Feature at a Glance

Multi-factor authentication for user login to Ariba Network

Rajesh Shastry, SAP Ariba

Target GA: February, 2021

CONFIDENTIAL

Ease of implementation ● High-Touch

Geographic relevance ● Global

Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Customer challenge

Currently, Ariba Network does not support multi-factor authentication for login, which makes basic login vulnerable.

Meet that challenge with SAP Ariba

Support **Multi-factor Authentication (MFA)** for basic login.

Experience key benefits

- Secure access to the Ariba Network
- Mitigate the risk of a nefarious entity gaining access to the SAP Ariba applications using compromised user account credentials

Solution area

Ariba Network

Implementation information

This feature is automatically on for all customers with the applicable solutions but requires **customer configuration.**

Prerequisites and Limitations

When multi-factor authentication is enabled for an organization, enabled users should install SAP authenticator apps from the App Store or Google Play Store to generate Time-based One-time Passcode (TOTP).

Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – Brief description

Once MFA feature is enabled:

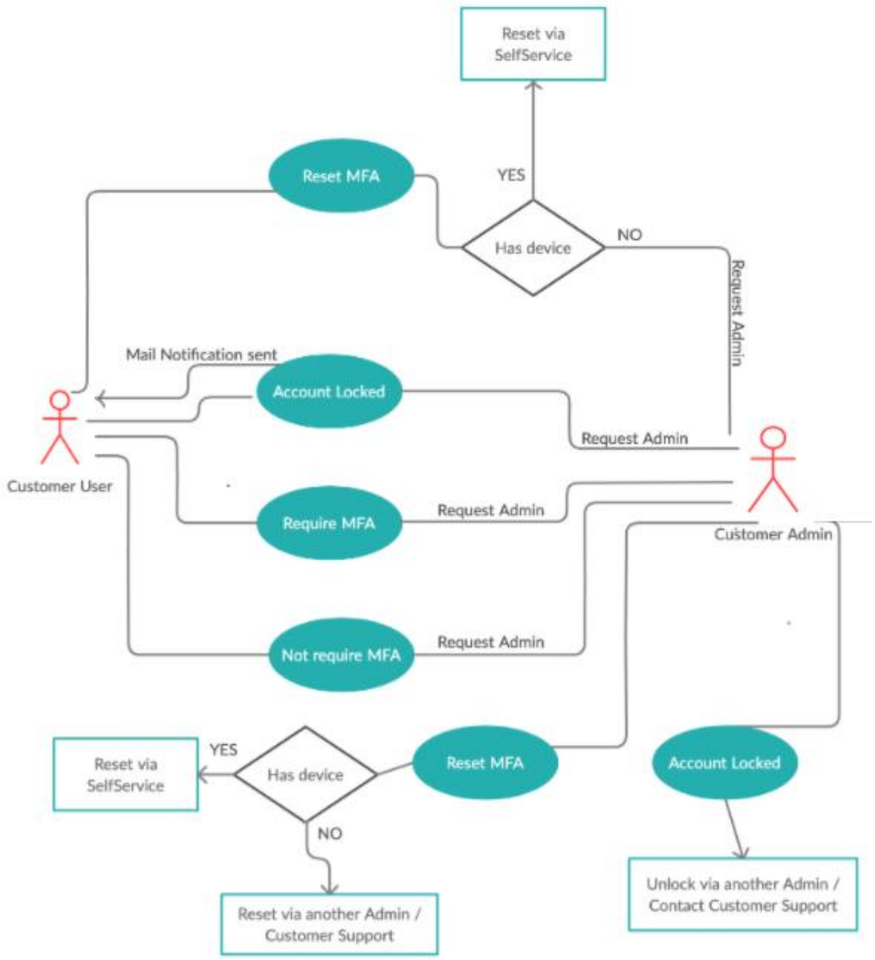
- Customer admins can maintain MFA configurations and enable MFA for the Users
- Users set up MFA by installing SAP authenticator app from the App Store and Google Play Store
- Next time users login, along with Username/Password, they will be required to enter MFA token to gain access to applications

Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – User login: Process Flow

- Persona: User (Application Users)
- Login Flow:
  1. **Input** the User ID and password
  2. **Install** SAP Authenticator app from the App Store and Google Play Store
  3. **Scan** the QR Code to get the passcode
  4. **Enter** the passcode into the MFA login screen within the period to expiration
  5. **Login** successfully, If the generated passcode has been input within the period to expiration
  6. **Attempt** to login again, if login failed – by default
     - **To be locked** with first 5 unsuccessful attempts for 120mins
     - **To be locked** with second 5 unsuccessful attempts for 2*120mins
     - **To be locked** with third 5 unsuccessful attempts
     - **Get unlocked or Reset** MFA by sending request to Admin



Feature at a Glance

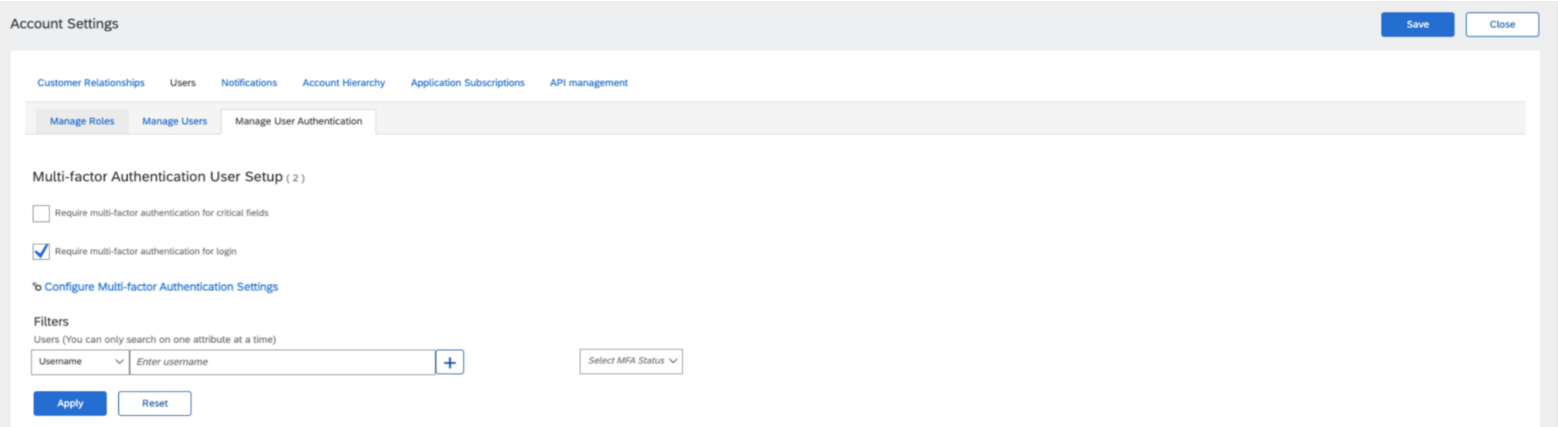
Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – Enable MFA for Login and Configure MFA Settings

The Admin navigates to **Users → Manage User Authentication**

The admin can enable MFA for login by selecting the Checkbox and configure the necessary MFA settings in the tenant:

- Time allowed to skip multi-factor authentication setup (Default Value: 5 Days)
- Number of invalid multi-factor authentication attempts allowed (Default Value: 5 attempts)
- Retry period for locked out users (Default Value: 120 mins)
- Enable the Remember me option (Default Value: No)
- Remember device for (Default Value: 5 Days) Applicable only if Remember me option is set to Yes



Multi-factor Authentication User Setup (2)

