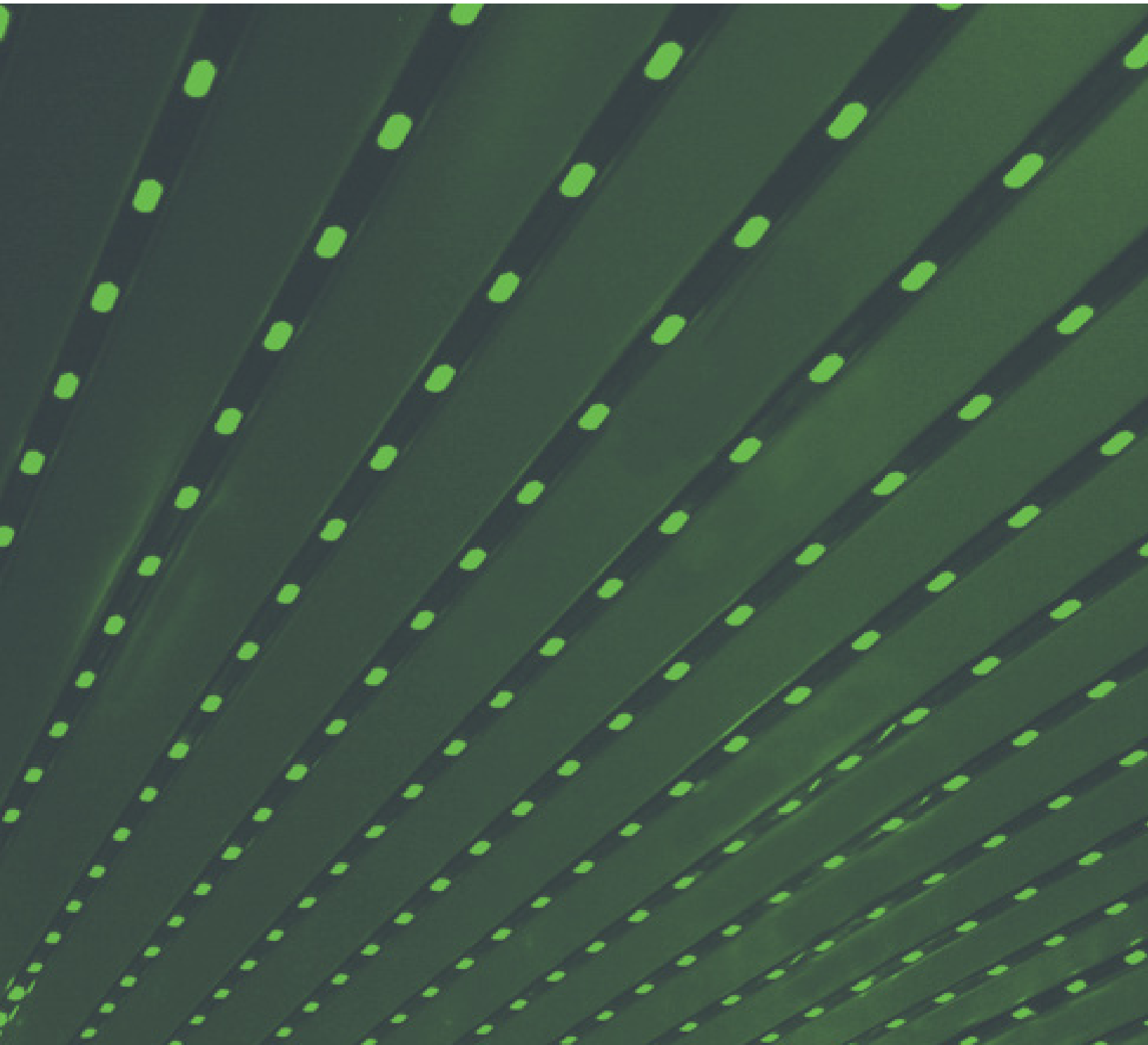
Guía de

preparación para la continuidad del negocio

Versión 3.0 publicada el 16 de agosto de 2022



Índice

Información general

¿Por qué necesito esta guía?

Incluso las soluciones más sólidas pueden, en ocasiones, experimentar una interrupción del servicio. Duo ha mantenido un tiempo de actividad mayor al 99,99 % durante más de cuatro años, lo que todavía deja una pequeña ventana en la que el servicio de Duo puede no estar disponible.

