



# Multi-Factor Authentication – Supplier Portal

May 2023

Public – SAP, Partners, and Customers Only

# 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**.

Supplier Login

User Name

Password

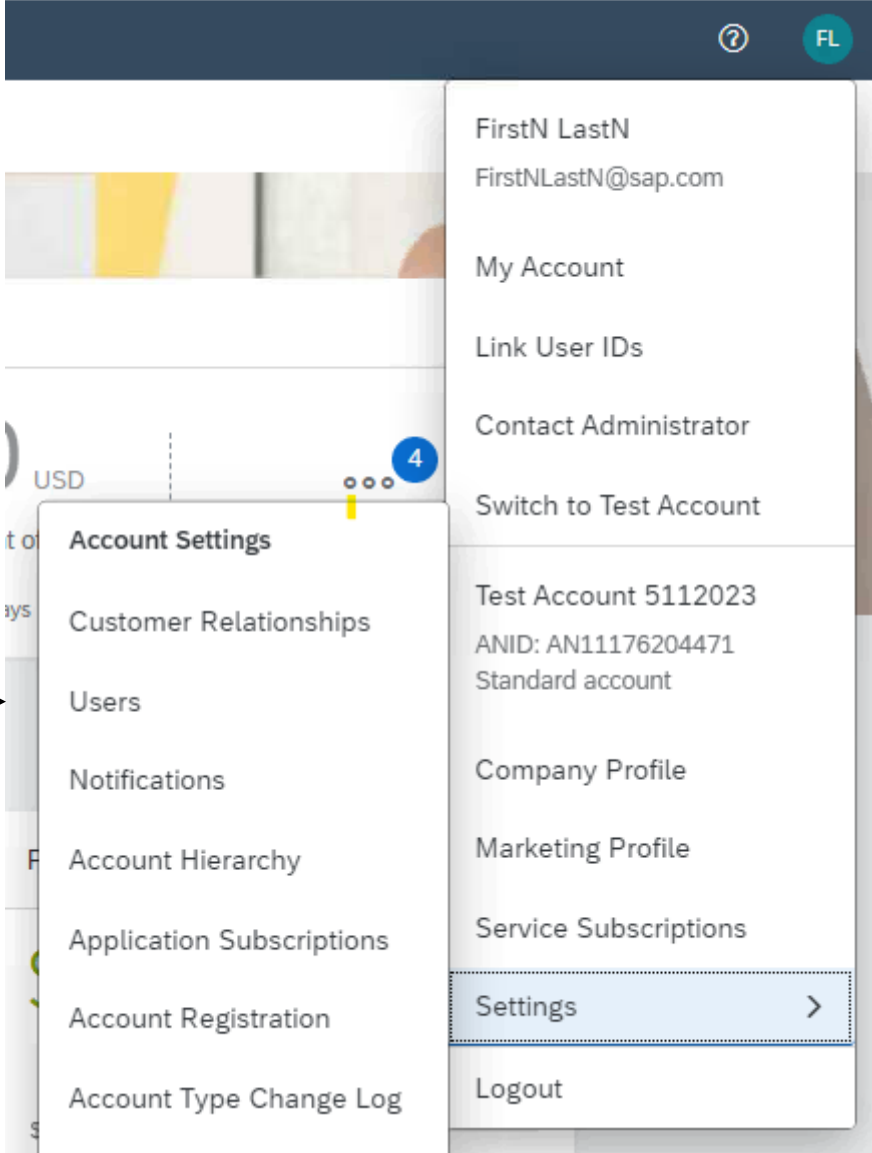
1 →

[Forgot Username](#) or [Password](#)

