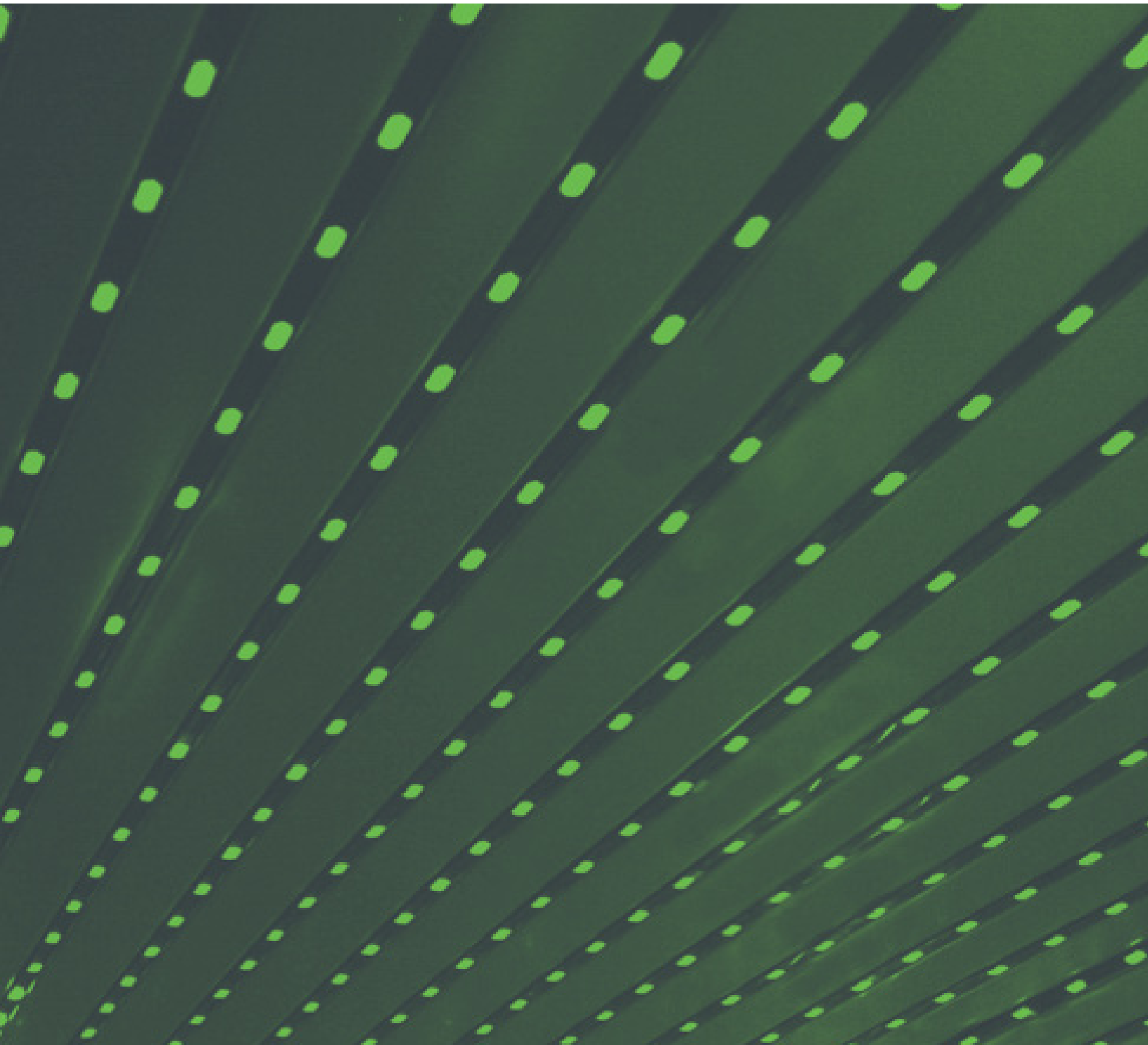
Guide de

préparation pour garantir la continuité des activités de l'entreprise

Version 3.0 publiée le 16 août 2022



Sommaire

Présentation

En quoi ce guide est-il utile ?

Même les solutions les plus robustes subissent parfois des interruptions de service. Duo assure un temps de fonctionnement supérieur à 99,99 % depuis plus de quatre ans, mais le risque d'indisponibilité du service existe, même s'il est très faible.

