Multi-Factor Authentication – Supplier Portal

May 2023

Multi-Factor Authentication (MFA) for Suppliers

What is MFA?

- MFA is a two-step verification process where users are required to authenticate themselves a second time using a time-based verification code.

Who can enable MFA?

- Only the supplier account administrator can enable MFA for their account and their sub-user accounts.

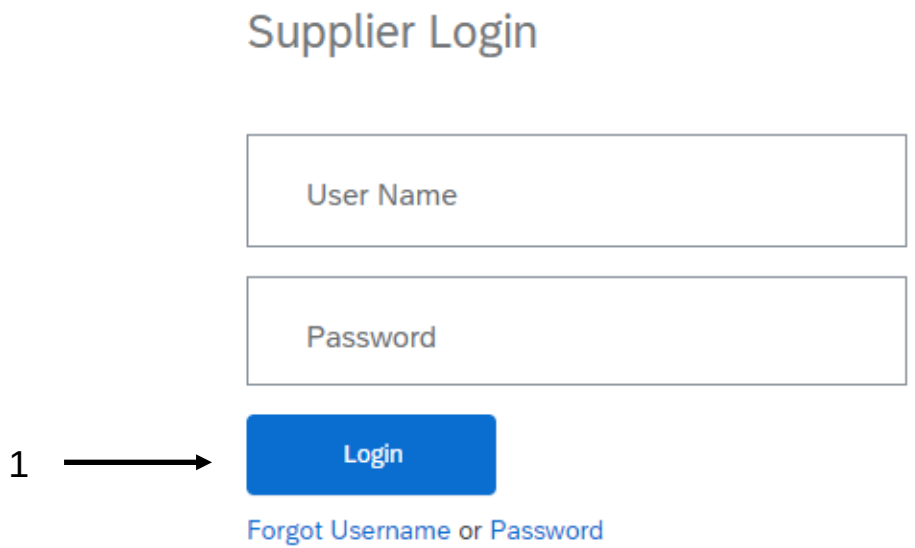
What available options are there for enabling MFA?

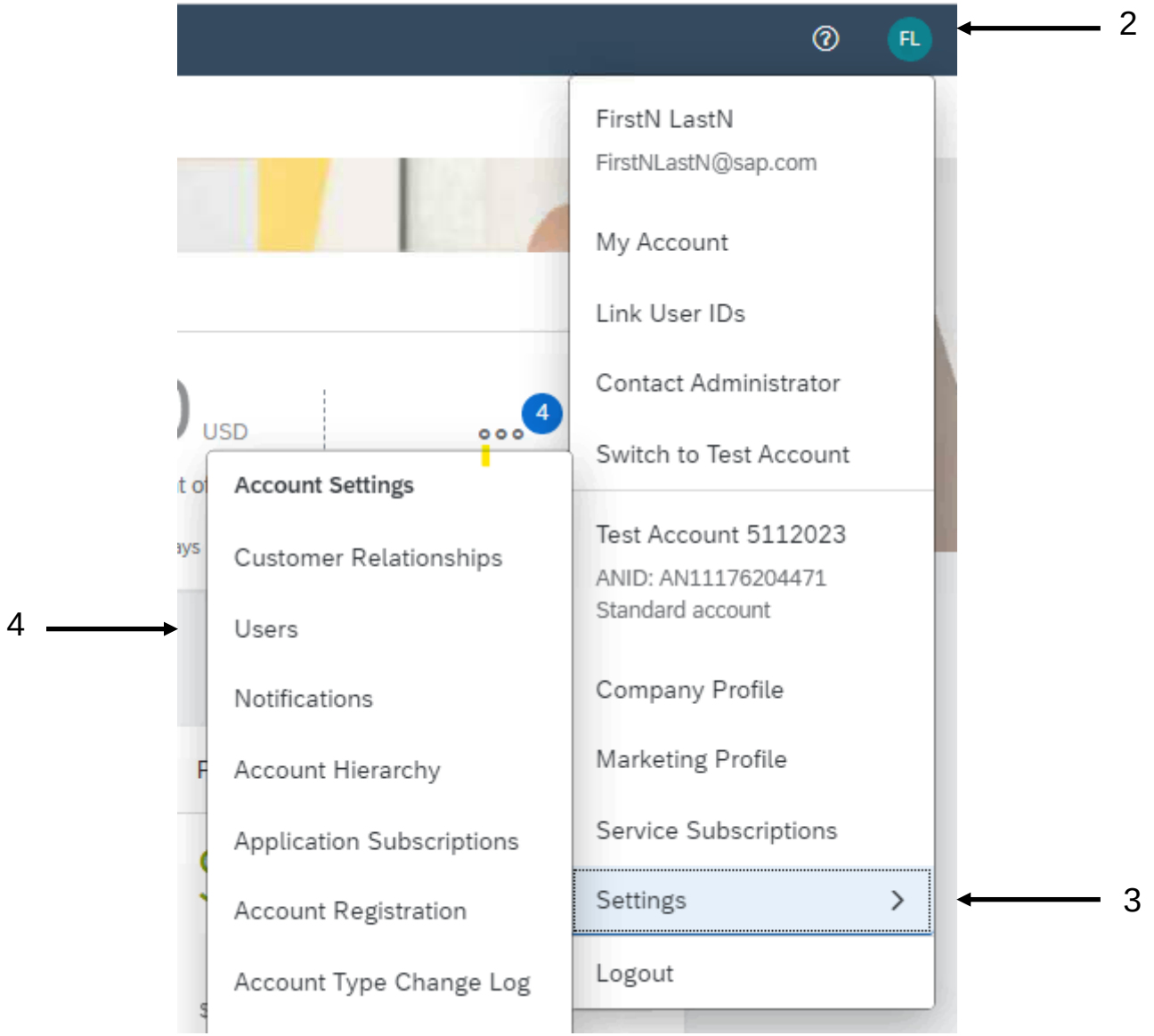
- **Require multifactor authentication for critical fields** – Users are required to enter a 6-digit verification code when updating critical fields in the supplier account. This includes changes made to a users ‘My Account’ section and the ‘EFT/Check Remittances’ section.

