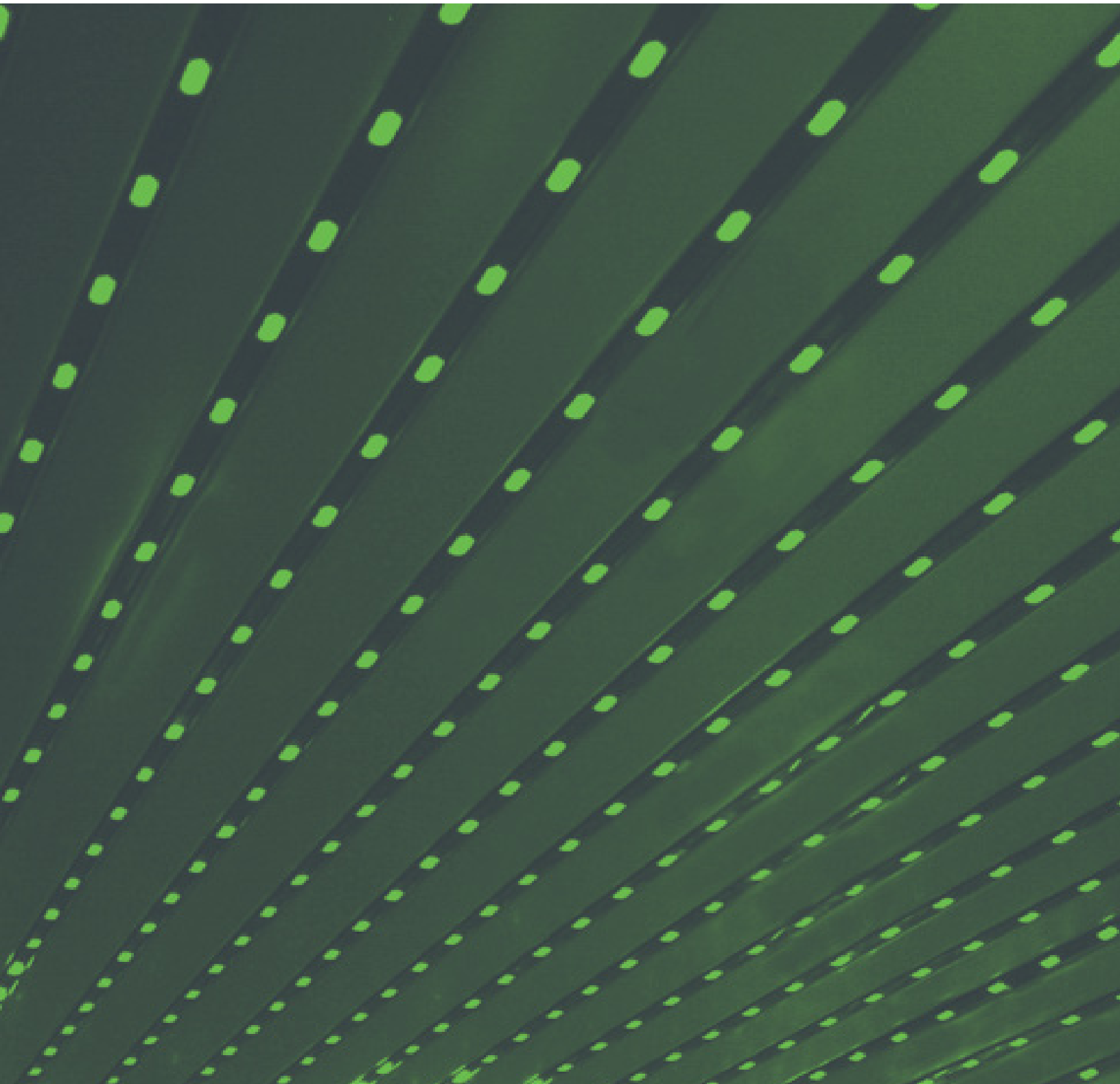
Leitfaden zur

Sicherstellung der Geschäftskontinuität

Version 3.0 veröffentlicht am 16. August 2022.



Inhaltsverzeichnis

Überblick

Warum benötige ich diesen Leitfaden?

Selbst bei robusten Lösungen kann es gelegentlich zu Serviceunterbrechungen kommen. Duo hat eine Betriebszeit von mehr als 99,99 % seit mehr als vier Jahren aufrechterhalten, was immer noch ein kleines Zeitfenster offen lässt, in dem der Duo-Service möglicherweise nicht verfügbar ist.

Ausfälle wirken sich auf die Produktivität Ihrer MitarbeiterInnen aus und können Ihren Sicherheitsstatus vorübergehend schwächen. Als Ihr vertrauenswürdiger Zugriffsanbieter möchten wir, dass Sie auf alle Situationen vorbereitet sind, und sicherstellen, dass Sie über einen Plan verfügen, um auf mögliche Ausfälle zu reagieren.

