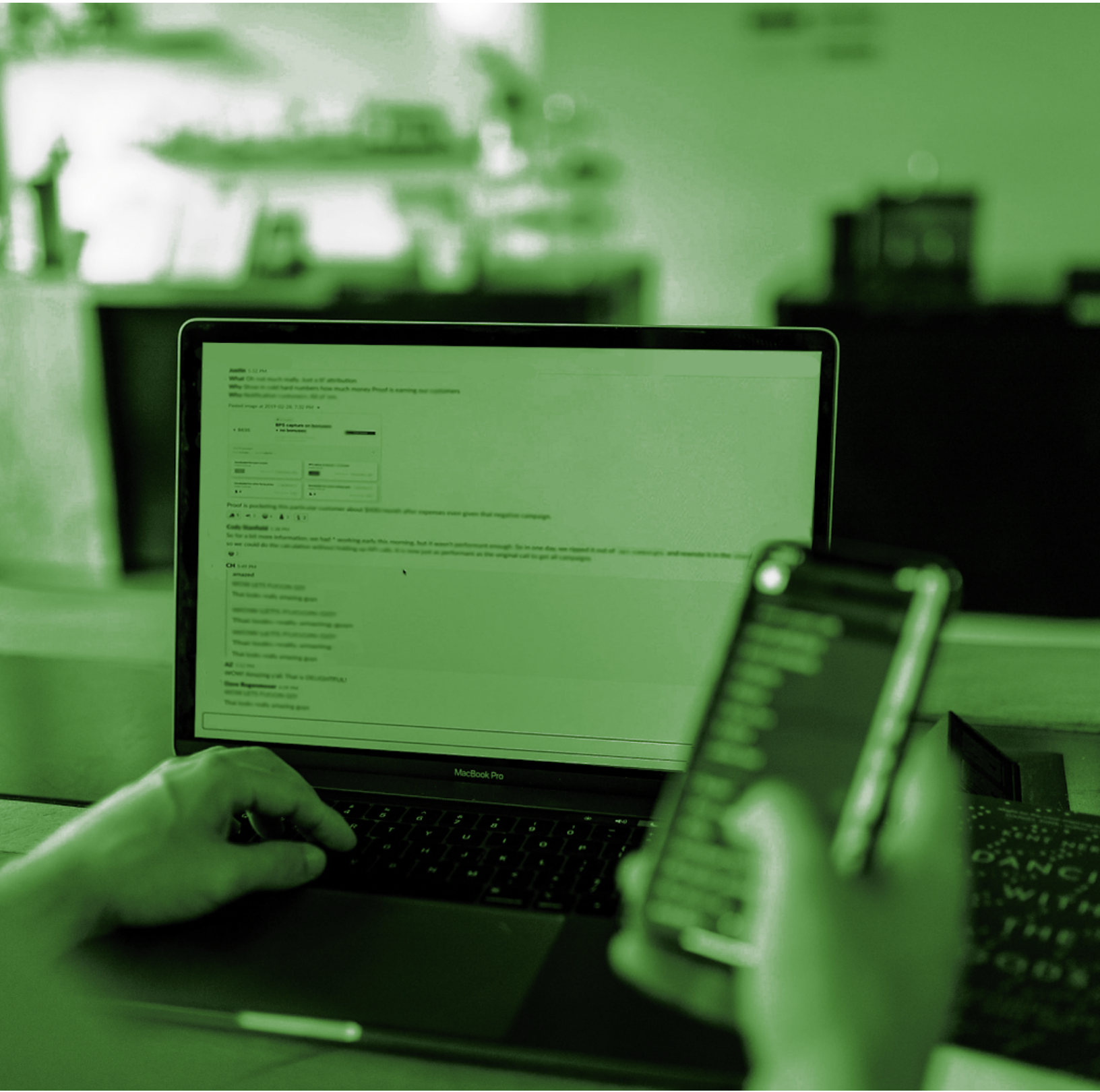
Duo Security gehört jetzt zu Cisco.