Las interrupciones afectan la productividad de sus trabajadores y tienen el potencial de debilitar temporalmente su estado de seguridad. Como proveedor de acceso de confianza, queremos que esté preparado para cualquier situación que pueda surgir y garantizarle que tiene un plan para responder a posibles interrupciones.

En nuestro informe técnico Confiabilidad del servicio encontrará más detalles sobre el servicio de Duo y la forma en que nuestra arquitectura en la nube y los procesos de desarrollo de productos están diseñados para garantizar una alta disponibilidad.

Comprenda las interrupciones y su entorno

Se debe tener en cuenta cómo reaccionarán las aplicaciones protegidas por Duo y la organización de TI si el servicio Duo no está disponible.

Estar preparado para navegar por posibles escenarios de interrupción del servicio, en definitiva, garantizará una mejor experiencia con Duo.

Esta guía lo ayudará a:

- comprender las dos categorías de interrupciones;
- comprender los modos de falla de Duo y cómo decidir entre Fail Safe (A prueba de fallos) y Fail Secure (Cierre en caso de falla);
- comprender cómo responderán sus aplicaciones a diferentes tipos de interrupciones; y
- enviar mensajes a los usuarios durante una interrupción.

Planificación para alcanzar el éxito

Una vez que haya leído esta guía y comprenda los escenarios de interrupción y los comportamientos del modo de falla de su aplicación, le recomendamos que cree planes de recuperación tras un desastre específicos para la aplicación. Esta planificación debe incluir:

- Comprensión de los procesos necesarios para bloquear o evitar el servicio en la nube de Duo si el comportamiento de modo de falla no se invoca como se esperaba
- Procedimientos para remover Duo del flujo de trabajo de autenticación para **cada aplicación protegida**

Decisiones de configuración

Considere cuidadosamente qué configuración de modo de falla (Protegido frente a Seguro) debe utilizar para cada aplicación (si está disponible).* Es probable que su elección dependa de:

- Factores de política y cumplimiento
- Tipos de datos contenidos en las aplicaciones protegidas
  - Historias clínicas, finanzas, información de identificación personal (PII), propiedad intelectual (IP), etc.
- Grupos de usuarios con diferentes niveles de acceso
- La necesidad de equilibrar la seguridad con la facilidad de uso

* Consulte la documentación específica de su aplicación en duo.com/docs para saber si cuenta con un modo de falla configurable.

Con respecto a las configuraciones de modo de falla y los planes de acción en caso de degradación del servicio, generalmente existen tres categorías principales a las que puede pertenecer la aplicación de una organización:

Nivel de restricción	Inalcanzable (se invocó el modo de falla)	Degradación (no se invocó el modo de falla)
Más restrictivo El contrato, la ley, la política o la confidencialidad de los datos contenidos en la aplicación protegida **requieren la autenticación de dos factores sin excepción**.	Fail Secure (Cierre en caso de falla)	Los usuarios y los grupos NO deben cambiar al estado “Evite”, ya que esto omitirá la autenticación de dos factores.
Restrictivo Algunos subconjuntos de usuarios siempre están obligados a pasar la autenticación de dos factores sin excepción.	Fail Secure (Cierre en caso de falla)	Los usuarios y grupos que, sin excepción, deben pasar la autenticación de dos factores NO deben cambiarse al estado “Evite”, ya que esto omitirá dicha autenticación. Los usuarios y grupos para los que es tolerable acceder a esta aplicación sin dos factores pueden cambiarse al estado “Evite” para permitirles omitir la autenticación de dos factores.
Menos restrictivo El contrato, la ley, la política o la confidencialidad de los datos contenidos en la aplicación protegida **no exigen que la autenticación de dos factores se utilice en todas las circunstancias**.	Fail Safe (A prueba de fallos)	Los usuarios y grupos para los que es tolerable acceder a esta aplicación sin dos factores, pueden cambiarse al estado “Evite” para permitirles omitir la autenticación de dos factores.

* Tenga en cuenta si un grupo de usuarios tiene acceso a más de una aplicación, ya que ponerlos en el estado “Evite” omitirá la autenticación de dos factores para todas las aplicaciones a las que tienen acceso. Si esto debe hacerse para que un grupo tenga acceso a otra aplicación, primero debe quitarse el acceso de ese grupo a la aplicación actual.