Weitere Informationen zum Service von Duo und dazu, wie unsere Cloud-Architektur und Produktentwicklungsprozesse konzipiert sind, um Hochverfügbarkeit zu gewährleisten, finden Sie in unserem Whitepaper zur Servicezuverlässigkeit.

Verständnis von Ausfällen in Ihrer Umgebung

Es sollte berücksichtigt werden, wie Ihre von Duo geschützten Anwendungen und die IT-Organisation reagieren, wenn der Duo-Service nicht verfügbar ist.

Wer darauf vorbereitet ist, sich mit Szenarien für potenzielle Serviceunterbrechungen auseinanderzusetzen, wird letztendlich für eine bessere Erfahrung mit Duo sorgen.

Dieser Leitfaden hilft Ihnen dabei:

- die beiden Kategorien von Ausfällen zu verstehen.
- die Fehlermodi von Duo zu verstehen und eine Entscheidung bezüglich Fail Safe oder Fail Secure zu treffen.
- zu verstehen, wie Ihre Anwendungen auf verschiedene Arten von Ausfällen reagieren.
- während eines Ausfalls Nachrichten an Ihre BenutzerInnen zu senden.

Erfolgsplanung

Nachdem Sie diesen Leitfaden gelesen und Ausfallszenarien und das Failmode-Verhalten Ihrer Anwendung verstanden haben, empfehlen wir dringend, anwendungsspezifische Disaster-Recovery(DR)-Pläne zu erstellen. Diese Planung sollte Folgendes umfassen:

- eine Verständnis für die Prozesse, die zum Blockieren oder Umgehen des Duo-Cloud-Service erforderlich sind, wenn das Failmode-Verhalten nicht wie erwartet aufgerufen wird
- ein Verfahren zum Entfernen von Duo aus dem Authentifizierungs-Workflow für **jede geschützte Anwendung**

Konfigurationsentscheidungen

Überlegen Sie sich gut, welche Failmode-Konfiguration (Safe vs Secure) Sie für jede Anwendung verwenden sollten (falls verfügbar).* Ihre Wahl hängt wahrscheinlich von Folgendem ab:

- Richtlinien- und Compliance-Faktoren
- der Art von Daten, die in geschützten Anwendungen enthalten sind
    - Patientenakten, Finanzen, personenbezogene Daten, geistiges Eigentum usw.
- Benutzergruppen mit unterschiedlichen Zugriffsebenen
- der Notwendigkeit, Sicherheit und Benutzerfreundlichkeit in Einklang zu bringen

* Lesen Sie die Dokumentation Ihrer spezifischen Anwendung auf duo.com/docs, um zu sehen, ob sie über einen konfigurierbaren Failmode verfügt.

In Bezug auf Failmode-Konfigurationen und Aktionspläne im Falle von Servicebeeinträchtigungen gibt es im Allgemeinen drei Hauptkategorien, unter die die Anwendung eines Unternehmens fallen kann:

Einschränkungsebene	Nichterreichbarkeit (Failmode aufgerufen)	Beeinträchtigung (Failmode nicht aufgerufen)
Am stärksten restriktiv Vertragsdaten, rechtliche Daten, Richtliniendaten oder vertrauliche Daten in einer geschützten Anwendung **erfordern ausnahmslos eine Zwei-Faktor-Authentifizierung.**	Fail secure	BenutzerInnen und Gruppen sollten NICHT in den Status „Umgehung“ gesetzt werden, da dadurch die Zwei-Faktor-Authentifizierung übersprungen wird.
Restriktiv Für einige Untergruppen von BenutzerInnen muss immer und ohne Ausnahme auf eine Zwei-Faktor-Authentifizierung bestanden werden.	Fail secure	BenutzerInnen und Gruppen, die ausnahmslos die Zwei-Faktor-Authentifizierung bestehen müssen, sollten NICHT in den Status „Umgehung“ gesetzt werden, da dadurch die Zwei-Faktor-Authentifizierung übersprungen wird. BenutzerInnen und Gruppen, für die ein Anwendungszugriff ohne Zwei-Faktor-Authentifizierung tolerierbar ist, können auf „Umgehung“ gesetzt werden, sodass die Zwei-Faktor-Authentifizierung übersprungen wird.
Weniger restriktiv Vertragsdaten, rechtliche Daten, Richtliniendaten oder vertrauliche Daten in einer geschützten Anwendung **erfordern keine Zwei-Faktor-Authentifizierung unter allen Umständen.**	Fail safe	BenutzerInnen und Gruppen, für die ein Anwendungszugriff ohne Zwei-Faktor-Authentifizierung tolerierbar ist, können auf „Umgehung“ gesetzt werden, sodass die Zwei-Faktor-Authentifizierung übersprungen wird.

* Beachten Sie: Wenn eine Gruppe von BenutzerInnen Zugriff auf mehr als eine Anwendung hat, bedeutet der Status „Umgehung“, dass die Zwei-Faktor-Authentifizierung für alle diese Anwendungen übersprungen wird. Wenn dieser Schritt erforderlich ist, um einer Gruppe Zugriff auf eine andere Anwendung zu gewähren, sollte der Zugriff der Gruppe auf diese bestimmte Anwendung zuerst verweigert werden.