□ Require multi-factor authentication for critical fields

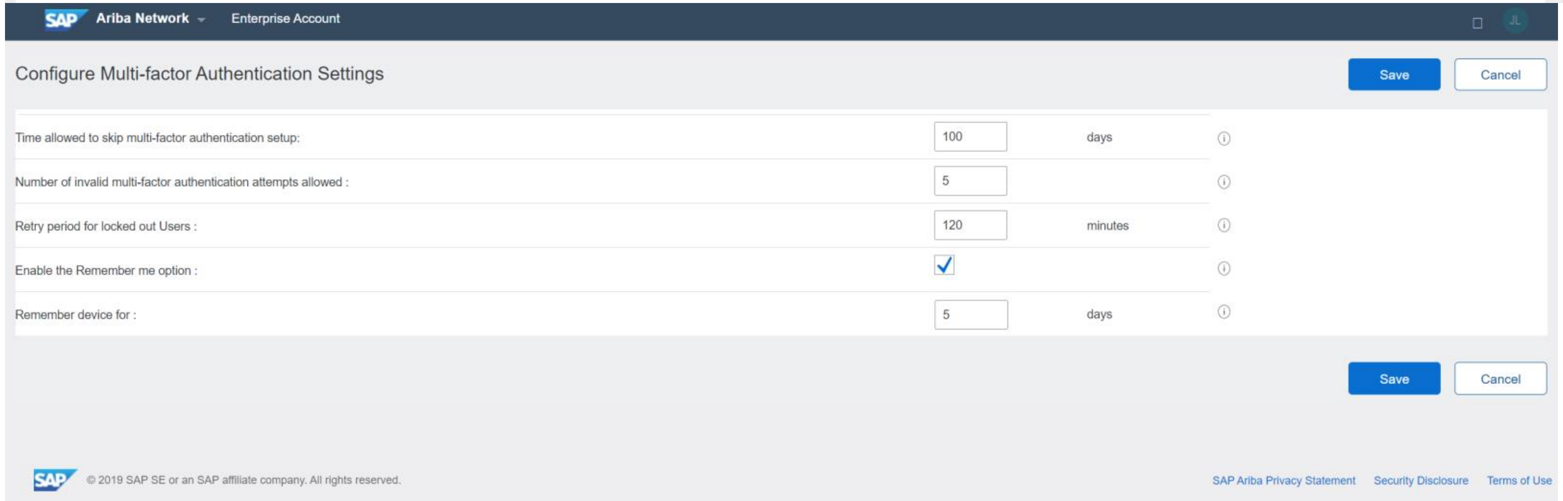
☑ Require multi-factor authentication for login

Configure Multi-factor Authentication Settings

Filters

Users (You can only search on one attribute at a time)

Username | Enter username | Select MFA Status



Configure Multi-factor Authentication Settings

Time allowed to skip multi-factor authentication setup:	100	days
Number of invalid multi-factor authentication attempts allowed :	5	
Retry period for locked out Users :	120	minutes
Enable the Remember me option :	☑	
Remember device for :	5	days

