Duo End User Education
Communication Templates

**Table of Contents**

[Email Communication Best Practices](#_Email_Communication_Best)

[End User Glossary + FAQs](#_End_User_Glossary)

[Glossary](#_Glossary)

[Frequently Asked Questions](#_Frequently_Asked_Questions)

[Email Templates - Introducing End Users to Duo](#_Email_Templates_-)

[Use these templates if your organization is introducing end users to MFA/Duo for the first time:](#_Use_these_email)

[Use these templates if your organization is replacing a pre-existing MFA solution with Duo:](#_yug77oc7ht31)

[Email Templates - New Policy Communication](#_Email_Templates_-_1)

[Use these templates to inform users of upcoming policy change(s)](#_Use_these_templates)

# Email Communication Best Practices

Below are a few best practices when emailing your users about the upcoming deployment of Duo 2FA:

* **Days to send emails:** Tuesdays, Wednesdays, and Thursdays are the best days to send emails users will open.
* **Who to send the email from:** We recommend this email come from a person (IT manager, Ops director, etc) or your helpdesk.

# End User Glossary + FAQs

Below are key terms and questions end users may find useful when introduced to Duo. Feel free to use this information as-is or customize as needed for your organization.

## Glossary

**2FA (two-factor authentication):** an additional layer of authentication beyond a username and password. 2FA involves something you know (password) plus something you have with you (like Duo Mobile on your smartphone) to prevent someone from logging in with only your password. With Duo 2FA, you still enter your username and password. The second factor provided by Duo is simply an added layer of security on top of your existing credentials. We recommend using Duo Push via the Duo Mobile app to perform 2FA.

**Duo Prompt:** this interactive prompt lets you choose how to verify your identity each time you log in (e.g. “Duo Push” or “Call Me”) to a web-based application. The Duo Prompt allows you to enroll and authenticate.



**Passcode:** these are numeric codes that can be generated either via the Duo Mobile app, SMS (text message), or a hardware token, depending on what your IT administrator permits. Passcodes may be used at any time and are particularly handy for authenticating when your 2FA device doesn't have internet or cellular service.



**Push Notification (Duo Push):** a push authentication request that is sent to the Duo Mobile app on an enrolled device. Push notifications include information like the geographical location of the access device, IP address of the access device, and the application being accessed so you can verify whether the push is real or fraudulent.

**Self-service portal:** if the self-service portal has been enabled for use in the Duo Prompt, you can click “Manage devices” (Universal Prompt) or “My Settings & Devices” (Traditional Prompt) to add additional devices or update authentication method settings right from the Duo Prompt.

## Frequently Asked Questions

Below are some key questions end users commonly have. *Depending on your organization’s specific applications and configuration, some questions may need editing or can be omitted.*

**Do I need a smartphone or data plan to use two-factor authentication?**

No. Having a smartphone makes for an easier and more secure experience with Duo Push. However, if your organization permits it, it is also possible to enroll a non-smartphone mobile device or landline to receive SMS passcodes or phone calls.

**What is Duo Mobile?**

Duo Mobile is a mobile application (app) that you install on your smartphone or tablet to generate passcodes for login or receive push notifications for easy, one-tap authentication on your mobile device. It works with Duo Security’s two-factor authentication (2FA) service to make your logins more secure.

**What is the recommended two-factor authentication method?**

If you have a smartphone or or tablet, we recommend Duo Push, as it is quick, easy-to-use, and secure. See an introduction to Duo Security and a demonstration of Duo Push in this short video: <https://www.youtube.com/watch?v=_T_sJXnSM98>

**How much data does a Duo Push request use?**

Duo Push authentication requests require a minimal amount of data -- less than 2KB per authentication. For example, you would only consume 1 megabyte (MB) of data if you were to authenticate 500 times in a given month.

**Why have I stopped receiving push notifications from Duo Mobile?**

There are several reasons this could be happening. Please try the following to troubleshoot:

1. Make sure your enrolled device has a cellular network or WiFi connection.
2. Have the Duo Mobile app open when you authenticate.
3. Try these additional push troubleshooting steps:
	* iPhone: <https://help.duo.com/s/article/2051>
	* Android: <https://help.duo.com/s/article/2050>
4. If the above solutions don’t work, try using another authentication method, such as passcodes provided in the Duo Mobile app.