Tipos de interrupciones

La interrupción del servicio Duo generalmente se puede clasificar en dos categorías: cuando el servicio Duo es **inalcanzable** o cuando hay una **degradación** del servicio Duo.

La distinción entre la inaccesibilidad de Duo y una degradación del servicio es importante porque afecta el comportamiento de las aplicaciones protegidas por Duo y, en última instancia, lo que experimentan los usuarios finales.

Servicio Duo inalcanzable

(se invocó el modo de falla)

- El servicio de Duo no está disponible en este momento:
  - El servicio Duo no puede mostrar Duo Prompt o responder a las solicitudes de Auth API en 180 segundos.
- Conectividad de red que impide que las aplicaciones de los clientes accedan al servicio de Duo. Suele ocurrir en la red local del cliente, pero a veces sucede a nivel regional o global:
  - Empresa constructora excava a través de la fibra
  - Problemas con el firewall o DNS
  - Problemas de conectividad o enrutamiento del ISP
- Problemas de aplicación/integración:
  - La aplicación protegida por Duo está mal configurada.

Degradación del servicio Duo

(no se invocó el modo de falla)

- Falla del método de dos factores:
  - El proveedor de telefonía de Duo (SMS/llamadas telefónicas) experimenta una interrupción propia.
  - APNS (servicio de notificación automática de Apple) no puede entregar notificaciones automáticas a los usuarios de iPhones.*
- No se completan las autenticaciones:
  - Duo inserta un código incorrecto que impide que los usuarios inicien sesión con éxito.
  - La latencia y las fallas de autenticación de Duo aumentan, pero el servicio sigue estando parcialmente disponible.

* Los usuarios con frecuencia se olvidan de permitir notificaciones en sus teléfonos, esto no califica como una degradación del servicio Duo. Los usuarios pueden iniciar su aplicación Duo Mobile y verán una solicitud de autenticación pendiente. Para obtener más información sobre la resolución de problemas del usuario final, consulte nuestras guías de iOS o Android.

¿Cómo sé cuándo se está produciendo una interrupción?

Si usted o sus usuarios están experimentando problemas que sospecha que pueden estar relacionados con una interrupción, primero consulte status.duo.com por cualquier noticia sobre posibles interrupciones. Si cree que está experimentando una interrupción o posee un problema técnico no relacionado con una interrupción del servicio, póngase en contacto con Soporte de Duo.

En este artículo de base de conocimientos, se documentan opciones adicionales para supervisar el servicio en la nube de Duo.

Modos de falla de Duo: servicio Duo inalcanzable

El modo de falla (con frecuencia denominado “failmode”) se invoca cuando el servicio Duo es inalcanzable o se detecta un problema crítico. Duo tiene mecanismos de detección de errores que activan el modo de falla en función de los errores detectados.

Para garantizar la disponibilidad continua del servicio de Duo, los clientes deben permitir la comunicación a todos los rangos IP de Duo. En este artículo, encontrará una lista de rangos IP con consideraciones adicionales.

A veces, las interrupciones del servicio se manifiestan de otras maneras. Por ejemplo, el servicio Duo podría estar disponible, pero la autenticación está fallando por otras razones. Para obtener más información, desplácese hacia abajo hasta Degradación del servicio Duo.

El modo de falla puede configurarse para comportarse de las siguientes maneras:

1. **Fail Safe [A prueba de fallos]** (también conocido como “Apertura en caso de falla”): si el servicio Duo es inalcanzable, los usuarios tendrán acceso **PERMITIDO** a las aplicaciones protegidas por Duo si pasan la autenticación primaria.
    - Esto debilita su postura de seguridad, ya que la autenticación de dos factores se elimina temporalmente.
    - Genera menos complicaciones para los usuarios y no interrumpe el flujo de trabajo: los empleados todavía pueden iniciar sesión y trabajar.
    - Por ejemplo, en un archivo authproxy.cfg, esto se indicará en una sección de servidor mediante la siguiente sintaxis:
      Para obtener más información sobre las configuraciones de proxy de autenticación, haga clic aquí.

```
failmode=safe
```

