Rublon End-User Communication Templates

Table of Contents

1. General Advice for Email Communication

When informing your users about the rollout of Rublon Multi-Factor Authentication (MFA), keep the communication clear, timely, and user-friendly. Here's some general advice:

- **Timing Matters:** Send significant MFA rollout emails mid-week (e.g., Tuesday, Wednesday, or Thursday). These days typically have higher email open rates. Avoid Mondays (when inboxes are full) and Fridays or holidays (when people may be away).
- **Recognizable Sender:** Send the emails from a person or team that users trust. For example, use the IT manager's or Help Desk's name/email instead of a generic no-reply address. A familiar sender increases the likelihood that users will open and read the message.
- **Friendly, Professional Tone:** Write in a welcoming and clear tone. Avoid heavy jargon. Explain technical terms in simple language. Let users know the change is intended to help protect them and the company. Sound helpful and positive, as if you are guiding them, not scaring them.
- **Highlight Key Points and Actions:** Make it easy for users to know what to do. If no immediate action is needed, say that up front. If action is required, call it out clearly (e.g., *"Action Required: Enroll by [DATE]"*). Use bold text or headers for sections like "Action Required" or questions in the email to grab attention.
- **Engage and Educate:** Use the rollout as an opportunity to educate users about security. Include a brief "What is Rublon MFA?" in early communications so users understand the purpose and benefits. Link to resources for those who want to learn more, but keep the email itself concise.
- **Provide Support Channels:** Always reassure users that help is available. Include contact info for your IT help desk or support team in each communication. This way, users know where to go if they have questions or run into issues during enrollment.
- **Plan Multiple Reminders:** Don't rely on a single email. Use a phased approach by sending reminders and updates. Repeating key information across several emails ensures users who missed earlier messages will catch the later ones.

2. Rublon MFA Essentials: Glossary & FAQs

When introducing Rublon MFA to end users, you may encounter some common questions. Below is a glossary of key terms and a list of frequently asked questions to help you communicate clearly with your users. Feel free to include these in your communications or training materials, and adjust as needed for your organization.

Glossary

- **Two-Factor Authentication (2FA):** An extra layer of security beyond just a password. 2FA (a type of MFA) means you verify your identity with two factors: something you know (your password) and something you have (for example, your phone) or something you are (for example, your fingerprint). This way, even if someone knows your password, they cannot log in without the second factor.
- **Multi-Factor Authentication (MFA):** Similar to 2FA, but can involve two or three verification factors. Rublon is an MFA solution. In practice, we often use “MFA” and “2FA” interchangeably when two authentication factors are involved.
- **Rublon Authenticator:** A mobile application you can install on your smartphone or tablet to confirm your identity when you log in. It can receive push notifications for one-tap approval, scan QR codes, and generate one-time passcodes.
- **Push Notification (Rublon Mobile Push):** A secure notification sent to your phone with the Rublon Authenticator app. It asks you to approve or deny a login attempt. By tapping “Approve,” you verify that you are the one trying to log in. Push notifications are fast and convenient, allowing you to log in with a single tap. They also show details like which application is requesting login and from where, so you can spot anything suspicious.
- **One-Time Passcode:** A one-time code used to verify your identity. Passcodes can be generated by the Rublon Authenticator app (even when you have no internet or cell service), generated by a third-party app like Google Authenticator, sent via SMS, or provided by a hardware token (e.g., YubiKey OTP). These are typically 6-digit codes that you enter during login as the second factor. Passcodes are handy backups for when push notifications are not available.

- **Self-Service Portal (the Manage Authenticators view):** A feature that allows you to manage your own authentication devices (if enabled by IT administrators). The Manage Authenticators view allows you to add a new phone, phone number, and security key, remove an old device, and change the device name. This empowers you to manage your 2FA devices without having to contact IT.

- **Enrollment:** The process of setting up Rublon MFA for your account. During enrollment, you will receive a link to register your device (such as your smartphone). Once enrolled, your account will require an additional MFA step when logging in.