Arten von Ausfällen

Duo-Serviceunterbrechungen können in der Regel in eine von zwei Kategorien eingeteilt werden: der Duo-Service ist entweder **nicht erreichbar** oder **beeinträchtigt**.

Die Unterscheidung zwischen der Nichterreichbarkeit oder der Beeinträchtigung des Duo-Services ist wichtig, da sie das Verhalten der von Duo geschützten Anwendungen und letztlich das Erlebnis Ihrer EndbenutzerInnen beeinflusst.

Der Duo-Service ist nicht erreichbar.

(Failmode aufgerufen)

- Der Duo-Service ist vorübergehend nicht verfügbar.
  - Der Duo-Service kann die Duo-Aufforderung nicht anzeigen oder innerhalb von 180 Sekunden auf Auth API-Anfragen antworten.
- Netzwerkkonnektivität, die Kundenanwendungen daran hindert, den Service von Duo zu erreichen. Diese treten in der Regel im lokalen Netzwerk des Kunden auf, können jedoch manchmal auf regionaler oder globaler Ebene auftreten.
  - Baufirma beschädigt Glasfaserleitung
  - Probleme mit Firewall oder DNS
  - Probleme mit der ISP-Konnektivität oder dem Routing
- Probleme bei der Anwendung/Integration
  - Von Duo geschützte Anwendung ist falsch konfiguriert.

Der Duo-Service ist beeinträchtigt.

(Failmode nicht aufgerufen)

- Fehler bei der Zwei-Faktor-Methode
  - Der Telefonieanbieter von Duo (SMS/Anrufe) ist selbst von einem Ausfall betroffen.
  - APNS (Apple Push Notification Service) übermittelt keine Push-Benachrichtigungen an iPhones* von BenutzerInnen.
- Authentifizierungen werden nicht abgeschlossen.
  - Duo pusht fehlerhaften Code, der BenutzerInnen daran hindert, sich erfolgreich anzumelden.
  - Die Duo-Authentifizierungslatenz und Authentifizierungsfehler nehmen zu, aber der Service bleibt teilweise verfügbar.

* BenutzerInnen vergessen häufig, Benachrichtigungen auf ihren Telefonen zuzulassen – dies gilt nicht als Beeinträchtigung des Duo-Service. BenutzerInnen können ihre Duo Mobile App starten und sehen eine ausstehende Authentifizierungsanfrage. Weitere Fehlerbehebungen für EndbenutzerInnen finden Sie in unseren iOS- oder Android-Leitfäden.

Woher weiß ich, dass ein Ausfall aufgetreten ist?

Wenn bei Ihnen oder Ihren BenutzerInnen Probleme auftreten, von denen Sie vermuten, dass sie mit einem Ausfall zusammenhängen, gehen Sie zunächst auf status.duo.com, um nach Meldungen über potenzielle Ausfälle zu suchen. Wenn Sie der Meinung sind, dass Sie von einem Ausfall betroffen sind, oder wenn Sie ein technisches Problem haben, das nicht mit einer Serviceunterbrechung zusammenhängt, wenden Sie sich an den Duo Support.

Weitere Optionen zur Überwachung des Cloud-Service von Duo sind in diesem Wissensdatenbankartikel dokumentiert.

Duo-Fehlermodus: Duo-Service nicht erreichbar

Der Fehlermodus (häufig als „Failmode“ bezeichnet) wird aufgerufen, wenn der Duo-Service nicht erreichbar ist oder ein kritisches Problem erkannt wird. Duo verfügt über Fehlererkennungsmechanismen, die den Failmode basierend auf erkannten Fehlern auslösen.

Um die weitere Erreichbarkeit des Duo-Service zu gewährleisten, müssen Kunden die Kommunikation mit allen IP-Bereichen von Duo ermöglichen. Eine Liste der IP-Bereiche und zusätzliche Überlegungen finden Sie in diesem Artikel.

Manchmal manifestieren sich Serviceunterbrechungen auf andere Weise. Beispielsweise könnte der Duo-Service erreichbar sein, aber die Authentifizierung schlägt aus anderen Gründen fehl. Weitere Informationen hierzu finden Sie nachstehend unter Duo-Servicebeeinträchtigung.