Les interruptions ont un impact sur la productivité des collaborateurs et peuvent temporairement affaiblir votre sécurité. En tant que fournisseur d'accès, nous voulons vous préparer à toutes les situations possibles et vous aider à planifier vos mesures en cas d'interruption.

Pour plus d'informations sur le service Duo et sur la prise en charge de la haute disponibilité par notre architecture cloud et nos processus de développement des produits, consultez notre livre blanc sur la fiabilité des services.

Comprendre les interruptions et votre environnement

Réfléchissez à la manière dont vos applications protégées par Duo et votre département informatique réagiront en cas d'indisponibilité soudaine du service.

En vous préparant à la prise en charge d'une interruption de service potentielle, vous améliorerez l'expérience d'utilisation de Duo.

Ce guide vous aidera à :

- Comprendre les deux catégories d'interruption
- Comprendre les modes de défaillance de Duo et choisir entre le mode Fail Safe et Fail Secure
- Comprendre comment vos applications réagissent à différents types d'interruption
- Envoyer un message à vos utilisateurs lors d'une interruption

Planifier votre réussite

Une fois que vous aurez lu ce guide et compris les scénarios d'interruption et les comportements de vos applications en cas de défaillance, nous vous recommandons de créer des plans de reprise après sinistre spécifiques à chaque application. Vous devez planifier les étapes suivantes :

- Compréhension des processus requis pour bloquer ou contourner le service cloud de Duo si le comportement failmode n'est pas invoqué comme prévu.
- Procédures de retrait de Duo du workflow d'authentification pour **chaque application protégée**.

Décisions relatives à la configuration

Réfléchissez bien à la configuration failmode (safe ou secure) à utiliser pour chaque application (si disponible).* Votre choix dépendra des éléments suivants :

- Politique et facteurs de conformité
- Le type de données contenues dans les applications protégées
  - Dossiers médicaux, données financières, informations personnelles identifiables (PII), propriété intellectuelle, etc.
- Groupes d'utilisateurs avec différents niveaux d'accès
- La nécessité d'équilibrer sécurité et facilité d'utilisation

*Consultez la documentation spécifique à votre application sur duo.com/docs pour savoir si elle permet de configurer le failmode.

Concernant les configurations failmode et les plans d'action en cas de détérioration du service, l'application d'une entreprise entre généralement dans l'une des trois grandes catégories suivantes :

Niveau de restriction	Injoignable (failmode invoqué)	Détérioration du service (failmode non invoqué)
Très restrictif Le contrat, la législation, la politique ou la sensibilité des données contenues dans l'application protégée **exigent une authentification à deux facteurs. Il n'y a pas d'exception**.	Fail secure	Les utilisateurs et les groupes ne doivent PAS basculer vers l'état « contournement », sinon l'authentification à deux facteurs est ignorée.
Restrictif Certains sous-ensembles d'utilisateurs doivent toujours passer l'authentification à deux facteurs. Il n'y a pas d'exception.	Fail secure	Les utilisateurs et les groupes qui, sans exception, doivent passer l'authentification à deux facteurs ne doivent PAS basculer vers l'état « contournement », sinon l'authentification à deux facteurs est ignorée. Les utilisateurs et les groupes qui sont autorisés à accéder à cette application sans authentification à deux facteurs peuvent basculer vers l'état « contournement » pour ignorer l'authentification à deux facteurs.
Peu restrictif Le contrat, la législation, la politique ou la sensibilité des données contenues dans l'application protégée **n'exigent pas l'utilisation de l'authentification à deux facteurs, quelles que soient les circonstances**.	Fail safe	Les utilisateurs et les groupes qui sont autorisés à accéder à cette application sans authentification à deux facteurs peuvent basculer vers l'état « contournement » pour ignorer l'authentification à deux facteurs.

*Si un groupe d'utilisateurs a accès à plus d'une application, le basculement vers l'état « contourner » a pour conséquence d'autoriser l'accès à toutes les applications en ignorant l'authentification à deux facteurs. Pour qu'un groupe accède à une autre application sans ignorer l'authentification à deux facteurs, vous devez d'abord retirer l'accès de ce groupe à cette application.

Types d'interruption

Les interruptions de service de Duo se classent généralement dans l'une des deux catégories suivantes : le service Duo est **inaccessible** ou le service Duo est **détérioré**.

