



SAP Ariba 

機能の概要 多要素認証による SAP Ariba ソリューション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

導入の難易度 ● ハイタッチ
対象エリア ● グローバル

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

今までの課題

現在、SAP Ariba ソリューション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る可能性があります。

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

- SAP Ariba アプリケーション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

- SAP Ariba Buying
- SAP Ariba Strategic Sourcing

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 SAP Ariba ソリューション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:

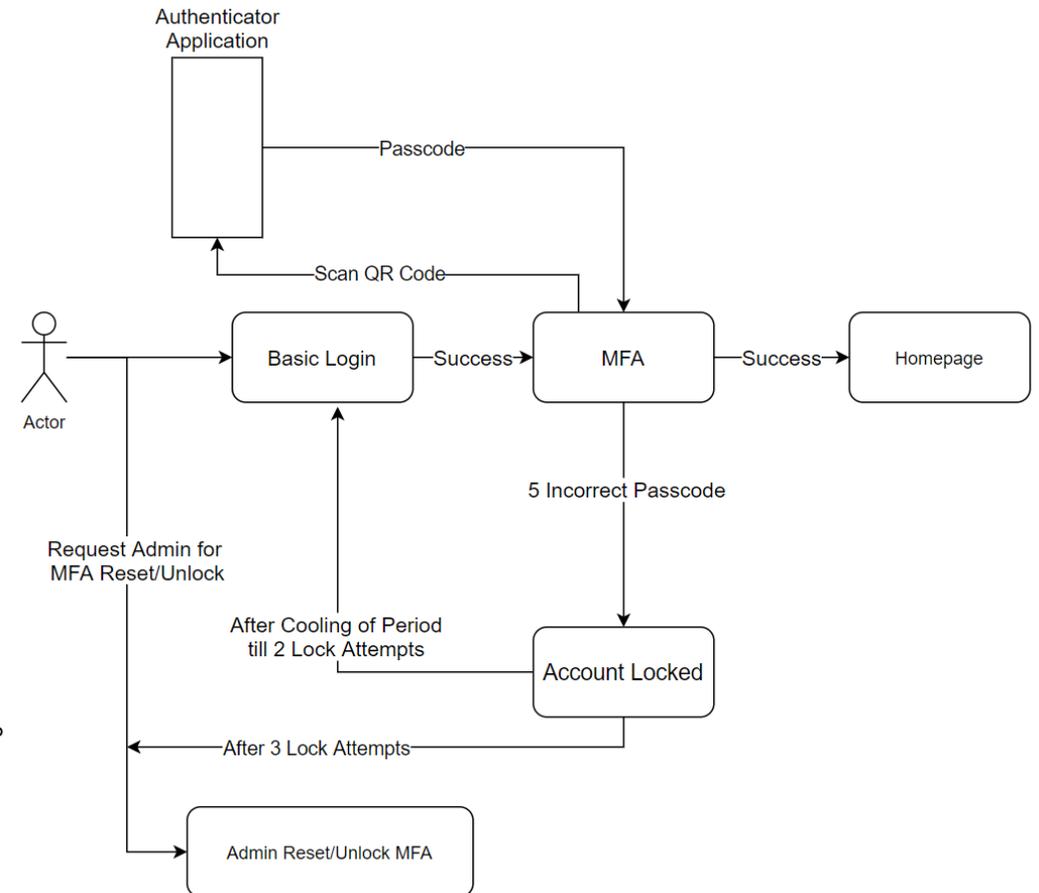
- 顧客管理者は MFA 設定を管理し、ユーザーに対して MFA を有効化することができます。
- ユーザーは App Store または Google Play ストアから SAP Authenticator アプリをインストールして MFA を設定します。
- 次回、ユーザーがユーザー名/パスワードを使用してログインすると、アプリケーションにアクセスするための MFA トークンの入力を要求されます。

機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - ユーザーログイン: プロセスフロー

- 対象: ユーザー (アプリケーションユーザー)
- ログインフロー:
 1. ユーザー ID とパスワードを入力します。
 2. 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ます。
 3. QR コードをスキャンし、パスコードを取得します。
 4. 有効時間内に、MFA ログイン画面にパスコードを入力します。
 5. 生成されたパスコードが有効時間内に入力されると、ログインが成功します。
 6. ログインに失敗した場合、再度ログインを試行します (通常設定)。
 - 1 回目のログイン試行で 5 回失敗すると、120 分間ロックされます。
 - 2 回目のログイン試行で 5 回失敗すると、2 × 120 分間ロックされます。
 - 3 回目のログイン試行で 5 回失敗すると、ロックされます。
 - 管理者にリクエストを送信して、ロックの解除またはリセットを依頼します。



機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - レルムレベルでの MFA の設定

管理者は [管理] → [カスタマイズマネージャ] セクションの順に移動します。

管理者は、レルムで必要な 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 shows the SAP Ariba Administration console interface. The top navigation bar includes 'SAP Ariba', 'Go To Dashboard', 'Return to Service Manager', 'Acting as: Customer Support Admin', 'Customize', 'Help', and 'Super User'. The main menu has 'HOME', 'SOURCING', 'ADMINISTRATION', and 'MORE...'. The 'ADMINISTRATION' section is active, showing 'Parameters' with 'Save' and 'Cancel' buttons. A search filter is applied for 'MultiFactor'. Below the search bar, a table lists MFA parameters with their current values and default values. Each row includes 'Reset' and 'Details' buttons.

