SAP Ariba

Feature at a Glance

Multi-factor authentication for user login to SAP Ariba solutions

Rajesh Shastry, SAP Ariba

Target GA: February, 2021

CONFIDENTIAL

THE BEST RUN SAP

Ease of implementation ● High-Touch
Geographic relevance ● Global

Feature at a Glance

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

Customer challenge

Currently, SAP Ariba applications do not support multi-factor authentication, which makes the basic login potentially vulnerable.

Meet that challenge with SAP Ariba

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

Experience key benefits

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

Solution area

- SAP Ariba Buying
- SAP Ariba Strategic Sourcing

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 SAP Ariba solutions**

Detailed feature information – Brief description

Once MFA feature is enabled:

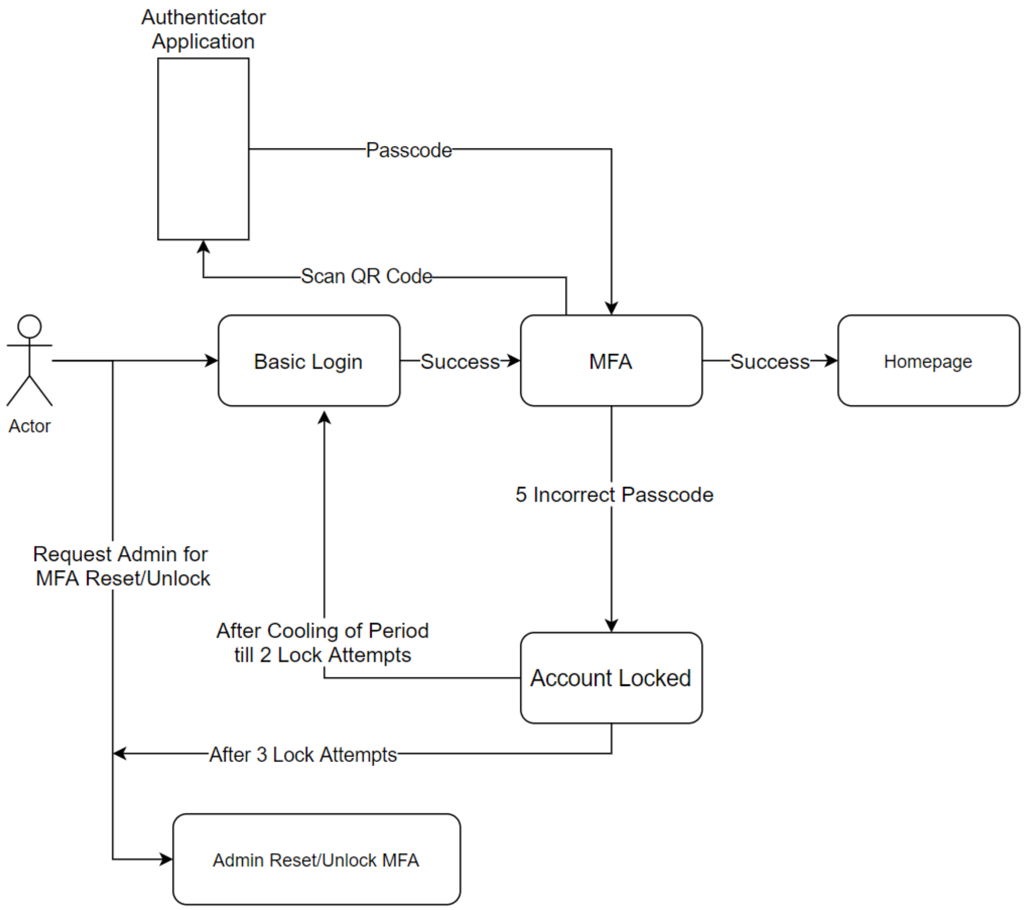
- Customer admins can maintain MFA configurations and enable MFA for the Users
- Users set up MFAs by installing SAP authenticator app from the App Store or Google Play Store
- Next time users login, along with Username/Password, they will be required to enter MFA token to gain access to applications

Feature at a Glance

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

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 or 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