- **Rublon Prompt:** The Rublon login interface that you will see when accessing a protected application (if supported by the given application). After entering your username and password, the Rublon Prompt will ask for your second factor (e.g., approve a push or enter a passcode). If self-enrollment is enabled, the prompt will also have the Manage Authenticators option.

Frequently Asked Questions

Q1: Do I need a smartphone to use Rublon MFA?
A: No, you don't need a smartphone, but it is the recommended and easiest way to authenticate. The Rublon Authenticator mobile app makes the MFA process very quick (via push notifications). However, if you don't have a smartphone or prefer not to use one, you can use a regular mobile phone or even a landline. In that case, you would verify logins with a text message code or a phone call. (Your organization's IT team can enable various options, so check which methods are allowed.)

Q2: What is the Rublon Authenticator mobile app?
A: The Rublon Authenticator is a free mobile app you install on your phone (iOS, Android, HarmonyOS). It is used to perform the second step of authentication. The app can receive push notifications for one-tap approval of logins, and it can generate one-time passcodes. You can also use the app to scan the QR code displayed during login. Rublon Authenticator essentially turns your phone into a secure key for login. The app only works with Rublon MFA. It doesn't share your data, and it won't spam you; it simply helps confirm "Yes, it's me logging in".

Q3: What authentication method is recommended with Rublon?
A: If you have a smartphone, we highly recommend using Mobile Push via the Rublon Authenticator app. Approving a push notification in the app is quick, easy, and secure. It's just a tap on your phone, much faster than typing a code. If you don't have a smartphone handy, the next best method is using a text message code/link or phone call. But push notifications provide the smoothest experience for most users. The most secure method is using FIDO security keys, but this requires obtaining a physical key and always keeping it around.

Q4: I stopped receiving push notifications on my phone. What should I do?
A: If push notifications aren't coming through, there are a few things to check:

1. **Internet Connection:** Make sure your phone has an active internet connection (cellular data or Wi-Fi). Push messages need an internet connection to reach your device.

2. **Notification Settings:** Check your phone's notification settings. Ensure that notifications are allowed for Rublon Authenticator.

3. **"Pull to Refresh":** Swipe down (pull) to manually check for any pending authentication requests.

4. **Alternate Method:** If none of the above steps work, you can still authenticate using a passcode. Open the Rublon Authenticator app and use the six-digit code for login, or use another backup method provided by IT. Then later, contact the IT help desk to troubleshoot the push issue further.

Q5: How can I log in if I have no cell signal or Wi-Fi?
A: Use the one-time passcode in the Rublon Authenticator app. It works offline. Check the following article: Will Rublon MFA work if there is no internet access?.

Q6: How do I manage or enroll new devices for Rublon MFA?
A: If the IT team has enabled the self-service feature, you can manage your 2FA devices yourself. Typically, when you see the Rublon Prompt (after entering your password), there is an option called Manage Authenticators. By clicking that, and after verifying with an existing device, you can do things like:

- **Add a new device:** For example, enroll a third-party app like Google Authenticator or a FIDO security key.

- **Set the default device:** If you have multiple devices enrolled, you can choose one as the default for convenience.
- **Reactivate or replace a device:** If you got a new phone, you have to enroll it and then delete the old phone, since it won't be used anymore.
- **Rename or remove a device:** You can label your devices ("Work Phone", or "Personal Phone") and remove any that you no longer use.

For more information and detailed instructions with screenshots, refer to: Rublon User Guide - Manage Authenticators.

If Manage Authenticators is not enabled, you will need to contact the IT help desk to add or change devices. They can send you a new enrollment link or assist with device updates.

Q7: What should I do if I lose my phone (or it's stolen)?
A: Inform the IT help desk immediately if your primary 2FA device (like your smartphone with the Rublon Authenticator app) is lost or stolen. They will help secure your account. The sooner you report a lost device, the better your account can be protected from unauthorized access.

