Duo-Endbenutzer-Weiterbildung Kommunikationsvorlagen

Inhalt

Best Practices für die E-Mail-Kommunikation

Nachfolgend finden Sie einige Best Practices bezüglich E-Mails an Ihre Benutzer über die bevorstehende Bereitstellung von Duo 2FA:

- **Tage, an denen die E-Mails gesendet werden sollten:** Dienstag, Mittwoch und Donnerstag sind die besten Tage zum Versenden der E-Mails, da sie dann am wahrscheinlichsten von den Benutzern gelesen werden.
- **Absender der E-Mail:** Wir empfehlen, dass diese E-Mail von einer Person (IT-Manager, Betriebsleiter usw.) oder von Ihrem Helpdesk gesendet wird.

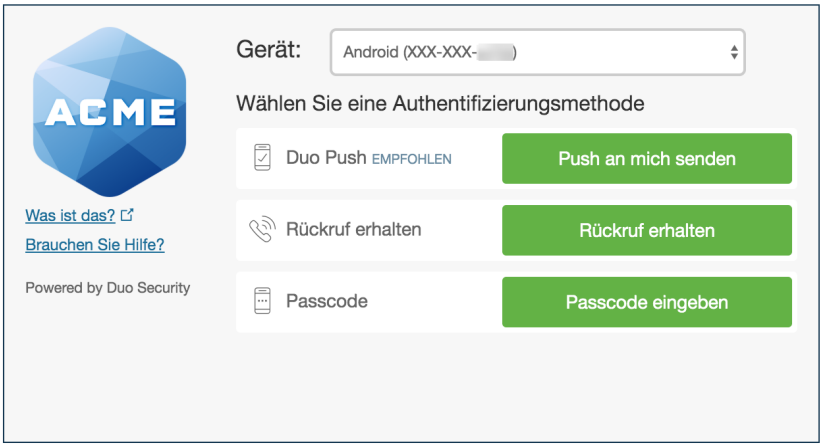
Endbenutzerglossar und häufig gestellte Fragen

Nachfolgend sind die wichtigsten Begriffe und Fragen aufgeführt, die Endbenutzer bei der Einführung in Duo nützlich finden könnten. Sie können diese Informationen genau so verwenden oder für Ihr Unternehmen entsprechend anpassen.

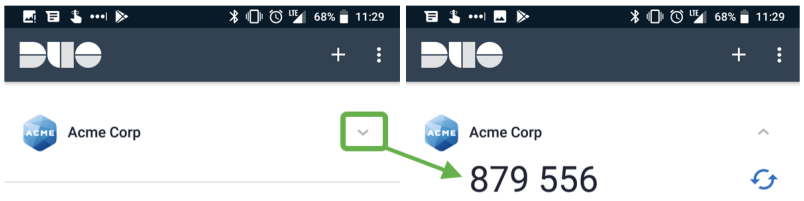
Glossar

2FA (Zweifaktor-Authentifizierung): Dies ist eine zusätzliche Authentifizierungsebene, die über einen Benutzernamen und ein Kennwort hinausgeht. 2FA beinhaltet etwas, das Sie kennen (Kennwort) und etwas, das Sie bei sich tragen (wie Duo Mobile auf Ihrem Smartphone). So wird verhindert, dass sich jemand nur mit Ihrem Kennwort anmelden kann. Mit Duo 2FA müssen Sie Ihren Benutzernamen und Ihr Kennwort immer noch eingeben. Der zweite Faktor, der über Duo bereitgestellt wird, ist einfach eine zusätzliche Sicherheitsebene zu Ihren Anmeldeinformationen. Zur Durchführung der 2FA empfehlen wir die Verwendung von Duo Push über die Duo Mobile-App.

Duo Prompt: In dieser interaktiven Eingabeaufforderung können Sie auswählen, wie Sie Ihre Identität bei jeder Anmeldung bei einer webbasierten Anwendung verifizieren möchten (z. B. „Duo Push“ oder „Anruf“). Mit Duo Prompt können Sie sich registrieren und authentifizieren.



Passcode: Dies sind numerische Codes, die entweder über die Duo Mobile App, SMS (Textnachricht) oder ein Hardware-Token generiert werden können, je nachdem, was Ihr IT-Administrator zulässt. Passcodes können jederzeit verwendet werden und sind besonders nützlich für die Authentifizierung, wenn Ihr 2FA-Gerät keinen Internet-oder Mobilfunkservice hat..



Push-Benachrichtigung (Duo Push): Dies ist eine Push-Authentifizierungsanfrage, die an die

Duo Mobile-App auf einem registrierten Gerät gesendet wird. Push-Benachrichtigungen enthalten Informationen wie den geografischen Standort eines zugreifenden Geräts, die IP-Adresse des zugreifenden Geräts und die Anwendung, auf die zugegriffen wird, damit Sie prüfen können, ob der Push-Prozess echt oder betrügerisch ist.