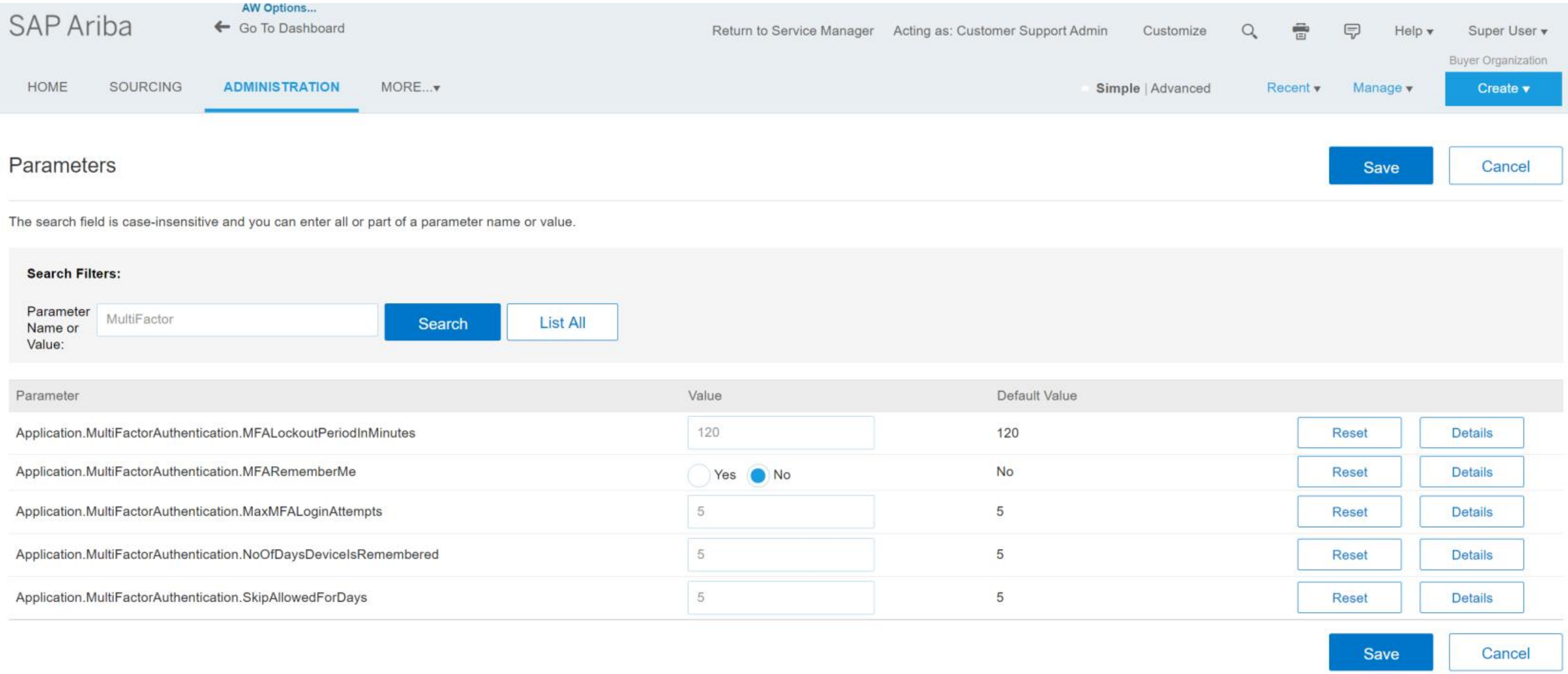
Introducing: **Multi-factor authentication for user login to SAP Ariba solutions**

Detailed feature information – Configure MFA Settings in Realm Level

The Admin navigates to **Administration → Customization Manager section**

The admins can configure the necessary MFA settings in the realm:

- 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 duration (Default Value: 5 Days) Applicable only if Remember me option is set to Yes.



Parameters

The search field is case-insensitive and you can enter all or part of a parameter name or value.

Search Filters:

Parameter Name or Value: MultiFactor

Parameter	Value	Default Value		
Application.MultiFactorAuthentication.MFALockoutPeriodInMinutes	120	120	Reset	Details
Application.MultiFactorAuthentication.MFARememberMe	○ Yes ● No	No	Reset	Details
Application.MultiFactorAuthentication.MaxMFALoginAttempts	5	5	Reset	Details
Application.MultiFactorAuthentication.NoOfDaysDeviceIsRemembered	5	5	Reset	Details
Application.MultiFactorAuthentication.SkipAllowedForDays	5	5	Reset	Details

