Email templates to communicate SecureAuth 2FA use

Planning and considerations

This section explains how administrators might plan to roll out the SecureAuth® Identity Platform.

Although each organization will have its own set of considerations, basic planning should include the following:

- Email to introduce end users to two-factor authentication (2FA)
- Email to end users describing how to set up 2FA methods
- Email to explain passwordless paradigm shift
- Roll-out strategy for admins to consider
- Additional considerations, such as policies and use cases

Timing email communications

Cadence: Start communication and education early to lessen the disruption for end users. How early you start depends on end user sophistication with security. You know your end users best, but consider the following:

- If end users are **sophisticated about security** but will use two-factor authentication (2FA) for the first time, consider the following checklist:
    - Start education a month ahead of setup.
    - Send out additional reminders to complete set up once or twice per week to ensure that end users are prepared on the go-live date.

- If end users have **some or no knowledge about security**, start education as early as you think necessary, and consider the following checklist:
    - Start education anywhere from 3 months to a year prior to your go-live date. See Explain security to end users for education topics to include in short, focused, monthly educational emails.
    - Two weeks before go-live, send the startup instructions in this packet.

- Send additional reminders to complete set up once or twice per week to ensure that end users are prepared on the go-live date.

Day to send email: Research shows that Tuesday is when most email users open and read emails, followed by Thursday and then Wednesday.

Who should send email: End users will have questions, so we suggest that your Security, IT, Operations, or Help Desk manager send the emails. If end users are resistant to using 2FA, have the CEO send the emails but add an email address for the person or team where end users can ask questions. (There is a fill-in field in the first email template for an email address.) Include the short FAQs document included in this toolkit; it will answer questions that end users will likely have.

Explain security to end users

If your end users are inexperienced, disinterested, or resistant to change, you probably want to begin communicating the change to 2FA early, anywhere from 3 months to a year before the roll-out.

The SecureAuth email templates include text to send a month and two weeks before the roll-out. The following topics offer guidance about how to start the security conversation with a time frame for each topic. Emails should be approximately one paragraph. Keep topics high-level, and the language simple and jargon-free. See 9 months before roll-out for an example of an educational email paragraph.

1 year of education email topics

The following are suggested email topics to educate end users about security and why to use it. The risk in starting communication so soon is that users may learn to ignore these emails if they find them uninteresting. You know your users best.

12 months before roll-out

Upbeat email announcement about SecureAuth® Identity Platform as the selected security tool. Convey the purpose of the change; answer the question...why is your organization using a security tool?

11 months before roll-out

What is data security and why is it important to your organization?

10 months before roll-out

Why does the organization need security? What is at stake without security?

If your organization must adhere to industry standards, such as HIPAA, PHI, PII, etc., this is a good time to remind the enterprise about the seriousness of adherence and that excellent security is one way to comply with standards.

9 months before roll-out

What is two-factor authentication (2FA) and why should end users care about it?

2FA is a way of logging into your corporate network securely. The first factor you enter is probably your username and password. The second factor you enter will be the options your SecureAuth administrator set up for you, such as a Notification Passcode you receive on your desktop or phone, a

set of security questions you answer, a fingerprint, or a security key (token) passcode you enter. These two factor methods provide "authentication," which is a fancy way of saying that you can prove you are who you say you are.

8 months before roll-out
What is “authentication” and why should end users care about it?

7 months before roll-out
Will using two-factor authentication (2FA) take a lot of extra time every day? What will logging in with 2FA mean for end users?

6 months before roll-out
State of the roll-out, now that your organization is at the halfway mark

5 months before roll-out
What is “single sign-on” and will your end users use it? (If they use it already, explain that they will continue to use it for their convenience.)

4 months before roll-out
Putting it together: Very simply explain how a second factor, authentication, and single sign-on help end users access data safely.

3 months before roll-out
What is “identity” and why is it important? What happens when identities are breached? View the video on the SecureAuth website: Modern Adaptive Authentication (2:28).