Feature at a Glance

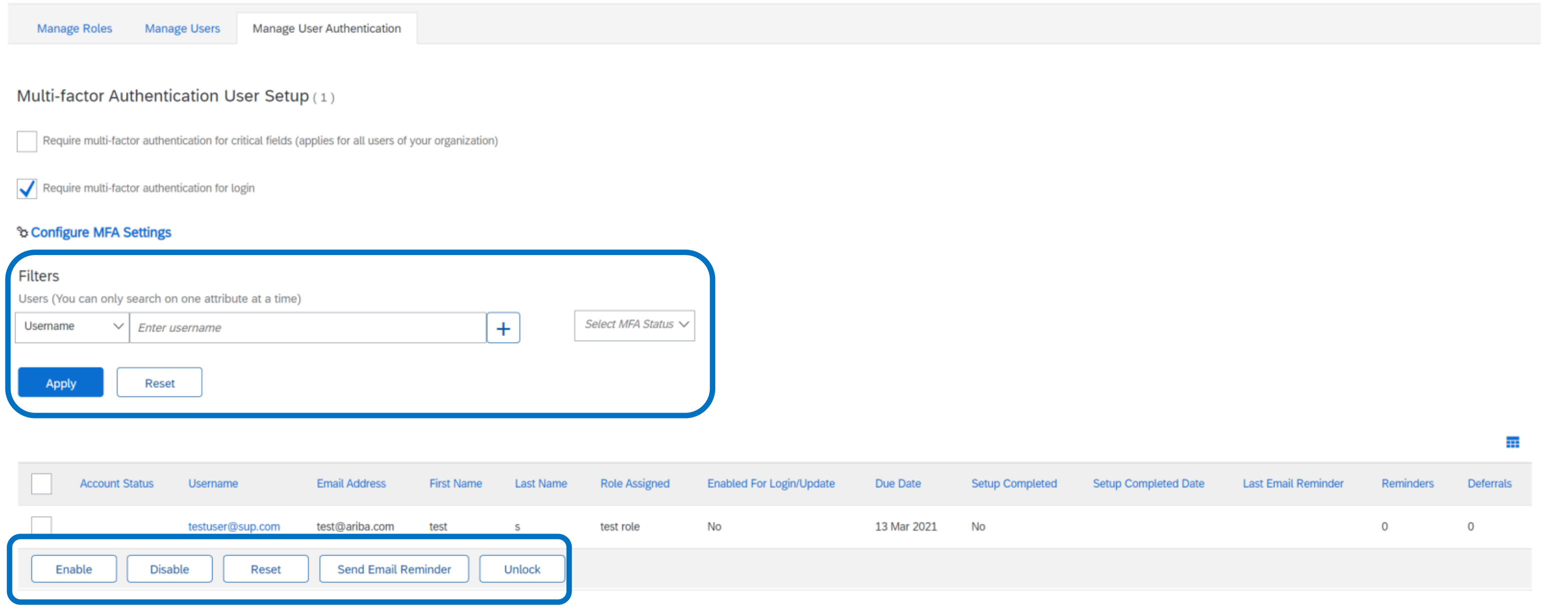
Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – MFA at User Level

The Admin navigates to **Users → Manage User Authentication**

The admins can do following operations for Users:

- **Search** specific user with MFA status and Setup status
- **Enable** MFA for users
- **Disable** MFA for enabled users
- **Reset** MFA for enabled users
- **Unlock** the user if locked due to entry of invalid passcode token entries
- **Send Email Reminder** to enabled users who have not setup MFA



Multi-factor Authentication User Setup (1)

□ Require multi-factor authentication for critical fields (applies for all users of your organization)

☑ Require multi-factor authentication for login

Configure MFA Settings

Filters

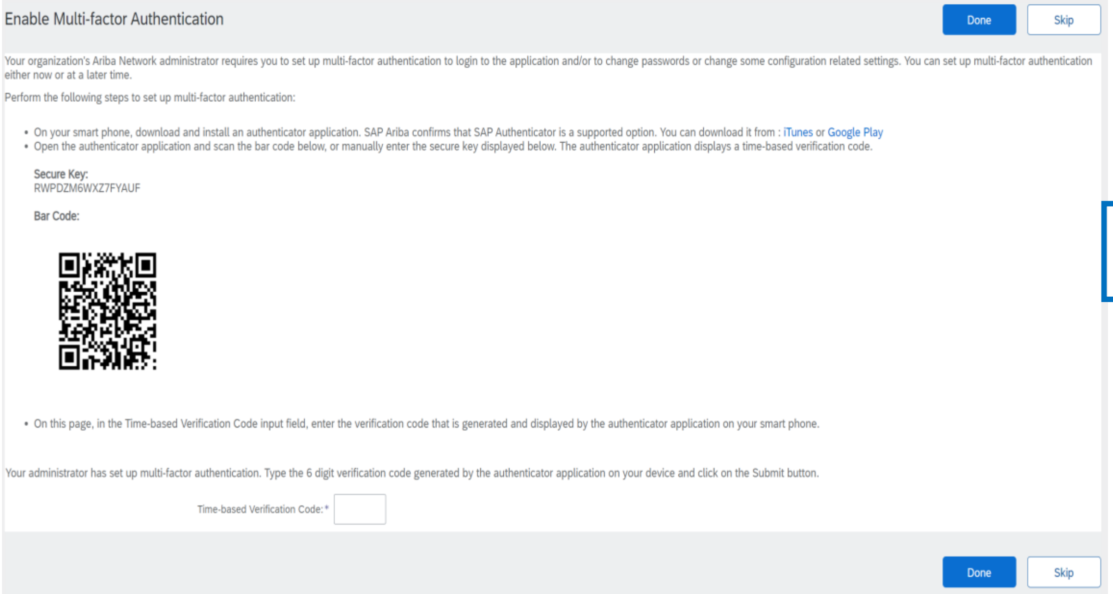
Users (You can only search on one attribute at a time)