Feature at a Glance

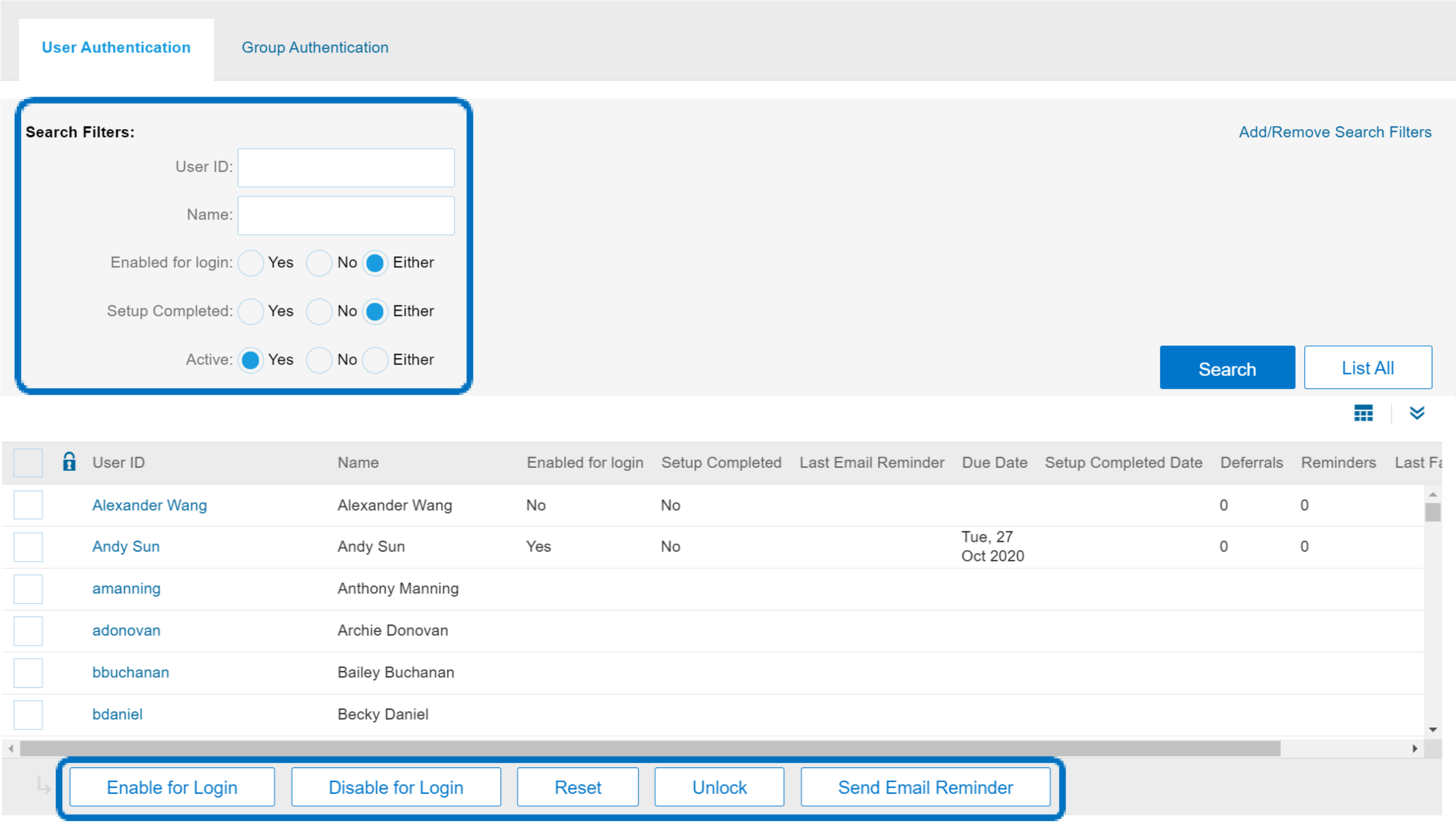
Introducing: **Multi-factor authentication for user login to SAP Ariba solutions**

Detailed feature information – MFA at User Level

The Admin navigates to **User Manager → Multi Factor Authentication → User Authentication**

The admins have the following operations for Users:

- **Search** specific user with MFA status and Setup status
- **Enable** MFA for users who are not enabled
- **Disable** MFA for users who are already enabled
- **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



Search Filters:

User ID:

Name:

Enabled for login: ○ Yes ○ No ● Either

Setup Completed: ○ Yes ○ No ● Either

Active: ● Yes ○ No ○ Either

□	User ID	Name	Enabled for login	Setup Completed	Last Email Reminder	Due Date	Setup Completed Date	Deferrals	Reminders	Last Fa
□	Alexander Wang	Alexander Wang	No	No				0	0	
□	Andy Sun	Andy Sun	Yes	No		Tue, 27 Oct 2020		0	0	
□	amanning	Anthony Manning								
□	adonovan	Archie Donovan								
□	bbuchanan	Bailey Buchanan								
□	bdaniel	Becky Daniel								

Feature at a Glance

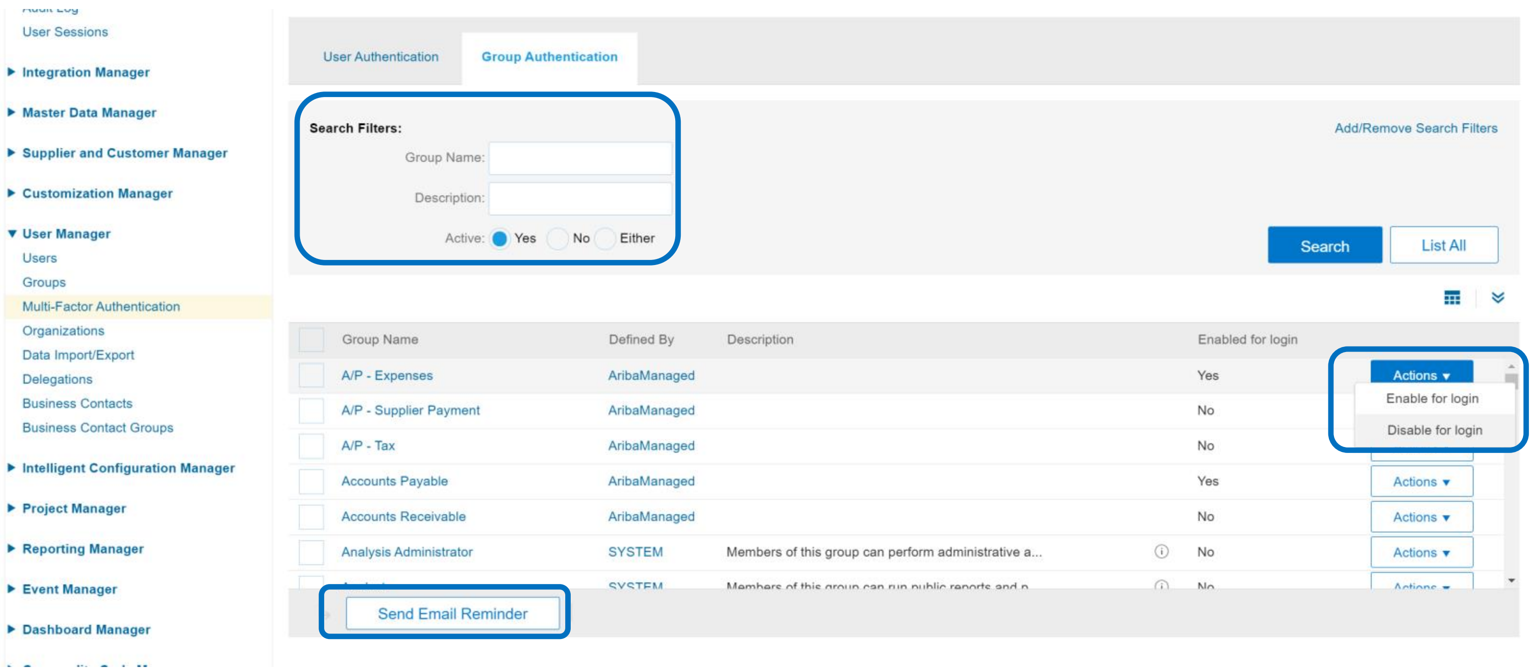
Introducing: **Multi-factor authentication for user login to SAP Ariba solutions**