2 months before roll-out
Review: Short, upbeat email that again announces the SecureAuth® Identity Platform as the new security tool, gives the roll-out date, and very briefly explains why your organization is rolling out a security solution. Include links to the emails already sent so users can easily refresh the knowledge they have gained over the last year.

1 month before roll-out
See Email 1: Coming soon: Secure Login with SecureAuth

2 weeks before roll-out
See Email 2: ACTION REQUIRED: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

If you have enabled FIDO2 WebAuthn for the passwordless workflow, see Passwordless secure login and How SecureAuth FIDO2 WebAuthn works. Both are written to be understandable by end users.

1 week after roll-out
See Email 3: ACTION REQUIRED: Reminder - Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

2 weeks after roll-out
See Email 4: FINAL REMINDER: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

Stage roll-outs across the enterprise

Large organizations that want to roll out 2FA to end users in stages will need to plan a roll-out strategy. The following are some points to consider:

- Where is the highest urgency?
  Which employees require immediate 2FA use to meet industry standards? These employees are good candidates to include in an early roll-out.

- Who is enthusiastic about the change?
  These employees are good candidates to include in a test roll-out.

- What kind of technical competency do your end users possess?
  If end users are comfortable with technology, consider building large groups per stage. If end users are uncomfortable with technology or resistant to change, consider building small groups per stage to offer more individual assistance with set up and when you go live.

- How many end users can your technical team support?
  This is particularly important if end users are uncomfortable with technology or resistant to change.

- Throughout the roll-out process, ensure that you communicate to end users the project timeline and when each team is scheduled to be included in a roll-out.

Additional considerations

Think about the following scenarios when you're crafting educational emails to your end users. How can you help make the journey to security use easiest for your end users?

Straggler strategy

Almost all organizations will have users who wait until the last minute to set up two-factor authentication. A typical consequence for users who do not meet the set-up deadline is to lock their account. Think about what else you can do to motivate your end users to complete set up in a timely fashion. If you can identify which users have not set up two-factor authentication, you could contact their managers, or otherwise incentivize users.

Session length

Some sites require short session lengths between 2FA log in and time out, which means that end users must authenticate in more often, possibly multiple times per day. Other sites allow long session lengths. Whatever your site needs are, be sure to tell your end users that they must log in *X* times in an *X* time frame to set expectations.

Example: For sites with long session lengths, you might include a sentence such as: You will only have to log in with 2FA once a week, or when you work off network.

Did you know that admins can customize the session time in SecureAuth® Identity Platform? Time frames are available in a variety of increments, such as once every 24 hours or once per month per session. The session length you choose for your organization will depend on how high a level of security your data requires, and if your end users work off-network or offline.

Policy adherence and scenarios

Each organization has policies based on industry standards and corporate culture. Sometimes a policy and a 2FA method might seem to be at odds, but there are ways to ensure that end users adhere to policies while gaining all the security benefits of 2FA, without compromise. The following are some scenarios to consider prior to roll-out.

- Policy: If your site is a hospital or another industry that has a policy against employees carrying personal mobile devices, consider the following solutions:
    - Offer 2FA methods other than text-based passcodes. Some options include face and fingerprint recognition on tablets and use of YubiKey security keys.
    - Address the policy in your set-up email to end users. If end users can carry mobile phones to log in, state this so end users are prepared on the go-live date.
- Scenario: If your site is a healthcare provider, where doctors and nurses do not want to take their attention away from patients to look at a cell phone to get a passcode to log into necessary software, offer 2FA methods, such as YubiKey security keys; if end users have an AppleWatch, they can set it up to receive login confirmations, passcode notifications, and find timed passcodes.
- Scenario: If your site has many employees who are often away from their desks, offer 2FA methods other than desktop email only.

  Example: This includes sites where employees need to log into kiosks and cash registers. A mobile app or YubiKey security key are good 2FA options for these employees.

SecureAuth email templates

Use the SecureAuth email templates to build communication between the team tasked with organizing and deploying the SecureAuth® Identity Platform and end users.