Q8: Can Rublon or the IT department see my password?
A: No. Your password remains private to you. Rublon never receives or stores your password. Rublon's role is only to provide the second-factor verification after you have entered the correct password. Think of it this way: the application first checks your password (without sharing it with Rublon), and if it's correct, then Rublon steps in to ask for the second factor. Rublon confirms "*Yes, this is the trusted device/person*", but it never sees your password at any point.

Q9: Does the Rublon Authenticator app change any settings on my phone?
A: No, the Rublon Authenticator app does not control your phone. It does not change settings or access your data. The app will request a few permissions after installation (like the ability to receive push notifications) and may gather basic device info (like your device OS version or whether you have a screen lock enabled), but this info is just to check compliance with security requirements. Rublon cannot take any actions on your phone; it can only ask you to approve logins. You remain in full control of your device. Any recommendations that Rublon provides are just suggestions, and it's up to you to take action.

3. Rublon MFA Rollout – Phased Email Templates

When deploying Rublon MFA, it's essential to prepare your end users with plenty of notice and clear instructions. The following email templates are designed to guide users through the introduction of Rublon.

Each template includes a suggested timeline for when to send it, an example subject line, and the email body text. **Be sure to replace placeholders (like [DATE])** and adjust any specifics as needed. The tone of these emails should remain helpful and reassuring.

Email #1 – Phase I: Initial Announcement ("Rublon MFA is Coming Soon")

Timeline: Send approximately **30 days before** the Rublon enrollment invitation or go-live date.

Subject: Rublon MFA is coming soon!

Body:

> **Hello everyone,**
>
> As part of our ongoing efforts to **strengthen our security**, we will soon be introducing **Rublon Multi-Factor Authentication (MFA)** into our login process.
>
> ***What is Multi-Factor Authentication (MFA)?***
>
> Multi-Factor Authentication is a fancy term for a simple security process: using at least two ways to prove your identity when you log in. The "two factors" are usually (1) your password, and (2) something else – in our case, typically your phone. This means that in addition to your username and password, you'll use a second step (like approving a push notification on your phone) when logging in to applications.
>
> ***Why are we adding MFA?***
>
> Passwords alone are no longer enough to keep accounts safe. By requiring a second factor that **only you** have, we can greatly improve the security of our systems and better protect your accounts. Even if someone knows your password, they won't be able to access your account without completing the second authentication step.

What is Rublon MFA?

Rublon MFA is a secure multi-factor authentication platform that will manage this two-factor login process for us. It's a cloud-based service trusted by organizations worldwide to protect logins. It adds a quick step to user verification and helps ensure that **only you** can access your account.

Action Required:

None at this time. This is an informational heads-up about the upcoming rollout of Rublon MFA.

Over the next few weeks, we will send more information about how to enroll in Rublon MFA, what steps you will need to take, and when the change will happen. **For now, you do not need to do anything.** This email is just to let you know what's coming and why.

Summary:

Rublon MFA is coming in about a month, and it will make our logins more secure. Soon we'll provide all the instructions you need to get set up. Thank you for your attention to this important update!

Stay tuned for more emails with the next steps, and feel free to reach out to our IT help desk if you have any immediate questions.

Thank you,
IT Security Team

Email #2 – Phase II: Reminder & More Details

Timeline: Send about **15 days** before the enrollment email or go-live date.