Detailed feature information – MFA at Group Level

The Admin navigates to **User Manager** → **Multi Factor Authentication** → **Group Authentication**

The admins have the following operations for Groups:

- **Enable at group level** to enable MFA for all the users who are part of the group
- **Disable at group level** to disable MFA for all the users who are part of the group
- **Send Email Reminder** to the users in the group who have not setup MFA
- **Search** for specific group



Search Filters:

Group Name:

Description:

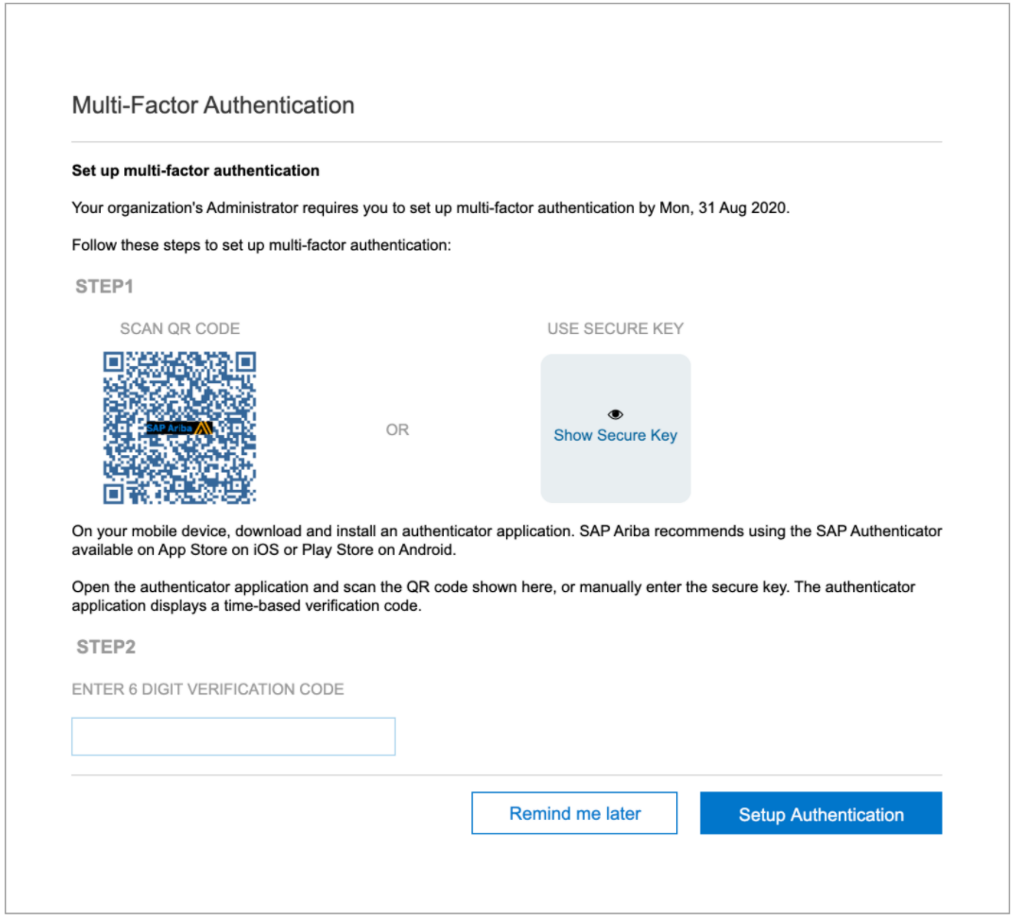
Active: ● Yes ○ No ○ Either

□	Group Name	Defined By	Description		Enabled for login	
□	A/P - Expenses	AribaManaged			Yes	Actions ▾
□	A/P - Supplier Payment	AribaManaged			No	
□	A/P - Tax	AribaManaged			No	
□	Accounts Payable	AribaManaged			Yes	Actions ▾
□	Accounts Receivable	AribaManaged			No	Actions ▾
□	Analysis Administrator	SYSTEM	Members of this group can perform administrative a...	ⓘ	No	Actions ▾
□	[illegible]	SYSTEM	Members of this group can run public reports and n...	ⓘ	No	Actions ▾

Feature at a Glance

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

Detailed feature information – User: MFA Setup



Multi-Factor Authentication

Set up multi-factor authentication

Your organization's Administrator requires you to set up multi-factor authentication by Mon, 31 Aug 2020.