Der Failmode kann so konfiguriert werden, dass er sich auf zwei Arten verhält:

1. **Fail safe** (auch als „fail open“ bezeichnet): Wenn der Duo-Service nicht erreichbar ist, wird BenutzerInnen Zugriff auf von Duo geschützte Anwendungen **GEWÄHRT**, wenn sie die primäre Authentifizierung bestehen.
    - Dies schwächt Ihren Sicherheitsstatus, da die Zwei-Faktor-Authentifizierung vorübergehend ausgesetzt wird.
    - Der Modus verursacht weniger Probleme für die BenutzerInnen und unterbricht den Workflow nicht, weil sich MitarbeiterInnen weiterhin anmelden und arbeiten können.
    - In einer authproxy.cfg-Datei wird dies beispielsweise in einem Serverabschnitt durch die folgende Syntax angezeigt:
      Weitere Informationen zu Konfiguration von Authentification Proxys finden Sie hier.

```
failmode=safe
```

2. **Fail secure** (auch als „fail closed“ bezeichnet): Wenn der Duo-Service nicht erreichbar ist, wird BenutzerInnen der Zugriff auf von Duo geschützte Anwendungen **VERWEIGERT**, *auch wenn* sie die primäre Authentifizierung bestehen.
    - Diese Option ist die sicherste.
    - Sie kann beträchtliche Störungen in Bezug auf den täglichen Arbeitsablauf bewirken, da BenutzerInnen der Zugriff auf die App verweigert wird.
    - In einer authproxy.cfg-Datei wird dies beispielsweise in einem Serverabschnitt durch die folgende Syntax angezeigt:

```
failmode=secure
```

Im nachstehenden Abschnitt zu Konfigurationsentscheidungen erhalten Sie Hilfe bei der Entscheidung, ob Sie den „fail safe“- oder den „fail secure“-Modus aktivieren sollen.

Duo-Fehlermodus: Duo-Service ist beeinträchtigt

In diesem Fall kann der Duo Authentication Proxy, der Duo Access Gateway oder eine andere von Duo geschützte Anwendung zwar den Duo-Service erreichen, die Authentifizierung kann jedoch nicht abgeschlossen werden. Der Failmode wird nicht aufgerufen.

Mögliche Szenarien

- Authentifizierung wird nicht abgeschlossen
  - Beispiel aus der Praxis: Duo hat Code gepusht, der die Authentifizierung für Kunden mit einer älteren Version der Duo-Aufforderung unterbrochen hat. BenutzerInnen konnten sich nicht anmelden, obwohl sie die primäre Authentifizierung erfolgreich bestanden und die sekundäre Authentifizierungsanforderung genehmigt hatten.

- Fehler bei einer oder mehrerer Authentifizierungsverfahren
  - Beispiel aus der Praxis: Der SMS-Dienst von Duo hat keine SMS an BenutzerInnen gesendet, sodass sie sich nicht authentifizieren konnten.

Lösungen

Einige Lösungen sind möglicherweise nicht für alle Kunden und alle Szenarien realisierbar. Beispielsweise kann eine Änderung der Firewall-Regel problematischer sein als die Nachrichtenübermittlung an Ihre BenutzerInnen. Ziehen Sie die Lösungen in Betracht, die für Ihr Unternehmen am besten sind. Probleme mit Servicebeeinträchtigungen werden in der Regel innerhalb von 30 Minuten behoben. Wenn Sie eine der folgenden Lösungen verwenden, **stellen Sie sicher, dass Sie die Änderungen nach der Lösung des Problems rückgängig machen.**

- Wenden Sie eine Authentifizierungsrichtlinie an, um die Zwei-Faktor-Authentifizierung zu umgehen, während die Servicebeeinträchtigung fortbesteht. Kunden mit kostenpflichtigen Editionen von Duo können Authentifizierungsrichtlinien nutzen. Sollte der Duo-Service nicht erreichbar sein, kann diese Lösung auch verwendet werden.
  - Vorgehensweise: Erstellen und wenden Sie vorübergehend eine Authentifizierungsrichtlinie auf Anwendungsebene an.
  - Wirkung: Ermöglicht BenutzerInnen den Zugriff auf eine bestimmte Anwendung, ohne dass sie die Zwei-Faktor-Authentifizierung abschließen müssen. Der Zugriff kann basierend auf der Gruppenmitgliedschaft der jeweiligen BenutzerInnen eingeschränkt oder gewährt werden.

- Informieren Sie die BenutzerInnen über die Unterbrechung und bieten Sie Problemumgehungen an, sofern Duo eine auf status.duo.com veröffentlicht hat.
  - Vorgehensweise: Lesen Sie den Abschnitt Kommunikationsvorlagen für EndbenutzerInnen weiter unten. Navigieren Sie zu status.duo.com, um festzustellen, ob Duo temporäre Problemumgehungen gemeldet hat.
  - Wirkung: Versichert den BenutzerInnen, dass Ihr Unternehmen und Duo sich des Problems bewusst sind und an dessen Behebung arbeiten.

- Verschieben Sie alle oder einige BenutzerInnen in eine Gruppe, für die der Status „Umgehen“ festgelegt ist.
  - Vorgehensweise: Aktualisieren Sie BenutzerInnen manuell oder in Massenbearbeitungsweise, um sie in eine Gruppe zu verschieben, falls sie noch keiner Gruppe zugeordnet sind. Diese Gruppe benötigt erstens Zugriff auf die geschützte Anwendung und muss zweitens auf den Status „Umgehen“ gesetzt werden.
  - Wirkung: Durch diese Vorgehensweise wird die Zwei-Faktor-Authentifizierung für jede/n BenutzerIn in der Gruppe umgangen.