Self-Service-Portal: Wenn das Self-Service-Portal für die Verwendung in Duo Prompt aktiviert wurde, können Sie auf „My Settings & Devices“ (Meine Einstellungen und Geräte) klicken, um weitere Geräte hinzuzufügen oder die Einstellungen zur Authentifizierungsmethode für Duo Prompt zu aktualisieren.

Häufig gestellte Fragen

Im folgenden finden Sie einige wichtige Fragen, die Endbenutzer häufig stellen. *Je nach den spezifischen Anwendungen und der Konfiguration Ihres Unternehmens müssen einige Fragen möglicherweise bearbeitet oder ausgelassen werden.*

Benötige ich ein Smartphone oder einen Datenplan, um die zweistufige Authentifizierung zu nutzen?

Nein. Ein Smartphone sorgt für eine einfachere und sicherere Handhabung von Duo Push. Wenn Ihr Unternehmen dies zulässt, ist es auch möglich, ein anderes Mobilgerät als ein Smartphone oder sogar das Festnetz zu nutzen, um SMS-Passcodes oder Telefonanrufe zu empfangen.

Was ist Duo Mobile?

Duo Mobile ist eine mobile Anwendung (App), die Sie auf Ihrem Smartphone oder Tablet installieren, um Passcodes für die Anmeldung zu generieren oder Push-Benachrichtigungen für eine einfache Authentifizierung auf Ihrem Mobilgerät zu erhalten. Der Duo Zweifaktor-Authentifizierungs- Service (2FA-Service) macht Ihre Anmeldung sicherer.

Was ist die empfohlene Zweifaktor-Authentifizierungsmethode?

Wenn Sie ein Smartphone oder Tablet besitzen, empfehlen wir Duo Push, da es schnell, einfach und sicher ist. Dieses kurze Video enthält eine Einführung in Duo Security sowie eine Demonstration von Duo Push: https://www.youtube.com/watch?v=_T_sJXnSM98

Wie viele Daten sind für einen Duo Push erforderlich?

Duo Push-Authentifizierungsanfragen erfordern eine minimale Datenmenge – weniger als 2 KB pro Authentifizierung. Wenn Sie also z. B. 500 Authentifizierungen pro Monat durchführen würden, wären das insgesamt nur 1 Megabyte (MB).

Warum erhalte ich keine Push-Benachrichtigungen von Duo Mobile mehr?

Dafür kann es mehrere Gründe geben. Versuchen Sie folgende Maßnahmen, um das Problem zu beheben:

1. Stellen Sie sicher, dass Ihr registriertes Gerät über ein Mobilfunknetz oder eine Wi-Fi-Verbindung verfügt.
2. Öffnen Sie die Duo Mobile-App, wenn Sie die Authentifizierung durchführen.
3. Versuchen Sie diese weiteren Schritte zur Behebung von Push-Problemen:
    - iPhone: https://help.duo.com/s/article/2051
    - Android: https://help.duo.com/s/article/2050
4. Wenn die oben genannten Lösungen nicht funktionieren, verwenden Sie eine andere Authentifizierungsmethode, z. B. Passcodes in der Duo Mobile App.

Wie kann ich mich authentifizieren, wenn ich an einem Ort ohne Mobilfunksignal oder WLAN-Zugriff bin?

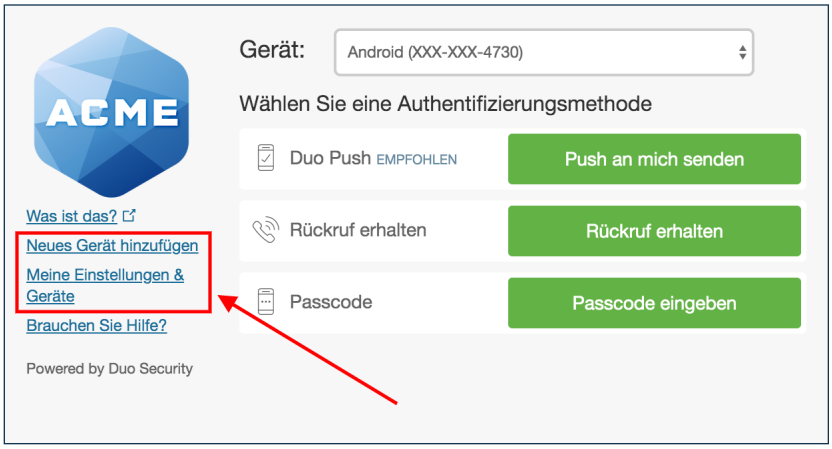
Informationen zur Authentifizierung ohne Mobilfunk- oder Internetservice finden Sie in diesem Duo-Artikel in der Wissensdatenbank: https://help.duo.com/s/article/4449

Wie verwalte ich die Geräte, die ich für Duo verwende?