Helpdesk-Leitfaden

Ursprünglich veröffentlicht am 22. Juni 2016
Version 4.0 veröffentlicht am 15. Januar 2020



Häufig verwendete Begriffe

Begriffe, die in der Duo-Dokumentation, in Ihrem internen Team oder bei Endnutzern vorkommen können:

2FA (Zwei-Faktor-Authentifizierung): eine zusätzliche Authentifizierungsebene neben Benutzername/Kennwort. 2FA umfasst einen Faktor, den Sie kennen (Kennwort), und einen Faktor, den Sie bei sich tragen (z. B. Duo Mobile auf Ihrem Smartphone), um zu verhindern, dass jemand, der Ihr Kennwort „kennt“, einfach auf Ihre Daten zugreifen kann. Wenn die 2FA von Duo aktiviert ist, geben Sie weiterhin Ihren Benutzernamen und Ihr Kennwort ein. Duo ersetzt nicht Ihren Benutzernamen und Ihr Kennwort. Es handelt sich lediglich um eine zusätzliche Sicherheitsebene, die Ihre vorhandenen Anmeldeinformationen ergänzt. Weitere Informationen finden Sie in diesem Video.

Duo-Administratorbereich: eine Login-geschützte Schnittstelle, über die Duo-Administratoren ihre Benutzer, Geräte, Integrationen, Rollen, Protokolle, Abrechnungsinformationen usw. verwalten können.

Duo Prompt: Hier können Benutzer auswählen, wie sie ihre Identität bei jeder Anmeldung bei einer webbasierten Anwendung verifizieren möchten (z. B. „Duo Push“ oder „Anruf“). Duo Prompt ermöglicht die Inline-Registrierung und -Authentifizierung.

Passcode: Passcodes können über die App Duo Mobile, per SMS (Textnachricht) oder über das Hardware-Token eines Benutzers generiert werden.

Plattform: der Typ des Authentifizierungsgeräts eines Benutzers (iPhone, Android, Festnetztelefon usw.).

Push-Benachrichtigung (Duo Push): Dies ist eine Out-of-Band-Authentifizierungsanfrage, die an die App Duo Mobile auf einem registrierten Gerät gesendet wird. Push-Benachrichtigungen enthalten Informationen wie den Benutzerstandort, die IP-Adresse und die Anwendung, auf die der Benutzer zugreifen möchte.

Self-Service-Portal: Wenn das Self-Service-Portal im Duo-Administratorbereich aktiviert wurde, kann der Benutzer zusätzliche Geräte hinzufügen oder seine Authentifizierungsmethode direkt über Duo Prompt aktualisieren. Verfügbar für alle kostenpflichtigen Editionen von Duo.

Teil 1: Übersicht

Warum benötige ich diesen Leitfaden?

Die Einführung der Zwei-Faktor-Authentifizierung (häufig mit „2FA“ abgekürzt) in Ihrem Unternehmen kann Fragen von Ihren Endnutzern hervorrufen. Obwohl wir stolz auf Duos einfache Einrichtung und benutzerfreundliche Oberfläche sind, verstehen wir, dass die Authentifizierung mit Duo für einige Personen zunächst verwirrend sein kann, insbesondere, wenn sie zuvor noch keine Zwei-Faktor-Authentifizierung verwendet haben. Dieses Dokument liefert Ihnen schnelle Antworten auf Probleme, auf die Ihre Endnutzer bei der Verwendung von Duo stoßen können.

Dieser Leitfaden richtet sich an Administratoren mit bestimmten Administratorrollen, um Endnutzern zu helfen, häufige Aufgaben zu erledigen und Probleme zu beheben. Hier erfahren Sie mehr über den Unterschied zwischen Duo-Konten für Administratoren und Endnutzer.

Duo empfiehlt die Ernennung von mindestens zwei Duo-Verantwortlichen für jedes Konto. Ebenso ist es wichtig, Ihre Administratorenliste regelmäßig zu aktualisieren, da die Verantwortlichen neu in Ihr Unternehmen kommen oder dieses verlassen können. Zwei Verantwortliche bieten redundanten Zugriff auf den Duo-Administratorbereich und gewährleisten einen konsistenteren Zugriff, wenn ein Verantwortlicher nicht erreichbar ist. Wir haben festgestellt, dass Kunden durch die Ernennung von mehreren Verantwortlichen Zeit sparen, indem sie ihre administrativen Aufgaben selbst erledigen.

