert ist.

[Manuelle Installation der Duo-Anwendung für IOS-Geräte](#)

[Manuelle Installation der Duo-Anwendung für Android-Geräte](#)

Schritt 2: Automatische Generierung von Code.

Fügen Sie die Telefonnummer des Benutzers wie im Bild dargestellt hinzu:

Phones
You may rearrange the phones by dragging and dropping in the table. [Add Phone](#)

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

Dashboard > Users > cpiplari > Add Phone

Add Phone


Type Phone Tablet


Phone number [Show extension field](#)


[Add Phone](#)

Wählen Sie **Activate Duo Mobile** wie im Bild gezeigt:

Device Info

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

 Model Unknown

 OS Generic Smartphone

Wählen Sie **Generate Duo Mobile Activation Code** wie im Bild gezeigt aus:

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.

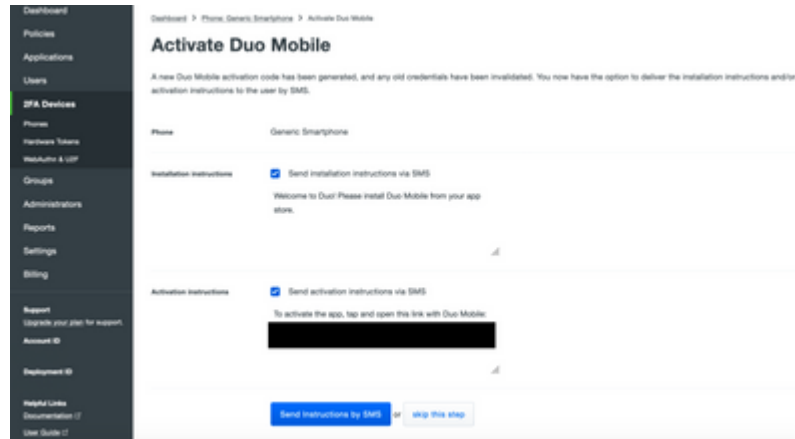
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

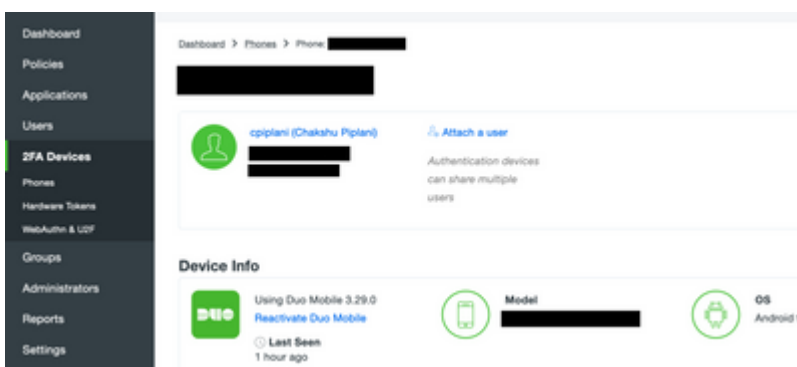
Expiration: after generation

[Generate Duo Mobile Activation Code](#)

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



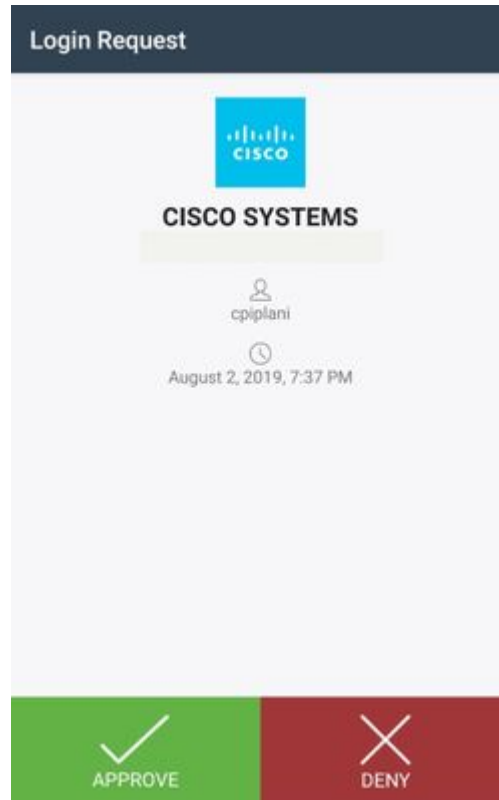
Klicken Sie in der SMS auf den Link, und die Duo App wird mit dem Benutzerkonto im Abschnitt "Geräteinformationen" verknüpft, wie im Bild gezeigt:



Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Melden Sie sich mit Ihren auf der ISE-Benutzeridentitätsseite hinzugefügten Benutzeranmeldeinformationen beim FMC an. Sie müssen eine Duo PUSH-Benachrichtigung für die Two Factor Authentication (2FA) auf Ihrem Endpunkt erhalten, diese genehmigen und FMC muss sich wie im Bild gezeigt anmelden:



Navigieren Sie auf dem ISE-Server zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle)**. Suchen Sie den Benutzernamen für die Authentifizierung auf FMC, und wählen Sie den detaillierten Authentifizierungsbericht in der Spalte "Details" aus. Hier müssen Sie überprüfen, ob die Authentifizierung erfolgreich war, wie im Bild gezeigt:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	cpiplani
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2019-07-11 03:50:38.694
Received Timestamp	2019-07-11 03:50:38.694
Policy Server	ROHAN-ISE
Event	5200 Authentication succeeded
Username	cpiplani
User Type	User
Authentication Identity Store	Internal Users

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlo
- 22072 Selected identity source sequence - All_Us
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore -
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15048 Queried PIP - Network Access.UserName
- 15048 Queried PIP - IdentityGroup.Name
- 15048 Queried PIP - EndPoints.LogicalProfile
- 15048 Queried PIP - Network Access.Authentication
- 15016 Selected Authorization Profile - PermitAcces
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session
- 11002 Returned RADIUS Access-Accept

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

- Überprüfen Sie die Fehlerbehebungen auf dem Duo-Authentifizierungsproxyserver. Die Protokolle befinden sich an folgender Stelle:

C:\Program Dateien (x86)\Duo Sicherheitsauthentifizierungsproxy\log

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

Protokollausschnitte bei Eingabe falscher Anmeldeinformationen und Ablehnung der Authentifizierung durch den ISE-Server.

```
<#root>
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from
```

```
10.197.223.76
```

```
to radius_server_auto
```

```
10.197.223.76 is the IP of the FMC
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524)
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):
```

```
login attempt for username u'cpiplani'
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.23', 1812);
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]
```

```
Got response
```

```
for id 199 from ('
```

```
10.197.223.23
```

```
', 1812);
```

```
code 3 10.197.223.23 is the IP of the ISE Server.
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials rejected
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):
```

```
Returning response code 3: AccessReject
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response
```

- Navigieren Sie auf der ISE zu **Operations > RADIUS > Live Logs**, um die Authentifizierungsdetails zu überprüfen.

Ausschnitte erfolgreicher Authentifizierung mit ISE und Duo protokollieren:

```
<#root>
```

```
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from
```

```
10.197.223.76
```

```

to radius_server_auto
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095)
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for user
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('
10.197.223.23
', 1812);
code 2 <<<< At this point we have got successful authentication from ISE Server.
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest
2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): C
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
Duo authentication returned 'allow': 'Success. Logging you in...
,
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
Returning response code 2: AccessAccept <<<< At this point, user has hit the approve button
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): S
2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC

```

Zugehörige Informationen

- [RA VPN-Authentifizierung mit Duo](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.