Wenn Sie Zugriff auf den Link „My Settings & Devices“ (Meine Einstellungen und Geräte) im Self-Service-Portal von Duo Prompt haben und sich derzeit mit einem Geräte authentifizieren können, können Sie Folgendes tun:

- Zusätzliche Geräte hinzufügen
- Ein „Standardgerät“ bestimmen, das zusätzlich zu Ihrer bevorzugten Authentifizierungsmethode auch Authentifizierungsanfragen empfängt.
- Duo Mobile deaktivieren, wenn Sie ein neues Telefon mit der gleichen Nummer haben
- Den Namen Ihres Geräts ändern (z. B. „Privathandy“ oder „Geschäftshandy“)
- Ein Gerät entfernen

Weitere Informationen zur Verwaltung Ihrer Geräte finden Sie hier:
https://guide.duo.com/manage-devices



Was muss ich tun, wenn ich mein Telefon verloren habe?

Wenden Sie sich umgehend an Ihren IT-Helpdesk.

Kann Duo mein Kennwort erkennen?

Nein. Ihr Kennwort wird nur von Ihrem Unternehmen überprüft und niemals an Duo gesendet. Duo bietet nur den zweiten Faktor. Anhand Ihres registrierten Geräts wird überprüft, dass Sie die Person sind, die sich gerade anmeldet.

Verliere ich durch die Verwendung von Duo die Kontrolle über mein Smartphone?

Nein. Die Duo Mobile-App hat keinen Zugriff, mit dem sie die Einstellungen Ihres Telefons ändern oder Ihre Telefon remote zurücksetzen könnte. Die Angaben, die Duo Mobile benötigt, sind für die Überprüfung der Sicherheit Ihres Geräts erforderlich. Hierzu zählen beispielsweise Betriebssystemversion, Geräteverschlüsselungsstatus, Bildschirmsperre usw. Wir verwenden dies, um Sicherheitsverbesserungen für Ihr Gerät zu empfehlen. Sie haben stets die Kontrolle darüber, ob Sie diese Empfehlungen umsetzen oder nicht.

E-Mail-Vorlagen – Einführung zu Duo für Endbenutzer

Verwenden Sie diese E-Mail-Vorlagen, wenn Ihr Unternehmen Benutzer zum ersten Mal MFA/Duo einführt:

E-Mail #1 *- Duo ist bald verfügbar, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

30 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Die zwei-Faktor-Authentifizierung von Duo ist in Kürze verfügbar!

HAUPTTEXT:

Wir werden Duo Security als Lösung zur Zweifaktor-Authentifizierung in unsere vorhandene IT-Infrastruktur integrieren, um unseren Sicherheitsstatus zu verbessern.

Erforderliche Maßnahme:

Es ist derzeit keine unmittelbare Aktion erforderlich. Diese E-Mail informiert Sie lediglich über den bevorstehenden Rollout der Zweifaktor-Authentifizierung von Duo.

Was ist Duo Security?

Duo Security stellt einen Cloud-basierten Softwareservice bereit, der die Zweifaktor-Authentifizierung nutzt, um einen sicheren Zugriff auf Services und Daten zu gewährleisten. Klicken Sie **hier**, um weitere Informationen zu erhalten.

Was ist die Zweifaktor-Authentifizierung?

Die Zweifaktor-Authentifizierung bietet eine zweite Sicherheitsebene für jede Art der Anmeldung. **Dabei wird für die Anmeldung zusätzlich zu Ihrem Kennwort eine Zusatzinformation oder ein physisches Gerät benötigt.**

Indem zwei unterschiedliche Authentifizierungskanäle genutzt werden, verhindern wir, dass durch einen Remote-Angriff gestohlene Benutzernamen und Kennwörter zum Einsatz kommen.

Zu den Faktoren gehören:

Etwas, das Sie kennen:

- ein eindeutiger Benutzername und das Kennwort.

Etwas, das Sie haben:

- ein Smartphone mit einer App, über die Authentifizierungsanfragen genehmigt werden können.

Etwas, das Sie sind:

- biometrische Daten, wie z. B. Ihr Fingerabdruck oder ein Netzhautscan.

Warum benötigen wir die Zweifaktor-Authentifizierung?

Anmeldeinformationen sind wertvoller als jemals zuvor und lassen sich auch immer leichter kompromittieren. Über 90 % der heutigen Sicherheitsverletzungen entstehen durch kompromittierte Benutzernamen und Kennwörter.

Die Zweifaktor-Authentifizierung erhöht die Sicherheit Ihres Kontos, indem ein sekundäres Gerät zur Überprüfung Ihrer Identität verwendet wird. **So wird verhindert, dass andere Personen als Sie selbst auf Ihr Konto zugreifen, auch wenn diese Ihr Kennwort kennen.**

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo den Abschluss der Anmeldung durch eine Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode. **Weitere Informationen zur Einführung von Duo erhalten Sie in Kürze.**

E-Mail #2 - *Duo ist ab <DATUM> verfügbar, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

15 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Registrierung zur Zweifaktor-Authentifizierung am **<DATUM DER REGISTRIERUNGS-E-MAIL>**

HAUPTTEXT:

Wir werden Duo Security als Lösung zur **Zweifaktor-Authentifizierung** in unsere vorhandene IT-Infrastruktur integrieren, um unseren Sicherheitsstatus zu verbessern.