Parameter	Value	Default Value	Reset	Details
Application.MultiFactorAuthentication.MFALockoutPeriodInMinutes	120	120	Reset	Details
Application.MultiFactorAuthentication.MFARememberMe	<input type="radio"/> Yes <input checked="" type="radio"/> No	No	Reset	Details
Application.MultiFactorAuthentication.MaxMFALoginAttempts	5	5	Reset	Details
Application.MultiFactorAuthentication.NoOfDaysDevicesRemembered	5	5	Reset	Details
Application.MultiFactorAuthentication.SkipAllowedForDays	5	5	Reset	Details

機能の概要

説明: 多要素認証による SAP Ariba ソリューション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 [ユーザーマネージャ] → [多要素認証] → [ユーザー認証] 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。
- 有効化されていないユーザーに対して MFA を有効化します。
- すでに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。
- 無効なパスワ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 shows the 'User Authentication' configuration page. A search filter box is highlighted with a blue border, containing the following fields:

- User ID:
- Name:
- Enabled for login: Yes No Either
- Setup Completed: Yes No Either
- Active: Yes No Either

Below the search filters is a table of users:

User ID	Name	Enabled for login	Setup Completed	Last Email Reminder	Due Date	Setup Completed Date	Deferrals	Reminders	Last Failed Login
<input type="checkbox"/> Alexander Wang	Alexander Wang	No	No				0	0	
<input type="checkbox"/> Andy Sun	Andy Sun	Yes	No		Tue, 27 Oct 2020		0	0	
<input type="checkbox"/> amanning	Anthony Manning								
<input type="checkbox"/> adonovan	Archie Donovan								
<input type="checkbox"/> bbuchanan	Bailey Buchanan								
<input type="checkbox"/> bdaniel	Becky Daniel								

At the bottom of the page, a row of action buttons is highlighted with a blue border:

- Enable for Login
- Disable for Login
- Reset
- Unlock
- Send Email Reminder

機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - グループレベルでの MFA

管理者は [ユーザーマネージャ] → [多要素認証] → [グループ認証] の順に移動します。

管理者は、グループに対して以下の操作を実行することができます。

- グループレベルで有効化して、グループに含まれるすべてのユーザーに対して MFA を有効化します。
- グループレベルで無効化して、グループに含まれるすべてのユーザーに対して MFA を無効化します。
- MFA を設定していないグループ内のユーザーに電子メールリマインダを送信します。
- 特定のグループを検索します。

Group Name	Defined By	Description	Enabled for login
<input type="checkbox"/> A/P - Expenses	AribaManaged		Yes
<input type="checkbox"/> A/P - Supplier Payment	AribaManaged		No
<input type="checkbox"/> A/P - Tax	AribaManaged		No
<input type="checkbox"/> Accounts Payable	AribaManaged		Yes
<input type="checkbox"/> Accounts Receivable	AribaManaged		No
<input type="checkbox"/> Analysis Administrator	SYSTEM	Members of this group can perform administrative a...	No
<input type="checkbox"/>	SYSTEM	Members of this group can run public reports, and o...	No