Follow these steps to set up multi-factor authentication:

STEP1

SCAN QR CODE

OR

USE SECURE KEY

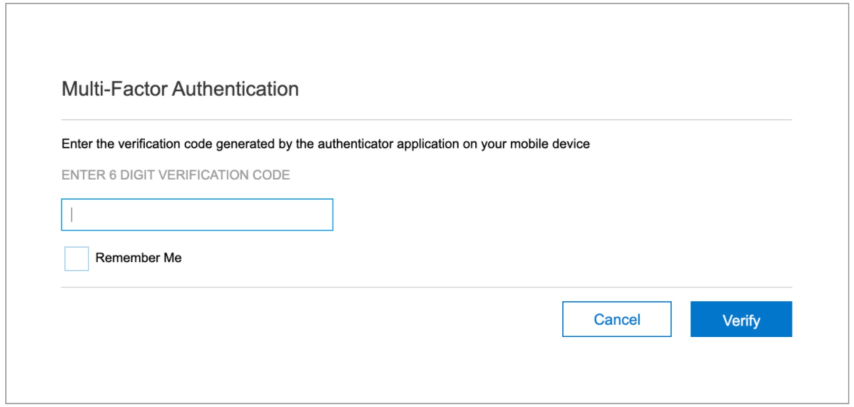
On your mobile device, download and install an authenticator application. SAP Ariba recommends using the SAP Authenticator available on App Store on iOS or Play Store on Android.

Open the authenticator application and scan the QR code shown here, or manually enter the secure key. The authenticator application displays a time-based verification code.

STEP2

ENTER 6 DIGIT VERIFICATION CODE

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



Multi-Factor Authentication

Enter the verification code generated by the authenticator application on your mobile device

