



SAP Ariba 

# 機能の概要

## 多要素認証による Ariba Network へのユーザーログイン

Rajesh Shastry, SAP Ariba  
一般提供予定: 2021 年 2 月

CONFIDENTIAL

## 機能の概要

# 説明: 多要素認証による Ariba Network へのユーザーログイン

### 今までの課題

現在、Ariba Network では多要素認証によるログインに対応していないため、基本的なログインが脆弱な状態にあります。

### SAP Ariba で問題解決

多要素認証 (MFA) による基本的なログインに対応します。

### 主なメリット

- Ariba Network へのアクセスが保護されます。
- 漏洩したユーザーアカウント認証情報を使用して SAP Ariba アプリケーションにアクセスする悪質なエンティティのリスクを軽減します。

### 対象ソリューション

Ariba Network

### 関連情報

この機能は、該当するソリューションを使用しているすべてのお客様に対して自動的に有効になりますが、お客様が設定する必要があります。

### 前提条件と制限事項

多要素認証が組織で有効になっている場合、有効なユーザーは App Store または Google Play ストアから SAP Authenticator アプリをインストールして、時間ベースのワンタイムパスワード (TOTP) を生成する必要があります。

## 機能の概要

### 説明: 多要素認証による Ariba Network へのユーザーログイン

#### 機能の詳細情報 - 簡単な説明

MFA を有効にした場合:

- 顧客管理者は MFA 設定を管理し、ユーザーに対して MFA を有効化することができます。
- ユーザーは App Store および Google Play ストアから SAP Authenticator アプリをインストールして MFA を設定します。
- 次回、ユーザーがユーザー名/パスワードを使用してログインすると、アプリケーションにアクセスするための MFA トークンの入力を要求されます。



# 機能の概要

## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - ログインの MFA の有効化および MFA 設定の構成

管理者は [ユーザー] → [ユーザー認証の管理] の順に移動します。

管理者は、チェックボックスを選択してログインの MFA を有効化し、テナントで必要な MFA 設定を構成することができます。

- 多要素認証設定をスキップできる日数 (初期値: 5 日)
- 多要素認証に対して許容される無効な試行回数 (初期値: 5 回)
- ロックされたユーザーの再試行までの期間 (初期値: 120 分)
- [認証情報を記憶する] オプションの有効化 (初期値: いいえ)
- 端末を記憶する期間 (初期値: 5 日) - [認証情報を記憶する] オプションが [はい] に設定されている場合にのみ適用できます。

The screenshot displays the 'Account Settings' interface for SAP Ariba Network. The 'Manage User Authentication' tab is active, showing the 'Multi-factor Authentication User Setup' section. Two checkboxes are present: 'Require multi-factor authentication for critical fields' (unchecked) and 'Require multi-factor authentication for login' (checked). Below this is a 'Filters' section with a search box for 'Username' and a 'Select MFA Status' dropdown. The bottom section, 'Configure Multi-factor Authentication Settings', contains a table of configuration options:

Setting	Value	Unit
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 :	<input checked="" type="checkbox"/>	
Remember device for :	5	days

# 機能の概要

## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - ユーザーレベルでの MFA

管理者は [ユーザー] → [ユーザー認証の管理] の順に移動します。

管理者は、ユーザーに対して以下の操作を実行することができます。

- MFA 状況および設定状況で特定のユーザーを検索します。
- ユーザーに対して MFA を有効化します。
- 有効化されているユーザーに対して MFA を無効化します。
- 有効化されているユーザーに対して MFA をリセットします。
- 無効なパスコードトークンエントリの入力によりロックされている場合に、ユーザーのロックを解除します。
- MFA を設定していない有効なユーザーに電子メールリマインダを送信します。

The screenshot displays the 'Manage User Authentication' section of the SAP Ariba Network interface. It includes a 'Multi-factor Authentication User Setup' configuration area with checkboxes for 'Require multi-factor authentication for critical fields' and 'Require multi-factor authentication for login'. Below this is a 'Configure MFA Settings' section with a search filter for users. A table lists user details, and a row for 'testuser@sup.com' is highlighted with a blue box, showing buttons for 'Enable', 'Disable', 'Reset', 'Send Email Reminder', and 'Unlock'.