Am **<DATUM DER REGISTRIERUNGS-E-MAIL>** erhalten Sie eine Registrierungs-E-Mail von Duo. In den kommenden Tagen erhalten Sie weitere Informationen.

Erforderliche Maßnahme:

Es ist derzeit keine unmittelbare Aktion erforderlich. Diese E-Mail informiert Sie lediglich über die bevorstehende Einführung der Zweifaktor-Authentifizierung von Duo am **<DATUM DER REGISTRIERUNGS-E-MAIL>.**

Was ist Duo Security?

Duo Security stellt einen Cloud-basierten Softwareservice bereit, der die Zweifaktor-Authentifizierung nutzt, um einen sicheren Zugriff auf Services und Daten zu gewährleisten. Klicken Sie **hier**, um weitere Informationen zu erhalten.

Was ist die Zweifaktor-Authentifizierung?

Die Zweifaktor-Authentifizierung bietet eine zweite Sicherheitsebene für jede Art der Anmeldung. **Dabei wird für die Anmeldung zusätzlich zu Ihrem Kennwort eine Zusatzinformation oder ein physisches Gerät benötigt.**

Indem zwei unterschiedliche Authentifizierungskanäle genutzt werden, verhindern wir, dass durch einen Remote-Angriff gestohlene Benutzernamen und Kennwörter zum Einsatz kommen.

Zu den Faktoren gehören:

Etwas, das Sie kennen:

- ein eindeutiger Benutzername und das Kennwort.

Etwas, das Sie haben:

- ein Smartphone mit einer App, über die Authentifizierungsanfragen genehmigt werden können.

Etwas, das Sie sind:

- biometrische Daten, wie z. B. Ihr Fingerabdruck oder ein Netzhautscan.

Warum benötigen wir die Zweifaktor-Authentifizierung?

Anmeldeinformationen sind wertvoller als jemals zuvor und lassen sich auch immer leichter kompromittieren. Über 90 % der heutigen Sicherheitsverletzungen entstehen durch kompromittierte Benutzernamen und Kennwörter.

Die Zweifaktor-Authentifizierung erhöht die Sicherheit Ihres Kontos, indem ein sekundäres Gerät zur Überprüfung Ihrer Identität verwendet wird. **So wird verhindert, dass andere Personen als Sie selbst auf Ihr Konto zugreifen, auch wenn diese Ihr Kennwort kennen.**

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo den Abschluss der Anmeldung durch eine Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode. **Weitere Informationen zur Einführung von Duo erhalten Sie in Kürze.**

E-Mail #3 - *Duo ist ab <DATUM> verfügbar + Registrierungsinformationen, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

3 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Erinnerung: Registrierung zur Zweifaktor-Authentifizierung am **<DATUM DER REGISTRIERUNGS-E-MAIL>**

HAUPTTEXT:

Wir werden Duo Security als Lösung zur **Zweifaktor-Authentifizierung** in unsere vorhandene IT-Infrastruktur integrieren, um unseren Sicherheitsstatus zu verbessern.

Am **<DATUM DER REGISTRIERUNGS-E-MAIL>** erhalten Sie eine Registrierungs-E-Mail von Duo. Diese E-Mail enthält einen **personalisierten Link, mit dem Sie sich bei Duo registrieren können**. Der Prozess zur Selbstregistrierung dauert nur zwei Minuten und vereinfacht die **Registrierung Ihres Telefons und die Installation der Duo Mobile-App.**

Wenn Sie kein Smartphone besitzen, können Sie sich auch über ein herkömmliches Mobiltelefon (SMS oder Anruf) oder ein Festnetztelefon (Anruf) für die Zweifaktor-Authentifizierung registrieren.

Erforderliche Maßnahme:

Es ist keine unmittelbare Aktion erforderlich. Diese E-Mail dient zur Erinnerung an die bevorstehende Einführung der Zweifaktor-Authentifizierung von Duo am **<DATUM DER REGISTRIERUNGS-E-MAIL>**.

Was sind Duo Mobile und Duo Push?

Duo Mobile ist die kostenlose App von Duo Security, mit der Sie eine Anfrage zur Zweifaktor-Authentifizierung mithilfe von **Duo Push** schnell und einfach genehmigen können.

Mit **Duo Mobile und Duo Push** benötigen Sie keine sperrigen Hardware-Token und verschwenden auch keine Zeit durch die manuelle Eingabe von Passcodes. Mit nur einem Tippen können Sie die Authentifizierung auf Ihrem Smartphone durchführen.

Hier sehen Sie ein Beispiel für Duo Push in Aktion.

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo den Abschluss der Anmeldung durch eine Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode.

Was ist Duo, was ist die Zweifaktor-Authentifizierung und warum benötigen wir sie?

Sollten Sie unsere vorherigen E-Mails nicht gelesen haben, erhalten Sie in **diesem Video** weitere Informationen.

