Guide to Business Continuity Preparedness

Released June 22, 2016
Revised March 10, 2017

Table of contents

1. Overview

Why do I need this guide?

Unavailability or degradation in quality of service can happen. Even with Duo's historical 99.995% uptime, that still leaves a small time where the Duo service may be unavailable.

Outages impact the productivity of your workers and have the potential to temporarily weaken your security posture. Have a plan in place to respond to potential outages. As your trusted access provider, we want you to be prepared for any situation that may arise.

Planning for success

Consideration should go into how your Duo-protected applications & IT organization will react should the service be unavailable for whatever reason.

Being prepared to navigate potential service disruption scenarios will ultimately ensure a better experience with Duo.

This guide will help you:

- Understand the two categories of outages
- Understand Duo's failmode and how to decide on Fail Safe vs Fail Secure
- Message your users during an outage

2. Types of outages

Duo service disruption can generally be placed in one of two categories: when the Duo service is **unreachable** or when there is a Duo service **degradation**.

The distinction between Duo being unreachable and a service degradation is important because it affects how Duo-protected applications behave, and ultimately what your end-users experience.

Duo service **unreachable**

(failmode invoked)

- Duo's service temporarily unavailable
  - *Duo service outage*
- Network issues preventing customer application from reaching Duo's service
  - *construction company digs through fiber*
  - *DNS issues*
- Application/Integration issues
  - *Duo-protected application is misconfigured*

Duo service **degradation**

(failmode not invoked)

- Two-factor method failure
  - *Duo's SMS provider experiences an outage of their own*
  - *APNS (Apple Push Notification Service) fails to deliver push notifications to users iPhones**
- Authentications not completing
  - *Duo pushes bad code preventing users from successfully logging in*

*Users frequently forget to allow notifications on their phones - this does not qualify as a Duo service degradation. Users can launch their Duo Mobile App and will see a pending authentication request. For additional end-user troubleshooting see our iOS or Android guides.

How do I know when an outage is occurring?

If you or your users are experiencing issues that you suspect may be related to an outage, first check status.duo.com for any news about potential outages. We also highly recommend you proactively subscribe to receive notifications from status.duo.com; email, SMS, Twitter, and RSS feeds are available. If you believe you are experiencing an outage or have a technical issue not related to a service disruption, contact Duo Support.

3. Duo service unreachable

Understanding Duo's failure modes

Failmode is invoked when the Duo service is *unreachable* or a critical problem is detected. Duo has sophisticated error detection mechanisms that trigger failmode based on detected errors.

Sometimes service disruptions manifest in other ways - for example, the Duo service could be reachable, but authentication is failing for other reasons. For more on this, scroll down to Duo service degradation.

IMPORTANT: Not all integrations have the option to use fail safe.

- Integrations that use the Authentication Proxy or Duo Access Gateway *do* have the option to enable fail safe mode.
- Visit duo.com/docs or reach out to your contact at Duo to discuss fail modes for each integration.

Failmode can be configured to behave in one of two ways:

1. **Fail Safe** (also known as "fail open") - if Duo service is unreachable, users will be ***ALLOWED*** access to Duo-protected applications if they pass primary authentication.
    - This weakens your security posture, as two-factor authentication is temporarily removed.
    - It causes less pain for users and does not interrupt workflow--employees can still log in and work.
    - In an authproxy.cfg file, this will be indicated in a Server section by the following syntax:

```
failmode=safe
```

    For more information on Authentication Proxy configurations, click here.

2. **Fail Secure** (also known as "fail closed") - if Duo service is unreachable, users will be ***DENIED*** access to Duo-protected applications *even if* they pass primary authentication.
    - This is the most secure option.
    - It can be the most disruptive option with regard to daily workflow as it denies the user access to the app.
    - In an authproxy.cfg file, this will be indicated in a Server section by the following syntax:

```
failmode=secure
```

See the Configuration Decisions section below for help on deciding whether you should enable fail safe or fail secure mode.

4. Duo service degradation

In this situation, the Duo Authentication Proxy, Duo Access Gateway, or other Duo-protected application is able to reach the Duo service, but authentication is unable to complete. Failmode is not being invoked.

Possible Scenarios

Authentication not completing

Real world example: Duo pushed code that broke authentication for customers using a legacy version of the Duo Authentication Prompt. Users were failing to login after having successfully passed primary authentication and approved the secondary authentication request.

Failure of one or more authentication methods

Real world example: Duo's SMS service was not successfully delivering text messages to users, leaving them unable to authenticate.

Solutions

Some solutions may not be viable for all customers in all scenarios. For example, a firewall rule change may be more burdensome than messaging your users. Consider the solutions best for your organization. Degradation issues are typically resolved within 30 minutes.