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
<input type="checkbox"/>	testuser@sup.com	test@ariba.com	test	s	test role	No	13 Mar 2021	No			0	0

# 機能の概要

## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - ユーザー: MFA 設定

Enable Multi-factor Authentication Done Skip


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:  
RWPDM6WXZ7FYAUF

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:\*

Done Skip

ユーザーが MFA 設定を完了している場合、ログイン後に MFA 認証ページが表示されます。

Multi-factor authentication OTP validation Done

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:\*

Done

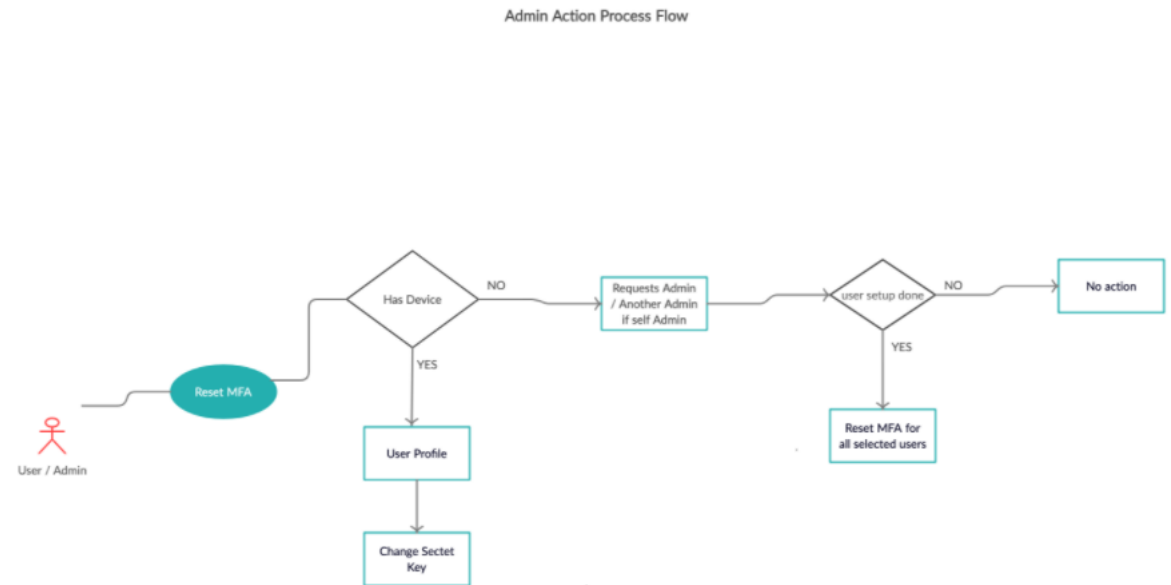
# 機能の概要

## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - ユーザー: MFA リセット

- 対象: ユーザー (アプリケーションユーザー)
- MFA リセットフロー:
  - ユーザーがロックされた場合:
    - 管理者に連絡し、ロックを解除するか、MFA をリセットします。
    - ロックが解除された場合、認証情報とパスコードを入力します。
    - リセットされた場合、新しい QR コードを使用して MFA を設定します。
  - ユーザーがモバイル端末を変更した場合:
    - [ユーザー設定] → [多要素認証]
    - 以前の端末のパスコードを入力します。
    - 新しい端末で新しい QR コードを使用して設定します。