□	Account Status	Username	Email Address	First Name	Last Name	Role Assigned	Enabled For Login/Update	Due Date	Setup Completed	Setup Completed Date	Last Email Reminder	Reminders	Deferrals
□		testuser@sup.com	test@ariba.com	test	s	test role	No	13 Mar 2021	No			0	0

Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – User: MFA Setup



Enable Multi-factor Authentication

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

Perform the following steps to set up multi-factor 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:
RWPDZM6WXZ7FYAUF

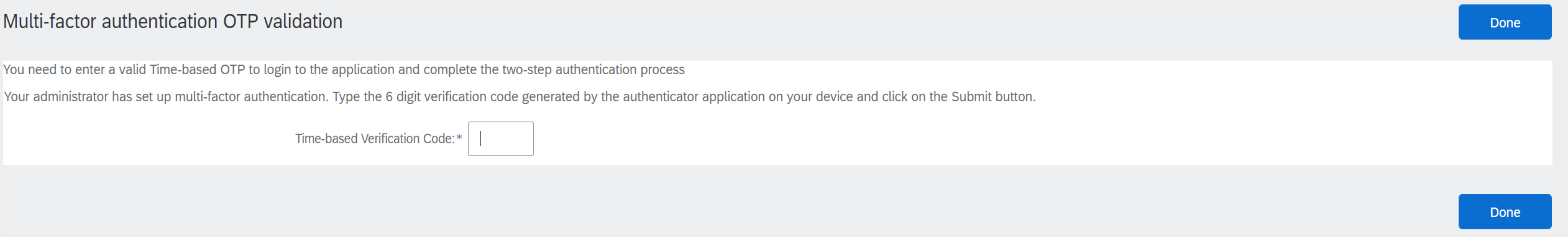
Bar Code:

- 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 multi-factor authentication. Type the 6 digit verification code generated by the authenticator application on your device and click on the Submit button.

Time-based Verification Code:*

If a user has completed MFA setup, the user will be redirected to MFA Authentication page after log in



Multi-factor authentication OTP validation

You need to enter a valid Time-based OTP to login to the application and complete the two-step authentication process

Your administrator has set up multi-factor authentication. Type the 6 digit verification code generated by the authenticator application on your device and click on the Submit button.

Time-based Verification Code:*

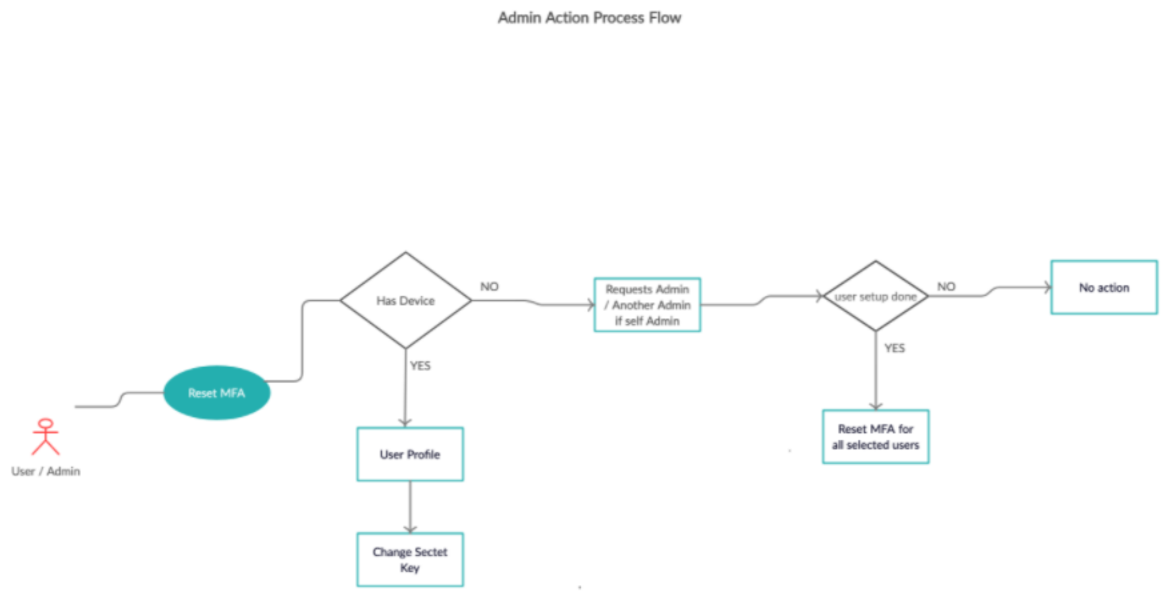
Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – User: MFA Reset