The email templates are yours to customize before sending to end users. The templates explain:

- Why the organization needs security across the enterprise
- Actions to be taken by end users
- Changes end users can expect at first log in and thereafter

The email templates include the following information:

- Email 1: Coming soon: Secure Login with SecureAuth
- Email 2: ACTION REQUIRED: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)
- Email 3: ACTION REQUIRED: Reminder - Set up Devices to use SecureAuth Two-Factor Authentication (2FA)
- Email 4: FINAL REMINDER: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)
- Setup templates for administrator
- FAQs

The following two additional documents are included in the Onboarding toolkit zip file and contain information for admins to create custom set-up steps and timelines for end users:

- *SecureAuth 2FA end user set-up instructions*
- *SecureAuth timelines template*

Email 1: Coming soon: Secure Login with SecureAuth

When to send:

4 weeks before deployment/end-user go-live

Email Subject:

Coming soon: Secure Login with SecureAuth

Text:

We want to keep our data and identities safe. To do this, all employees will log in with a username, password, **and** a second factor, effective <insert approximate date here>. We will use SecureAuth two-factor authentication to provide secure login to our corporate network to protect your information, as well as the company's.

Why the change? Added security to keep your identity and data safe.

When you enter your username and password to log in, that's the first security "factor" you provide. Soon, all employees will enter a second factor, such as <a passcode delivered to your email or a personal identification number (PIN)>. Available second factors will be announced later.

Logging in with two-factor authentication at work is like logging into a payment app, such as Venmo or your banking website. You must enter a password and then some kind of second factor—a passcode texted to you, a fingerprint, etc.-- so the app can check that you are who you say you are, and then let you into the app to access your account.

What to do now

This email is educational. No action is required now.

Questions? Read FAQs. If you have questions that are not answered in this email or the FAQs, please contact <your.contact.team@company.com>.

Email 2: ACTION REQUIRED: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

When to send:

2 weeks before deployment/end-user go-live

Email Subject:

ACTION REQUIRED: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

Text:
We are rolling out SecureAuth two-factor authentication (2FA) to provide secure login to our corporate network and to data and applications on the Cloud, such as Office 365.

Starting <date>, all employees will log into the network with a <username, password, and a second factor. Admin: If offering a passwordless experience, describe the passwordless workflow you set up.> The following instructions will guide you to set up your two-factor authentication methods so you're ready to log in securely on <date>.

To do now:

1. Open the packet attached to this email and follow the instructions to set up two-factor authentication.
2. After you have set up your methods, test them to ensure they work: <Enter test environment URL here>
   <Delete this step if you have not set up a test environment>

Questions? Read FAQs. If you have questions that are not answered in this email or the FAQs, please contact <your.contact.team@company.com>.

<Admin: Add customized instructions as an attachment to this email. Instructions for each 2FA method are in the file *SecureAuth 2FA end user set-up instructions.*

You must complete setting up two-factor authentication by <date>. Failure to do so by <date> will <insert consequence such as, "your account will be locked, and you will not be able to log in" or "your manager will be notified">.

Email 3: ACTION REQUIRED: Reminder - Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

When to send:

1 week after initial set up email

Email Subject:

ACTION REQUIRED: Reminder - Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

Text:

You must complete setting up two-factor authentication by <date>. Failure to do so by <date> will <insert consequence such as, "your account will be locked, and you will not be able to log in" or "your manager will be notified">.

Starting <date>, all employees will log in with a <username, password, and a second factor or passwordless> to log into the network. The following instructions will guide you to set up two-factor authentication methods so you're ready to log in securely on <date>.

To do now:

1. Open the packet attached to this email and follow the instructions to set up two-factor authentication.
2. After you have set up your methods, test them to ensure they work: <Enter test environment URL here>
   <Delete this step if you have not set up a test environment>

Questions? Read FAQs. If you have questions that are not answered in this email or the FAQs, please contact <your.contact.team@company.com>.