- Stellen Sie die Konfiguration/das Profil für Anwendungen zurück, um Duo nicht aufzurufen.
  - Vorgehensweise: Lesen Sie die Dokumentation zu Ihrer spezifischen Anwendung auf duo.com/docs.
  - Wirkung: Hierdurch wird die Zwei-Faktor-Authentifizierung aus dem Authentifizierungs-Workflow entfernt.

- Verwenden Sie für Anwendungen, die den Duo Authentication Proxy verwenden, die Funktion Nur primärer Modus.
    - Vorgehensweise: Diese Funktion wurde in der Authentication Proxy-Version 2.14.0 eingeführt und wird durch Ausführen eines Befehls auf dem Proxyserver ausgelöst.
    - Wirkung: Durch diese Vorgehensweise wird die Duo-Authentifizierung für alle Anmeldungen zu RADIUS- oder LDAP-Konfigurationen, die das standardmäßige „fail safe“-Verhalten verwenden, vorübergehend übersprungen (standardmäßig eine Stunde oder maximal vier Stunden).

- Blockieren Sie den Service von Duo manuell über eine Firewall-Regel, um effektiv ein Szenario für eine Nichterreichbarkeit zu erstellen.
    - Vorgehensweise: Blockieren Sie *.duo.com und *.duosecurity.com auf dem TCP-port 443.
    - Wirkung: Hierdurch wird der Failmode aufgerufen. Wenn „fail safe“ konfiguriert ist, wird der Zugriff auf die Anwendung ohne Zwei-Faktor-Authentifizierung gewährt. Wenn „fail secure“ konfiguriert ist, wird der Zugriff blockiert. Beobachten Sie status.duo.com genau, um zu wissen, wann diese Änderung rückgängig gemacht werden kann.

Verständnis des Failmode-Verhaltens Ihrer Anwendung

Die Failmode-Konfigurationsoptionen und das Verhalten während eines Ausfalls können je nach der von Duo geschützten Anwendung unterschiedlich sein. In diesem Abschnitt besprechen wir wichtige Unterscheidungen und Details zu von Duo entwickelten Anwendungen, dem Duo Web-SDK und beliebte Anwendungen, die von Drittanbietern entwickelt wurden, damit Sie besser verstehen können, wie sich Ausfälle auf Ihre von Duo geschützten Anwendungen auswirken.

Von Duo entwickelte Anwendungen, die eine Failmode-Steuerung bieten

In der folgenden Tabelle sind die von Duo entwickelten und unterstützten Anwendungen aufgeführt, die eine Failmode-Steuerung sowie zusätzliche Details dazu bereitstellen, wie der Failmode-Modus in verschiedenen Ausfallszenarien aufgerufen werden kann (oder nicht). Um sicherzustellen, dass Sie über alle Funktionen und Sicherheitsverbesserungen verfügen, empfehlen wir immer, auf die neueste verfügbare Version zu aktualisieren.

- Duo Authentication Proxy
- Duo Access Gateway (DAG)
- Duo für Windows-Anmeldung/RDP
- Duo Unix
- AD FS 2.X
- AD FS 3/4
- OWA
- RD Web/Gateway
- Oracle Access Manager

Von Duo entwickelte Anwendungen, die keine Failmode-Steuerung bieten

- Duo Network Gateway (DNG)
- Microsoft Azure Active Directory (bedingter Zugriff)
- Duo Single Sign-On

WebSDKv2

Das WebSDKv2 von Duo verfügt nicht über einen integrierten Mechanismus, der den Failmode auslöst oder automatisch überprüft, ob der Duo-Service von Ihrer Web-SDK-Anwendung aus erreichbar ist.Wenn der Cloud-Service von Duo nicht mehr erreichbar ist, lässt das Web-SDK für BenutzerInnen keine Authentifizierung zu, wenn sie die Zwei-Faktor-Authentifizierung nicht erfolgreich abschließen.

Die Bedingungen, unter denen die Anwendung in den fail safe-Modus (offen) geht, müssen unbedingt sorgfältig programmiert werden, um ein unbeabsichtigtes Szenario für die Umgehung der Zwei-Faktor-Authentifizierung zu vermeiden.Zur Überwachung des Service können Sie den Ping-Endpunkt der Auth-API von Duo verwenden, um einen Lifetest für den Duo-Service zu implementieren (für den keine Duo-Integrationsinformationen erforderlich sind). Sie können dann den Endpunkt für die Auth-API-Prüfung verwenden (empfohlen), um die Integrationsinformationen und die Signatur zu überprüfen. Weitere Informationen erhalten Sie hier in unserer Dokumentation.

