

DUO Security

2FA auf Mandantenserver

- [2FA-CISCO DUO SECURITY Installation Anleitung für Benutzer auf dem Mandantenserver](#)

2FA-CISCO DUO SECURITY

Installation Anleitung für Benutzer auf dem Mandantenserver



1) Was benötigen wir für die Zwei-Faktor-Authentifizierung (2FA)?

1. Duo Mobile App
2. Ihrer Telefonnummer in DUO
3. Aktivierung der Duo Mobile App auf Ihrem Smartphone

2) Auf Handy – Duo Mobile App einrichten

Auf Ihrem Handy – Duo Mobile App einrichten. (Android oder Apple)

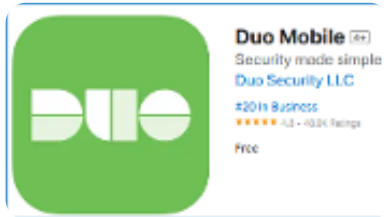
<https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

<https://apps.apple.com/gb/app/duo-mobile/id422663827>

a) Android



b) Apple



c) Duo 2Factor Support

Duo Security unterstützt folgende Faktortypen für die Zwei-Faktor-Authentifizierung:

- Duo Push (Duo Mobile)
- Duo Mobile Passcodes
- Hardware Token OTP passcodes (including Yubikey OTP)
- Phone Call

3) Verbindung von Duo Security mit Ihrer Telefonnummer

Duo Security benötigt eine Verbindung zu Ihrer angegebenen Telefonnummer, um die Zwei-Faktor-Authentifizierung (2FA) zu ermöglichen. Nachdem wir Sie in das System aufgenommen haben, wird ein Aktivierungslink an Ihre Nummer gesendet.

Durch Klicken auf diesen Link wird die Duo Mobile App auf Ihrem Smartphone automatisch aktiviert und mit Ihrem Benutzerkonto verknüpft. Diese Verbindung gewährleistet, dass Sicherheitsbenachrichtigungen und Authentifizierungsanfragen direkt an Ihr Gerät gesendet werden.

a) Aktivierung von Duo Mobile

1. Wir aktivieren Ihr Duo Mobile. Dann bekommen Sie eine Nachricht von DUOSEC.
2. DUOSEC wird an die von Ihnen angegebene Telefonnummer einen Aktivierungslink senden.

3. Wenn Sie auf den Link in dieser Nachricht klicken, wird die Duo Mobile App geöffnet und ein Konto erstellt. Dieses Konto stellt die Verbindung zwischen der Duo Mobile App auf Ihrem Telefon und dem Server her.

Jetzt haben Sie 2FA. Wenn Sie sich anmelden möchten, verwenden Sie als erstes Ihre RDP Zugangsdaten (Benutzername + Passwort) und Authentifizieren Sie als zweites DUO Security.

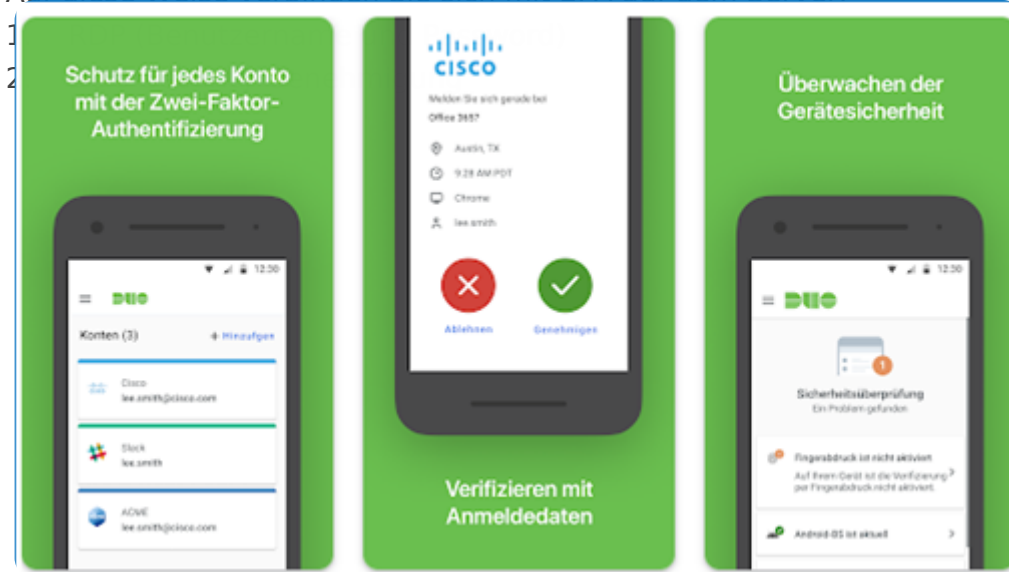
4) Auf dem Mandantenserver Anmelden

Wenn Sie sich mit dem Server anmelden möchten, geben Sie zunächst Ihren Benutzernamen und Ihr Passwort in die RDP-Verbindung ein.

Wenn diese Informationen korrekt sind, wird automatisch eine Nachricht an die Duo Mobile App auf Ihrem Telefon gesendet. Sobald Sie die Nachricht anklicken, werden Sie aufgefordert, die Sitzung des Benutzers auf dem Server zu genehmigen oder abzulehnen. Wenn Sie die Genehmigung anklicken, wird Ihre Serversitzung geöffnet. Wenn Sie Ablehnen anklicken, wird die Serversitzung nicht geöffnet.

NOTE: Geben Sie nur Verbindungen Frei die Sie selbst initiiert haben.