**How can I authenticate if I’m somewhere with no cell signal or WiFi access?**

See this Duo Knowledge Base article for information on authenticating without cell or internet service: <https://help.duo.com/s/article/4449>

**How can I manage the devices I use for Duo?**

If you have access to the “My Settings & Devices” link (the self-service portal) at the Duo Prompt and are currently able to authenticate with a device, you may:

* Add additional devices
* Designate your “default” device that receives authentication requests in addition to your preferred authentication method (available in the Traditional Prompt)
* Deactivate Duo Mobile if you got a new phone but kept your number
* Change the name of your device (ex. “Personal Cell” or “Work Phone”)
* Remove a device

Learn more about managing your devices here: <https://guide.duo.com/manage-devices>

****

 **What should I do if I lost my phone?**

Please contact your IT help desk immediately.

**Can Duo see my password?**

No. Your password is only verified by your organization and never sent to Duo. Duo provides only the second factor, using your enrolled device to verify it’s actually you who is logging in.

**Does using Duo give up control of my smartphone?**

No. The Duo Mobile app has no access to change settings or remotely wipe your phone. The visibility Duo Mobile requires is to verify the security of your device, such as OS version, device encryption status, screen lock, etc. We use this to help recommend security improvements to your device. You always are in control of whether or not you take action on these recommendations.

# Email Templates - Introducing End Users to Duo

### Use these email templates if your organization is introducing end users to MFA/Duo for the first time:

Email #1 - *Duo is coming soon, no immediate action required. .*

**TIMELINE:**

30 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE:**

Duo two-factor authentication is coming soon!

**BODY:**

To improve our security posture, we will be incorporating Duo Security as a **two-factor authentication** solution into our existing IT infrastructure.

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming rollout of Duo two-factor authentication.

**What is Duo Security?**



Duo Security is a company that provides a cloud-based software service that utilizes two-factor authentication to ensure secure access to services and data. Learn more by clicking [here](https://www.youtube.com/watch?v=0mvCeNsTa1g).

**What is two-factor authentication?**

Two-factor authentication provides a second layer of security to any type of login, **requiring extra information or a physical device to log in,** in addition to your password.

By requiring two different channels of authentication, we can protect user logins from remote attacks that may exploit stolen usernames and passwords.

**The factors may include:**

|  |  |
| --- | --- |
| image29.jpg | **Something you know:*** A unique username and password.
 |
| image18.jpg | **Something you have:*** A smartphone with an app to approve authentication requests.
 |
| image42.jpg | **Something you are:*** Biometrics - like your fingerprint or a retina scan.
 |

## Why do we need two-factor authentication?

Login credentials are more valuable than ever and are increasingly easy to compromise. Over 90% of breaches today involve compromised usernames and passwords.

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. **This prevents anyone but you from accessing your account, even if they know your password.**

##

## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to complete a method of second-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method. **More information on the rollout of Duo is coming soon.**

Email #2 - *Duo is coming on <DATE>, no immediate action required.*

**TIMELINE:**

15 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE**:

Enroll in Duo two-factor authentication on **<DATE OF ENROLLMENT EMAIL>**

**BODY:**

To improve our security posture, we will be incorporating Duo Security as a **two-factor authentication** solution into our existing IT infrastructure.

You will receive an enrollment email from Duo on **<DATE OF ENROLLMENT EMAIL>**. Expect to see more on this in the coming days.

##

## Action required:

**No immediate action is necessary.** This email is to notify and educate you about the upcoming rollout of Duo two-factor authentication on **<DATE OF ENROLLMENT EMAIL>**.

**What is Duo Security?**



Duo Security is a company that provides a cloud-based software service that utilizes two-factor authentication to ensure secure access to services and data. Learn more by clicking [here](https://www.youtube.com/watch?v=0mvCeNsTa1g).

**What is two-factor authentication?**

Two-factor authentication provides a second layer of security to any type of login, **requiring extra information or a physical device to log in,** in addition to your password.

By requiring two different channels of authentication, we can protect user logins from remote attacks that may exploit stolen usernames and passwords.

**The factors may include:**

|  |  |
| --- | --- |
| image28.jpg | **Something you know:*** A unique username and password.
 |
| image37.jpg | **Something you have:*** A smartphone with an app to approve authentication requests.
 |
| image23.jpg | **Something you are:*** Biometrics - like your fingerprint or a retina scan.
 |

##

## Why do we need two-factor authentication?

Login credentials are more valuable than ever and are increasingly easy to compromise. Over 90% of breaches today involve compromised usernames and passwords.