機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - ユーザー: MFA 設定

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 USE SECURE KEY

 OR 

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



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

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

ENTER 6 DIGIT VERIFICATION CODE

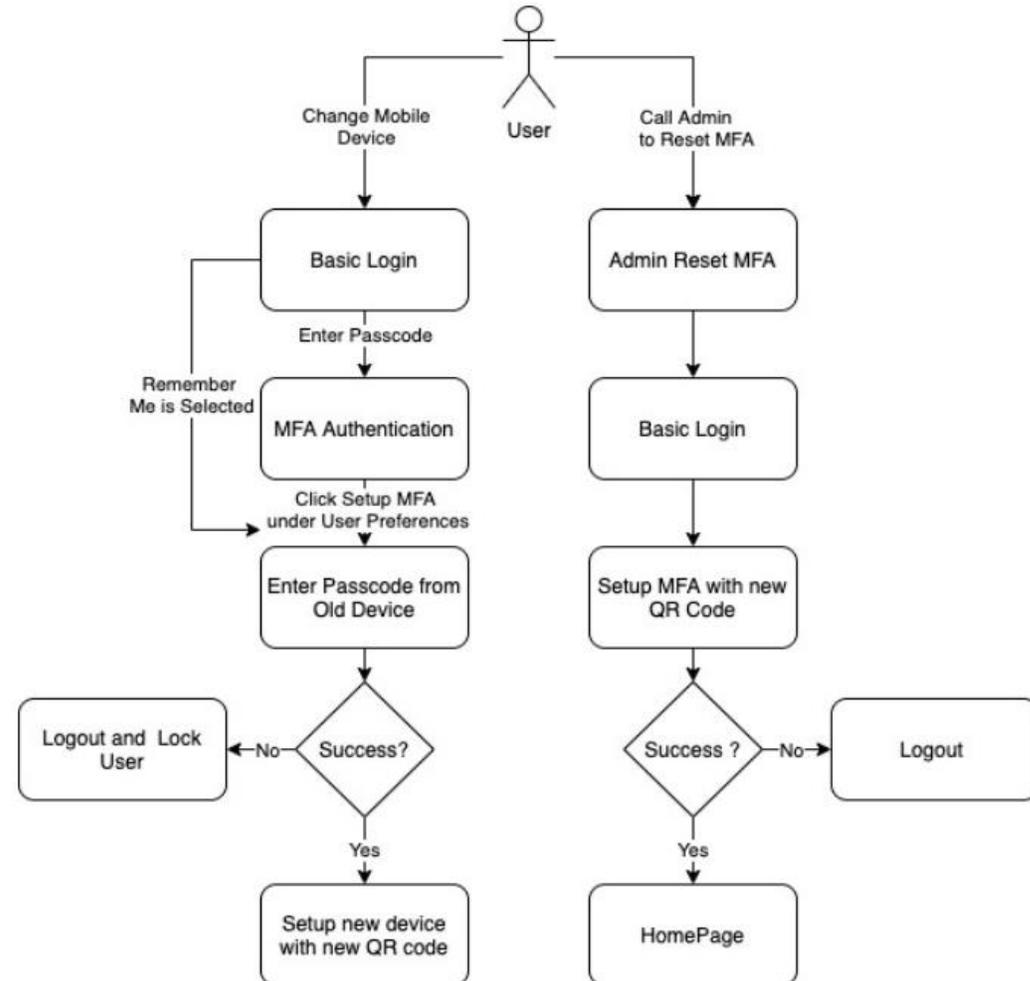
Remember Me

機能の概要

説明: 多要素認証による SAP Ariba ソリューション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。



機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

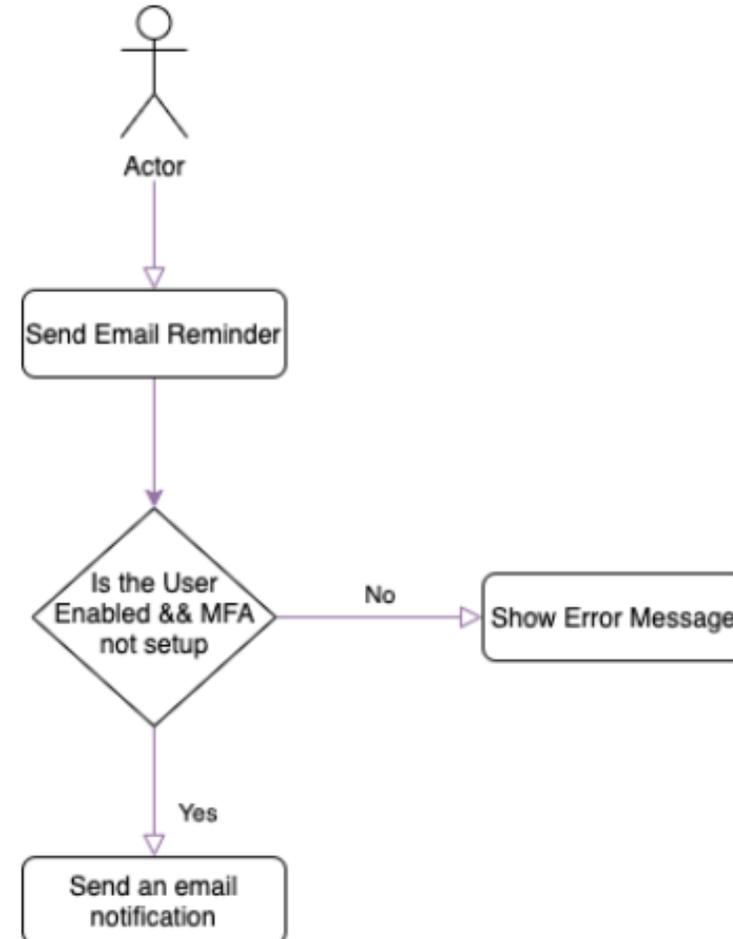
機能の詳細情報 - 電子メールの UI モックアップ

以下のタイミングでレルム/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
- 管理者がユーザーに対して MFA のロックを解除したとき

