**Duo Trusted Endpoints**

**End User Communication Templates**

**Table of Contents**

[How to Use These Templates](#_Toc14172006)

[Email Communication Best Practices](#_Toc14172007)

[FAQs](#_Toc14172008)

[Email Templates - Trusted Endpoints Enforcement Communication](#_Toc14172009)

[Email Templates - Trusted Endpoints with Duo Mobile Enforcement Communication](#_Toc14172014)

**How to Use These Templates**

Please note: As this document is a template and intended to be customized, there are verbiage and suggestions listed that can be changed to be more suitable to your organization. Some examples include:

* **“Trusted Device”**
	+ Depending on how your organization chooses to refer to devices with certs on them or devices utilizing [Trusted Endpoints with Duo Mobile](https://duo.com/docs/trusted-endpoints-duo-mobile), alternatives could be: Corporate Device, Company-Approved Device, Company-Managed Device, Approved Device, Managed Device, etc.
* **Action Required?**
	+ In the event that end users need to supply or prepare any devices for cert deployment, install Duo Mobile because they aren’t already using the app, etc. you may need to edit this section.
* **Timelines**
	+ Edit the timeline of these emails to a cadence more appropriate for your organization.

Additionally, there are yellow and bolded text areas highlighted to indicate areas likely to require customization, but please adapt this content as much or as little as you need.

**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.

**FAQs**

Below are some key questions end users may have. *Depending on your organization’s specific applications and configuration, some questions may need editing. Also feel free to include questions you anticipate receiving from users.*

**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 and can be used to verify your device security.

**Why do I need the Duo Mobile app to access applications?**

Beyond performing 2FA with Duo Push or passcodes, the Duo Mobile app occasionally performs a check when you access certain applications to verify that the device meets security criteria set by our organization.

**Email Templates - Trusted Endpoints Enforcement Communication**

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

**TIMELINE:**

30 days prior to policy enforcement.

**SUBJECT LINE:**

Changes to Duo 2FA login: **<Trusted Device>** required **<for access to X Y Z application(s)>** starting **<DATE>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require you to use a **<trusted device>** to access the following application(s):

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

Your **<trusted device>** will be your **<work computer / work laptop / company-issued phone>**.If you attempt access from another device, access will be denied.

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change. **<This organization’s IT staff>** will be performing all necessary changes and providing assistance if needed.

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

**TIMELINE:**

1 week prior to policy enforcement.

**SUBJECT LINE:**

Changes to Duo 2FA login: **<Trusted Device>** required **<for access to X Y Z application(s)>** starting **<DATE>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require you to use a **<trusted device>** to access the following application(s):

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

Your **<trusted device>** will be your **<work computer / work laptop / company-issue phone>.** Starting next week on **<DATE>** if you attempt to access one of the restricted applications with a device that is not trusted, you will see this message in the Duo Prompt:



**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change. **<This organization’s IT staff>** will be performing all necessary changes and providing assistance if needed.

**Email #3 - *Changes to Application Access TOMORROW, action may be required.***

**TIMELINE:**

1 day prior to policy enforcement.

**SUBJECT LINE:**

Changes to Duo 2FA login: **<Trusted Device>** required **<for access to X Y Z application(s)>** startingTOMORROW

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, starting **tomorrow** we will require you to use a **<trusted device>** to access the following application(s):

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

If you attempt to access one of the restricted applications with a device that is not managed, you will see this message in the Duo Prompt:



**Action Required:**

Tomorrow, begin using a **<trusted device>** for access. **<This organization’s IT Staff>** has handled all necessary changes. If you encounter a problem and need assistance, please contact **<this organization’s IT Help Desk>**, ***not*** Duo Support.

**Email Templates - Trusted Endpoints with Duo Mobile Enforcement Communication**

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

**TIMELINE:**

30 days prior to policy enforcement.

**SUBJECT LINE:**

Change Coming **<DATE>**: Duo Mobile apprequired **<for access to X Y Z application(s)>**  **BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require a device check via the Duo Mobile app to access the following application(s):

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

Once this goes into effect, after you enter your username and password, you will occasionally see this message in the Duo Prompt when Duo determines that the Duo Mobile app needs to open and validate if your device is safe to access the application:



When the device check is complete, you will be prompted for a second factor of authentication as usual and then allowed into the protected application.

Duo Mobile is available in the Google Play Store (Android) [here](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile) and in the Apple App Store (iOS) [here](https://itunes.apple.com/us/app/duo-mobile/id422663827?mt=8).

Please also note that with this change you may also need to **<update/enable X>** on your device to meet new security hygiene standards enforced by the Duo Mobile app.

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change.

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

**TIMELINE:**

1 week prior to policy enforcement.

**SUBJECT LINE:**

Change Coming **<DATE>**: Duo Mobile apprequired **<for access to X Y Z application(s)>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, we will soon require a device check via the Duo Mobile app to access the following application(s):

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

Once this goes into effect, after you enter your username and password, you will occasionally see this message in the Duo Prompt when Duo determines that the Duo Mobile app needs to open and validate if your device is safe to access the application:



When the device check is complete, you will be prompted for a second factor of authentication as usual and then allowed into the protected application.

Please also note that in the interest of security the Duo Mobile app will require you update your **<mobile or access device>** to satisfy the following device hygiene requirements:

* **X**
* **Y**
* **Z**

**Action Required:**

**No immediate action is necessary.** This email is to notify and educate you about the upcoming change so you can download and install the Duo Mobile app if you haven’t already. (Duo Mobile is available in the Android Play Store [here](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile) and in the Apple App Store [here](https://itunes.apple.com/us/app/duo-mobile/id422663827?mt=8).) You may also need to **<update/enable X>** on the device to meet new security hygiene standards enforced by the Duo Mobile app. **<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 Application Access TOMORROW, action may be required.***

**TIMELINE:**

1 day prior to policy enforcement.

**SUBJECT LINE:**

Change Coming TOMORROW: Duo Mobile apprequired **<for access to X Y Z application(s)>**

**BODY:**

To improve our security posture and to ensure continued access to Duo-protected applications, tomorrow we will require a device check via the Duo Mobile app to access the following application(s):

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

Once this goes into effect, after you enter your username and password, you will occasionally see this message in the Duo Prompt when Duo determines that the Duo Mobile app needs to open and validate if your device is safe to access the application:



When the device check is complete, you will be prompted for a second factor of authentication as usual and then allowed into the protected application.

Please also note that in the interest of security the Duo Mobile app will require you update your **<mobile or access device>** to satisfy the following device hygiene requirements:

* **X**
* **Y**
* **Z**

**Action Required:**

**Download and install Duo Mobile today.** This email is to notify and educate you about the change so you can download and install the Duo Mobile app if you haven’t already. (Duo Mobile is available in the Android Play Store [here](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile) and in the Apple App Store [here](https://itunes.apple.com/us/app/duo-mobile/id422663827?mt=8).)

You may also need to **<update/enable X>** on the device. **<Include instructions for how to check for/enable encryption/biometrics/screen lock or check their browser/plugin/OS version and perform updates.**

If you encounter a problem and need assistance, please contact **<this organization’s IT Help Desk>**, ***not*** Duo Support.