La distinction entre inaccessibilité et détérioration du service Duo est importante, car elle affecte le comportement des applications protégées par Duo et par conséquent l'expérience des utilisateurs finaux.

Service Duo inaccessible

(failmode invoqué)

- Service Duo temporairement indisponible
  - Le service ne parvient pas à afficher l'invite Duo ou ne répond pas aux demandes Auth API dans un délai de 180 secondes
- Connectivité réseau ne permettant pas aux applications du client de contacter le service Duo. Ces problèmes se produisent généralement sur le réseau local du client, mais peuvent parfois se produire à un niveau régional ou mondial.
  - Une entreprise de construction a touché la fibre en creusant
  - Problèmes de pare-feu ou de DNS
  - Problèmes de connectivité ou de routage du FAI
- Problèmes d'application/intégration
  - L'application protégée par Duo est mal configurée

Détérioration du service Duo

(failmode non invoqué)

- Échec de la méthode d'authentification à deux facteurs
  - L'opérateur de téléphonie de Duo (SMS/appels téléphoniques) subit lui-même une interruption de service
  - Impossible pour APNS (service de notifications push Apple) d'envoyer des notifications push aux utilisateurs d'iPhone*
- Authentifications non achevées
  - Le code transmis par Duo est incorrect, empêchant les utilisateurs de se connecter
  - La latence d'authentification de Duo et les défaillances augmentent, mais le service reste partiellement disponible

*Les utilisateurs oublient fréquemment d'autoriser les notifications sur leurs mobiles, ce qui ne constitue pas une détérioration du service Duo. Ils peuvent lancer leur application Duo Mobile pour afficher leur demande d'authentification en attente. Pour résoudre d'autres problèmes des utilisateurs, consultez nos guides iOS ou Android.

Comment puis-je savoir qu'il y a une interruption ?

Si vous ou vos utilisateurs rencontrez des problèmes qui pourraient être liés à une interruption de service, rendez-vous d'abord sur status.duo.com pour vous renseigner sur les interruptions potentielles. Si vous pensez être victime d'une panne ou d'un problème technique qui n'est pas lié à une interruption de service, contactez l'assistance Duo.

Vous trouverez d'autres options pour surveiller le service cloud de Duo dans cet article de la base de connaissances.

Modes de défaillance Duo : service Duo inaccessible

Le mode de défaillance (généralement appelé « failmode ») est invoqué lorsque le service Duo est inaccessible ou qu'un problème critique est détecté. Les mécanismes de détection d'erreurs de Duo déclenchent le comportement failmode lorsque des erreurs sont détectées.

Pour assurer l'accessibilité permanente du service Duo, les clients doivent autoriser la communication vers toutes les plages d'adresses IP de Duo. Vous trouverez une liste des plages d'adresses IP et d'autres informations dans cet article.

Parfois, les interruptions de service se manifestent différemment. Par exemple, le service Duo est accessible, mais l'authentification échoue pour d'autres raisons. Pour en savoir plus à ce sujet, consultez la section Détérioration du service Duo.

Vous pouvez configurer deux comportements failmode différents :

1. **Fail safe** (ou « fail open ») – si le service Duo est inaccessible, les utilisateurs sont **AUTORISÉS** à accéder aux applications protégées par Duo s'ils passent le processus d'authentification principale.
    - Votre niveau de sécurité est réduit, car l'authentification à deux facteurs est temporairement supprimée.
    - Ce mode est le plus pratique pour les utilisateurs, car il n'interrompt pas le flux de travail. Les collaborateurs peuvent toujours se connecter et travailler.
    - Dans un fichier authproxy.cfg, par exemple, ce mode est indiqué dans la section Serveur avec la syntaxe suivante :
      Pour plus d'informations sur les configurations du service Authentication Proxy, cliquez ici.

      ```
      failmode=safe
      ```

2. **Fail secure** (ou « fail closed ») – si le service Duo est inaccessible, les utilisateurs sont **INTERDITS** d'accès aux applications protégées par Duo, *même s'ils* passent l'authentification principale.
    - C'est l'option la plus sécurisée.
    - C'est aussi l'option qui perturbe le plus le flux de travail quotidien, car l'utilisateur n'est pas autorisé à accéder à l'application.
    - Dans un fichier authproxy.cfg, par exemple, ce mode est indiqué dans une section Serveur avec la syntaxe suivante :

      ```
      failmode=secure
      ```

Reportez-vous à la section Décisions concernant la configuration ci-dessous pour déterminer si vous devez utiliser le mode Fail safe ou Fail secure.