Subject: Reminder: Enroll in Rublon MFA starting on ***[DATE]***

Body:

> **Hello everyone,**
>
> This is a reminder that **in about two weeks (on *[DATE]*)**, we will begin enrolling all users in **Rublon Multi-Factor Authentication**. Rublon will become a required part of the login process for our systems to enhance security.
>
> ***What's happening on [DATE]?***
>
> On that date, you will receive an official **Rublon Enrollment Email** in your inbox. That email will have a personalized link for you to set up Rublon MFA on your device. The setup is quick and takes about 2-3 minutes. You'll install the Rublon Authenticator app on your smartphone and link it to your account. Don't worry, detailed instructions will be provided!
>
> ***Why Rublon MFA and why now?***
>
> As mentioned earlier, adding MFA with Rublon will significantly improve our defenses against unauthorized access. Cyber incidents often start with a stolen password, and Rublon helps prevent those incidents by requiring a second form of verification. We chose Rublon because it's user-friendly (one-tap approvals on your phone) and highly secure.
>
> ***Action Required:***
>
> ***Nothing to do just yet.*** This email is just a **heads-up** that the Rublon enrollment is coming on ***[DATE]***. We want everyone to be prepared and not surprised.

What should you expect next?

- On ***[DATE]***: Look out for an email from **Rublon** with the subject “Enroll your authenticator.” It will contain your enrollment link.

- **Enrollment process:** The enrollment email will guide you to install the Rublon Authenticator app on your mobile device. It’s straightforward, and we’ll provide step-by-step guidance.

We’ll send one more reminder. For now, mark your calendar for ***[DATE]*** to complete your Rublon MFA setup that day. If you have any questions about what’s coming, please contact **IT support** at **[help desk contact info]**. We’re here to help make this a smooth transition.

Thank you,
IT Security Team

Email #3 – Phase III: Final Enrollment Reminder

Timeline: Send about **3 days before** the enrollment/go-live date.

Subject: Final Reminder: Rublon MFA is launching on ***[DATE]*** (What you need to know)

Body:

Hello everyone,

Only a few days left until we roll out **Rublon Multi-Factor Authentication** on ***[DATE]***. This email is the final reminder and includes important information to help you be ready.

What to expect on [DATE]:

- On ***[DATE]***: Look out for an email from **Rublon** with the subject "Enroll your authenticator." It will contain your enrollment link.
- **Enrollment process:** The enrollment email will guide you to install the Rublon Authenticator app on your mobile device. It's straightforward, and we'll provide step-by-step guidance.
- If you **do not have a smartphone**, don't worry. The enrollment will allow you to register a regular mobile or landline phone number (to verify your identity by SMS or phone call). Rublon supports multiple methods, and the Rublon Authenticator app is not a hard requirement.

Action Required:

Not today, but **on *[DATE]*, you will need to complete your Rublon MFA enrollment**. We suggest planning a couple of minutes that day to get set up. It's simple, and we will send the instructions.

What are the benefits of Rublon MFA?

- **Convenience:** If you have a smartphone, you'll be able to just tap "Approve" on a notification (called a **push notification**) to finish logging in.
- **Security:** Rublon's two-factor authentication means even if a password leaks, your account remains secure. It greatly reduces the risk of breaches.

How will my login change with Rublon MFA?

Starting ***[DATE]***, when you log in to protected apps, you will:

1. Enter your username and password as usual.
2. **Then** you'll be prompted by Rublon MFA for a second authentication step. For example, a push notification will pop up on your phone for approval, or you'll be asked to enter a one-time code from your app/phone.
3. Once you approve the push or enter the code, you'll gain access as normal.

Your normal password **still works** and doesn't change; Rublon just adds one more quick step to the login sequence. Think of Rublon as an extra lock that only you can open (because you have the key on your phone).

Questions or need help?

Our team is ready to support you. If you're unsure about anything or face issues during enrollment, reach out to the **Help Desk:**

- Help Desk Phone: 123-456-7890
- Help Desk Email: support@yourcompany.com

We appreciate your cooperation as we make this security improvement. Thank you for helping to keep our organization safe!

Thank you,
IT Security Team

Email #4 – Phase IV: Day-of-Enrollment – Action Required

Timeline: Send **on the day Rublon MFA enrollment begins** (go-live day), ideally in the morning just before or as the enrollment emails are being sent out.