2. **Fail Secure [Bloqueo]** (también conocido como “Cierre en caso de falla): si el servicio Duo es inalcanzable, los usuarios tendrán acceso **DENEGADO** a las aplicaciones protegidas por Duo *incluso si* pasan la autenticación primaria.
    - Esta es la opción más segura.
    - Puede ser la opción más perturbadora con respecto al flujo de trabajo diario, ya que deniega al usuario el acceso a la aplicación.
    - Por ejemplo, en un archivo authproxy.cfg, esto se indicará en una sección de servidor mediante la siguiente sintaxis:

```
failmode=secure
```

Consulte la sección Decisiones de configuración a continuación para obtener ayuda sobre cómo decidir si debe activar el modo Fail Safe o Fail Secure.

Modos de falla de Duo: degradación del servicio Duo

En esta situación, Duo Authentication Proxy, Duo Access Gateway u otra aplicación protegida por Duo pueden conectarse con el servicio Duo, pero no se puede completar la autenticación. No se está invocando el modo de falla.

Situaciones posibles

- No se completa la autenticación
  - Ejemplo del mundo real: Duo insertó un código que dañó la autenticación para los clientes que usaban una versión antigua de Duo Prompt. Los usuarios no pudieron iniciar sesión después de haber pasado correctamente la autenticación primaria y haber aprobado la solicitud de autenticación secundaria.
- Error de uno o más métodos de autenticación
  - Ejemplo del mundo real: el servicio de SMS de Duo no estaba enviando mensajes de texto a los usuarios correctamente, dejándolos incapaces de autenticarse.

Soluciones

Algunas soluciones pueden no ser viables para todos los clientes en todos los escenarios. Por ejemplo, un cambio de regla de firewall puede resultar más engorroso que enviar mensajes a los usuarios. Considere las mejores soluciones para su organización. Los problemas de degradación normalmente se resuelven en 30 minutos. Si emplea cualquiera de las siguientes soluciones, **asegúrese de revertir los cambios tras la resolución del problema**.

- Aplique una política de autenticación para evitar la autenticación de dos factores mientras persiste la degradación del servicio. Los clientes con ediciones pagas de Duo pueden utilizar las políticas de autenticación. En caso de que el servicio Duo sea inalcanzable, también se puede utilizar esta solución.
  - Cómo: cree y aplique temporalmente una política de autenticación a nivel de la aplicación.
  - Qué hace: permite a los usuarios acceder a una aplicación específica sin completar la autenticación de dos factores. El acceso se puede restringir o activar en función de la membresía de grupo que posea el usuario.
- Informe a los usuarios de la interrupción y ofrezca soluciones alternativas si Duo ha publicado alguna en status.duo.com.
  - Cómo: consulte la sección Plantillas de mensajes de usuarios finales a continuación. Navegue a status.duo.com para ver si Duo ha identificado alguna solución temporal.
  - Qué hace: garantiza a los usuarios que tanto su organización como Duo reconocen el problema y están trabajando para solucionarlo.
- Mueva a todos o algunos usuarios a un grupo configurado con el estado “Evite”.
  - Cómo: actualice los usuarios de forma manual o masiva para moverlos a un grupo si aún no están en uno. Ese grupo necesita: 1) acceso a la aplicación protegida y 2) estar configurado en el estado “Omisión”.
  - Qué hace: evitará la autenticación de dos factores para cualquier usuario del grupo.
- Revierta la configuración/perfil en las aplicaciones para no invocar Duo.
  - Cómo: consulte la documentación específica de su aplicación en duo.com/docs.
  - Qué hace: removerá la autenticación de dos factores del flujo de trabajo de autenticación.
- Para las aplicaciones que utilizan Duo Authentication Proxy, utilice la función de solo modo principal.
  - Cómo: esta característica se introdujo en la versión 2.14.0 del proxy de autenticación y se activa mediante la ejecución de un comando en el servidor proxy.
  - Qué hace: omite temporalmente la autenticación de Duo (la función predeterminada es de una hora con un máximo de cuatro horas) para todos los inicios de sesión en las configuraciones RADIUS o LDAP que utilizan el comportamiento predeterminado “Fail Safe”.
- Bloquee manualmente el servicio de Duo mediante una regla de firewall para crear de forma eficaz un escenario de interrupción inalcanzable.
  - Cómo: bloquee *.duo.com y *.duosecurity.com en el puerto TCP 443.
  - Qué hace: invocará el modo de falla. Si se configura Fail Safe, se otorgará acceso a la aplicación sin autenticación de dos factores. Si se configura Fail Secure, se bloqueará el acceso. Controle status.duo.com atentamente para saber cuándo se puede revertir este cambio.