Modes de défaillance Duo : détérioration du service Duo

Dans ce cas, Duo Authentication Proxy, Duo Access Gateway ou toute autre application protégée par Duo peut contacter le service Duo, mais l'authentification n'est pas achevée. Failmode n'est pas invoqué.

Scénarios possibles

- L'authentification ne s'achève pas
  - Exemple en conditions réelles : Duo a transmis un code qui a interrompu l'authentification des clients utilisant une version existante de l'invite Duo. Impossible pour les utilisateurs de se connecter après avoir passé l'authentification principale et approuvé la demande d'authentification secondaire.

- Défaillance d'une ou plusieurs méthodes d'authentification
  - Exemple en conditions réelles : le service SMS de Duo ne distribuait pas les messages texte aux utilisateurs, les empêchant de s'authentifier.

Solutions

Certaines solutions ne sont pas viables pour tous les clients dans tous les scénarios. Par exemple, la modification d'une règle de pare-feu est une tâche plus lourde que l'envoi de messages aux utilisateurs. Optez pour les solutions les mieux adaptées à votre entreprise. Les problèmes de détérioration du service sont généralement résolus dans un délai de 30 minutes. Si vous utilisez l'une des solutions suivantes, **n'oubliez pas d'annuler les modifications suite à la résolution du problème**.

- Appliquez une politique d'authentification pour contourner l'authentification à deux facteurs pendant la durée de la détérioration du service. Les clients disposant d'éditions payantes de Duo peuvent utiliser des politiques d'authentification. Si le service Duo devient inaccessible, vous pouvez également recourir à cette solution.
  - Action : Créez et appliquez temporairement une politique d'authentification au niveau de l'application.
  - Résultat : Les utilisateurs ont accès à une application spécifique sans passer par l'authentification à deux facteurs. L'accès peut être restreint ou activé en fonction de l'appartenance au groupe de l'utilisateur.

- Informez les utilisateurs de l'interruption et proposez des solutions de contournement si Duo en a publié sur status.duo.com.
  - Action : Reportez-vous à la section Modèles de messages pour les utilisateurs ci-dessous. Rendez-vous sur status.duo.com pour voir si Duo a identifié des solutions de contournement temporaires.
  - Résultat : Vos utilisateurs sont rassurés quant au fait que votre entreprise et Duo sont conscients du problème et s'efforcent de le résoudre.

- Déplacez les utilisateurs de votre choix dans un groupe configuré pour « contourner » l'état.
  - Comment : faites une mise à jour manuelle ou groupée des utilisateurs pour les déplacer vers un groupe s'ils n'en ont aucun pour le moment. Ce groupe doit 1) avoir accès à l'application protégée et 2) être défini sur l'état « contournement ».
  - Résultat : Aucun utilisateur du groupe n'aura à passer l'authentification à deux facteurs.

- Annulez la configuration/le profil sur les applications pour ne pas invoquer Duo.
  - Action : Consultez la documentation spécifique à votre application sur duo.com/docs.
  - Résultat : L'authentification à deux facteurs est retirée du workflow d'authentification.

- Pour les applications exécutant Duo Authentication Proxy, utilisez la fonction Mode principal seulement.
  - Action : Cette fonctionnalité a été introduite dans Authentication Proxy version 2.14.0 et est déclenchée par l'exécution d'une commande sur le serveur proxy.
  - Résultat : L'authentification Duo est temporairement ignorée (pendant une heure par défaut, avec un maximum de quatre heures) pour toutes les connexions aux configurations RADIUS ou LDAP qui utilisent le comportement « Fail safe » par défaut.

- Bloquez manuellement le service Duo via une règle de pare-feu pour créer une situation d'interruption due à l'inaccessibilité.
  - Action : Bloquez *.duo.com et *.duosecurity.com sur le port TCP 443.
  - Résultat : Failmode est invoqué. Si le mode Fail safe est configuré, l'accès à l'application est accordé sans authentification à deux facteurs. Si le mode Fail Secure est configuré, l'accès est bloqué. Surveillez status.duo.com de près pour savoir quand vous pourrez annuler cette modification.