Subject: **Action Required:** Enroll in Rublon MFA today

Body:

> **Hello everyone,**
>
> **Today is the day!** We have officially started the rollout of **Rublon Multi-Factor Authentication**. You should receive an **Enrollment Email from Rublon** with the subject "**Enroll your authenticator**" in your inbox. Please locate that email and follow the instructions to enroll **today**.
>
> ***What do I need to do right now?***
>
> 1. **Find the enrollment email** titled "Enroll your authenticator" (it will be sent to your company email).
> 2. Open the email and select **Enroll Your Authenticator**. It will take you to Rublon's setup page for your account.
> 3. **Set up your device.** The page will guide you through the Rublon Authenticator enrollment process. For detailed instructions, refer to: How to enroll a mobile device with Rublon Authenticator?. If you wish to enroll a different device, refer to: Rublon User Guide - Enrollment.
> 4. Once done, you'll have Rublon MFA enabled on your account! Going forward, logins to our protected systems will require a second authentication step.
>
> ***If you don't have the Enrollment Email:***
>
> Check your spam folder just in case, or contact IT for assistance. The Enrollment Email is unique to you, so do not use someone else's.
>
> ***If you do not have a smartphone:***

The enrollment process will let you choose an alternative option (like registering your phone number for text/call verification). Follow the on-screen instructions, check the step-by-step instructions at Rublon User Guide - Enrollment, or reach out to IT if you need help with a non-smartphone setup.

Deadline:

Please complete your Rublon enrollment by ***[DATE]***. After that date, access to applications will **require** Rublon MFA, and you will not be able to log in until you have enrolled in Rublon. We've given a grace period of a few days to get everyone on board, but it's best to do it **immediately**.

Why is this important?

Enrolling in Rublon MFA protects your account and our organization. It only takes a couple of minutes, and it will significantly boost our security. After ***[DATE]***, anyone not enrolled will be unable to access our applications until they complete enrollment, so **to avoid any work interruption, please enroll as soon as possible**.

Need help?

If you have any trouble with the enrollment process or have questions, contact the **Help Desk** immediately. We have support staff on standby today to assist with Rublon MFA setup issues.

- **Help Desk Phone:** 123-456-7890
- **Help Desk Email:** support@yourcompany.com

Thank you for your prompt attention to this. By taking this step, you're helping secure our company's data and your own accounts.

Thank you,
IT Security Team

4. Rublon Policy Change – Email Templates

In addition to initial rollout communications, you may later need to inform your users about **changes in the Rublon Policy or specific connector settings. Be sure to replace placeholders (like *[DATE]*)** and adjust any specifics as needed. Feel free to remove parts of messages if necessary (e.g., if you only changed the Remembered Devices Policy, you can delete information on other policies). The tone of all these emails should remain helpful and reassuring.

Email #1 – Rublon Policy Will Be Changed Announcement

Timeline: Send approximately **7 days** before the new Rublon policies take effect.

Subject: Important Update: Upcoming Changes to Rublon Security Policies

Body:

> **Hello everyone,**
>
> As part of our continued efforts to maintain the highest level of security, we will update our Rublon Multi-Factor Authentication security policies **on *[DATE]***. Please review the details below:
>
> ***Who Will Be Affected?***
>
> These changes will impact how Multi-Factor Authentication is handled, and they will apply **[globally/on selected applications/for specific user groups]**.
>
> ***What's Changing?***
>
> **1. Remembered Devices Policy:**
>
> - **What is it?** The Remembered Devices Policy determines whether and for how long users can add their devices as trusted to reduce the frequency of MFA prompts.
> - **Change Details:**
>   - The duration for remembering your device will be **[increased/decreased]** to **[value in hours/days]**.

- The Remembered Devices Policy will be **[enabled/disabled]**.

- **What This Means for You:**
  - If the policy is changed, your devices will be remembered for a **[longer/shorter]** duration.
  - If the policy is enabled, once you mark a device as trusted, you will not be prompted for MFA as often.
  - If the policy is disabled, you will be asked to verify your identity each time you log in.