Sie haben Fragen?

Wenn Sie Fragen zur Registrierung bei oder der Nutzung von Duo haben, wenden Sie sich an **<den Helpdesk/den Servicedesk>**.

- **<Helpdesk/Servicedesk> Telefonnummer:**
- **<Helpdesk/Servicedesk> E-Mail-Adresse:**

E-Mail #4 - *Durchsuchen Sie Ihren Posteingang nach der Duo-Registrierungs-E-Mail – Jetzt registrieren.*

ZEITPLAN:

Tag des Versands der Registrierungs-E-Mail/der Einführung der Anwendung.

BETREFFZEILE:

Erforderliche Aktion: Registrieren Sie sich noch heute bei Duo

HAUPTTEXT:

Wir werden Duo Security als Lösung zur Zweifaktor-Authentifizierung in unsere vorhandene IT-Infrastruktur integrieren, um unseren Sicherheitsstatus zu verbessern.

Heute erhalten Sie die Registrierungs-E-Mail von Duo Security. Diese E-Mail enthält einen **personalisierten Link, mit dem Sie sich bei Duo registrieren können**. Der Prozess zur Selbstregistrierung dauert nur zwei Minuten und vereinfacht die **Registrierung Ihres Telefons und die Installation der Duo Mobile-App**.

Wenn Sie kein Smartphone besitzen, können Sie sich auch über ein herkömmliches Mobiltelefon (SMS oder Anruf) oder ein Festnetztelefon (Anruf) für die Zweifaktor-Authentifizierung registrieren.

Sie können sich bis zum **<DATUM DER EINFÜHRUNG DER ANWENDUNG UND VON DUO>** registrieren. Nach diesem Datum erfordert der Zugriff auf **<ANWENDUNG>** die Duo-Zweifaktor-Authentifizierung.

Erforderliche Maßnahme:

Registrieren Sie sich noch heute. Suchen Sie in Ihrem Posteingang nach der Registrierungs-E-Mail von Duo und schließen Sie den Registrierungsprozess ab.

Was sind Duo Mobile und Duo Push?

Duo Mobile ist die kostenlose App von Duo Security, mit der Sie eine Anfrage zur Zweifaktor-Authentifizierung mithilfe von **Duo Push** schnell und einfach genehmigen können.

Mit **Duo Mobile und Duo Push** benötigen Sie keine sperrigen Hardware-Token und verschwenden auch keine Zeit durch die manuelle Eingabe von Passcodes. Mit nur einem Tippen können Sie die Authentifizierung auf Ihrem Smartphone durchführen.

Hier sehen Sie ein Beispiel für Duo Push in Aktion.

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo den Abschluss der Anmeldung durch eine Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode.

Was ist Duo, was ist die Zweifaktor-Authentifizierung und warum benötigen wir sie?

Sollten Sie unsere vorherigen E-Mails nicht gelesen haben, erhalten Sie in diesem Video weitere Informationen.

Sie haben Fragen?

Wenn Sie Fragen zur Registrierung bei oder der Nutzung von Duo haben, wenden Sie sich an **<den Helpdesk/den Servicedesk>**.

- **<Helpdesk/Servicedesk> Telefonnummer:**
- **<Helpdesk/Servicedesk> E-Mail-Adresse:**

Verwenden Sie diese E-Mail-Vorlagen, wenn Ihr Unternehmen eine vorhandene MFA-Lösung mit Duo ersetzt:

E-Mail #1 - *Duo ist bald verfügbar, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

30 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Duo-Zweifaktor-Authentifizierung ersetzt **<Aktueller 2FA-Anbieter>**

HAUPTTEXT:

Um unseren Sicherheitsstatus und die Benutzerfreundlichkeit der **Zweifaktor-Authentifizierung** zu verbessern werden wir **<Aktueller 2FA-Anbieter>** ersetzen und die **Zweifaktor-Authentifizierung** von Duo Security in unsere vorhandene IT-Infrastruktur integrieren.

Erforderliche Maßnahme:

Es ist derzeit keine unmittelbare Aktion erforderlich. Diese E-Mail informiert Sie lediglich über die bevorstehende Änderung bei der Durchführung der Zweifaktor-Authentifizierung.

Warum bietet Duo Security ein besseres Benutzererlebnis?

Mit der kostenlosen mobilen App von Duo Security, Duo Mobile, benötigen Sie bei der Anmeldung bei einer geschützten Anwendung keine sperrigen Hardware-Token mehr und müssen auch keine Passcodes manuell eingeben.

Mit Duo Mobile können Sie schnell und einfach eine Anfrage zur Zweifaktor-Authentifizierung auf Ihrem Smartphone mithilfe von **Duo Push genehmigen**. Wenn Sie zuvor ein Hardware-Token oder einen Passcode verwendet haben, **ersetzt Ihr Smartphone diese jetzt.** Hier sehen Sie ein Beispiel für Duo Push in Aktion.

Warum benötigen wir die Zweifaktor-Authentifizierung?