Comprenda el comportamiento del modo de falla de su aplicación

Las opciones de configuración y el comportamiento del modo de falla durante una interrupción pueden variar según la aplicación que Duo esté protegiendo. En esta sección, examinaremos diferencias y detalles importantes sobre las aplicaciones desarrolladas por Duo, WebSDK de Duo y las aplicaciones populares desarrolladas por terceros para que pueda comprender mejor cómo las aplicaciones protegidas por Duo se verán afectadas por una interrupción.

Aplicaciones desarrolladas por Duo que proporcionan control de modo de falla

En la siguiente tabla, se enumeran las aplicaciones compatibles y desarrolladas por Duo que proporcionan control de modo de falla, junto con detalles adicionales sobre cómo se pueden invocar o no modos de falla en diferentes escenarios de interrupción. Para asegurarse de tener todas las mejoras en funciones y seguridad, siempre recomendamos actualizar a la última versión disponible.

- Duo Authentication Proxy
- Duo Access Gateway (DAG)
- Duo para Windows Logon/RDP
- Duo Unix
- AD FS 2.X
- AD FS 3/4
- OWA
- RD Web/Gateway
- Administrador de acceso a Oracle

Aplicaciones desarrolladas por Duo que no proporcionan control de modo de falla

- Duo Network Gateway (DNG)
- Microsoft Azure Active Directory (acceso condicional)
- Duo Single Sign-On

WebSDKv2

WebSDKv2 de Duo no tiene un mecanismo integrado para activar el modo de falla o validar automáticamente que el servicio Duo esté disponible desde la aplicación WebSDK.Si el servicio en la nube de Duo se vuelve inalcanzable, WebSDK por sí solo no permitirá a los usuarios autenticarse sin completar correctamente la autenticación de dos factores.

Es muy importante programar cuidadosamente las condiciones bajo las cuales la aplicación quedará en modo Fail Safe (apertura) para evitar la creación de un escenario de desvío de la 2FA involuntario.Para supervisar el servicio, puede utilizar el terminal ping de Auth API de Duo a fin de implementar una verificación de vitalidad para el servicio Duo (que no requiere ninguna información de integración de Duo) y, a continuación, utilizar el terminal de verificación de Auth API (recomendado) para comprobar la información de integración y la firma. Obtenga más información en nuestra documentación aquí.

Si desarrolla un comportamiento a prueba de fallos (Fail Safe) personalizado, asegúrese de probar exhaustivamente las condiciones que invocan el comportamiento de modo de falla. Como siempre, Fail Secure (Cierre en caso de falla) sigue siendo la opción más segura en todos los escenarios.

WebSDKv4

WebSDKv4 de Duo incluye una función incorporada para determinar si los servidores de Duo son accesibles y están disponibles para aceptar la solicitud de 2FA. La documentación sobre cómo llamar a esta función está disponible aquí. Al igual que WebSDKv2, los desarrolladores de aplicaciones aún deben programar la aplicación con la lógica sobre cómo debe proceder la aplicación si la función de Duo devuelve un error (Fail Safe o Fail Secure). Si la aplicación no incluye comprobaciones en el servicio o la lógica de Duo para determinar cómo manejar una falla, se establecerá de manera predeterminada como segura (cerrada).

Como siempre, Fail Secure (Cierre en caso de falla) sigue siendo la opción más segura en todos los escenarios.

Desarrolladas por terceros

Si bien Duo intenta trabajar con la mayor cantidad de terceros posible para garantizar que las integraciones sigan los procedimientos recomendados, Duo no requiere que los terceros envíen integraciones desarrolladas para su revisión o que nos las notifiquen. Como consecuencia, Duo no necesariamente tiene en cuenta todas las integraciones de terceros ni la forma en que esas integraciones podrían proporcionar controles de modo de falla.