- Persona: User (Application Users)
- MFA Reset Flow:
  - **When User is locked**:
    a. **Call** Admin to unlock or reset MFA
    b. **If Unlocked,** enter credentials and passcode.
    c. **If Reset,** setup MFA with new QR Code
  - **When User changes mobile device**:
    a. **User Preference → MFA**
    b. **Enter** passcode from the old device
    c. **Setup** on new device with new QR code

MFA Reset Flow


Admin Action Process Flow
User / Admin
Reset MFA
Has Device
NO
YES
User Profile
Change Sectet Key
Requests Admin / Another Admin if self Admin
user setup done
NO
YES
No action
Reset MFA for all selected users

Feature at a Glance

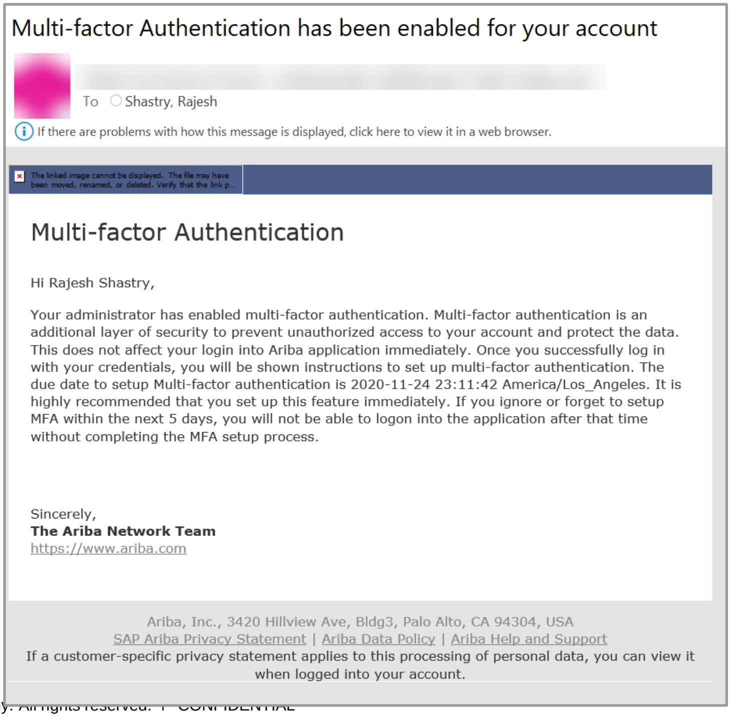
Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – User: Email Notification

Users in a tenant will be sent an email when:

- the Admin **enables** MFA for Users
- the Admin **disables** MFA for Users
- the Admin **resets** MFA for Users
- the Admin **unlocks** the Users
- the Admin **reminds** Users to setup MFA
- the User is **locked** out for invalid login attempts

SAMPLE EMAIL



Multi-factor Authentication has been enabled for your account

[redacted]

To ○ Shastry, Rajesh

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

☒ The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link p...