ENTER 6 DIGIT VERIFICATION CODE

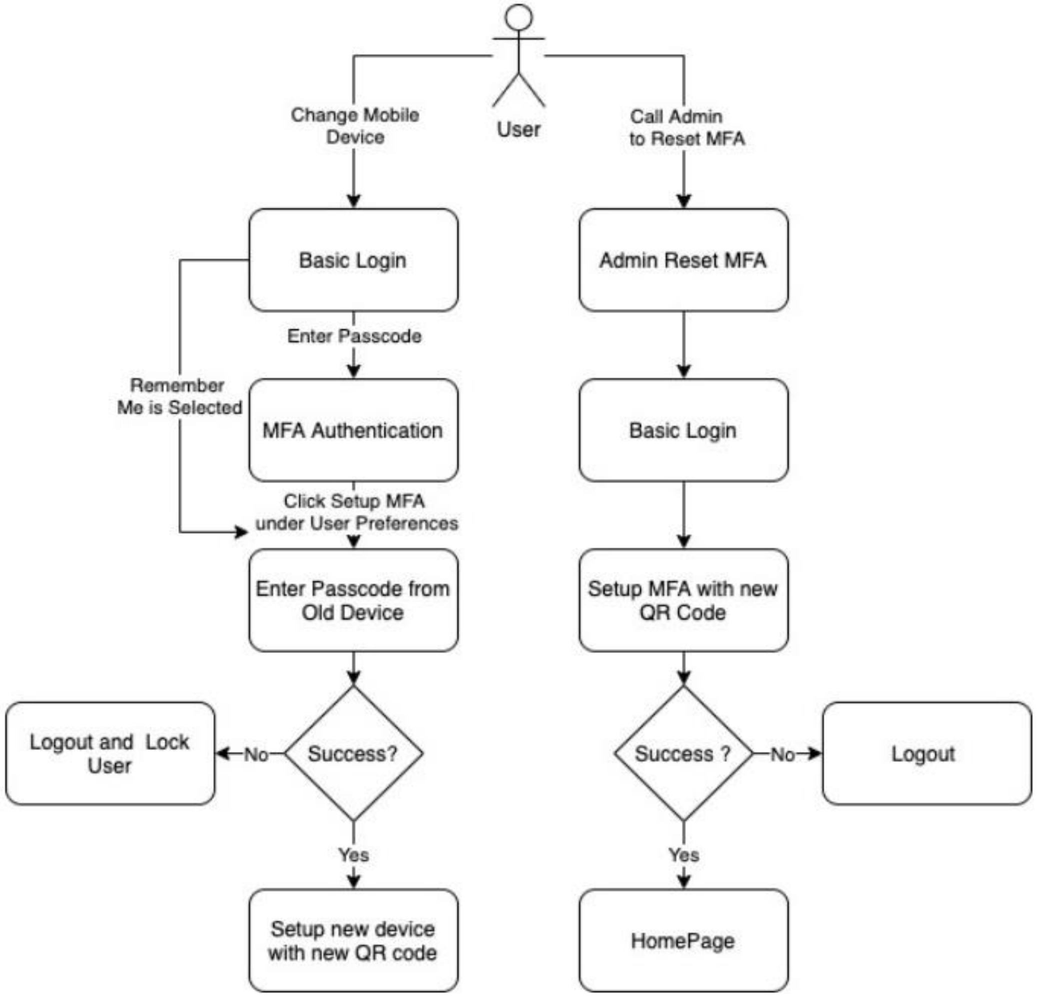
□ Remember Me

Feature at a Glance

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

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



Feature at a Glance

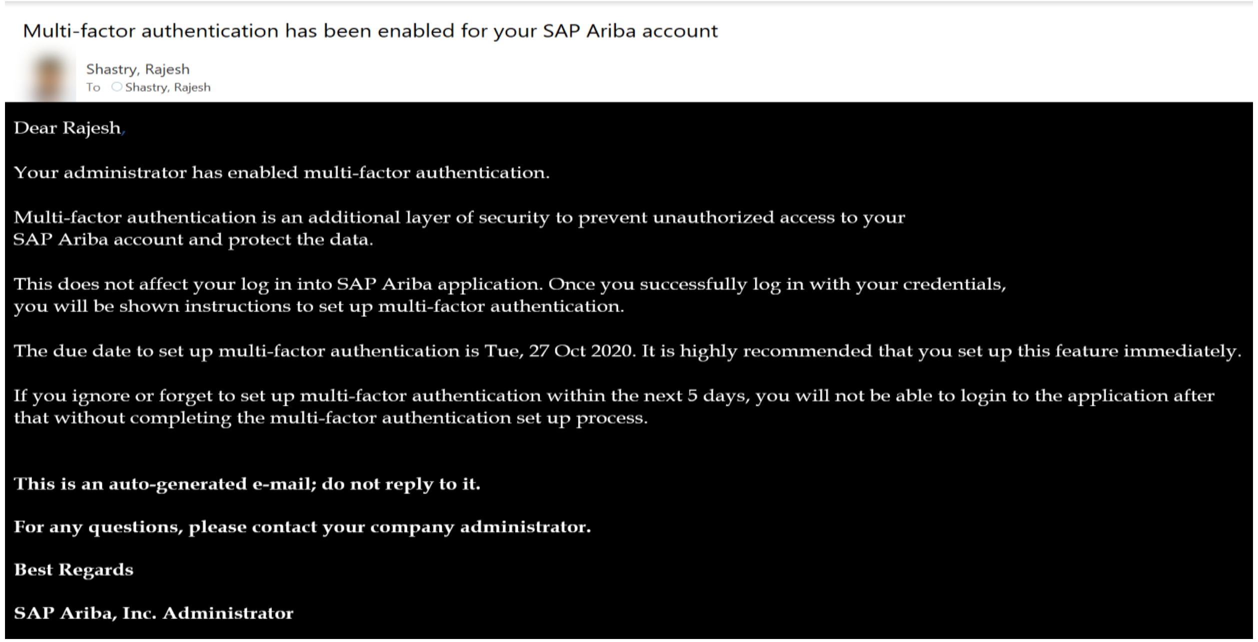
Introducing: **Multi-factor authentication for user login to SAP Ariba solutions**

Detailed feature information – UI Mock-ups for Emails

Users in a realm / tenant will be sent an email when:

- the Admin **enable**s MFA for Users
- the Admin **disable**s MFA for Users
- the Admin **reset**s MFA for Users
- the Admin **unlocks** MFA for Users
- the Admin **reminds** Users to setup MFA
- the User is **locked** out for invalid passcode entries

SAMPLE EMAIL



Multi-factor authentication has been enabled for your SAP Ariba account

Shastry, Rajesh
To ○ Shastry, Rajesh

Dear Rajesh,

Your administrator has enabled multi-factor authentication.

Multi-factor authentication is an additional layer of security to prevent unauthorized access to your SAP Ariba account and protect the data.

This does not affect your log in into SAP Ariba application. Once you successfully log in with your credentials, you will be shown instructions to set up multi-factor authentication.

The due date to set up multi-factor authentication is Tue, 27 Oct 2020. It is highly recommended that you set up this feature immediately.

If you ignore or forget to set up multi-factor authentication within the next 5 days, you will not be able to login to the application after that without completing the multi-factor authentication set up process.