2 →

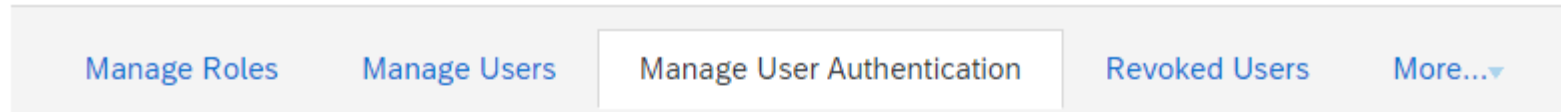
4 →

3 →



The screenshot shows the Ariba Supplier Account Settings menu. The menu is open, displaying a list of options. The 'Settings' option is highlighted with a blue background and a right-pointing arrow. The 'Users' option is also visible in the list. The menu is titled 'FirstN LastN' and 'FirstNLastN@sap.com'. Other options include 'My Account', 'Link User IDs', 'Contact Administrator', 'Switch to Test Account', 'Test Account 5112023', 'ANID: AN11176204471', 'Standard account', 'Company Profile', 'Marketing Profile', 'Service Subscriptions', and 'Logout'. A blue circle with the number '4' is visible in the top right corner of the menu.

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.



### Multifactor Authentication User Setup ( 2 )

6 → ☒ Require multifactor authentication for critical fields

☒ Require multifactor authentication for login

7 →  [Configure multifactor authentication settings](#)

8. Configure the following four settings.

| Configure Multifactor Authentication Settings                  |                                  |         |
|----------------------------------------------------------------|----------------------------------|---------|
| Time allowed to skip multifactor authentication setup:         | <input type="text" value="5"/>   | days    |
| Number of invalid multifactor authentication attempts allowed: | <input type="text" value="5"/>   |         |
| Retry period for locked out users :                            | <input type="text" value="120"/> | minutes |
| Enable the Remember me option :                                | <input type="checkbox"/>         |         |

**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.

The screenshot shows a user management interface. At the top, there is a header row with a checkbox, 'Account Status', and 'Username'. Below this, there are two rows of users, each with a checked checkbox and an email address: 'FirstNLastN@sap.com' and 'TestUser17@sap.com'. At the bottom of the list, there are three buttons: 'Enable', 'Disable', and 'Reset'. An arrow labeled '9' points to the 'Enable' button.