Multi-factor Authentication

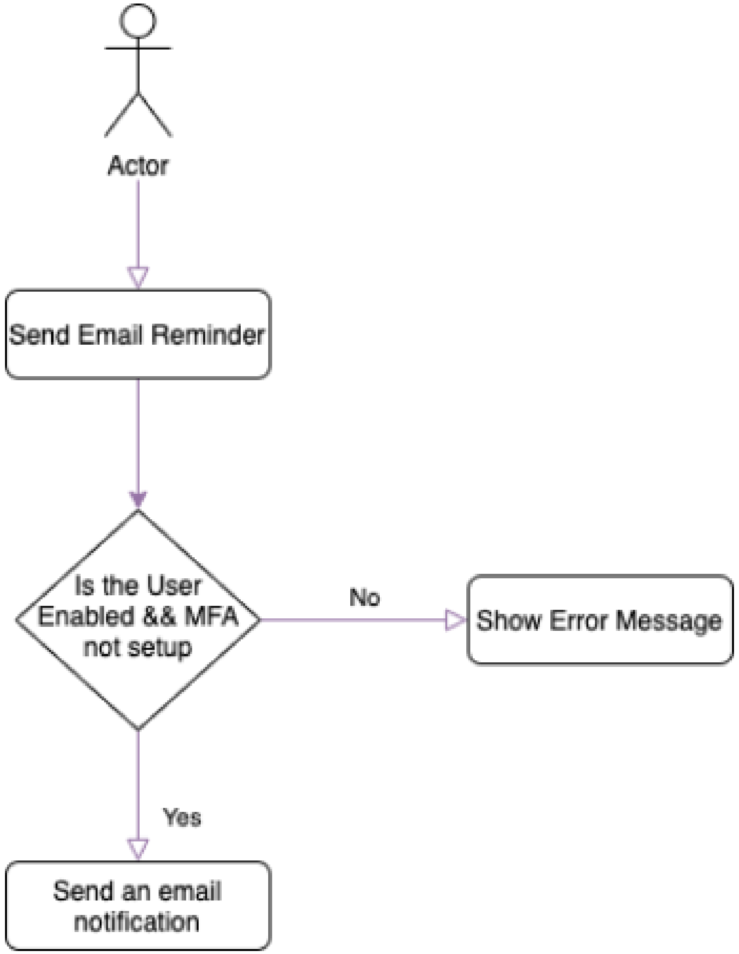
Hi Rajesh Shastry,

Your administrator has enabled multi-factor authentication. Multi-factor authentication is an additional layer of security to prevent unauthorized access to your account and protect the data. This does not affect your login into Ariba application immediately. Once you successfully log in with your credentials, you will be shown instructions to set up multi-factor authentication. The due date to setup Multi-factor authentication is 2020-11-24 23:11:42 America/Los_Angeles. It is highly recommended that you set up this feature immediately. If you ignore or forget to setup MFA within the next 5 days, you will not be able to logon into the application after that time without completing the MFA setup process.

Sincerely,
The Ariba Network Team
https://www.ariba.com

Ariba, Inc., 3420 Hillview Ave, Bldg3, Palo Alto, CA 94304, USA
SAP Ariba Privacy Statement | Ariba Data Policy | Ariba Help and Support
If a customer-specific privacy statement applies to this processing of personal data, you can view it when logged into your account.