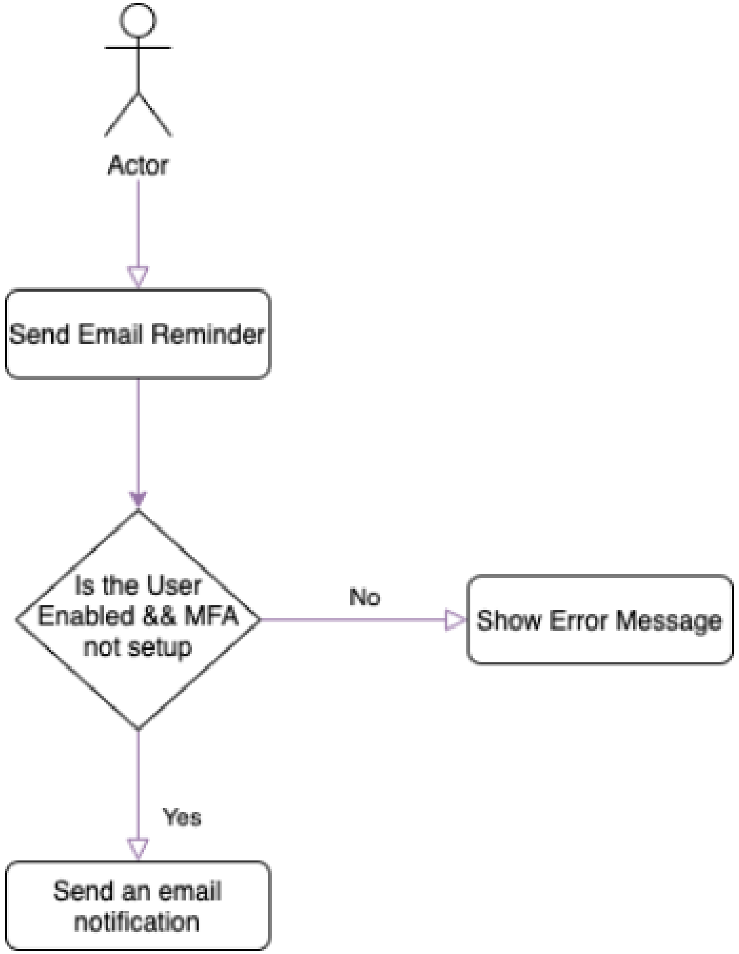
This is an auto-generated e-mail; do not reply to it.

For any questions, please contact your company administrator.

