



SAP Ariba 

Feature at a Glance

Two factor authentication support for Ariba Network

Sildy Augustine / Sourabh Kothari, SAP Ariba
Target GA: May, 2020

CONFIDENTIAL

Feature at a Glance

Ease of implementation  Low touch / simple
Geographic relevance  Global

Introducing: Two factor authentication support for Ariba Network

Customer challenge

Today, Ariba Network does not support multi-factor authentication.

For sensitive areas like remittance address changes or password changes, customer IT departments require their users to have the option to have an additional factor for authentication.

Meet that challenge with SAP Ariba

Ariba Network with this feature will support two factor authentication for Buyer and Supplier users.

This feature requires users to enter the 2nd factor authentication to make changes to certain areas such as change of password or remittance details.

Experience key benefits

The introduction of two factor authentication for Ariba Network access prevents unauthorized changes in situations where the first factor (i.e. password) may have been compromised.

Solution area

Ariba Network

Implementation information

This feature is automatically on for all customers with the applicable solutions but requires **customer configuration** by Buyer/Supplier admin users to activate it for the users within organization.

Prerequisites and Restrictions

When the two-factor authentication is enabled for an organization, all users must install any one of the SAP Ariba certified authenticator tools to generate the TOTP.

Feature at a Glance

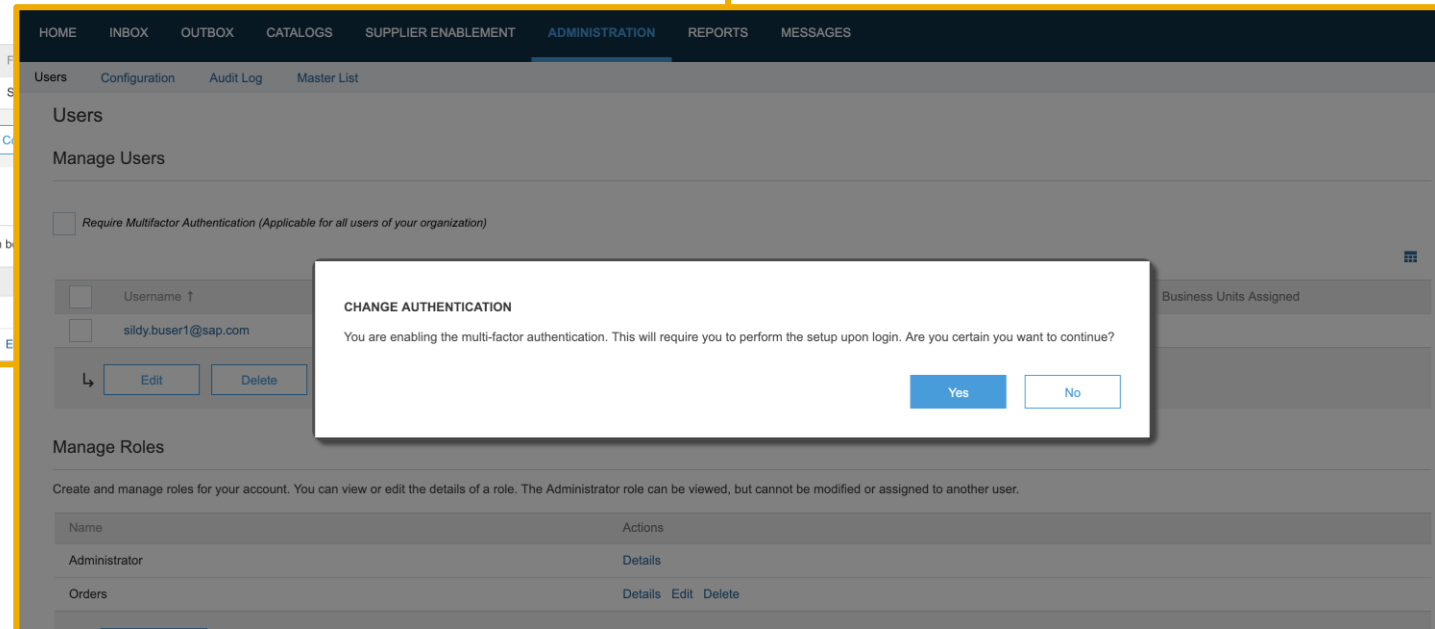
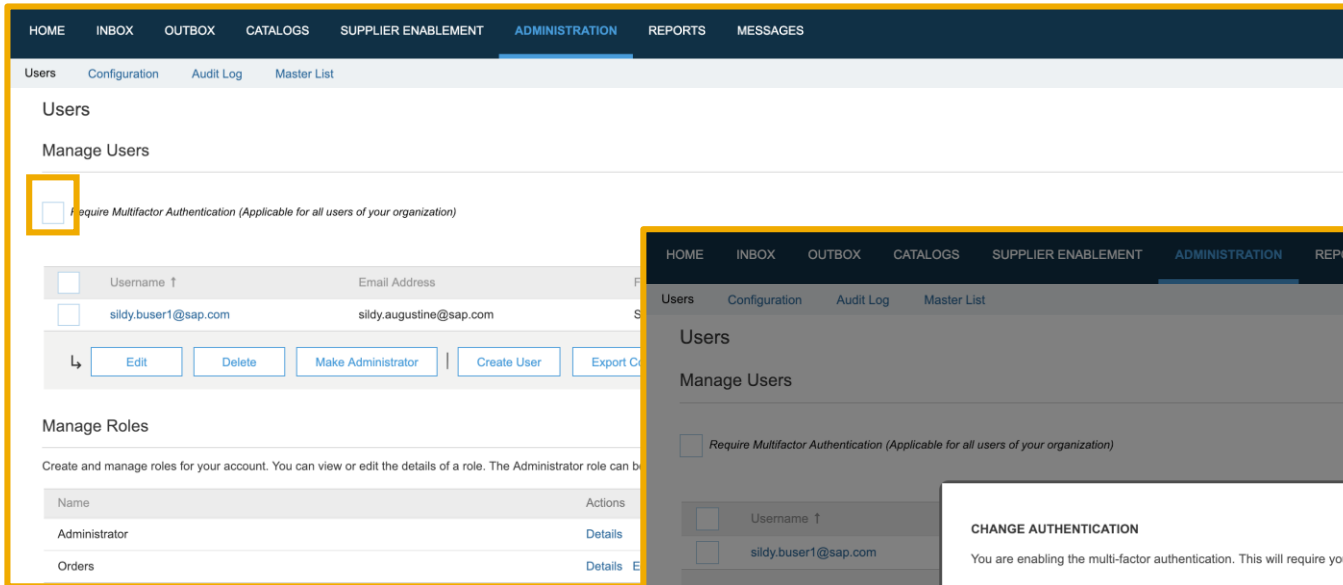
Introducing: **Two factor authentication support with Ariba Network**