2. Authentication Methods Policy:

- **What is it?** The Authentication Methods policy governs the available methods for multi-factor authentication, including the Default Authentication Method used at login.
- **Change Details:**
  - The **[authentication method name]** will be **[activated/deactivated]**.
  - The Default Authentication Method will be set to **[authentication method name]**.
- **What This Means for You:**
  - If you use the deactivated authentication method, switch to an alternative method now to avoid hiccups later. Here's how you can enroll an alternative MFA option.
  - If an authentication method is set to default, you will be prompted to authenticate with this method without having to choose it from the Rublon Prompt. If you prefer to use a different method or enroll additional authenticators, select "Back" and then select "Manage Authenticators."

3. Authorized Networks Policy:

- **What is it?** The Authorized Networks Policy defines specific IP ranges that are considered secure and bypasses (skips) MFA for users with those IPs.
- **Change Details:**
    - Users from Authorized Networks will be bypassed (MFA will be skipped).
    - Authorized Networks will be disabled, so all networks will require MFA unless another policy is in place.
- **What This Means for You:**
    - If you log in from an authorized IP address, you will experience a simplified authentication process without MFA. However, if you are outside the authorized IP ranges or the Authorized Networks Policy has been disabled, standard MFA procedures will apply.

If you have any questions or need assistance, please contact our IT Help Desk at **[Help Desk Contact Info]**.

Thank you for your attention to this important update.

Thank you,
IT Security Team

Email #2 – Day-of-Change Policy Change Announcement

Timeline: Send on the day the changes to the Rublon policies take effect.

Subject: Rublon Security Policies Updated – Here's What's Changed

Body:

Hello everyone,

As of today, our Rublon Multi-Factor Authentication security policies have been updated. These changes are now in effect and will impact how you log in to applications.

Who Is Affected?

These policy changes apply **[globally/on selected applications/for specific user groups]**. If you are part of an affected group, your login experience may be slightly different starting today.

What's Changed?

1. **Remembered Devices Policy:**

- **What's New:**
    - The Remembered Devices feature has been **[enabled/disabled]**.
    - The time devices are remembered has been set to **[value in hours/days]**.

- **What This Means for You:**
    - If the policy is changed, your devices will be remembered for a **[longer/shorter]** duration.
    - If the policy is enabled, you can now remember your device to reduce the number of MFA prompts.
    - If the policy is disabled, you will be prompted for MFA every time you log in, regardless of device.

2. Authentication Methods Policy:

- **What's New:**
    - The **[authentication method name]** authentication method has been **[activated/deactivated]**.
    - The Default Authentication Method is now set to **[authentication method name]**.

- **What This Means for You:**
    - If you were previously using a method that has now been deactivated, you must switch to another supported option. Here's how.
    - With the Default Authentication Method enabled, you will be automatically prompted to authenticate using **[authentication method name]**. If you want to use a different method or enroll a new device, click "Back" at the Rublon Prompt and then select "Manage Authenticators."

3. Authorized Networks Policy:

- **What's New:**
    - MFA will now be bypassed (skipped) for users accessing from specific IP addresses.
- **What This Means for You:**
    - Your login will no longer require a second authentication step if your IP address is within the authorized range.
    - If the policy is disabled, all users will now be prompted for MFA regardless of their IP address.

Need Help?

If you have any questions about these changes or need help switching your authentication method or managing your authenticators, please contact our IT Help Desk:

- **Phone:** 123-456-7890
- **Email:** support@yourcompany.com

Thank you for your attention and cooperation as we continue improving our security practices.

Thank you,
IT Security Team

5. Rublon MFA Outage – Email Templates

For email templates related to Rublon MFA outages and service disruptions, refer to the Rublon Business Continuity Preparedness Guide.

Rublon sp. z o.o.
ul. Stanisława Wyspiańskiego 11
65-036 Zielona Góra

www.rublon.com