Auf diese Weise verbinden Sie sich mit 2FA auf dem Server:



a) RDP Verbindung: Benutzername – Passwort

Der erste Schritt zur Verbindung mit dem Zwei-Faktor-System ist die Anmeldung am Mandantenserver über RDP.

Sie müssen die IP-Adresse zusammen mit Ihrem Benutzernamen und Passwort in die RDP-Verbindung eingeben, um sich mit dem Server zu verbinden.

Anmeldeinformationen eingeben

Diese Anmeldeinformationen werden für das Herstellen einer Verbindung mit [redacted] verwendet.

N00C [redacted]@[redacted].de

Kennwort

Anmeldedaten speichern

Weitere Optionen

b) 2FA auf Ihrem Handy

Wenn Sie diese Informationen (RDP) korrekt eingeben und sich mit dem Server verbinden, erscheint der DUO Security-Bildschirm auf RDP Verbindung.

Für die Zwei-Faktor-Authentifizierung (2FA) erhalten Sie eine Benachrichtigung auf Ihr Telefon.

Wenn Sie die Benachrichtigung ablehnen, wird die Duo Mobile App geöffnet.

Duo Security

Device: Android (+XX XXX XXX3387)

Choose an authentication method

Duo Push

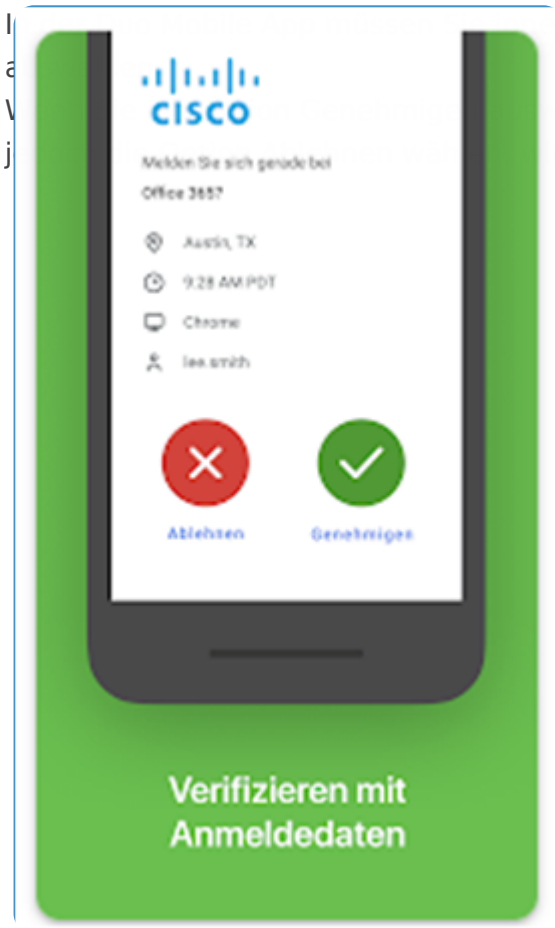
Phone Call

Passcode

Powered by Duo Security

Pushed a login request to your device...

c) Genehmigen oder Ablehnen auf Duo Mobile



Innerhalb einer bestimmten Zeit eine der beiden Optionen

auswählen, wird Ihre Sitzung auf dem Server geöffnet. Wenn Sie innerhalb dieser Zeit keine der beiden Optionen auswählen, wird der Zugriff auf den Server verweigert.

5) Fragen und Antworten

a) Was passiert, wenn jemand den RDP-Benutzernamen und das Passwort erlangt?

Falls jemand den RDP-Benutzernamen und das Passwort erlangt, kann ohne Ihre Zustimmung über die Duo Mobile App keine Verbindung zum Server hergestellt werden. Selbst wenn diese Informationen gestohlen werden, wird der Zugriff auf den Server nur mit Ihrer expliziten Genehmigung über Duo Security möglich sein.

b) Zeitlimit für die Auswahl

Wenn Sie innerhalb von etwa 10–15 Sekunden keine der Optionen auswählen, wird der Zugriff auf den Server nicht genehmigt. In diesem Fall müssen Sie erneut versuchen, sich über RDP mit dem

Server zu verbinden.

c) Kann ein Benutzerkonto mehrere Telefonnummern hinzugefügt werden?

Ja, es können mehrere Telefonnummern zu einem Benutzerkonto hinzugefügt werden. Nach der RDP-Verbindung können Sie auf dem Duo Security-Bildschirm die gewünschte Telefonnummer auswählen, sodass eine Nachricht an die entsprechende Telefonnummer für die Anmeldung gesendet wird.

d) Was tun, wenn Ihr Telefon defekt ist und Sie die Duo Mobile App nicht nutzen können?

Falls Ihr Telefon defekt ist und Sie die Duo Mobile App nicht verwenden können, gibt es alternative Lösungen, um sich mit dem Mandantenserver zu verbinden.

Sie sollen uns darüber informieren. In diesem Fall können wir Änderungen im Duo Security-Bereich vornehmen.

Zum Beispiel:

- Wenn Ihre SIM-Karte in ein anderes Handy eingesetzt wird, können wir Ihnen den Zugriff per SMS oder Telefonanruf ermöglichen.
 - Auf Wunsch können wir Ihnen auch den Zugriff über einen Hardware-Token OTP einrichten.
- Zusammenfassend stehen Ihnen viele Optionen zur Verfügung, damit Sie sicher und geschützt auf dem Mandantenserver arbeiten können.

Wir wünschen Ihnen eine sichere und erfolgreiche Arbeit!

[Alpha-Netzwerkpartner Team](#)