Two-factor authentication **enhances the security of your account by using a secondary device to verify your identity**. This prevents anyone but you from accessing your account, even if they know your password.

## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to complete a method of second-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method. **More information on the rollout of Duo is coming soon.**

Email #3 - *Duo is coming on <DATE> + enrollment information, no action needed right now.*

**TIMELINE:**

3 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE**:

Reminder: Duo two-factor authentication is coming on **<DATE OF ENROLLMENT EMAIL>**

**BODY:**

To improve our security posture, we will be incorporating Duo Security as a **two-factor authentication** solution into our existing IT infrastructure.

You will receive an enrollment email from Duo on **<DATE OF ENROLLMENT EMAIL>**. This email will contain a **personalized link allowing you to enroll with Duo**. This 2-minute self-enrollment process makes it easy to **register your phone and install the Duo Mobile application.**

If you do not have a smartphone, you can enroll a regular cell phone (SMS and calls) or landline (calls) for two-factor authentication.

## Action required:

**No immediate action required**. This email is to remind you of the upcoming rollout of Duo two-factor authentication on **<DATE OF ENROLLMENT EMAIL>**.

## What are Duo Mobile and Duo Push?

**Duo Mobile** is Duo Security’s free app that allows you to quickly and easily approve a second-factor authentication request using **Duo Push**.

With **Duo Mobile and Duo Push**, there is no need to carry a bulky token or waste time manually entering in passcodes. Just tap to authenticate right on your smartphone.

[Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to complete a method of second-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method.

## What is Duo, what is two-factor authentication, and why do we need it?

If you’ve missed our previous emails, watch[this video](https://www.youtube.com/watch?v=0mvCeNsTa1g)to learn more.

**Questions?**

Please reach out to the **<Help Desk/Service Desk>** with any questions about enrolling or using Duo.

* **<Help Desk/Service Desk> Phone Number:**
* **<Help Desk/Service Desk> Email:**

Email #4 - *Check Your Inbox for Duo Enrollment Email - Enroll Now.*

**TIMELINE:**

Day of enrollment email send/application go-live.

**SUBJECT LINE**:

Action required: Enroll in Duo today

**BODY:**

To improve our security posture, we will be incorporating Duo Security as a **two-factor authentication** solution into our existing IT infrastructure.

Today you will receive an enrollment email from Duo Security. This email will contain a **personalized link allowing you to enroll with Duo**. This 2-minute self-enrollment process makes it easy to **register your phone and install the Duo Mobile application.**

If you do not have a smartphone, you can enroll a regular cell phone (SMS + calls) or landline (calls) for two-factor authentication.

You will have until **<DATE OF APPLICATION + DUO GO-LIVE>** to enroll. After this date, access to **<APPLICATION>** will require Duo two-factor authentication.

##

## Action required:

**Enroll today**. Check your inbox for an enrollment email from Duo and complete the enrollment process.

##

## What are Duo Mobile and Duo Push?

**Duo Mobile** is Duo Security’s free app that allows you to quickly and easily approve a second-factor authentication request using **Duo Push**.

With **Duo Mobile and Duo Push**, there is no need to carry a bulky token or waste time manually entering in passcodes. Just tap to authenticate right on your smartphone.

[Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to complete a method of second-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method.

## What is Duo, what is two-factor authentication, and why do we need it?

If you’ve missed our previous emails, watch[this video](https://www.youtube.com/watch?v=0mvCeNsTa1g)to learn more.

**Questions?**

Please reach out to the **<Help Desk/Service Desk>** with any questions about enrolling or using Duo.

* **<Help Desk/Service Desk> Phone Number:**
* **<Help Desk/Service Desk> Email:**

### Use these email templates if your organization is replacing a pre-existing MFA solution with Duo:

Email #1 - *Duo is coming soon, no immediate action required. .*

**TIMELINE:**

30 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE:**

Duo two-factor authentication to replace **<Current 2FA Provider>**

**BODY:**

To improve our security posture and current user experience with **two-factor authentication**, we will be replacing **<Current 2FA Provider>** and incorporating Duo Security as our new **two-factor authentication** solution into our existing IT infrastructure.

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change in the way we perform two-factor authentication.