### MFA Reset Flow





# 機能の概要

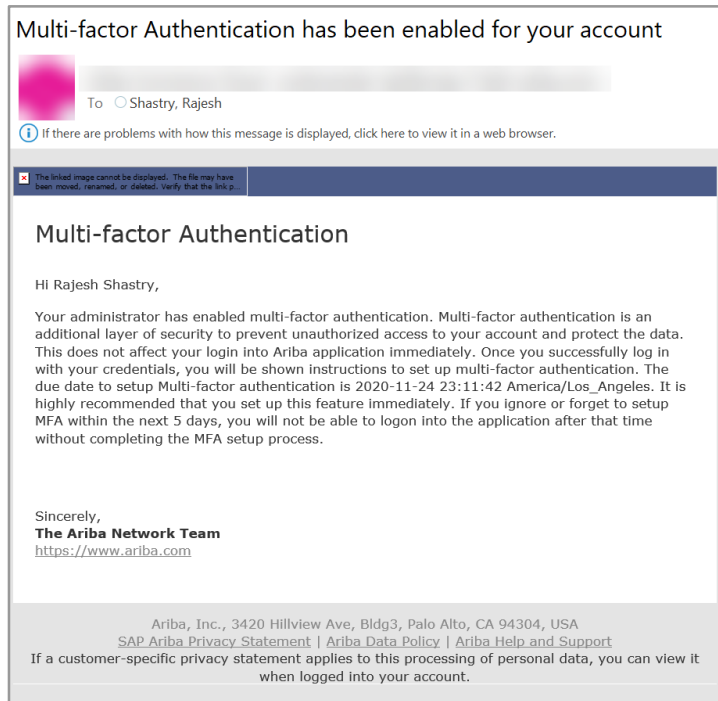
## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - ユーザー: 電子メール通知

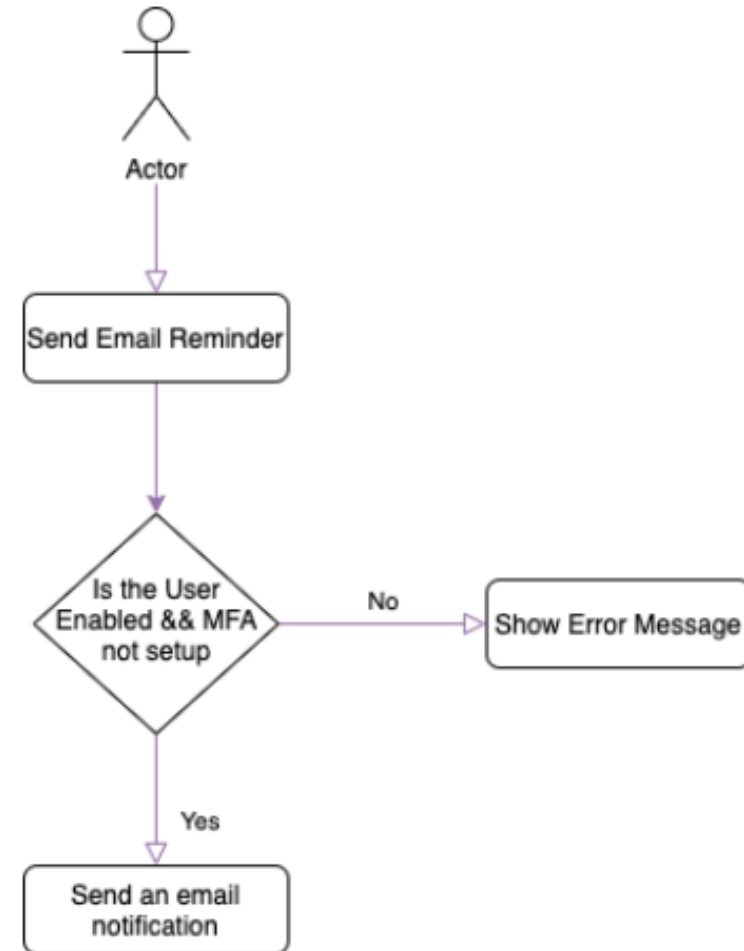
以下のタイミングでテナント内のユーザーに電子メールが送信されます。

- 管理者がユーザーに対して MFA を有効化したとき
- 管理者がユーザーに対して MFA を無効化したとき
- 管理者がユーザーに対して MFA をリセットしたとき
- 管理者がユーザーのロックを解除したとき
- 管理者が MFA の設定に関するリマインダをユーザーに送信したとき
- 無効なログイン試行によりユーザーがロックされたとき

### 電子メールの例



### 管理者: 電子メールリマインダ通知



# 機能の概要

## 説明: 多要素認証による Ariba Network へのユーザーログイン

### 機能の詳細情報 - 管理者: プロセスフロー

- 対象: 管理者 (顧客管理者)
- MFA 管理フロー:
  - MFA の有効化
  - MFA の無効化