Anmeldeinformationen sind wertvoller als jemals zuvor und lassen sich auch immer leichter kompromittieren. Über 90 % der heutigen Sicherheitsverletzungen entstehen durch kompromittierte Benutzernamen und Kennwörter.

Die Zweifaktor-Authentifizierung erhöht die Sicherheit Ihres Kontos, indem ein sekundäres Gerät zur Überprüfung Ihrer Identität verwendet wird. **So wird verhindert, dass andere Personen als Sie selbst auf Ihr Konto zugreifen, auch wenn diese Ihr Kennwort kennen.**

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo Ihre Genehmigung für eine Duo Push-Benachrichtigung oder eine andere Methode der Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode. **Weitere Informationen zur Einführung von Duo erhalten Sie in Kürze.**

E-Mail #2 - *Duo ist ab <DATUM> verfügbar, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

15 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Registrierung bei der Zweifaktor-Authentifizierung am **<DATUM DER REGISTRIERUNGS-E-MAIL>**

HAUPTTEXT:

Um unseren Sicherheitsstatus und die Benutzerfreundlichkeit der **Zweifaktor-Authentifizierung** zu verbessern werden wir **<Aktueller 2FA-Anbieter>** ersetzen und die **Zweifaktor-Authentifizierung** von Duo Security in unsere vorhandene IT-Infrastruktur integrieren.

Am **<DATUM DER REGISTRIERUNGS-E-MAIL>** erhalten Sie eine Registrierungs-E-Mail von Duo.

Erforderliche Maßnahme:

Es ist derzeit keine unmittelbare Aktion erforderlich. Mit dieser E-Mail benachrichtigen wir Sie über den Wechsel unserer Zweifaktor-Authentifizierung von **<Aktueller 2FA-Anbieter>** zu **Duo Security am <DATUM DER REGISTRIERUNGS-E-MAIL>**.

Warum bietet Duo Security ein besseres Benutzererlebnis?

Mit der kostenlosen mobilen App von Duo Security, **Duo Mobile**, benötigen Sie bei der Anmeldung bei einer geschützten Anwendung keine sperrigen Hardware-Token mehr und müssen auch keine Passcodes manuell eingeben.

Mit Duo Mobile können Sie schnell und einfach eine Anfrage zur Zweifaktor-Authentifizierung auf Ihrem Smartphone mithilfe von **Duo Push genehmigen**. Wenn Sie zuvor ein Hardware- Token oder einen Passcode verwendet haben, **ersetzt Ihr Smartphone diese jetzt**. Hier sehen Sie ein Beispiel für Duo Push in Aktion.

Warum benötigen wir die Zweifaktor-Authentifizierung?

Anmeldeinformationen sind wertvoller als jemals zuvor und lassen sich auch immer leichter kompromittieren. Über 90 % der heutigen Sicherheitsverletzungen entstehen durch kompromittierte Benutzernamen und Kennwörter.

Die Zweifaktor-Authentifizierung **erhöht die Sicherheit Ihres Kontos, indem ein sekundäres Gerät zur Überprüfung Ihrer Identität verwendet wird**. So wird verhindert, dass andere Personen als Sie selbst auf Ihr Konto zugreifen, auch wenn diese Ihr Kennwort kennen.

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo Ihre Genehmigung für eine Duo Push-Benachrichtigung oder eine andere Methode der Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode. **Weitere Informationen zur Einführung von Duo erhalten Sie in Kürze.**

E-Mail #3 - *Duo ist ab <DATUM> verfügbar + Registrierungsinformationen, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

3 Tage vor dem Versand der Registrierungs-E-Mail/vor dem Einführungsdatum der Anwendung.

BETREFFZEILE:

Erinnerung: Duo-Zweifaktor-Authentifizierung ersetzt **<Aktueller 2FA-Anbieter>** am **<DATUM DER REGISTRIERUNGS-E-MAIL>**

HAUPTTEXT:

Um unseren Sicherheitsstatus und die Benutzerfreundlichkeit der **Zweifaktor-Authentifizierung** zu verbessern werden wir **<Aktueller 2FA-Anbieter>** ersetzen und die **Zweifaktor-Authentifizierung** von Duo Security in unsere vorhandene IT-Infrastruktur integrieren.

Am **<DATUM DER REGISTRIERUNGS-E-MAIL>** erhalten Sie eine Registrierungs-E-Mail von Duo. Diese E-Mail enthält einen **personalisierten Link, mit dem Sie sich bei Duo registrieren können**. Der Prozess zur Selbstregistrierung dauert nur zwei Minuten und vereinfacht die **Registrierung Ihres Telefons und die Installation der Duo Mobile-App**.

Wenn Sie kein Smartphone besitzen, können Sie sich auch über ein herkömmliches Mobiltelefon (SMS-Textnachrichten oder Anruf) oder ein Festnetztelefon (Anruf) für die Zweifaktor-Authentifizierung registrieren.