Wenn Sie ein benutzerdefiniertes fail safe-Verhalten entwickeln, stellen Sie sicher, dass Sie die Bedingungen zum Aufruf des Failmode-Verhaltens gründlich testen. Wie immer bleibt das fail secure-Verhalten (geschlossen) in allen Szenarien die sicherste Option.

WebSDKv4

Duo WebSDKv4 verfügt über eine integrierte Funktion, mit der festgestellt werden kann, ob die Server von Duo zugänglich und verfügbar sind, um die 2FA-Anfrage zu akzeptieren. Dokumentation zum Aufruf dieser Funktion finden Sie hier. Wie bei WebSDKv2 müssen Anwendungsentwickler die Anwendung dennoch mit einer Logik programmieren, um zu bestimmen, wie die Anwendung vorgehen soll, wenn die Duo-Funktion einen Fehler zurückgibt (fail safe oder fail secure). Wenn die Anwendung keine Prüfungen für den Service oder die Logik von Duo enthält, um zu bestimmen, wie mit einem Fehler umgegangen werden soll, wird standardmäßig fail secure (geschlossen) verwendet.

Wie immer bleibt das fail secure-Verhalten (geschlossen) in allen Szenarien die sicherste Option.

Von Drittanbietern entwickelt

Obwohl Duo versucht, mit möglichst vielen Drittanbietern zusammenzuarbeiten und sicherzustellen, dass Integrationen nach bewährten Verfahren verfolgen, verlangt Duo nicht, dass Drittanbieter entwickelte Integrationen zur Überprüfung einreichen oder Duo benachrichtigen. Daher ist Duo nicht unbedingt über alle Integrationen von Drittanbietern oder darüber informiert, wie diese Integrationen mit einer Failmode-Steuerung umgehen.

Im Folgenden finden Sie eine Liste mit beliebten, von Drittanbietern entwickelten Duo-Integrationen und Hinweise dazu, ob/wie sie den Failmode unterstützen:

- LastPass
  - Kein konfigurierbarer Failmode
  - BenutzerInnen können einem Gerät vertrauen und müssen dann für einen bestimmten Zeitraum keine MFA mehr ausführen.
  - In DR-Szenarien müssen sich AdministratorInnen bei LastPass anmelden und Duo aus dem Authentifizierungs-Workflow entfernen.
- 1Password
  - Kein konfigurierbarer Failmode
  - Benötigt keine MFA für Offline-Zugriff oder eigenständigen Passwort-Tresor
- Okta
  - Kein konfigurierbarer Failmode
  - In DR-Szenarien müssen sich AdministratorInnen anmelden, um Duo aus dem Authentifizierungs-Workflow zu entfernen.
- OneLogin
  - Kein konfigurierbarer Failmode
  - In DR-Szenarien müssen sich AdministratorInnen anmelden, um Duo aus dem Authentifizierungs-Workflow zu entfernen.
- Ping Federate
  - Bietet konfigurierbaren Failmode. Dokumentation finden Sie hier.
- CAS
  - Bietet konfigurierbaren Failmode. Dokumentation finden Sie hier.

WICHTIG: Nicht alle Integrationen bieten einen Mechanismus zur Steuerung des Failmode-Verhaltens.

- Integrationen, die den Authentication Proxy oder Duo Access Gateway verwenden, **haben die Möglichkeit**, einen Failmode zu bestimmen.
- Die meisten von Duo entwickelten Integrationen erlauben eine Failmode-Konfiguration während des Installationsvorgangs. Beispielsweise ist der Failmode der Duo-Authentifizierung für die Windows-Anmeldung und RDP im Installationsprogramm konfigurierbar. Die meisten Duo-Anwendungspakete bieten auch eine Möglichkeit, das Failmode-Verhalten nach der Installation zu ändern (z. B. bei Duo Unix und der Windows-Anmeldung).
- Duo-Integrationen, die von Drittanbietern wie Thycotic, Ping Federate und Lastpass erstellt wurden, bieten eventuell keine Möglichkeit, den Failmode zu steuern, und können standardmäßig für „fail secure“ konfiguriert sein.Bitte lesen Sie die Dokumentation des Anbieters, um alle Failmode-Funktionen zu überprüfen.
- Die WebSDKv2-Integration enthält keine Failmode-Prüflogik. Weitere Informationen finden Sie im Abschnitt „Verstehen Sie, wie Ihre Anwendungen auf verschiedene Arten von Ausfällen reagieren“.
- Azure Conditional Access (CA) geht in den fail closed-Modus, wenn der Cloud-Service von Azure den Cloud-Service von Duo nicht erreichen kann.
    - Bei langfristigen Ausfällen müssen Kunden möglicherweise die Duo 2FA-Anforderung aus der CA-Richtlinie entfernen, damit BenutzerInnen auf Anwendungen ohne 2FA zugreifen können.
- Das Duo Network Gateway (DNG) geht in den fail closed-Modus, wenn es den Cloud-Service von Duo nicht erreichen kann.
- BenutzerInnen können sich nicht mit Anwendungen authentifizieren, die mit Duo SSO verbunden sind.
    - Da Duo SSO sowohl die primäre als auch die sekundäre Authentifizierung übernimmt, müssen BenutzerInnen den Service direkt erreichen können.
    - Bei längerfristigen Ausfällen müssen Kunden möglicherweise die Anwendung manuell aus Duo SSO entfernen und die Anwendung für die Verwendung einer anderen Authentifizierungsquelle konfigurieren. Dies ist für viele Anwendungen häufig umständlich und unpraktisch und sollte nur als letzte Möglichkeit betrachtet werden.