Best Regards

SAP Ariba, Inc. Administrator

Admin : Email Reminder Notification

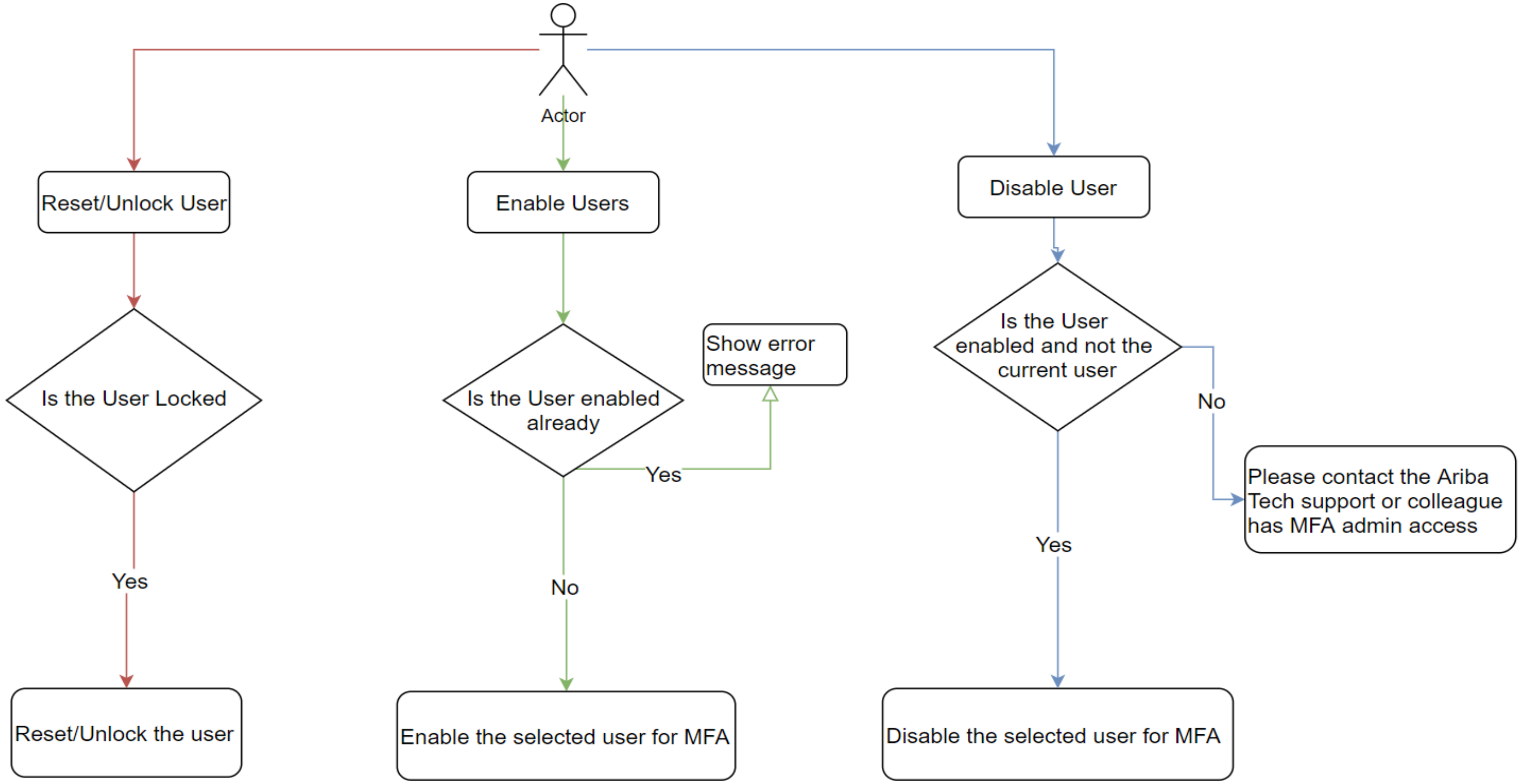

Actor
Send Email Reminder
Is the User Enabled && MFA not setup
No
Show Error Message
Yes
Send an email notification

Feature at a Glance

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

Detailed feature information – Admin : MFA Process Flow

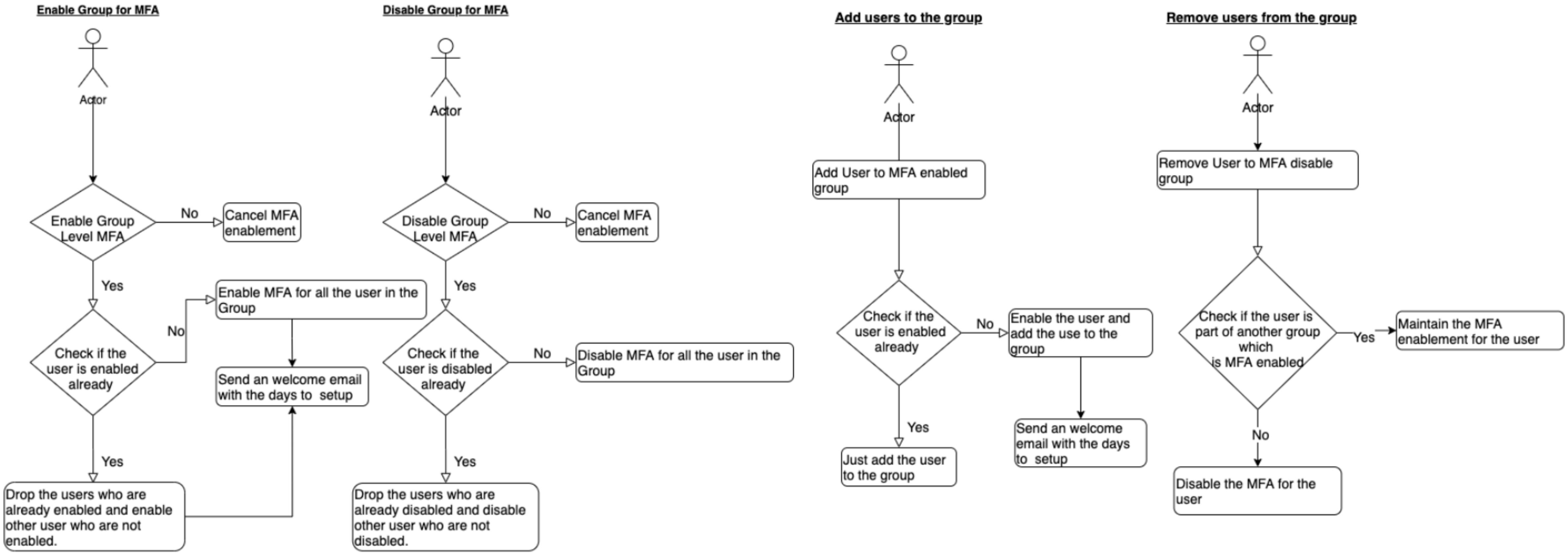
- Persona: Admin (Customer administrators)
- MFA Management Flow:
  - Enable
  - Disable
  - Reset
  - Unlock


Actor
Reset/Unlock User
Enable Users
Disable User
Is the User Locked
Yes
Reset/Unlock the user
Is the User enabled already
Yes
Show error message
No
Enable the selected user for MFA
Is the User enabled and not the current user
No
Please contact the Ariba Tech support or colleague has MFA admin access
Yes
Disable the selected user for MFA

Feature at a Glance

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

Detailed feature information – Admin: Group Level Enable/Disable



Enable Group for MFA

Actor

Enable Group Level MFA

No

Cancel MFA enablement

Yes

Check if the user is enabled already

No

Enable MFA for all the user in the Group

Send an welcome email with the days to setup

Yes

Drop the users who are already enabled and enable other user who are not enabled.

Disable Group for MFA

Actor

Disable Group Level MFA

No

Cancel MFA enablement

Yes

Check if the user is disabled already

No

Disable MFA for all the user in the Group

Yes

Drop the users who are already disabled and disable other user who are not disabled.

Add users to the group

Actor

Add User to MFA enabled group

Check if the user is enabled already

No

Enable the user and add the use to the group

Send an welcome email with the days to setup

Yes

Just add the user to the group

Remove users from the group

Actor

Remove User to MFA disable group

Check if the user is part of another group which is MFA enabled

Yes

Maintain the MFA enablement for the user

No

Disable the MFA for the user