- **Require multifactor authentication for login** – Users are required to follow a two step verification process when logging into their account. First the account password and then the SAP Authenticator 6-digit code.

How to setup MFA:

1. Login to the supplier account as the admin at http://supplier.ariba.com.
2. Click on **Account Settings** (initials) in the top right.
3. Next, click on **Settings.**
4. Then, click on **Users**.

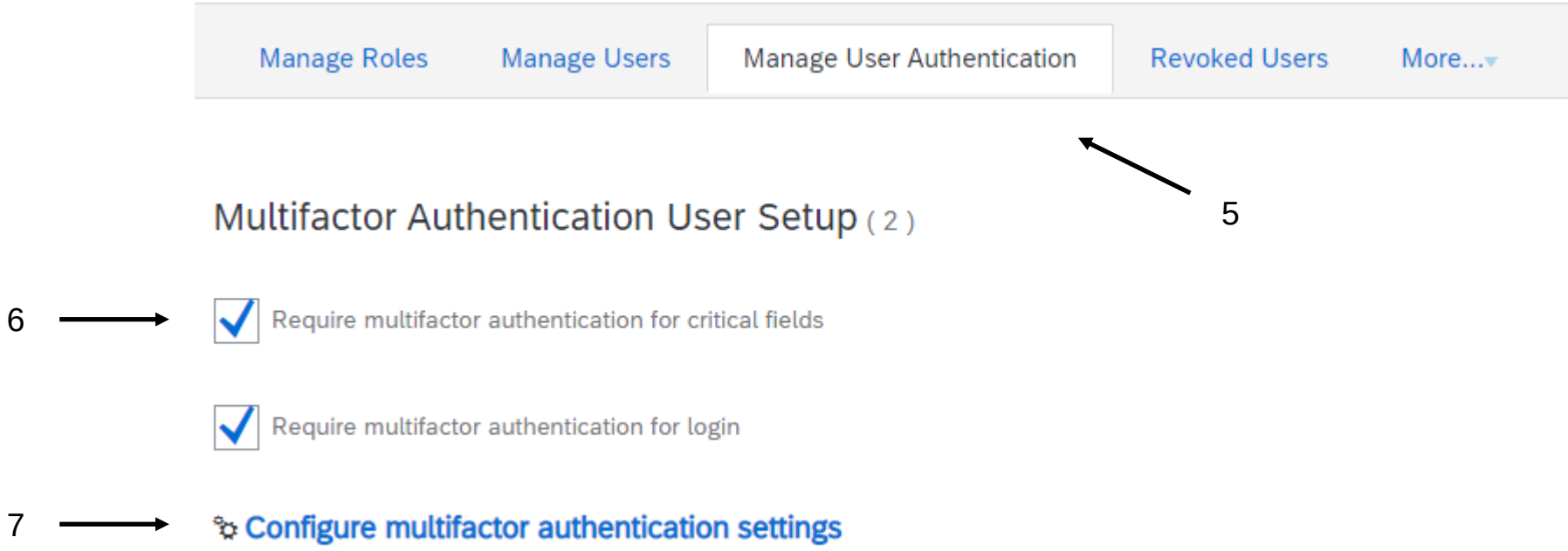




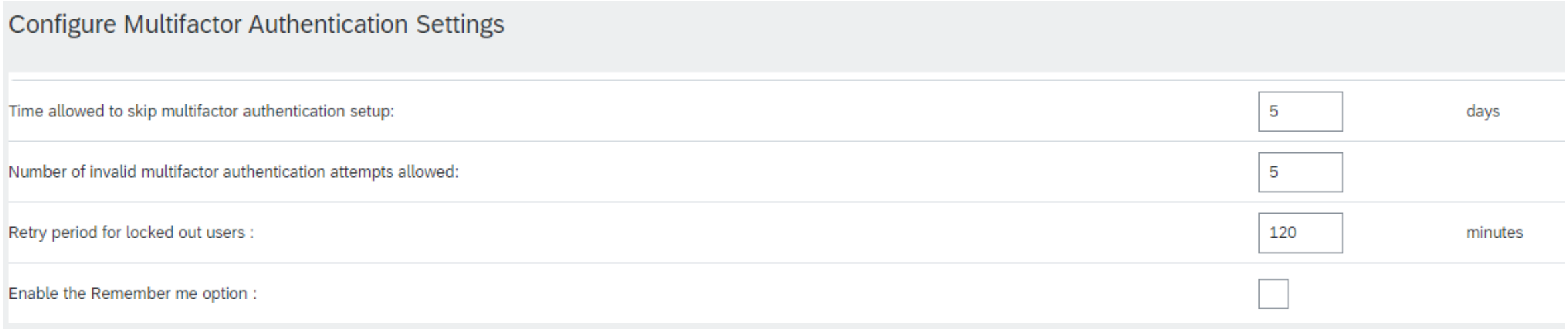
5. Click on the **Manage User Authentication** tab.