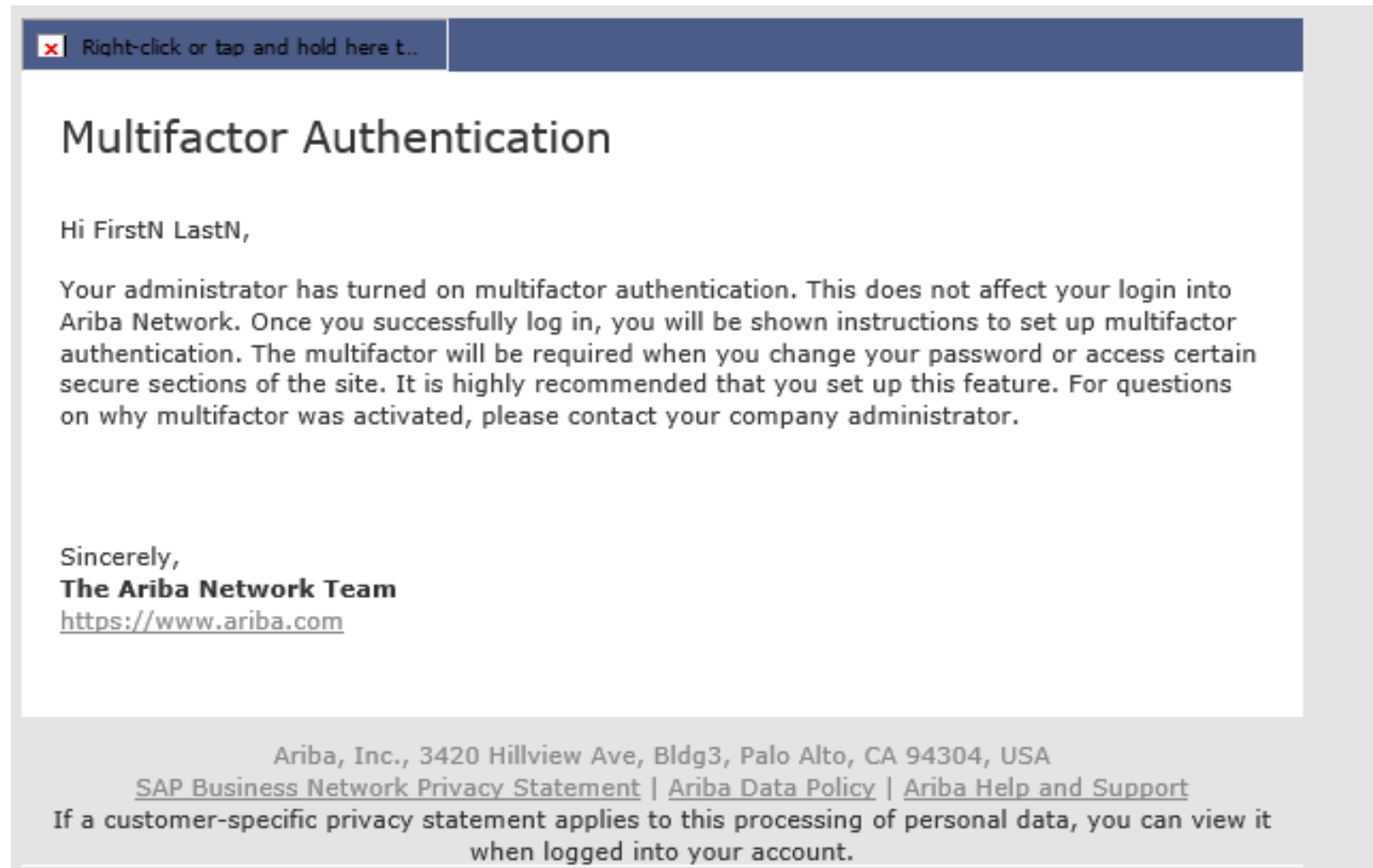
A confirmation dialog box is overlaid on the right side. It has a title 'CONFIRMATION' and a message 'Are you sure that you want to perform the action for below set of users'. Below the message is a table with the following data:

| Username ↑          | Email Address | Last Name | First Name |
|---------------------|---------------|-----------|------------|
| FirstNLastN@sap.com | [REDACTED]    | LastN     | FirstN     |
| TestUser17@sap.com  | [REDACTED]    | LastN     | FirstN     |

At the bottom right of the dialog box, there are two buttons: 'OK' and 'Cancel'. An arrow labeled '10' points to the 'OK' button.

## 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.

Enable Multi-factor Authentication

DoneSkip

Your organization's Ariba Network administrator requires you to set up multifactor authentication to login to the application and/or to change passwords or change some configuration related settings. You can set up multifactor authentication either now or at a later time. Perform the following steps to set up multifactor authentication:

- On your smart phone, download and install an authenticator application. SAP Ariba confirms that SAP Authenticator is a supported option. You can download it from: [iTunes](#) or [Google Play](#)
- Open the authenticator application and scan the bar code below, or manually enter the secure key displayed below. The authenticator application displays a time-based verification code.

**Secure Key:**  
BVKOZ52RSOGJ4LBD

**Bar Code:**



• On this page, in the Time-based Verification Code input field, enter the verification code that is generated and displayed by the authenticator application on your smart phone.

Your administrator has set up multifactor authentication. Type the 6 digit verification code generated by the authenticator application on your device and click on the Done button.

Time-based Verification Code:\*

DoneSkip



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.

## Multi-factor Authentication Required

Click "Use security key". When prompted by browser, choose the FIDO-compliant security key authentication method.

Type the 6 digit verification code generated by the authenticator application on your existing device and click on the Done button.

Time-based Verification Code: \*

**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.