- Buyer and supplier administrators enable this feature for their users. The administrators may also disable the configuration.
- Once the administrators enable the feature for active users, an email is sent to the users with instructions.
- Users are prompted at the time of login if their admins have enabled the requirement for an additional factor.
- Two factor authentication is not mandatory for login but is required for key profile and configuration changes.
- Administrators may set up the two factor authentication (2FA) on login or skip it and later configure it in their account settings.
- Buyers may see a report that shows which of the suppliers have enabled the 2FA feature.

Feature at a Glance

Introducing: Two factor authentication support for Ariba Network

A setting is now available in the Administration section for Admin users to activate multifactor authentication for users in their organization.






Feature at a Glance


Introducing: **Two factor authentication support for Ariba Network**

Once the feature is enabled by admins, the users will get the mail as below with instructions.

--- Ariba Internal Testing ---Two factor authentication enabled

 Ariba Commerce Cloud <ordersender-dev3@ansmtp.lab1.ariba.com>
To  Augustine, Sildy

 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 points to the correct file and location.

Two-factor Authentication

Hi Sildy Augustine1,

Your administrator has turned on two-factor authentication. This does not affect your log in into Ariba Network. Once you successfully log in, you will be shown instructions to set up two-factor authentication. The second factor will be required when you change your password or access certain secure sections of the site. It is highly recommended that you set up this feature. For questions on why two-factor was activated, please contact your company administrator.

Sincerely,
The Ariba Network Team
<http://www.ariba.com>

Feature at a Glance

Introducing: **Two factor authentication support for Ariba Network**

If enabled, after login the user is prompted to setup their second factor. It is recommended to use SAP Authenticator. Users can scan the QR code and enter the verification code for the setup.

Users can skip this step and access the setup link in their profile if desired.

It is important for users to complete this setup to ensure that they may reset or change their password.

Enable Multi-factor Authentication


Your organization's Ariba Network administrator requires you to set up multi-factor authentication to change passwords and to 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 recommends using SAP Authenticator available at [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:
v4ke rrvd cnq5 nieh 3znn eveg zni7 vq3z

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:*

Feature at a Glance

Introducing: **Two factor authentication support for Ariba Network**

Users may setup two factor authentication on the profile using the below highlighted link before they change the password. This option is available in situations where the setup is not completed during the initial login.

Once it is setup, the below link will not be accessible.