6. Select **Require multifactor authentication for critical fields** and/or **Require multifactor authentication for login.**
   - Both options can be selected at the same time.

7. Click on the **Configure multifactor authentication settings** link.



8. Configure the following four settings.



Time allowed to skip MFA setup – Specifies the maximum number of days a user can skip the MFA setup when an admin had enabled it for that user. The default value is 5 days.

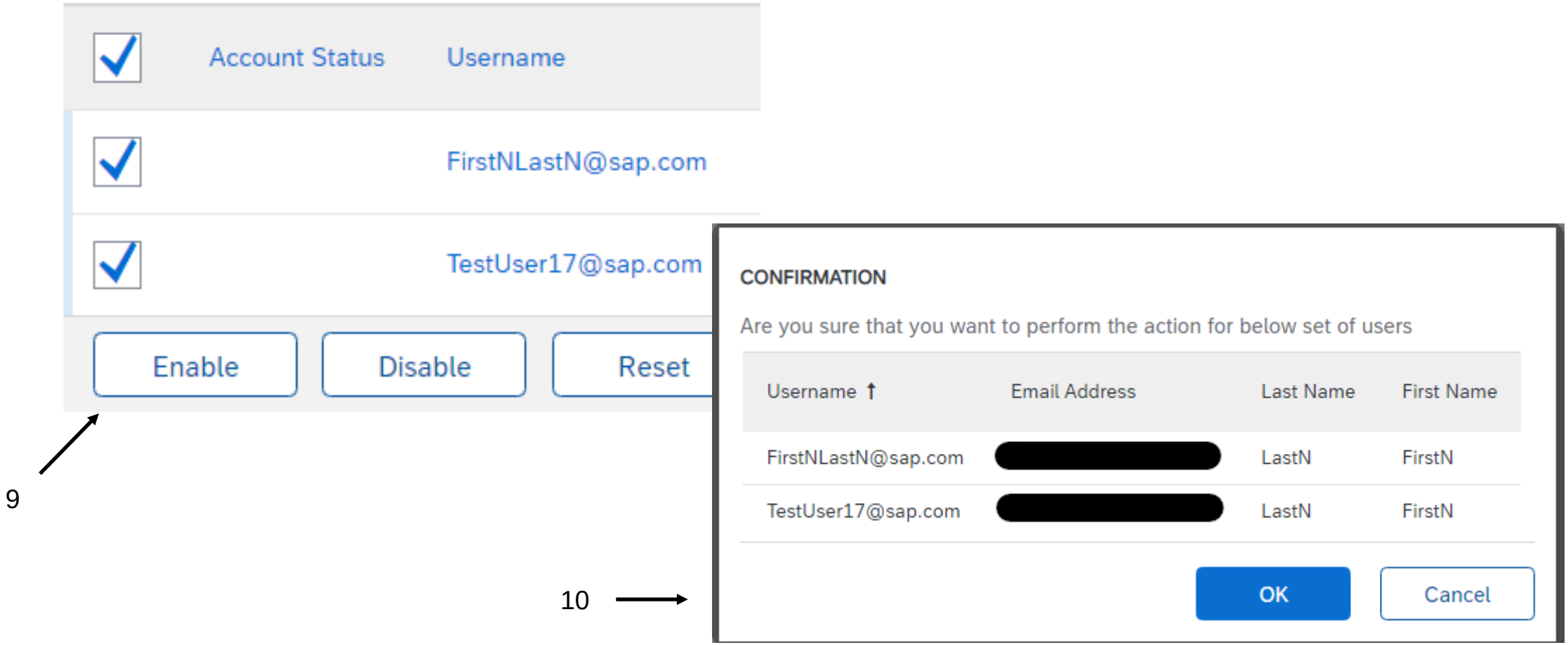
Number of invalid MFA attempts allowed – Specifies the maximum number of invalid MFA attempts a user can make. The default value is 5 attempts.