A continuación, se enumeran las integraciones populares de Duo desarrolladas por terceros, si admiten el modo de falla y de qué manera lo hacen:

- LastPass
  - Modo de falla no configurable.
  - Los usuarios pueden confiar en un dispositivo asociado y, luego, no tener que realizar la MFA de nuevo durante un período de tiempo.
  - En escenarios de recuperación ante desastres, los administradores deben iniciar sesión en LastPass y remover Duo del flujo de trabajo de autenticación.

- 1Password
  - Modo de falla no configurable.
  - No requiere MFA para el acceso sin conexión o bóveda independiente.

- Okta
  - Modo de falla no configurable.
  - En escenarios de recuperación ante desastres, los administradores deben iniciar sesión para remover Duo del flujo de trabajo de autenticación.

- OneLogin
  - Modo de falla no configurable.
  - En escenarios de recuperación ante desastres, los administradores deben iniciar sesión para remover Duo del flujo de trabajo de autenticación.

- Ping Federate
  - Ofrece modo de falla configurable. Documentación aquí.

- CAS
  - Ofrece modo de falla configurable. Documentación aquí.

IMPORTANTE: No todas las integraciones proporcionan un mecanismo para controlar el comportamiento del modo de falla.

- Las integraciones que utilizan el proxy de autenticación o Duo Access Gateway **tienen la opción** de especificar un modo de falla.
- La mayoría de las integraciones desarrolladas por Duo permiten la configuración del modo de falla durante el proceso de instalación. Por ejemplo, el modo de falla para la autenticación de Duo para Windows Logon y RDP se puede configurar al instalarlo. La mayoría de los paquetes de aplicaciones de Duo también ofrecen una manera de modificar el comportamiento del modo de falla después de la instalación (por ejemplo, con Duo Unix y Windows Logon).
- Las integraciones de Duo creadas por terceros, como Thycotic, Ping Federate y LastPass, pueden no ofrecer una manera de controlar el modo de falla y recurrir al modo Fail Secure de forma predeterminada.Consulte la documentación del proveedor para revisar las capacidades del modo de falla.
- La integración de WebSDKv2 no incluye la lógica de verificación del modo de falla. Más detalles en la sección “Comprenda cómo responderán sus aplicaciones a diferentes tipos de interrupciones”.
- El acceso condicional (CA) de Azure se cerrará en caso de falla si el servicio en la nube de Azure no puede conectarse con el servicio en la nube de Duo.
    - Para las interrupciones de larga duración, es posible que los clientes deban considerar eliminar el requisito de Duo 2FA de la política de CA para permitir que los usuarios accedan a las aplicaciones sin 2FA.
- Duo Network Gateway (DNG) se cerrará en caso de falla si no puede conectarse con el servicio en la nube de Duo.
- Los usuarios no podrán autenticarse con aplicaciones federadas en Duo SSO.
    - Dado que Duo SSO maneja la autenticación principal y secundaria, los usuarios se deben poder comunicar con el servicio directamente.
    - Para las interrupciones de larga duración, es posible que los clientes deban considerar la eliminación manual de la aplicación Duo SSO y la configuración de la aplicación para utilizar una fuente de autenticación diferente. Esto suele ser un cambio engorroso y poco práctico para muchas aplicaciones y solo se debe considerar como último recurso.

Plantillas de mensajes de usuarios finales

Considere en qué momento su organización prefiere enviar mensajes a usuarios finales durante un incidente. Podría ser tan pronto como los usuarios comiencen a reportar problemas, después de que Duo publique una notificación en status.duo.com, pero antes de que los usuarios hayan informado algo, o podría ser solo si un incidente ha permanecido sin resolver durante 20 minutos o más.

Hora del día

- Un incidente a las 11 a. m. de un día de semana puede requerir mensajes inmediatos a los usuarios.
- Es posible que un incidente que ocurra a las 11 p. m. de un fin de semana no necesite notificarse a los usuarios de inmediato.

Momento del trimestre

- Un incidente durante la última semana de un trimestre puede requerir mensajes inmediatos a los usuarios, independientemente de la hora del día.

Criticidad del acceso

- Un incidente que afecte el acceso a una aplicación crítica puede requerir mensajes inmediatos independientemente de la hora, la fecha u otros factores.

Servicio Duo inalcanzable o degradado

Si utiliza Fail Safe cuando Duo es inalcanzable o invoca el modo de falla manualmente durante la degradación:

ASUNTO: Problemas de autenticación: en curso

CUERPO: Duo está reportando problemas con su servicio. Como solución temporal, estamos suprimiendo el requisito de autenticación de dos factores de Duo. El mismo se restablecerá una vez resuelto el problema.