Kommunikationsvorlagen für EndbenutzerInnen

Überlegen Sie, welcher Zeitpunkt für Ihr Unternehmen günstig ist, um EndbenutzerInnen zu benachrichtigen. Diese Möglichkeiten gibt es: sobald Ihre BenutzerInnen Probleme melden, nachdem Duo eine Benachrichtigung auf status.duo.com veröffentlicht hat, bevor Ihre BenutzerInnen etwas gemeldet haben oder wenn ein Vorfall 20 Minuten oder länger ungelöst geblieben ist.

Uhrzeit

- Ein Vorfall, der sich um 11.00 Uhr an einem Wochentag ereignet, kann eine sofortige Benachrichtigung der BenutzerInnen erfordern.
- Ein Vorfall um 23 Uhr an einem Wochenende muss den BenutzerInnen möglicherweise nicht sofort mitgeteilt werden.

Zeitpunkt im Quartal

- Ein Vorfall in der letzten Woche eines Quartals kann eine sofortige Benachrichtigung der BenutzerInnen erfordern.

Kritikalität des Zugriffs

- Ein Vorfall, der den Zugriff auf eine kritische Anwendung beeinträchtigt, kann unabhängig von der Uhrzeit, dem Datum oder anderen Faktoren eine sofortige Benachrichtigung erfordern.

Duo-Service ist nicht erreichbar oder beeinträchtigt

Wenn Sie den fail safe-Modus verwenden, wenn Duo nicht erreichbar ist, oder den Failmode während der Beeinträchtigung manuell aufrufen:

BETREFF:	Authentifizierungsprobleme – in Bearbeitung
TEXTKÖRPER:	Duo meldet Probleme mit seinem Service. Als vorübergehende Problemumgehung heben wir die Anforderung der Zwei-Faktor-Authentifizierung von Duo auf. Sobald das Problem behoben ist, wird die Zwei-Faktor-Authentifizierung wieder aktiviert.

Wenn Sie den fail secure-Modus verwenden:

BETREFF:	Authentifizierungsprobleme – in Bearbeitung
TEXTKÖRPER:	Wir haben Probleme mit der Zwei-Faktor-Authentifizierung von Duo. Aufgrund der Art der in <Ihrer Anwendung> enthaltenen Daten wird der Zugriff verweigert, bis dieses Problem behoben ist.

Problem mit dem Authentifizierungsverfahren

BETREFF:	Authentifizierungsprobleme – in Bearbeitung
TEXTKÖRPER:	Duo meldet Probleme mit dem <Push/SMS/Telefon>-Service. Verwenden Sie als temporäre Problemumgehung die <SMS-/Push-/Rückruffunktion>. Sie können mit einer weiteren Aktualisierung rechnen, wenn das Problem behoben wurde.

Häufig gestellte Fragen

Kann ich benachrichtigt werden, wenn der Failmode aufgerufen wird?

Der Failmode wird lokal in Ihrem Duo Authentication Proxy oder in der von Duo geschützten Anwendung konfiguriert und aufgerufen. Es wird empfohlen, ein Überwachungstool oder eine SIEM-Lösung zu verwenden, um eine Failmode-Transaktion zu beobachten.

Sie können feststellen, ob der Failmode aufgerufen wurde, indem Sie die Protokolle zu Ihren Authentication Proxys lesen. Das Standardverzeichnis zum Speichern von Protokollen ist „C:\Program Files (x86)\Duo Security Authentication Proxy\log“ auf einem 64-Bit-Windows-Computer und „C:\Program Files\Duo Security Authentication Proxy\log“ auf einem 32-Bit-Windows-Computer.

Im Folgenden sehen Sie zwei Beispiele für Protokolle für Duo Authentication Proxys, die angezeigt werden, wann der Failmode aufgerufen wurde.