Retry period for locked out users – Specifies the time period, in minutes, that a user is locked out of their account after reaching the maximum invalid login attempts. Default value is 120 minutes.

Enable the Remember me option – This setting is not enabled by default. This checkbox specifies if users can choose the Remember me option for MFA in the one-time password input screen. If enabled, a 'Remember device for' field appears. The default value is 5 days. There is not a limit on the amount of days that can be entered.

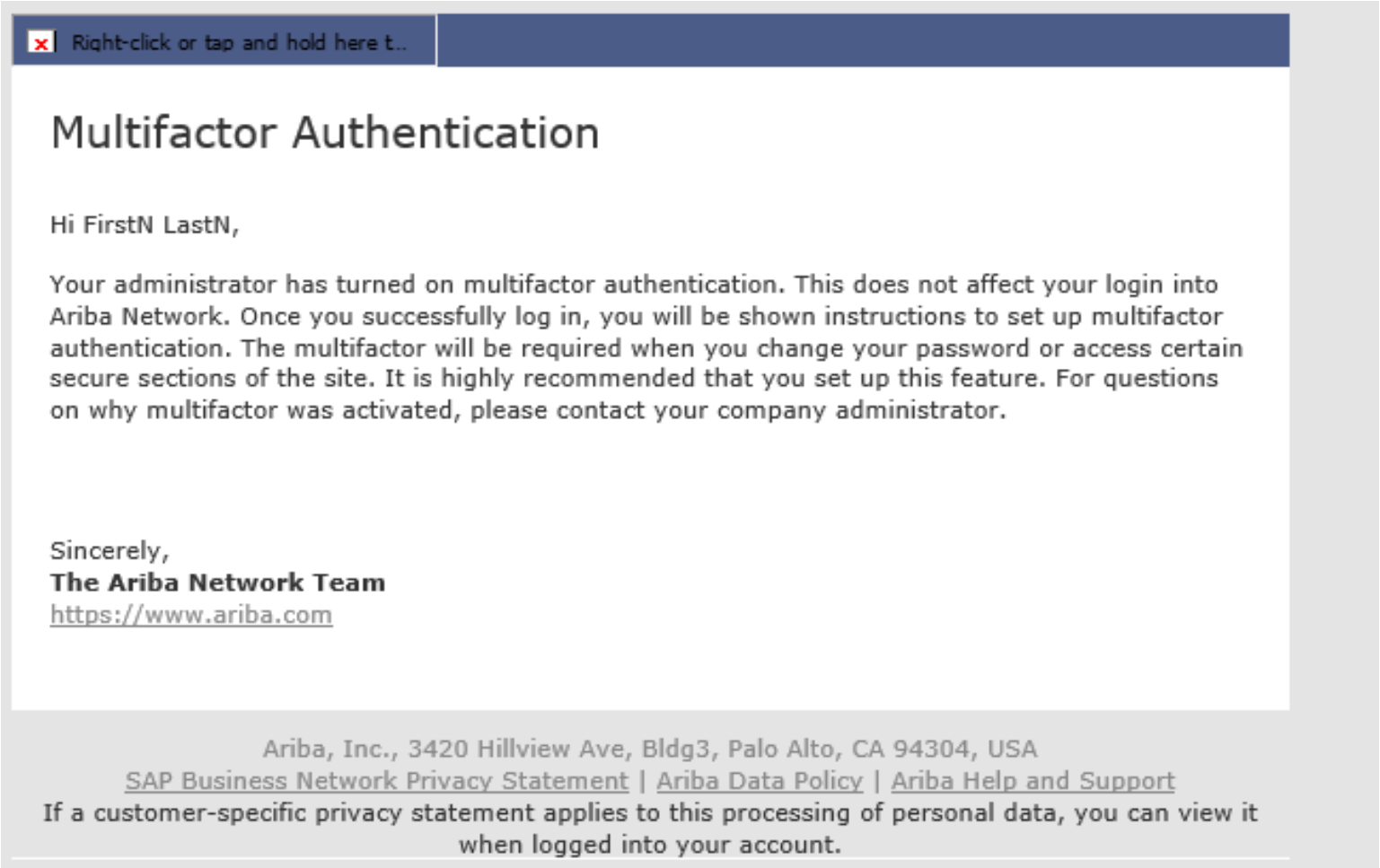
9. Then, check the user/users and click the **Enable** button. Multiple users can be selected at once.