Comprendre le comportement failmode de votre application

Les options de configuration de failmode et le comportement pendant une interruption peuvent différer en fonction de l'application protégée par Duo. Cette section vous présente les différences entre les applications développées par Duo, Duo WebSDK et les applications populaires développées par des tiers, et vous fournit des informations importantes pour mieux comprendre la réaction des applications protégées par Duo en cas d'interruption.

Applications développées par Duo qui permettent de contrôler le comportement failmode

Le tableau suivant répertorie les applications développées et prises en charge par Duo qui permettent de contrôler le comportement failmode, ainsi que des informations supplémentaires sur la manière dont failmode est ou non invoqué dans différents scénarios d'interruption. Pour profiter constamment des toutes dernières fonctionnalités et améliorations de la sécurité, nous vous recommandons de toujours effectuer la mise à jour vers la dernière version disponible.

- Duo Authentication Proxy
- Duo Access Gateway (DAG)
- Duo pour l'ouverture de session Windows/RDP
- Duo Unix
- AD FS 2.X
- AD FS 3/4
- OWA
- RD Web/Gateway
- Oracle Access Manager

Applications développées par Duo qui ne permettent pas de contrôler le comportement failmode

- Duo Network Gateway (DNG)
- Microsoft Azure Active Directory (Accès conditionnel)
- Duo Single Sign-On

WebSDKv2

Duo WebSDKv2 n'intègre pas de dispositif de déclenchement du comportement failmode ou de validation automatique de l'accessibilité du service Duo à partir de votre application WebSDK. Si le service cloud de Duo devient inaccessible, WebSDK seul ne permet pas aux utilisateurs de s'authentifier en contournant l'authentification à deux facteurs.

Il est très important de programmer soigneusement les conditions dans lesquelles l'application passe en mode Fail safe (ouverture). Vous éviterez ainsi un scénario de contournement involontaire de l'authentification à deux facteurs. Pour surveiller le service, vous pouvez utiliser la commande ping de l'application Auth API de Duo qui contrôle la vivacité du service Duo (sans demander d'informations sur l'intégration Duo), puis la commande check d'Auth API (recommandé) qui vérifie les informations d'intégration et la signature. Pour en savoir plus, consultez notre documentation ici.

Si vous développez un comportement Fail safe personnalisé, assurez-vous de tester minutieusement les conditions invoquant le comportement failmode. Comme toujours, Fail secure (fermeture) reste l'option la plus sécurisée dans toutes les situations.

WebSDKv4

Duo WebSDKv4 inclut une fonction intégrée qui détermine si les serveurs de Duo sont accessibles et disponibles pour accepter la demande d'authentification à deux facteurs. La documentation sur l'appel de cette fonction est disponible ici. Comme ils le font avec WebSDKv2, les développeurs d'applications doivent programmer une logique dans l'application qui détermine le mode à activer si la fonction Duo renvoie une erreur (Fail safe ou Fail secure). Si

l'application n'inclut pas de vérification du service ou de la logique Duo pour déterminer comment gérer une défaillance, le mode Fail secure (fermeture) est activé par défaut.

Comme toujours, Fail secure (fermeture) reste l'option la plus sécurisée dans toutes les situations.

Intégrations développées par un tiers

Bien que Duo tente de fonctionner avec autant d'applications tierces que possible pour garantir des intégrations conformes aux bonnes pratiques, le service n'exige pas des tiers qu'ils soumettent les intégrations développées pour les examiner ou simplement en être informé. Par conséquent, Duo ne connaît pas toutes les intégrations tierces et ne sait pas si elles permettent ou non de contrôler le comportement failmode.

La liste ci-dessous présente les intégrations Duo développées par des tiers les plus populaires et indique si le comportement failmode est pris en charge et comment :

- LastPass
  - Pas de failmode configurable
  - Les utilisateurs peuvent se fier à un appareil et ne pas avoir à réitérer ensuite l'authentification multifacteur pendant un certain temps.
  - Dans les scénarios de reprise après sinistre, les administrateurs doivent se connecter à LastPass et retirer Duo du workflow d'authentification.