**Why is Duo Security a better user experience?**

With Duo Security’s free mobile app, **Duo Mobile**, you no longer need to carry a bulky token or waste time entering in a passcode when logging into a protected application.

**Duo Mobile** allows you to quickly and easily approve a second-factor authentication request on your smartphone via **Duo Push.** If you previously used a hardware token or passcode, **your smartphone now replaces that.** [Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



## Why do we need two-factor authentication?

Login credentials are more valuable than ever and are increasingly easy to compromise. Over 90% of breaches today involve compromised usernames and passwords.

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. **This prevents anyone but you from accessing your account, even if they know your password.**

##

## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to approve a Duo Push notification or other method of two-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method. **More information on the rollout of Duo is coming soon.**

Email #2 - *Duo is coming on <DATE>, no immediate action required.*

**TIMELINE:**

15 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE**:

Enroll in Duo two-factor authentication on **<DATE OF ENROLLMENT EMAIL>**

**BODY:**

To improve our security posture and current user experience with **two-factor authentication**, we will be replacing **<Current 2FA Provider>** and incorporating Duo Security as our new **two-factor authentication** solution into our existing IT infrastructure.

You will receive an enrollment email from Duo on **<DATE OF ENROLLMENT EMAIL>**.

##

## Action required:

**No immediate action is necessary.** This email is to notify you that we will be changing our two-factor authentication from **<Current 2FA Provider>** to **Duo Security on** **<DATE OF ENROLLMENT EMAIL>**.

**Why is Duo Security a better user experience?**

With Duo Security’s free mobile app, **Duo Mobile**, you no longer need to carry a bulky token or waste time entering in a passcode when logging into a protected application.

**Duo Mobile** allows you to quickly and easily approve a second-factor authentication request on your smartphone via **Duo Push**.If you previously used a hardware token or passcode, **your smartphone now replaces that.** [Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



##

## Why do we need two-factor authentication?

Login credentials are more valuable than ever and are increasingly easy to compromise. Over 90% of breaches today involve compromised usernames and passwords.

Two-factor authentication **enhances the security of your account by using a secondary device to verify your identity**. This prevents anyone but you from accessing your account, even if they know your password.

## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to approve a Duo Push notification or other method of two-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method. **More information on the rollout of Duo is coming soon.**

Email #3 - *Duo is coming on <DATE> + enrollment information, no action needed right now.*

**TIMELINE:**

3 days prior to the enrollment email send/application go-live date.

**SUBJECT LINE**:

Reminder: Duo two-factor authentication to replace **<Current 2FA Provider>** on **<DATE OF ENROLLMENT EMAIL>**

**BODY:**

To improve our security posture and current user experience with **two-factor authentication**, we will be replacing **<Current 2FA Provider>** and incorporating Duo Security as our new **two-factor authentication** solution into our existing IT infrastructure.

You will receive an enrollment email from Duo on **<DATE OF ENROLLMENT EMAIL>**. This email will contain a **personalized link allowing you to enroll with Duo**. This 2-minute self-enrollment process makes it easy to **register your phone and install the Duo Mobile application.**

If you do not have a smartphone, you can enroll a regular cell phone (SMS text messages and calls) or landline (calls) for two-factor authentication.

## Action required:

**No immediate action required**. This email is to remind you of the upcoming change for two-factor authentication from **<Current 2FA Provider>** to **Duo Security** on **<DATE OF ENROLLMENT EMAIL>**.

## What is Duo, what is two-factor authentication, and why do we need it?

If you’ve missed our previous emails, watch[this video](https://www.youtube.com/watch?v=0mvCeNsTa1g)to learn more.

**Why is Duo Security a better user experience?**

With Duo Security’s free mobile app, **Duo Mobile**, you no longer need to carry a bulky token or waste time entering in a passcode when logging into a protected application.

**Duo Mobile** allows you to quickly and easily approve a second-factor authentication request on your smartphone via **Duo Push**.If you previously used a hardware token or passcode, **your smartphone now replaces that.** [Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to approve a Duo Push notification or other method of two-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method.

**Questions?**

Please reach out to the **<Help Desk/Service Desk>** with any questions about enrolling or using Duo.

* **<Help Desk/Service Desk> Phone Number:**
* **<Help Desk/Service Desk> Email:**

Email #4 - *Check Your Inbox for Duo Enrollment Email - Enroll Now.*

**TIMELINE:**

Day of enrollment email send/application go-live.