Hier sehen Sie einen kurzen Überblick über die Rollen und deren Zugriff auf Aufgaben im Duo-Administratorbereich:

	Rolle „Verantwortlicher“	Rolle „Administrator“	Rolle „Anwendungs-manager“	Rolle „Benutzermanager“	Rolle „Helpdesk“	Rolle „Abrechnung“	Rolle „Nur lesen“
Protokolle anzeigen und herunterladen	✅	✅	✅	✅	✅		✅
2FA-Geräte und Umgehungscodes verwalten	✅	✅		✅	✅		
Benutzer und Gruppen verwalten	✅	✅		✅			
Anwendungen verwalten	✅	✅	✅				
Globale Einstellungen ändern	✅	✅					
Abrechnung anzeigen und verwalten	✅					✅	
Andere Administratoren verwalten	✅						

Darüber hinaus ermöglichen die **Administrationseinheiten** von Duo Administratoren von kostenpflichtigen Editionen die Gruppierung von Duo-Benutzern und -Anwendungen sowie die Zuweisung von Management-Berechtigungen für bestimmte Administratoren. Weitere Informationen zu den Administrationseinheiten finden Sie hier: https://duo.com/docs/administrative-units. Hinweis: Administratoren mit eingeschränkten Rechten sehen keine Benutzer oder Anwendungen in anderen Gruppen.

Teil 2: Registrierung und Aktivierung

Wie gestaltet sich die Aktivierung für Endnutzer?

Benutzer haben zwei Optionen: Sie können den Registrierungsprozess über ein anderes Gerät beginnen als jenes, mit dem sie sich authentifizieren möchten (z. B. ein Laptop oder Desktop-PC, den sie für den Zugriff auf von Duo geschützte Dienste nutzen werden), oder über ihr letztendliches Authentifizierungsgerät (z. B. ihr Mobiltelefon).

Registrierung über einen Laptop, Desktop oder ein sonstiges nicht zur Authentifizierung verwendetes Gerät

Die Benutzer beginnen mit dem Link aus ihrer Registrierungs-E-Mail. Bei Verwendung der Registrierungsaufforderung können die Benutzer einen QR-Code mit ihrem Authentifizierungsgerät scannen.

Vergewissern Sie sich, dass Ihre Endnutzer der Duo Mobile App Zugriff auf die Kamera des Smartphones gegeben haben, damit der QR-Code gescannt werden kann.Andernfalls kann der Code nicht gescannt werden. Weitere Informationen zu diesem Prozess finden Sie in unserem Registrierungsleitfaden: https://guide.duo.com/enrollment.

Registrierung über das Authentifizierungsgerät

Mit dieser Methode beginnen die Benutzer über die Registrierungs-E-Mail auf ihrem Mobilgerät mit der Einrichtung, führen die Registrierung durch und installieren schließlich bei Bedarf Duo Mobile. Weitere Informationen finden Sie in diesem Artikel aus der Wissensdatenbank: https://help.duo.com/s/article/3890.

Wie kann ich Registrierungs-E-Mails erneut senden?

E-Mails können erneut an Benutzer gesendet werden, die per Massenregistrierung oder Active Directory Sync erstellt wurden und die Registrierung noch nicht abgeschlossen haben. Befolgen Sie den in Schritt 5 der Massenregistrierung beschriebenen Prozess, um Registrierungs-E-Mails erneut zu senden: https://duo.com/docs/enrolling_users#bulk-self-enrollment.

Teil 3: Authentifizierung und Authentifizierungsverfahren

Wie kann ich ein neues Authentifizierungsgerät hinzufügen oder aktivieren?

In diesem Prozess wird erklärt, wie ein neues Authentifizierungsgerät (z. B. ein Mobiltelefon, Festnetztelefon, Tablet oder U2F-Token) für einen Benutzer hinzugefügt und/oder aktiviert wird. Wenn das Self-Service-Portal im Duo Prompt aktiviert ist (nur für kostenpflichtige Editionen von Duo verfügbar), können Benutzer selbst neue Geräte hinzufügen. Wenn das Self-Service-Portal nicht aktiviert ist, können Geräte nur von Administratoren hinzugefügt werden.

Beachten Sie, dass Benutzer nur dann über das Self-Service-Portal ein neues Gerät hinzufügen können, wenn sie Zugriff auf ein anderes zuvor aktiviertes Authentifizierungsgerät oder einen Umgehungscode haben. Wenn sie keinen Zugriff darauf haben, muss ein Administrator sie beim Hinzufügen eines neuen Geräts unterstützen.

Bei aktiviertem Self-Service-Portal: https://guide.duo.com/add-device
Manuell über den Duo-Administratorbereich: https://duo.com/docs/administration-devices

Was sollte ich tun, wenn ein Benutzer sein Gerät vergisst?

Hat ein Benutzer sein Telefon oder Hardware-Token zu Hause gelassen? In diesem Artikel aus der Wissensdatenbank finden Sie Möglichkeiten zur Unterstützung: https://help.duo.com/s/article/3302.