- 1Password
  - Pas de failmode configurable
  - Aucune authentification multifacteur requise pour l'accès hors ligne ou le coffre-fort autonome

- Okta
  - Pas de failmode configurable
  - Dans les scénarios de reprise après sinistre, les administrateurs doivent se connecter pour retirer Duo du workflow d'authentification.

- OneLogin
  - Pas de failmode configurable
  - Dans les scénarios de reprise après sinistre, les administrateurs doivent se connecter pour retirer Duo du workflow d'authentification.

- Ping Federate
  - Failmode configurable. Documentation ici.

- CAS
  - Failmode configurable. Documentation ici.

IMPORTANT : toutes les intégrations ne prévoient pas de dispositif pour contrôler le comportement failmode.

- Les intégrations qui utilisent Authentication Proxy ou Duo Access Gateway **ont la possibilité** de spécifier un comportement failmode.
- La majorité des intégrations développées par Duo permettent de configurer un comportement failmode pendant le processus d'installation. Par exemple, le comportement failmode de l'authentification Duo pour l'ouverture de session Windows et RDP est configurable dans le programme d'installation. La plupart des paquets d'applications Duo permettent également de modifier le comportement failmode après l'installation (avec Duo Unix et l'ouverture de session Windows, par exemple).
- Les intégrations de Duo créées par des tiers tels que Thycotic, Ping Federate et LastPass n'offrent pas forcément la possibilité de contrôler le comportement failmode et sont configurées par défaut sur Fail secure. Pour connaître les possibilités de configuration du comportement failmode, consultez la documentation du fournisseur.
- L'intégration de WebSDKv2 n'inclut pas la logique de vérification du comportement failmode. Pour plus d'informations, consultez la section « Comprendre comment vos applications réagissent à différents types d'interruption ».
- L'accès conditionnel Azure bascule en mode fermeture (Fail secure) si le service cloud d'Azure ne peut pas contacter le service cloud de Duo.
    - En cas d'interruption de longue durée, les clients ont la possibilité de retirer l'obligation d'authentification à deux facteurs Duo de la politique d'accès conditionnel pour autoriser les utilisateurs à accéder aux applications.
- La passerelle Duo Network Gateway (DNG) bascule en mode fermeture si elle ne peut pas contacter le service cloud de Duo.
- Les utilisateurs ne peuvent pas s'authentifier auprès des applications fédérées via Duo SSO.
    - Comme Duo SSO gère à la fois l'authentification principale et secondaire, les utilisateurs doivent pouvoir accéder directement au service.
    - En cas d'interruption de longue durée, les clients ont la possibilité de dé-fédérer manuellement l'application de Duo SSO et de configurer l'application pour qu'elle utilise une autre source d'authentification. Cette modification, qui pour de nombreuses applications s'avère fastidieuse et peu pratique, ne doit être envisagée qu'en dernier recours.

Modèles de messages pour les utilisateurs

En cas d'incident, réfléchissez au moment le plus opportun pour envoyer un message aux utilisateurs. Par exemple, vous pouvez l'envoyer dès que les utilisateurs commencent à signaler les problèmes, ou après la publication d'une notification par Duo sur status.duo.com mais avant que des utilisateurs vous signalent des problèmes, ou encore seulement si l'incident n'est pas résolu dans un délai d'au moins 20 minutes.

Heure du jour

- Un incident survenu à 11 h en semaine peut nécessiter l'envoi immédiat d'un message aux utilisateurs.
- Un incident survenu à 23 h le week-end n'a peut-être pas besoin d'être signalé immédiatement aux utilisateurs.

Moment du trimestre

- Un incident survenu au cours de la dernière semaine du trimestre peut nécessiter l'envoi immédiat d'un message aux utilisateurs, quelle que soit l'heure de la journée.

Criticité de l'accès

- Un incident affectant l'accès à une application critique peut nécessiter l'envoi immédiat d'un message, indépendamment de l'heure, de la date ou d'autres facteurs.

Service Duo inaccessible ou détérioré

Si vous utilisez le mode Fail safe lorsque Duo est inaccessible ou que vous invoquez failmode pendant une détérioration :

OBJET : Problèmes d'authentification – En cours de traitement

CORPS : Duo signale des problèmes de service. Pour y remédier temporairement, nous avons levé l'exigence d'authentification à deux facteurs de Duo. Une fois le problème résolu, l'authentification à deux facteurs sera rétablie.