**SUBJECT LINE**:

Action Required: Enroll in Duo today

**BODY:**

To improve our security posture and current user experience with **two-factor authentication**, we will be replacing **<Current 2FA Provider>** and incorporating Duo Security as our new **two-factor authentication** solution into our existing IT infrastructure.

## Action required:

Today you will receive an enrollment email from Duo Security. This email will contain a **personalized link allowing you to enroll with Duo**. This 2-minute self-enrollment process makes it easy to **register your phone and install the Duo Mobile application.**

If you do not have a smartphone, you can enroll a regular cell phone (SMS text messages + calls) or landline (calls) for two-factor authentication.

You will have until **<DATE OF APPLICATION + DUO GO-LIVE>** to enroll. After this date, access to **<APPLICATION>** will require Duo two-factor authentication and **<Current 2FA Provider>** two-factor authentication will be decommissioned.

##

## What is Duo, what is two-factor authentication, and why do we need it?

If you’ve missed our previous emails, watch[this video](https://www.youtube.com/watch?v=0mvCeNsTa1g)to learn more.

**Why is Duo Security a better user experience?**

With Duo Security’s free mobile app, **Duo Mobile**, you no longer need to carry a bulky token or waste time entering in a passcode when logging into a protected application.

**Duo Mobile** allows you to quickly and easily approve a second-factor authentication request on your smartphone via **Duo Push**.If you previously used a hardware token or passcode, **your smartphone now replaces that.** [Here](https://www.youtube.com/watch?v=tPLxe9HUDjY) is an example of Duo Push in action.



## How will Duo change my login experience?

When logging in to an application that is protected by Duo, you will still enter your username and password.After inputting your login information, **Duo requires you to approve a Duo Push notification or other method of two-factor authentication**.

Duo does not replace or require you to change your username and password*.* Think of Duo as a layer of security added to your pre-existing login method.

**Questions?**

Please reach out to the **<Help Desk/Service Desk>** with any questions about enrolling or using Duo.

* **<Help Desk/Service Desk> Phone Number:**
* **<Help Desk/Service Desk> Email:**

# Email Templates - New Policy Communication

### Use these templates to inform users of upcoming policy change(s):

Email #1 - *Upcoming changes to Duo Policy on <DATE>, no immediate action required.*

**TIMELINE:**

30 days prior to the policy change is enforced.

**SUBJECT LINE:**

Changes to Duo 2FA login: **<Version X.XX of OS/Browser/Plugin or Biometric Authentication/Disk Encryption/Screen Lock** required starting **<DATE>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require you to update your **<mobile or access device>** to satisfy the following requirements:

* **A**
* **B**
* **C**

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change so you can take proactive steps if needed.

However if you would like to make these changes now, please reference the following:

 **<Include instructions for how to check for/enable encryption/biometrics/screen lock or check their browser/plugin/OS version and perform updates.>**

Email #2 - *Upcoming changes to Duo Policy on <DATE>, no immediate action required.*

**TIMELINE:**

1 week prior to the policy change is enforced.

**SUBJECT LINE:**

Reminder: Upcoming changes to Duo 2FA login - **<Version X.XX of OS/Browser/Plugin or Biometric Authentication/Screen Lock Required starting DATE>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require you to update your **<mobile or access device>** to satisfy the following requirements:

* **A**
* **B**
* **C**

**Action Required:**

**No immediate action is necessary, but you have one week to perform the needed updates (if needed).** This email is to notify and educate you about the upcoming change so you can take proactive steps.

However if you would like to make these changes now, please reference the following:

 **<Include instructions for how to check for/enable encryption/biometrics/screen lock or check their browser/plugin/OS version and perform updates.**

Email #3 - *Changes to Duo Policy TOMORROW, device/software updates may be required.*

**TIMELINE:**

1 day prior to policy enforcement.

**SUBJECT LINE:**

Reminder: Upcoming changes to Duo 2FA login TOMORROW - **<device/software>** updates may be needed or risk losing access.

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require you to update your **<mobile or access device>** to satisfy the following requirements:

* **A**
* **B**
* **C**

**Action Required:**

**Please update your <device/software> today** or you will lose access to your applications.

**<Include instructions for how to check for/enable encryption/biometrics/screen lock or check their browser/plugin/OS version and perform updates.**