<Admin: Add customized instructions as an attachment to this email. Instructions for each 2FA method are in the file *SecureAuth 2FA end user set-up instructions.*>

Email 4: FINAL REMINDER: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

When to send:

1 week before setup ends

Email Subject:

FINAL REMINDER: Set up Devices to use SecureAuth Two-Factor Authentication (2FA)

Text:

You are receiving this email because you have not yet set up two-factor authentication to protect your identity and data. **If you do not set up two-factor authentication by <date>, <insert consequence, such as "your account will be locked, and you will not be able to log in" or "your manager will be notified">.**

1. Open the packet attached to this email and follow the instructions to set up two-factor authentication.
2. After you have set up your methods, test them to ensure they work: <Enter test environment URL here>
   <Delete this step if you have not set up a test environment>

Questions? Read FAQs. If you have questions that are not answered in this email or the FAQs, please contact <your.contact.team@company.com>.

<Admin: Add customized instructions as an attachment to this email. Instructions for each 2FA method are in the file *SecureAuth 2FA end user set-up instructions.*>

Setup templates for administrator

Use the instructions in *SecureAuth 2FA end user set-up instructions* as guides for the 2FA methods available to end users. Only include the 2FA methods you make available to your end users. Be sure to include sample guidance screenshots where mentioned in.

FAQs

Admins: This information is geared for end users. Add a link to this section at the end of the emails you send to end users. Be sure to reference it so end users know to read the FAQs to get answers. Add any questions that most of your end users will have.

Q: Why do we need to use 2FA?

> **A**: Security attacks are on the rise and we want to keep our identities and information safe. Logging into the network with passwords alone does not provide enough security. Entering a second factor, such as a login confirmation, security answers, or YubiKey passcode provides the extra layer of security to keep our identities and information safe.

Q: Is SecureAuth storing my personal data?

> **A**: No. SecureAuth provides identity and data protection. SecureAuth does not read data on your devices or on the network.

Q: This change is really hard!

> **A**: We get that! Remember that you are taking just one extra step and you are doing it to keep **your** identity and data safe.

Q: How much money will I spend on passcode texts to my phone?

> **A**: Standard text message rates apply, but the same as when you receive passcode texts from a banking app (Chase, Bank of America) or other service app (Venmo, Kohls, etc.).

Q: What should I do if I lose the phone, tablet, or YubiKey that I use to log in with 2FA?

> **A**: Contact your SecureAuth administrator or Help Desk right away. Your admin will disable authentication for your lost or stolen device and will provide a different login option for you, until you get another device.

Q: I already have a YubiKey that I use for personal data security...can I use that one for work?

> **A**: This is up to your SecureAuth administrator and your company's policies. Check with your SecureAuth administrator.

Q: I travel a lot for the company. How will I be able to use 2FA on travel?

> **A**: You can log into your corporate network while traveling by using the same method as when you work from home or from your neighborhood coffee shop. If you have already set up your two-factor methods, they will be ready for your use during your trip. Be sure to test this **before** your trip by attempting to log into your corporate network from home or a public WiFi, such as Starbucks.
>
> **<Include the following line if you are using timed passcodes (TOTPs) from the mobile app**: You can also log in when offline with timed passcodes from the SecureAuth Authenticate mobile app.>
>
> If you have not set up your two-factor methods, see your SecureAuth administrator to do so now. Do not wait until you are on a trip to set up these methods just in case you run into any difficulties.

Copyright Information

©2021 SecureAuth Corporation. All Rights Reserved. The Circle Split-S Design Logo, the Circle with Intersecting S Design Logo, SecureAuth, and SecureAuth Labs are trademarks of SecureAuth Corporation and/or its affiliates, some of which are registered in the US and/or other countries. Other names may be trademarks of their respective owners. SecureAuth® Identity Platform and SecureAuth IdP software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

For information on support, contact your SecureAuth support or sales representative:

Email: support@secureauth.com
inside-sales@secureauth.com

Phone: +1-949-777-6959 or +1-866- 859-1526

Website: https://www.secureauth.com/support
https://www.secureauth.com/contact