Si vous utilisez Fail secure :

OBJET : Problèmes d'authentification – En cours de traitement

CORPS : Nous rencontrons des problèmes avec l'authentification à deux facteurs de Duo. En raison de la nature des données contenues dans <votre application>, l'accès sera refusé jusqu'à la résolution du problème.

Problème spécifique à la méthode d'authentification

OBJET : Problèmes d'authentification – En cours de traitement

CORPS : Duo signale des problèmes avec son service de <transmission/SMS/téléphone>. Pour remédier temporairement au problème, utilisez les <rappels de SMS/transmission/téléphone>. Une fois le problème résolu, une mise à jour sera mise à disposition.

Foire aux questions

Puis-je être informé lorsque failmode est invoqué ?

Failmode est configuré et invoqué localement dans votre application Duo Authentication Proxy ou protégée par Duo. Nous vous recommandons d'utiliser un outil de surveillance ou une solution SIEM pour examiner une transaction failmode.

Vous pouvez déterminer si failmode a été invoqué en examinant vos journaux Authentication Proxy. Le répertoire par défaut de stockage des journaux est C:\Program Files (x86)\Duo Security Authentication Proxy\log sur un ordinateur Windows 64 bits et C:\Program Files\Duo Security Authentication Proxy\log sur un ordinateur Windows 32 bits.

Vous trouverez ci-dessous deux exemples de journaux Duo Authentication Proxy indiquant quand failmode a été invoqué.

1. Exemple de journal **fail safe**

```
!! 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. Exemple de journal **fail secure**

```
!! 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
```

Voici la sortie d'un journal authevents.log compatible avec une solution SIEM :

1. Exemple de journal **fail safe**

```
!! 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. Exemple de journal **fail secure**

```
!! 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"}
```

Les déploiements Duo sont-ils conçus pour assurer la haute disponibilité ou créés en mode « actif/actif » ?

Les déploiements Duo ne doivent pas être considérés comme un seul nœud. Duo utilise de nombreux clusters indépendants ou « déploiements » de sa technologie qui peuvent être mis à l'échelle pour prendre en charge la croissance du client, ainsi que réduire l'impact d'une défaillance sur un déploiement. Les composants d'infrastructure sous-jacents de chacun de ces déploiements s'appuient sur la réplication en temps réel entre les différents data centers physiques qui composent les zones de disponibilité Amazon Web Services (AWS). Duo reproduit également les données des clients en temps réel dans au moins une région AWS supplémentaire pour chaque déploiement individuel.

Comment Duo protège-t-il les déploiements contre les attaques DDoS ?

AWS prend des mesures pour atténuer de façon transparente les attaques DDoS contre l'infrastructure de Duo en utilisant sa technologie exclusive de protection DDoS AWS Shield. Si une attaque contre les services Duo n'est pas automatiquement atténuée par AWS ou l'infrastructure renforcée de Duo, les équipes Duo sont immédiatement alertées du problème pour pouvoir réagir comme il convient. Cette réaction peut inclure la mise systématique sur liste blackhole des adresses IP/netblocks spécifiques, voire la relocalisation du trafic client sur une infrastructure et/ou des adresses IP non touchées.

Mon compte peut-il être transféré vers un autre déploiement en cas d'interruption ?

La technologie utilisée pour déplacer les clients entre les déploiements est conçue pour minimiser l'impact sur le déploiement source et de destination. Le processus est relativement long car il s'exécute en arrière-plan. Ce processus ne peut pas être mis en pratique dans le cadre d'un scénario de défaillance. En outre, dans certains cas, le déplacement des charges de travail des clients vers une autre infrastructure ne résout pas le problème sous-jacent et peut même augmenter l'impact d'une interruption. Pour certains types d'interruptions, le déplacement des comptes clients touchés vers un autre déploiement peut également déplacer le problème sous-jacent, prolongeant potentiellement l'interruption.

Nous avons subi une interruption. Le déplacement vers un autre déploiement est-il possible ?

Tous les déploiements Duo créés sont identiques et partagent les mêmes propriétés de haute disponibilité et les mêmes performances garantissant une disponibilité optimale. C'est pourquoi le déplacement de votre déploiement actuel ne permettra pas de réduire intrinsèquement le risque d'interruption.