- Apply a Group Access Policy to bypass two-factor authentication while the service degradation persists. Customers with paying editions of Duo can utilize Group Access Policies. In the event of the Duo service being unreachable, this solution can also be used.
    - **How:** Create and temporarily apply an Application-level Group Access Policy.
    - **What it does:** Allows users to access a specific application without completing two-factor authentication. Access can be restricted or enabled based on a user's membership in a Duo Group.
- Inform users of the interruption and offer workarounds if Duo has posted any on status.duo.com.
    - **How**: Refer to the End-user messaging templates section below. Navigate to status.duo.com to see if Duo has identified any temporary workarounds.
    - **What it does**: Ensures users that your organization and Duo are both aware of the problem and are working to fix it.
- Move all or some users into a group set to "bypass" status.
    - **How**: Manually or bulk update users to move them to a group if they are not in one already. That group needs 1) access to the protected application and 2) to be set to "bypass" status.
    - **What it does**: This will bypass two-factor authentication for any user in the group.
- Revert configuration/profile on applications so as to not invoke Duo.

    - **How**: Consult your specific application's documentation on duo.com/docs
    - **What it does**: This will remove two-factor authentication from the authentication workflow
- Manually block Duo's service via a firewall rule to effectively create an **unreachable** outage scenario:
    - **How**: Block *.duo.com and *.duosecurity.com on TCP port 443.
    - **What it does**: This will invoke failmode. If fail safe is configured, access to the application will be granted without two-factor authentication. If fail secure is configured, access will be blocked. Monitor status.duo.com closely to know when this change can be reversed.

5. Configuration decisions

Carefully consider which failmode configuration you should use for your application (if available).* Your choice will likely hinge upon:

- Policy and compliance factors.
- The type of data contained within protected applications.
    - Health records, financials, Personally Identifiable Information (PII), Intellectual Property (IP), etc.
- Groups of users with varying levels of access.
- The need to balance security with usability.

**Consult your specific application's documentation on duo.com/docs to see whether it features a configurable failmode.*

With regard to failmode configurations and action plans in the event of service degradations, there are generally 3 main categories an organization's application can fall under:

	Unreachable *(failmode invoked)*	**Degradation** *(failmode not invoked)*
Most restrictive **Contract, law, policy, or sensitivity of data** contained within the protected application requires two-factor authentication, without exception.	Fail secure	Users and Groups should NOT be switched to "bypass" status, as this will skip two-factor authentication.
Restrictive Some **subsets of users** are *always* required to pass two-factor authentication, without exception.	Fail secure	Users and Groups who without exception are required to pass two-factor authentication should NOT be switched to "bypass" status, as this will skip two-factor authentication. Users and Groups for whom it is tolerable to access this application without two-factor can be switched to "bypass," allowing them to skip two-factor authentication.
Less restrictive Contract, law, policy, or sensitivity of data contained within the protected application does ***not*** mandate that two-factor authentication be used in all circumstances.	Fail safe	Users and Groups for whom it is tolerable to access this application without two-factor can be switched to "bypass," allowing them to skip two-factor authentication.

* Take consideration if a Group of users has access to more than one application, as putting them in "bypass" will skip two-factor authentication for all applications they have access to. If this must be done for a Group to access another application, that Group's access to this application should first be removed.

6. End-user messaging templates

Consider at what point during an incident your organization is comfortable with messaging end-users. It could be as soon as your users begin reporting problems, it could be after Duo posts a notification on status.duo.com but before your users have reported anything, or it could be only if an incident has remained unresolved for 20 or more minutes.

Time of day

- An incident at 11am on a weekday may require immediate messaging to users.
- An incident at 11pm on a weekend may not need to be messaged to users immediately.

Time of quarter

- An incident during the last week of a quarter may require immediate messaging to users, regardless the time of day.

Criticality of access

- An incident affecting access to a critical application may require immediate messaging regardless the time, date or other factors.

Duo service unreachable or degraded

If you're using **fail safe** when Duo is unreachable or invoking failmode manually during degradation**:**

SUBJECT: Authentication problems - In Progress

BODY: Duo is reporting problems with their service. As a temporary workaround, we are lifting the requirement of Duo two-factor authentication. Once the problem is resolved, two-factor authentication will be reinstated.

If you're using **fail secure**:

SUBJECT: Authentication problems - In Progress

BODY: We are experiencing problems with Duo two-factor authentication. Due to the nature of data contained within <your application>, access will be denied until this problem is resolved.

Authentication method-specific issue

SUBJECT: Authentication problems - In Progress

BODY: Duo is reporting problems with their <push/SMS/phone> service. As a temporary workaround, please use <sms/push/phone callbacks>. Expect another update when the issue has been resolved.

7. FAQs

Can I be notified when failmode is invoked?

Failmode is configured and invoked locally in your Duo Authentication Proxy or Duo-protected application. We recommend using a monitoring tool or SIEM solution to watch for a failmode transaction.

You can determine whether failmode has been invoked by examining your Authentication Proxy's logs. The default directory for storing logs is C:\Program Files (x86)\Duo Security Authentication Proxy\log on a 64-bit Windows machine and C:\Program Files\Duo Security Authentication Proxy\log on a 32-bit Windows machine.

Below are two examples of Duo Authentication Proxy logs showing when failmode has been invoked.

fail safe log example

```
duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: TimeoutError('',)
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
```

fail secure log example

```
duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: TimeoutError('',)
2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Error in Duo login
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
```

How can I monitor Duo?

Duo continuously monitors the health and availability of our service. Subscribe to notifications at status.duo.com.

To monitor your locally installed Duo Authentication Proxy, we recommend monitoring the service itself and the port it uses (1812 by default).