Erforderliche Maßnahme:

Es ist keine unmittelbare Aktion erforderlich. Mit dieser E-Mail erinnern wir Sie an den bevorstehenden Wechsel unserer Zweifaktor-Authentifizierung von **<Aktueller 2FA-Anbieter>** zu Duo Security am **<DATUM DER REGISTRIERUNGS-E-MAIL>**.

Was ist Duo, was ist die Zweifaktor-Authentifizierung und warum benötigen wir sie?

Sollten Sie unsere vorherigen E-Mails nicht gelesen haben, erhalten Sie in **diesem Video** weitere Informationen.

Warum bietet Duo Security ein besseres Benutzererlebnis?

Mit der kostenlosen mobilen App von Duo Security, **Duo Mobile**, benötigen Sie bei der Anmeldung bei einer geschützten Anwendung keine sperrigen Hardware-Token mehr und müssen auch keine Passcodes manuell eingeben.

Mit **Duo Mobile** können Sie schnell und einfach eine Anfrage zur Zweifaktor-Authentifizierung auf Ihrem Smartphone mithilfe von **Duo Push** genehmigen. Wenn Sie zuvor ein Hardware- Token oder einen Passcode verwendet haben, **ersetzt Ihr Smartphone diese jetzt**. **Hier** sehen Sie ein Beispiel für Duo Push in Aktion.

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo Ihre Genehmigung für eine Duo Push-Benachrichtigung oder eine andere Methode der Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode.

Sie haben Fragen?

Wenn Sie Fragen zur Registrierung bei oder der Nutzung von Duo haben, wenden Sie sich an **<den Helpdesk/den Servicedesk>**.

- **<Helpdesk/Servicedesk> Telefonnummer:**
- **<Helpdesk/Servicedesk> E-Mail-Adresse:**

E-Mail #4 - *Durchsuchen Sie Ihren Posteingang nach der Duo-Registrierungs-E-Mail – Jetzt registrieren.*

ZEITPLAN:

Tag des Versands der Registrierungs-E-Mail/der Einführung der Anwendung.

BETREFFZEILE:

Erforderliche Aktion: Registrieren Sie sich noch heute bei Duo

HAUPTTEXT:

Um unseren Sicherheitsstatus und die Benutzerfreundlichkeit der **Zweifaktor-Authentifizierung** zu verbessern werden wir **<Aktueller 2FA-Anbieter>** ersetzen und die **Zweifaktor-Authentifizierung** von Duo Security in unsere vorhandene IT-Infrastruktur integrieren.

Erforderliche Maßnahme:

Heute erhalten Sie die Registrierungs-E-Mail von Duo Security. Diese E-Mail enthält einen **personalisierten Link, mit dem Sie sich bei Duo registrieren können**. Der Prozess zur Selbstregistrierung dauert nur zwei Minuten und vereinfacht die **Registrierung Ihres Telefons und die Installation der Duo Mobile-App**.

Wenn Sie kein Smartphone besitzen, können Sie sich auch über ein herkömmliches Mobiltelefon (SMS-Textnachrichten und Anruf) oder ein Festnetztelefon (Anruf) für die Zweifaktor-Authentifizierung registrieren.

Sie können sich bis zum **<DATUM DER EINFÜHRUNG DER ANWENDUNG UND VON DUO>** Nach diesem Datum erfordert der Zugriff auf **<ANWENDUNG>** die Duo-Zweifaktor-Authentifizierung und die Zweifaktor-Authentifizierung durch **<Aktueller 2FA-Anbieter>** wird eingestellt.

Was ist Duo, was ist die Zweifaktor-Authentifizierung und warum benötigen wir sie?

Sollten Sie unsere vorherigen E-Mails nicht gelesen haben, erhalten Sie in **diesem Video** weitere Informationen.

Warum bietet Duo Security ein besseres Benutzererlebnis?

Mit der kostenlosen mobilen App von Duo Security, **Duo Mobile**, benötigen Sie bei der Anmeldung bei einer geschützten Anwendung keine sperrigen Hardware-Token mehr und müssen auch keine Passcodes manuell eingeben.

Mit **Duo Mobile** können Sie schnell und einfach eine Anfrage zur Zweifaktor-Authentifizierung auf Ihrem Smartphone mithilfe von **Duo Push genehmigen**. Wenn Sie zuvor ein Hardware- Token oder einen Passcode verwendet haben, **ersetzt Ihr Smartphone diese jetzt**. **Hier** sehen Sie ein Beispiel für Duo Push in Aktion.

Wie wird sich mit Duo das Anmeldeverfahren ändern?

Wenn Sie sich bei einer mit Duo geschützten Anwendung anmelden, müssen Sie weiterhin Ihren Benutzernamen und Ihr Kennwort eingeben. Nach Eingabe Ihrer Anmeldeinformationen **erfordert Duo Ihre Genehmigung für eine Duo Push-Benachrichtigung oder eine andere Methode der Zweifaktor-Authentifizierung.**

Duo ersetzt nicht die Eingabe Ihres Benutzernamens und Kennworts und erfordert auch nicht die Änderung dieser Informationen. Betrachten Sie Duo als eine zusätzliche Sicherheitsebene zu Ihrer bestehenden Anmeldemethode.