Was kann ich tun, wenn mein Gerät verloren geht oder gestohlen wird?

Weisen Sie Benutzer stets darauf hin, dass sie sich sofort an einen Administrator wenden sollten, wenn ihr 2FA-Authentifizierungsgerät verloren geht oder gestohlen wird.

Wenn das Self-Service-Portal aktiviert ist und ein Benutzer über ein zweites Authentifizierungsgerät verfügt, sollte er sofort das Menü „Meine Einstellungen und Geräte“ in Duo Prompt öffnen und das verlorene oder gestohlene Gerät löschen. Wenn das Self-Service-Portal für den Benutzer nicht aktiviert ist oder über kein zweites Authentifizierungsgerät verfügt wird, muss ein Administrator das Gerät aus Duo löschen, nachdem sichergestellt wurde, dass ein neues Authentifizierungsverfahren hinzugefügt wurde.

Bei aktiviertem Self-Service-Portal: https://guide.duo.com/common-issues#lost-phone
Manuell über den Duo-Administratorbereich: https://duo.com/docs/administration-devices#dealing-with-lost-or-stolen-phones

Wie kann ich Benutzern helfen, die sich in einem Flugzeug authentifizieren müssen oder zu einem entlegenen Ort unterwegs sind?

Informieren Sie die Benutzer, dass die Anwendung Duo Mobile genutzt werden kann, um in Flugzeugen oder an anderen Orten, an denen Duo Push, neue Batches von per SMS versandten Passcodes oder telefonische Rückrufe nicht verfügbar sind, Passcodes zu generieren. Weitere Informationen finden Sie in den Benutzerhandbüchern für die Authentifizierung mit per Duo Mobile generierten Passcodes unter Android oder iOS. Weitere Informationen im Duo-Reiseführer.

Warum erhalte ich keine Push-Benachrichtigungen von Duo?

Vergewissern Sie sich zuerst, dass der Benutzer Benachrichtigungen auf seinem Telefon erlaubt.

Benutzer können Probleme beim Empfang von Push-Anfragen haben, wenn Netzwerkprobleme zwischen ihrem Telefon und dem Duo-Dienst vorliegen. Viele Telefone haben Schwierigkeiten zu bestimmen, ob sie Wi-Fi oder den Mobilfunk-Datenkanal nutzen sollen, wenn sie Push-Anfragen abrufen. Diese Probleme können häufig durch einfaches Aktivieren und Deaktivieren des Flugzeugmodus auf dem Telefon behoben werden, wenn eine zuverlässige Internetverbindung verfügbar ist. Ebenso kann das Problem durch Deaktivieren der Wi-Fi-Verbindung auf dem Gerät und die Nutzung der mobilen Datenverbindung behoben werden. Eine Push-Benachrichtigung von Duo ist nur 2 kB groß.

Überprüfen Sie Uhrzeit und Datum am Telefon und vergewissern Sie sich, dass sie korrekt sind. Wenn Datum und Uhrzeit auf einem Telefon manuell eingestellt werden, versuchen Sie, die Konfiguration des Geräts so zu ändern, dass Datum und Uhrzeit automatisch mit dem Netzwerk synchronisiert werden.

Darüber hinaus haben wir umfassende Leitfäden zur Fehlerbehebung für die Zustellung von Push-Benachrichtigungen von Duo für iOS: https://help.duo.com/s/article/2051 und Android: https://help.duo.com/s/article/2050 zusammengestellt. Beachten Sie, dass je nach konkretem Problem ggf. ein IT-Administrator mit der Möglichkeit, den Portzugriff zu ändern, herangezogen werden muss.

Wie ordne ich Benutzern Token zu?

Von Duo erworbene Token werden automatisch in Ihr Konto importiert. OTP-Token-Informationen von Drittanbietern müssen von Administratoren manuell in Duo importiert werden. Beachten Sie beim Importieren von Token, dass die Token zwischen Duo-Konten eindeutig sein sollten.

Duo unterstützt FIDO-U2F-Token, allerdings können U2F-Token nicht über den Administratorbereich importiert oder Benutzern zugewiesen werden. Stattdessen registrieren Benutzer das U2F-Token selbst über die Duo-Registrierungsaufforderung oder das Self-Service-Portal Weitere Informationen finden Sie in unserer Dokumentation zur Aktivierung der U2F-Authentifizierung und zum U2F-Registrierungsprozess für Endnutzer.