電子メールの例 MFA の設定に関するリマインダをユーザー

管理者: 電子メールリマインダ通知



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

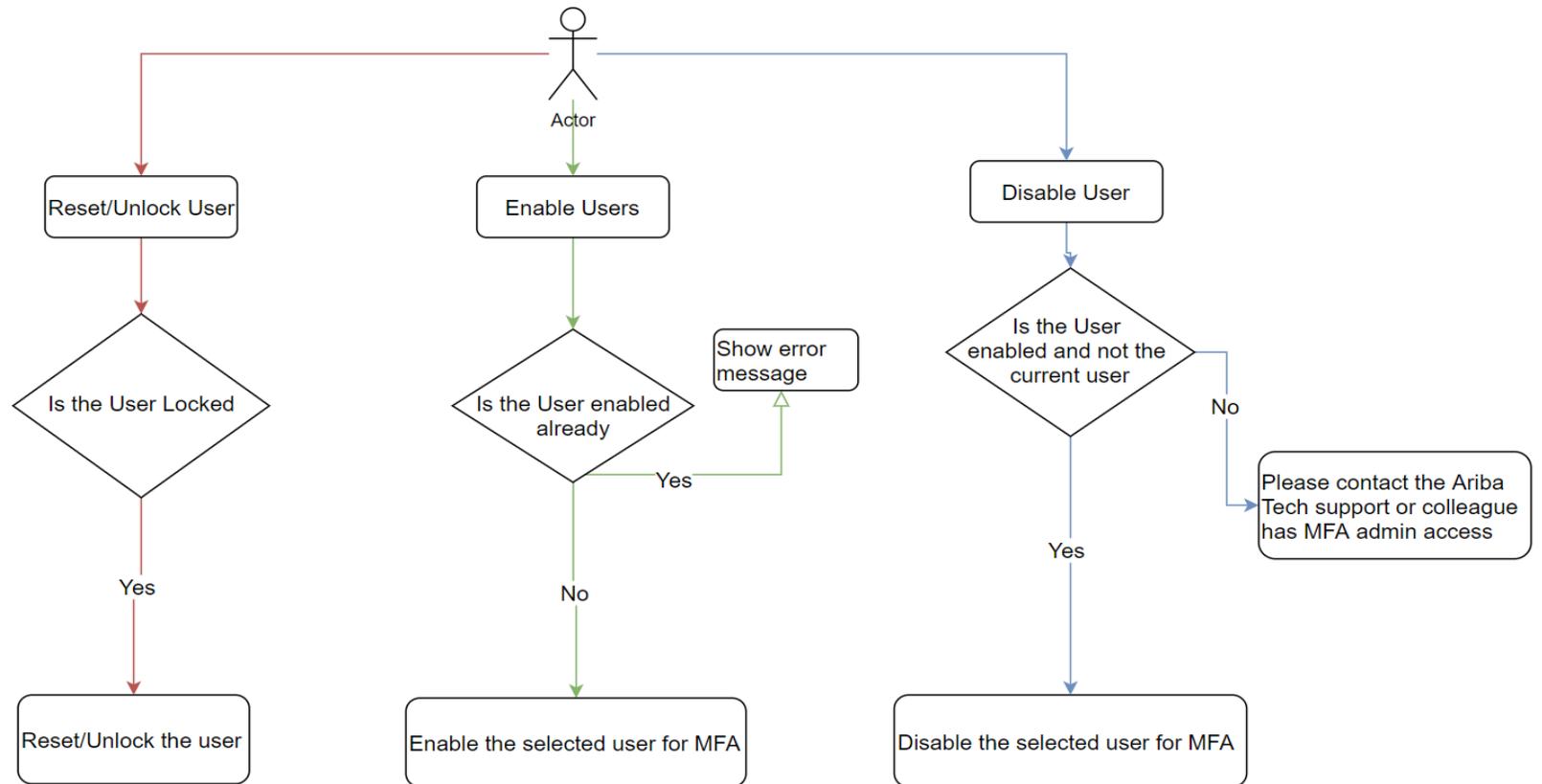
SAP Ariba, Inc. Administrator

機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - 管理者: MFA プロセスフロー

- 対象: 管理者 (顧客管理者)
- MFA 管理フロー:
 - 有効化
 - 無効化
 - リセット
 - ロック解除



機能の概要

説明: 多要素認証による SAP Ariba ソリューションへのユーザーログイン

機能の詳細情報 - 管理者: グループレベルでの有効化/無効化