Si utiliza Fail Secure:

ASUNTO: Problemas de autenticación: en curso

CUERPO: Estamos experimentando problemas con la autenticación de dos factores de Duo. Debido a la naturaleza de los datos contenidos en <su aplicación>, se denegará el acceso hasta que se resuelva el problema.

Problema específico del método de autenticación

ASUNTO: Problemas de autenticación: en curso

CUERPO: Duo está reportando problemas con su servicio <push/SMS/teléfono>. Como solución temporal, utilice <sms/push/devolución de la llamada>. Espere otra actualización cuando se haya resuelto el problema.

Preguntas frecuentes

¿Puedo recibir una notificación cuando se invoca el modo de falla?

El modo de falla se configura e invoca a nivel local en el proxy de autenticación de Duo o en la aplicación protegida por Duo. Se recomienda utilizar una herramienta de monitoreo o una solución SIEM para detectar una transacción de modo de falla.

Puede determinar si se ha invocado el modo de falla examinando los registros del proxy de autenticación. El directorio predeterminado para guardar los registros es C:\Program Files (x86)\Duo Security Authentication Proxy\log en una máquina con Windows de 64 bits y C:\Program Files\Duo Security Authentication Proxy\log en una máquina con Windows de 32 bits.

A continuación, se detallan dos ejemplos de registros de proxy de autenticación de Duo que muestran cuándo se ha invocado el modo de falla.

1. Ejemplo de registro de **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. Ejemplo de registro de **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
```

A continuación, se muestra la salida de un archivo authevents.log compatible con SIEM:

1. Ejemplo de registro de **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. Ejemplo de registro de **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"}
```

¿Las implementaciones de Duo están desarrolladas con alta disponibilidad o diseñadas con el modo “Activo/Activo”?

Sí, las implementaciones de Duo no deben considerarse un solo nodo. Duo utiliza numerosos clústeres o “implementaciones” independientes de su tecnología a fin de generar escalabilidad tanto para apoyar el crecimiento del cliente como para garantizar que se minimice el impacto de un error en cualquier implementación. Los componentes de infraestructura subyacentes de cada una de estas implementaciones están respaldados por la replicación en tiempo real entre los múltiples centros de datos físicos que componen las zonas de disponibilidad de Amazon Web Services (AWS). Duo también replica los datos de los clientes en tiempo real en al menos una región de AWS adicional para cada implementación individual.

¿Cómo protege Duo las implementaciones contra ataques de DDoS?

AWS toma medidas para mitigar de forma transparente los ataques de DDoS contra la infraestructura de Duo, utilizando su tecnología de prevención de DDoS de AWS Shield. En caso de un ataque contra los servicios de Duo que no se mitigue automáticamente por la propia infraestructura reforzada de AWS o Duo, el personal de Duo recibiría alertas sobre el problema inmediatamente y responderá según sea necesario. Esta respuesta podría incluir el descarte sistemático de direcciones IP/netblocks específicas, o incluso la reubicación del tráfico de clientes a una infraestructura o direcciones IP no afectadas.

¿Se pueden mover mis cuentas a otra implementación en caso de una interrupción?

La tecnología utilizada para mover clientes entre implementaciones está diseñada para minimizar el impacto tanto en la implementación de origen como en la de destino; a menudo puede ser un proceso relativamente largo, ya que se ejecuta en segundo plano. Este proceso no es adecuado para ejercerse como parte de un escenario de falla. Además, en algunos casos, mover las cargas de trabajo de los clientes a una infraestructura alternativa puede no resolver el problema subyacente e incluso podría aumentar el impacto de una interrupción. En algunos escenarios de interrupción, mover las cuentas de cliente afectadas a otra implementación puede generar un problema subyacente, lo que podría extender la línea de tiempo de la interrupción.

Sufrimos una interrupción. ¿Podemos movernos a otra implementación?

Todas las implementaciones de Duo se crean iguales y comparten las mismas propiedades de alta disponibilidad y el historial de trayectoria durante un excelente tiempo de actividad. Por eso, salir de la implementación actual no reduce intrínsecamente el riesgo de una interrupción.