Admin : Email Reminder Notification



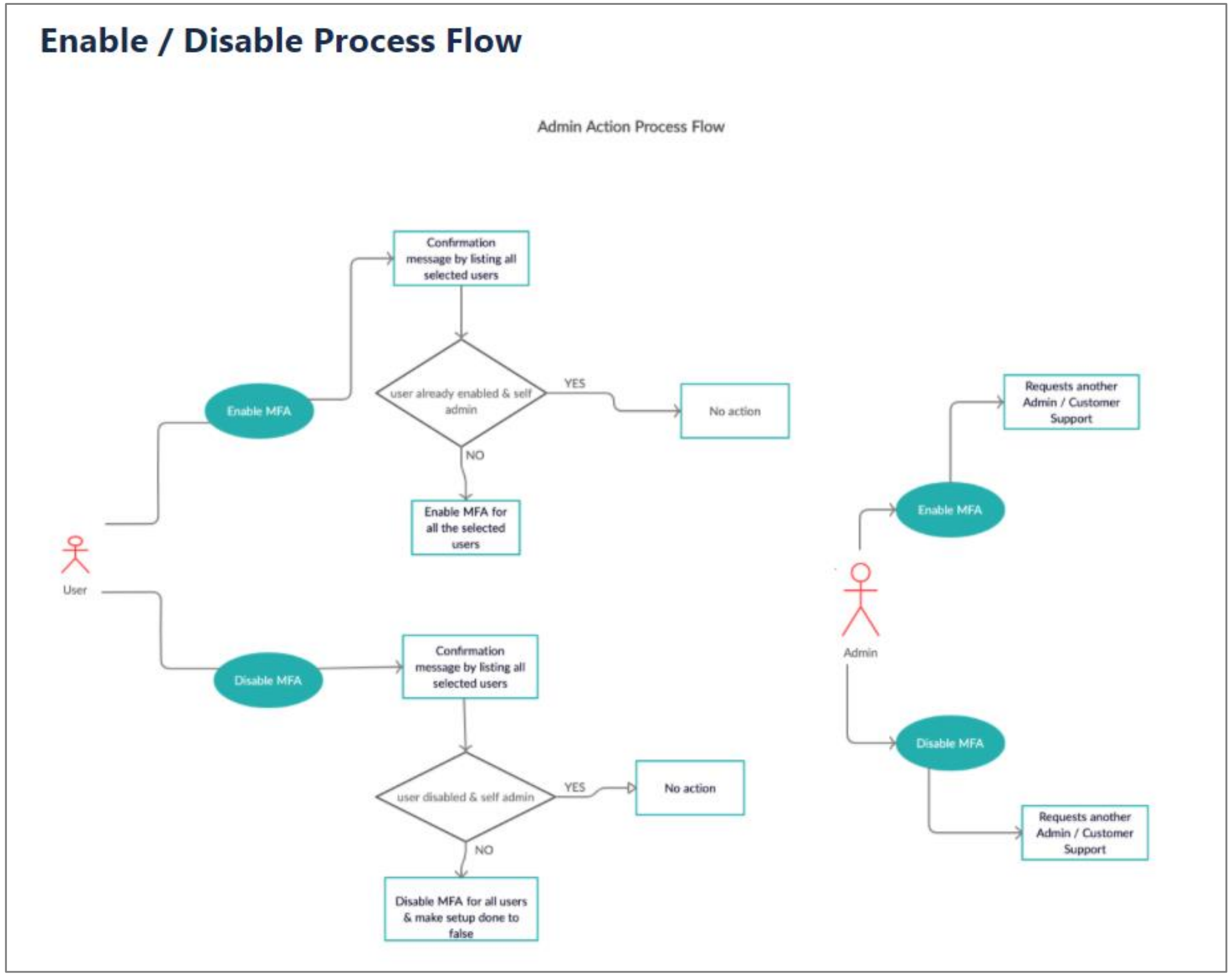
Actor
Send Email Reminder
Is the User Enabled && MFA not setup
No
Show Error Message
Yes
Send an email notification

Feature at a Glance

Introducing: **Multi-factor authentication for user login to Ariba Network**

Detailed feature information – Admin : Process Flow

- Persona: Admin (Customer administrators)
- MFA Management Flow:
  - Enable MFA
  - Disable MFA



Enable / Disable Process Flow

Admin Action Process Flow
User
Enable MFA
Confirmation message by listing all selected users
user already enabled & self admin
YES
No action
NO
Enable MFA for all the selected users
Disable MFA
Confirmation message by listing all selected users
user disabled & self admin
YES
No action
NO
Disable MFA for all users & make setup done to false
Admin
Enable MFA
Requests another Admin / Customer Support
Disable MFA
Requests another Admin / Customer Support