Sie haben Fragen?

Wenn Sie Fragen zur Registrierung bei oder der Nutzung von Duo haben, wenden Sie sich an **<den Helpdesk/den Servicedesk>**.

- **<Helpdesk/Servicedesk> Telefonnummer:**
- **<Helpdesk/Servicedesk> E-Mail-Adresse:**

E-Mail-Vorlagen – Kommunikation der neuen Richtlinie

Verwenden Sie diese Vorlagen, um Benutzer über bevorstehende Richtlinienänderungen zu informieren:

E-Mail #1 - *Bevorstehende Änderungen an der Duo-Richtlinie am keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

30 Tage bevor die Richtlinie angewendet wird.

BETREFFZEILE:

Änderungen bezüglich der Duo-2FA-Anmeldung: **<Version X.XX von BS/Browser/Plug-in oder biometrische Authentifizierung/Festplattenverschlüsselung/Bildschirmsperre** benötigt ab **<DATUM>**

HAUPTTEXT:

Um Ihren Sicherheitsstatus zu verbessern und kontinuierlichen Zugriff auf mit Duo geschützte Anwendungen zu gewährleisten, müssen Sie demnächst ein Update von **<Mobil- oder Zugriffsgerät>** durchführen, damit die folgenden Anforderungen erfüllt werden:

- **A**
- **B**
- **C**

Erforderliche Maßnahme:

Es ist derzeit keine unmittelbare Aktion erforderlich. Diese E-Mail informiert Sie über die bevorstehende Änderung, damit Sie, falls erforderlich, entsprechende Schritte proaktiv durchführen können.

Wenn Sie diese Änderungen jetzt vornehmen möchten, beachten Sie die folgenden Punkte: **<Anweisungen zur Prüfung/Aktivierung der Verschlüsselungs-/Biometrie-/Bildschirmsperren-Optionen oder zur Prüfung von Browser-/Plug-in-/BS-Versionen und Durchführung von Updates integrieren.>**

E-Mail #2 - *Bevorstehende Änderungen an der Duo-Richtlinie am <DATUM>, keine unmittelbare Aktion erforderlich.*

ZEITPLAN:

Eine Woche bevor die Richtlinienänderung angewendet wird.

BETREFFZEILE:

Erinnerung: Bevorstehende Änderungen bezüglich der Duo-2FA-Anmeldung -- **<Version X.XX von BS/Browser/Plug-in oder biometrische Authentifizierung/Bildschirmsperre benötigt ab DATUM>**

HAUPTTEXT:

Um Ihren Sicherheitsstatus zu verbessern und kontinuierlichen Zugriff auf mit Duo geschützte Anwendungen zu gewährleisten, müssen Sie demnächst ein Update von **<Mobil- oder Zugriffsgerät>** durchführen, damit die folgenden Anforderungen erfüllt werden:

- **A**
- **B**
- **C**

Erforderliche Maßnahme:

Es ist keine unmittelbare Aktion erforderlich, aber Sie haben eine Woche Zeit, um (falls erforderlich) die nötigen Updates durchzuführen. Diese E-Mail informiert Sie über die bevorstehende Änderung, damit Sie entsprechende Schritte proaktiv durchführen können.

Wenn Sie diese Änderungen jetzt vornehmen möchten, beachten Sie die folgenden Punkte:
<Anweisungen zur Prüfung/Aktivierung der Verschlüsselungs-/Biometrie-/Bildschirmsperren-Optionen oder zur Prüfung von Browser-/Plug-in-/BS-Versionen und Durchführung von Updates integrieren.>

E-Mail #3 - *Änderungen an der Duo-Richtlinie MORGEN, Geräte-/Softwareupdates sind möglicherweise erforderlich.*

ZEITPLAN:

Ein Tag bevor die Richtlinie angewendet wird.

BETREFFZEILE:

Erinnerung: Bevorstehende Änderungen bezüglich der Duo-2FA-Anmeldung MORGEN – Geräte-/Softwareupdates sind möglicherweise erforderlich, um weiterhin Zugriff zu erhalten.

HAUPTTEXT:

Um Ihren Sicherheitsstatus zu verbessern und kontinuierlichen Zugriff auf mit Duo geschützte Anwendungen zu gewährleisten, müssen Sie demnächst ein Update von **<Mobil- oder Zugriffsgerät>** durchführen, damit die folgenden Anforderungen erfüllt werden:

- **A**
- **B**
- **C**

Erforderliche Maßnahme:

Aktualisieren Sie <Gerät/Software> noch heute oder Sie können nicht mehr auf die Anwendungen zugreifen.

<Anweisungen zur Prüfung/Aktivierung der Verschlüsselungs-/Biometrie-/Bildschirmsperren-Optionen oder zur Prüfung von Browser-/Plug-in-/BS-Versionen und Durchführung von Updates integrieren.>