10. Click the **Ok** button on the popup window requiring confirmation before enabling MFA for the selected user/users.

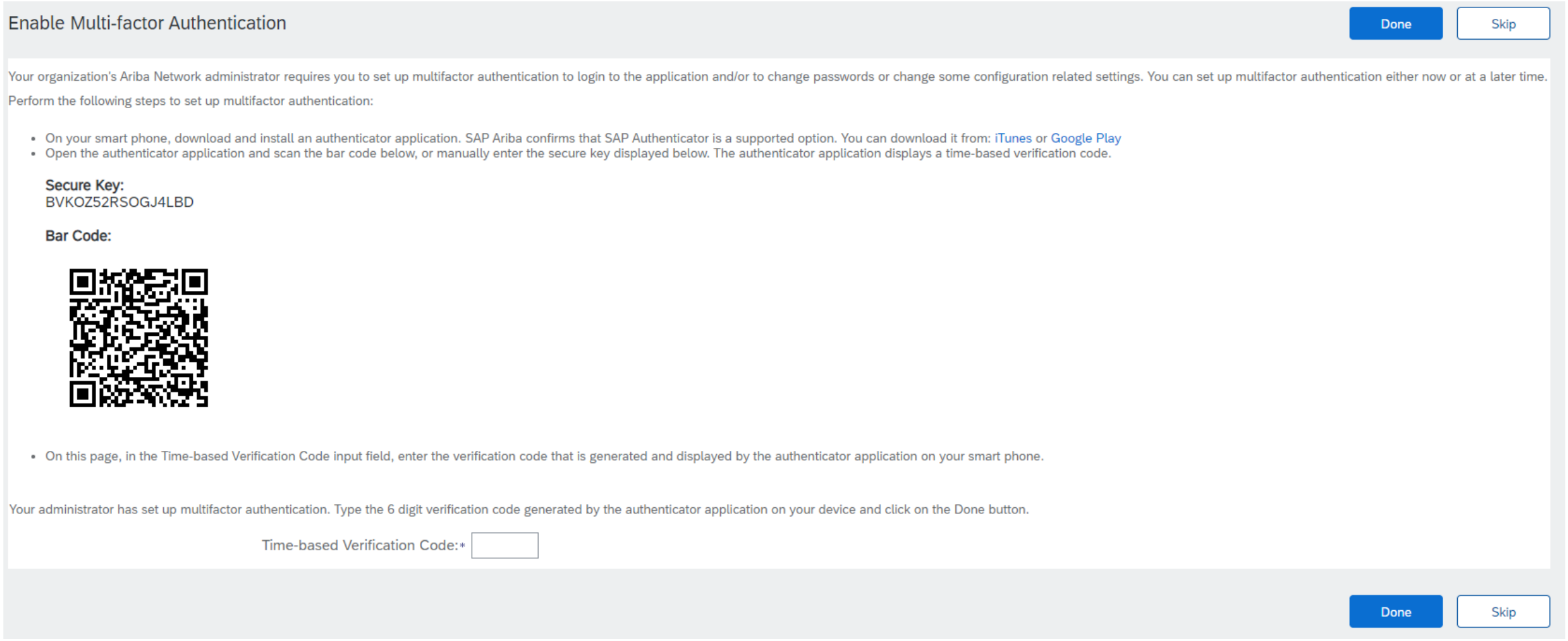


User Enablement Notification

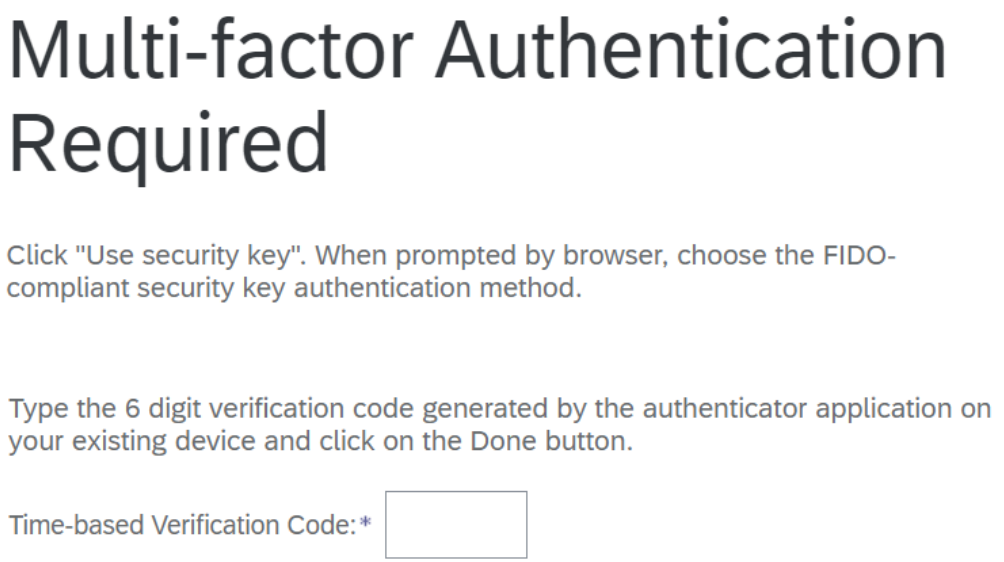
Note - After MFA is enabled for the user, they will receive the below notification from **ordersender-prod@ansmtp.ariba.com.**



11. The next time the user tries to login, they will receive the below message asking them to download **SAP Authenticator** (from iTunes or Google Play) to receive a 6-digit verification code to access their account. After entering the code, the user needs to click the **Done** button to finish MFA configuration.



12. After configuration is complete, the user will receive the below screen requiring a 6-digit verification code from SAP Authenticator during future login attempts.



Note – Users will still be required to enter a 6-digit verification code after changing their account password through a password reset email.

Multi-Factor Authentication FAQs

Is MFA available for both Enterprise and Standard accounts?

- Yes, MFA is available for both account types.

Is there a fee associated with configuring MFA?

- No, MFA is free for suppliers.

If a user changes their password after requesting a password reset email, will they still be required to enter the 6-digit verification code if MFA is enabled on their account?

- Yes, a password reset does not reset the MFA settings for a user account. They will still need to enter a 6-digit verification code after entering their username and password.

Can users update the MFA settings?

- No, only the account admin can make edits to the MFA settings.

If a user is locked out of their account because of failed MFA attempts, can the admin unlock their account?

- Yes, the admin can select the user in the Manage User Authentication section of their account and click the Unlock button. Then, the user will not need to wait the specified amount of time configured in the MFA settings.

Can the admin reset MFA for a user requiring them to go through the configuration process again?

- Yes, the admin can do this by selecting the user and clicking the Reset button in the User Authentication section of their account.

Multi-Factor Authentication FAQs

Can MFA for critical fields be configured to access the SLP Registration Questionnaire?

- No, MFA can not be configured to access the SLP Registration Questionnaire. MFA can be configured to access the account that houses the questionnaire.

Can MFA for critical fields be configured to access sourcing events?

- No, MFA can not be configured to access a sourcing event. MFA can be configured to access the account that houses the sourcing event.

Where can suppliers learn more about MFA?

- How to enable Multi-Factor Authentication on the SAP Business Network (Knowledge Article)
- Multi-Factor Authentication (SAP Help Portal)

Where can suppliers go if they need assistance configuring MFA?

- Suppliers can contact SAP Business Network Customer Support here.

Thank you.