So weisen Sie einem Endnutzer ein Token zu: https://duo.com/docs/administration-devices#assigning-a-token-to-an-end-user

Wie generiere ich Umgehungscodes?

Ein Umgehungscode ist ein temporärer Passcode, der von einem Administrator für einen Benutzer erstellt wird. Diese Codes werden in der Regel als „Backup-Codes“ verwendet, damit Benutzer, die Probleme mit ihren Mobilgeräten haben (z. B. Störung der Mobilfunkverbindung, verlorenes oder gestohlenes Gerät usw.), weiterhin auf ihre von Duo geschützten Systeme zugreifen können. Umgehungscodes können auch verwendet werden, um einem Benutzer vorübergehend Zugriff auf Anwendungen zu ermöglichen, die keine Selbstregistrierung ohne registriertes Gerät unterstützen. Umgehungscodes laufen nach der zulässigen Anzahl von Verwendungen oder nach einer vom Administrator definierten Zeitspanne ab. Standardmäßig laufen Umgehungscodes nach einmaliger Verwendung oder nach einer Stunde ab, je nachdem, was zuerst eintritt.

Befolgen Sie diesen Prozess, um Umgehungscodes zu generieren:
https://duo.com/docs/administration-users#generating-a-bypass-code

Wie kann ich einem gesperrten Benutzer helfen?

Ein Benutzer mit dem Status „gesperrt“ hat den festgelegten Grenzwert für Authentifizierungsversuche überschritten und muss seinen Status wieder auf „aktiv“ ändern lassen. Weitere Informationen zu Benutzerstatus und wie Sie sie ändern können finden Sie hier:
https://duo.com/docs/administration-users#changing-user-status

Teil 4: Expertentipps

Benutzer können wegen Phishing in höchster Alarmbereitschaft sein

Wenn Sie Duo erst vor Kurzem intern eingeführt haben, sind die Benutzer möglicherweise äußerst argwöhnisch bei eingehenden Mitteilungen, z. B. der Registrierungs- und Aktivierungs-E-Mail von Duo. Möglicherweise teilen Benutzer Ihnen mit, dass sie besorgt sind, dass diese E-Mail einen Phishing-Versuch darstellt. Wenn Sie die gesendeten Mitteilungen überprüfen möchten, können Sie die Kopie der E-Mail oder SMS im Duo-Administratorbereich ansehen und/oder den Benutzer bitten, Ihnen eine Kopie der Mitteilung weiterzuleiten, die er erhalten hat, damit Sie überprüfen können, ob es sich um eine sichere Nachricht handelt, und der Benutzer mit der Registrierung/Authentifizierung fortfahren kann.

Ermuntern Sie Benutzer, Duo Push zu verwenden

Ermuntern Sie Ihre Benutzer, soweit möglich, immer, Duo Push zu verwenden. Duo Push ist die beste Option: Es ist bequem, sicher und äußerst günstig (für die Push-Authentifizierung werden keine Telefongebühren berechnet). Benutzer können Push auch nutzen, wenn sie keine Mobilfunkverbindung haben, und es funktioniert in jedem Land.

Darüber hinaus haben wir einen Leitfaden erstellt, um die Nutzung von Duo Push bei Benutzern zu unterstützen: https://help.duo.com/s/article/promoting-push

Überprüfen Sie die Identität Ihrer Benutzer mit Help Desk Push

Sie sollten möglicherweise die Identität von Benutzern mit einem kurzen Duo-Push überprüfen, bevor Sie sie unterstützen oder auf ihren Wunsch hin Änderungen vornehmen. Weitere Informationen zur Verwendung von Help Desk Push finden Sie in der folgenden Dokumentation:
https://duo.com/docs/administration-users#verifying-users-with-duo-push

Der Duo Prompt eines Benutzers ist möglicherweise anders formatiert als erwartet

Wenn ein Benutzer sich über ein kleineres Gerät (z. B. ein Tablet) oder ein kleines Browserfenster anmeldet, sieht der Duo Prompt ggf. etwas anders aus als in der Dokumentation für Endnutzer. Allerdings erhält er immer noch die gleichen Funktionen und Rechte wie andere Benutzer.

Setzen Sie no-reply@duosecurity.com auf die Allowliste (Ausnahmeliste)

Wenn Ihr Unternehmen E-Mail-Filterung nutzt, setzen Sie diese Adresse auf die Ausnahmeliste. Andernfalls erhalten Benutzer möglicherweise keine Registrierungs- oder Aktivierungs-E-Mails.