My Account Save Close

Account Settings

* Indicates a required field

Account Information

Username: * ⓘ
[Change Password](#)
[Setup Multi-factor Authentication](#)

Email Address: *

First Name: *

Middle Name:

Last Name: *

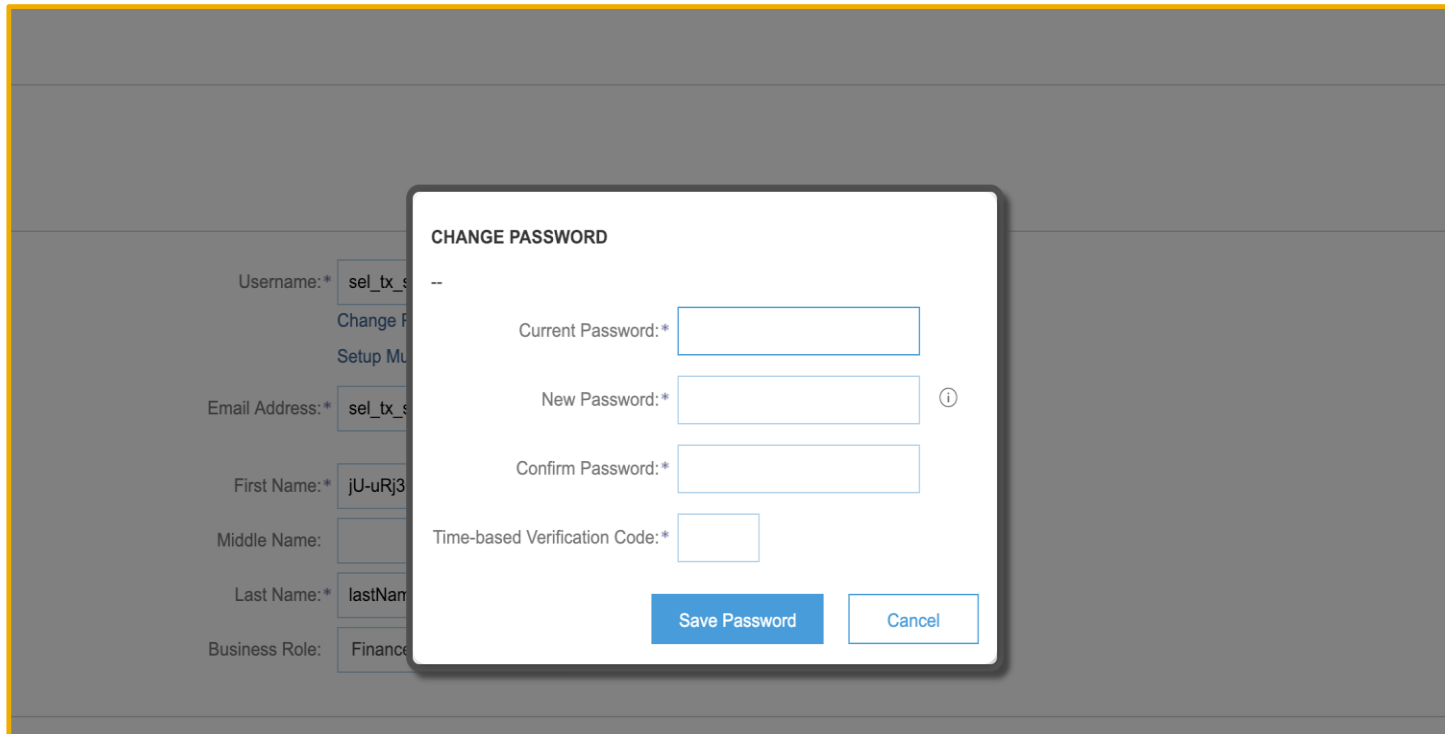
Business Role: ▼

Preferences

Feature at a Glance

Introducing: **Two factor authentication support for Ariba Network**

A change password request, email or phone number change as well as a password reset will require a verification code if the admin has enabled two factor authentication.



The image shows a 'CHANGE PASSWORD' dialog box overlaid on a user management form. The dialog box contains the following fields and buttons:

- CHANGE PASSWORD** (Title)
- Current Password: *
- New Password: * ⓘ
- Confirm Password: *
- Time-based Verification Code: *
- Save Password** (Blue button)
- Cancel** (White button)

The background form is partially visible and includes the following fields:

- Username: * sel_tx_s --
- Change P...
- Setup M...
- Email Address: * sel_tx_s
- First Name: * jU-uRj3
- Middle Name:
- Last Name: * lastNam
- Business Role: Finance

Feature at a Glance

Introducing: **Two factor authentication support for Ariba Network**

Supplier users will be required to provide a verification code for remittance edit, delete or creation once the administrator has enabled second factor authentication.

Ariba Network Company Settings jU-uRj3QcJu5c540c2b...

Create Remittance Address / Payment Info

OK Cancel

Add a remittance address. Indicate your preferred payment method for the new address. Then, enter information for customers about payment methods you support. Review your information carefully, since customers use it to send you payments.

Do not enter personal bank account information. Enter only corporate bank details.

Since your organization has enabled multi-factor authentication, you must enter a valid time-based verification code before you can save any changes.

* Indicates a required field

Remittance Address

Address 1:*

Address 2:

Address 3:

City:*

State:* Alabama

Zip:*

Country:* United States [USA]

Contact: Select contact

Make this address default

Factoring Service ⓘ