1. **Beispiel für fail safe**-Protokoll

```
!! Auth Proxy versions 2.11.0 and later

2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Failmode Safe - Allowed Duo login on
preauth failure
2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Returning response code 2: AccessAccept
2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Sending response


!! Auth Proxy versions 2.10.1 and earlier

2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Allowed Duo login on unexpected failure
2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Returning response code 2:
AccessAccept
2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Sending response
```

2. **Beispiel für fail secure**-Protokoll

```
!! Auth Proxy versions 2.11.0 and later


2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Failmode Secure - Denied Duo login on
preauth failure
2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Returning response code 3: AccessReject
2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Sending response


!! Auth Proxy versions 2.10.1 and earlier


2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Denied Duo login on unexpected failure
2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Returning response code 3:
AccessReject
2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Sending response
```

Unten steht die Ausgabe von einem SIEM-freundlichen authevents.log:

1. **Beispiel für fail safe**-Protokoll

```
!! Auth Proxy versions 2.11.0 and later

{"username": "testuser1", "status": "Allow", "client_ip": null, "server_section":
"radius_server_auto", "timestamp": "2018-11-09T21:53:57.950000Z", "auth_stage": "Secondary
authentication", "factor": null, "msg": "Failmode Safe - Allowed Duo login on preauth failure"}

!! Auth Proxy versions 2.10.1 and earlier

{"username": "testuser1", "status": "Allow", "client_ip": null, "server_section":
"radius_server_auto", "msg": "Allowed Duo login on unexpected failure", "timestamp": "2018-04-
17T21:39:13.416000Z", "auth_stage": "Secondary authentication"}
```

2. **Beispiel für fail secure**-Protokoll

```
!! Auth Proxy versions 2.11.0 and later

{"username": "testuser1", "status": "Reject", "client_ip": null, "server_section":
"radius_server_auto", "timestamp": "2018-11-09T21:57:51.326000Z", "auth_stage": "Secondary
authentication", "factor": null, "msg": "Failmode Secure - Denied Duo login on preauth failure"}

!! Auth Proxy versions 2.10.1 and earlier

{"username": "testuser1", "status": "Reject", "client_ip": null, "server_section":
"radius_server_auto", "msg": "Denied Duo login on unexpected failure", "timestamp": "2018-04-
17T21:38:11.822000Z", "auth_stage": "Secondary authentication"}
```

Werden Duo-Bereitstellungen mit Hochverfügbarkeit erstellt oder als „aktiv/aktiv“ konzipiert?

Ja, Duo-Bereitstellungen sollten nicht als einzelner Knoten betrachtet werden. Duo nutzt zahlreiche unabhängige Cluster oder „Bereitstellungen“ seiner Technologie, um das Wachstum des Kundenunternehmens zu unterstützen und sicherzustellen, dass die Auswirkungen eines Fehlers in einer Bereitstellung minimiert werden. Die zugrunde liegenden Infrastrukturkomponenten jeder dieser Bereitstellungen werden durch Echtzeitreplikation zwischen mehreren physischen Rechenzentren unterstützt, welche die Verfügbarkeitszonen von Amazon Web Services (AWS) ausmachen. Duo repliziert Kundendaten auch in Echtzeit in mindestens eine zusätzliche AWS-Region für jede einzelne Bereitstellung.

Wie schützt Duo Bereitstellungen vor DDoS-Angriffen?

AWS unternimmt Schritte, um DDoS-Angriffe auf die Infrastruktur von Duo mithilfe der proprietären AWS Shield-Präventionstechnologie gegen DDoS transparent abzuwehren. Im Falle eines Angriffs auf Duo-Services, der nicht automatisch durch AWS oder durch die abgesicherte Infrastruktur von Duo behandelt wird, werden Duo-MitarbeiterInnen sofort auf das Problem aufmerksam gemacht, damit sie bei Bedarf Maßnahmen ergreifen. Diese Reaktion könnte das systematische Blackholing bestimmter IP-Adressen/Netzblöcke oder sogar die Verlagerung des Datenverkehrs beim Kunden auf nicht betroffene Infrastrukturen und/oder IP-Adressen umfassen.

Können meine Konten im Falle eines Ausfalls zu einer anderen Bereitstellung umverlegt werden?

Die Technologie zum Verschieben zwischen Bereitstellungen wurde entwickelt, um die Auswirkungen auf die Quell- und Zielbereitstellung zu minimieren. Sie kann häufig ein relativ langwieriger Prozess sein, da sie im Hintergrund ausgeführt wird. Dieser Prozess ist nicht für die Ausführung als Teil eines Fehlerszenarios geeignet. Darüber hinaus kann das Verschieben von Kunden-Workloads in eine andere Infrastruktur in einigen Fällen das zugrunde liegende Problem möglicherweise nicht beheben und sogar die Auswirkungen eines Ausfalls verstärken. In einigen Ausfallszenarien kann das Verschieben betroffener Kundenkonten in eine andere Bereitstellung das zugrunde liegende Problem mit übertragen und möglicherweise die Dauer des Ausfalls verlängern.

Wir waren von einem Ausfall betroffen. Können wir zu einer anderen Bereitstellung umverlegt werden?

Alle Duo-Bereitstellungen werden gleich erstellt, verfügen über dieselbe Hochverfügbarkeit und können hinsichtlich der Betriebszeit eine Erfolgsbilanz vorweisen. Aus diesen Gründen verringert das Verschieben der aktuellen Bereitstellung nicht von Natur aus das Risiko eines Ausfalls.