Aktivierungslinks und Registrierungslinks haben unterschiedliche Ablaufdaten

Ein Registrierungslink läuft nach 30 Tagen ab. Wenn Sie eine Registrierungs-E-Mail erneut senden, wird das Datum für die Registrierung nicht zurückgesetzt.
Ein Aktivierungslink läuft standardmäßig nach 24 Stunden ab. Benutzern, denen kürzlich Aktivierungslinks über den Duo-Administratorbereich gesendet wurden, kann kein neuer Link gesendet werden, bis der bestehende Link abgelaufen ist.
Weitere Informationen zu den Aktivierungs- und Registrierungsbenachrichtigungen finden Sie unter https://duo.com/docs/enrolling_users.

Teil 5: Fehlerbehebung und Support

Ressourcen für die Fehlerbehebung

Sämtliche Prozesse und Empfehlungen zur Anwendungskonfiguration für den Duo-Administratorbereich finden Sie in der ausführlichen Dokumentation von Duo unter duo.com/docs.

Unter help.duo.com finden Sie die Wissensdatenbank von Duo – ein durchsuchbares Archiv mit Ressourcen zur Fehlerbehebung und Self-Service-Inhalten.

Sehen Sie in der Duo Community unter community.duo.com nach, ob die Antwort, nach der Sie suchen, in einem früheren Beitrag zu finden ist, oder beginnen Sie eine eigene Diskussion.

Haben Sie Probleme bei der Authentifizierung oder beim Zugriff auf den Duo-Administratorbereich? Unser Supportteam aktualisiert die Statusseite von Duo unter https://status.duo.com in Echtzeit, um alle Probleme mit dem Dienst wiederzugeben. Duo-Administratoren mit den Rollen „Administrator“ und „Verantwortlicher“ werden automatisch für den Empfang von Aktualisierungen der Statusseite für ihre Bereitstellung angemeldet.

Dieses Abonnement empfehlen wir Ihnen ausdrücklich! Erfahren Sie mehr über das Abonnement der Statusseite.

Die Bezugnahme auf das Authentifizierungsprotokoll kann bei der Behebung von Anmeldungsproblemen der Benutzer hilfreich sein. Machen Sie sich insbesondere mit den Gründen für verweigerte Authentifizierungen vertraut. Weitere Informationen finden Sie in diesem Artikel aus der Wissensdatenbank: https://help.duo.com/s/article/1023

Der optimale Support für Duo

Wenn Sie die nötigen Informationen nicht finden konnten, brauchen Sie Folgendes, wenn Sie sich an das Supportteam von Duo wenden:

- Vergewissern Sie sich, dass die Person, die sich an den Support wendet, im Duo-Administratorbereich als Administrator aufgeführt ist.
    - Wenn sie eine andere Administratorrolle als „Verantwortlicher“ hat, kann der Duo-Support sie nur im Rahmen ihrer Zugriffsberechtigungen unterstützen.
- Wenn andere Appliances oder Anwendungen als Duo involviert sind (z. B. Active Directory), stellen Sie sicher, dass ein Administrator mit Zugriff darauf verfügbar ist.
- Stellen Sie, soweit möglich, Screenshots und Protokolldateien bereit.
- Ihre Konto-ID.
- Die Möglichkeit, Ihre Identität über die Duo-Authentifizierung zu überprüfen. Anweisungen zur Aktivierung von Duo Push für die Administrator-Authentifizierung auf Ihrem Smartphone finden Sie hier: https://duo.com/docs/administration-admins#use-duo-push-for-administrator-authentication

    - Wenn Sie Duo Push für die Administratorüberprüfung nicht aktivieren können, dauert es ggf. länger, Ihre Identität zu Beginn eines Supportanrufs zu validieren, da wir ein anderes Verfahren anwenden müssen.
- Wenn Sie Ihren Authentifizierungs-Proxy, .cfg oder andere vertrauliche Dateien übermitteln, stellen Sie sicher, dass Sie **niemals** einen geheimen Schlüssel (SKEY) im Klartext weitergeben. Wir empfehlen GPG-Verschlüsselung.
- Wenn Sie sich bereits mit dem gleichen Problem an den Duo-Support gewendet hatten, geben Sie bitte alle bestehenden Ticketnummern an.

Bestimmen Sie auf der Grundlage Ihrer Edition und Dringlichkeit, wie und wann Sie sich an den Duo-Support wenden sollten: https://help.duo.com/s/article/1441