



SAP Ariba 

Feature at a Glance

Enabling multi-factor authentication for the SAP Ariba developer portal

Andy Rubinson, SAP Ariba
Target GA: February, 2022

PUBLIC

Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Customer challenge

Currently customer users accounts only require username and password for login, leaving them more susceptible to security breach.

Meet that challenge with SAP Ariba

We've implemented multi-factor authentication (MFA) when authenticating via single sign-on (SSO) from SAP ID Service to the SAP Ariba developer portal.

With the implementation of MFA, authentication to the developer portal is performed exclusively via SSO, eliminating the ability to enter username/password credentials.

SAP Ariba customer organization admin users seeking to add, edit, and delete users do so via the user management link available on the portal.

Experience key benefits

Users logging into the Developer Portal must now use two factor authentication, creating an additional layer of security, reducing the risk of unauthorized access.

Solution area

SAP Ariba developer portal
SAP Ariba APIs

Implementation information

This feature is **automatically on** for all customers with the applicable solutions and is ready for immediate use

End users will need to configure time-based, one-time passwords (TOTP) via accounts.sap.com.

Prerequisites and Restrictions

To authenticate users to the SAP Ariba developer portal using MFA via SSO, the organization and its users must be SSO-enabled. The first time you try to log in using SSO, you will be asked to enable your organization and users for SSO authentication

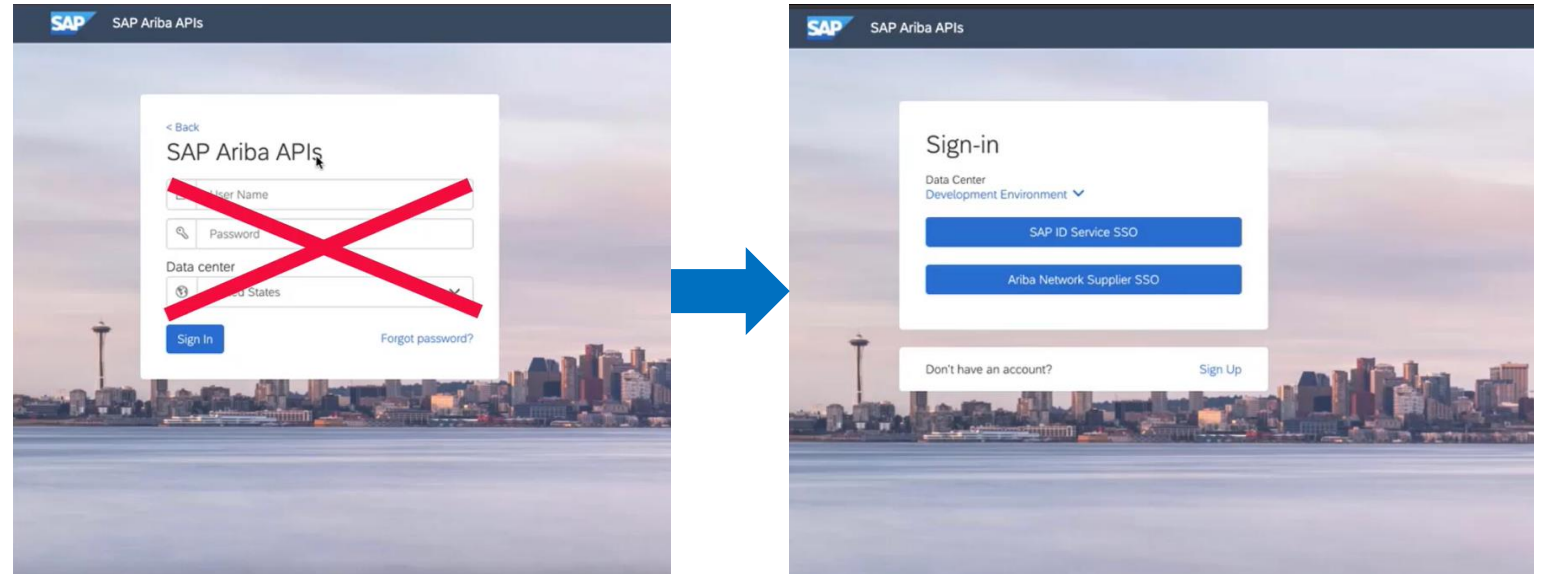
Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Overview

The login method of user name and password is being replaced by single sign on (SSO).

- Only SSO will be supported going forward, with no option to enter a user ID and password.
- Outside the US Data Center, there will only be an option for SAP ID Service SSO.
- Multi-factor authentication was released for Ariba Network in the Feb 2021 release. Please refer to that [Feature at a Glance](#) document for details.



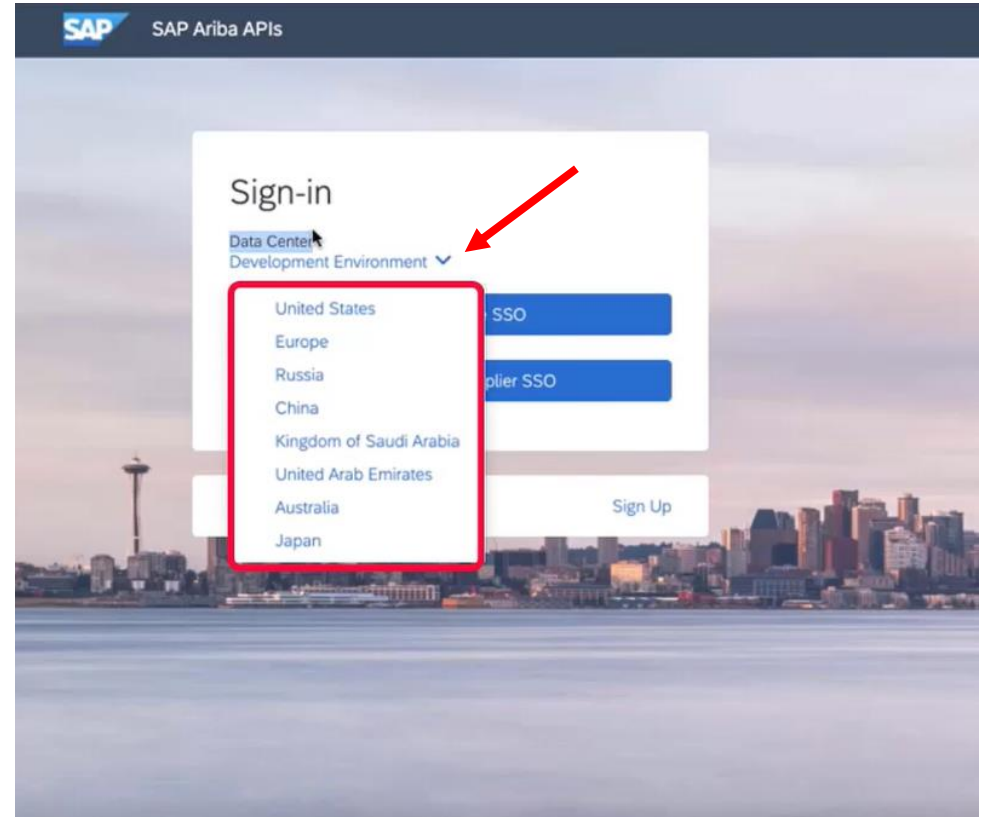
Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Overview

The login method of username and password is being replaced by single sign on (SSO).

- Users can select the appropriate data center by clicking on the dropdown list using the arrow for the environment menu.



Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Changing Password

- Users can change their SSO password via accounts.sap.com.
- This can also be accomplished by using the link in the help documentation.

The screenshot shows the 'Profile' and 'Authentication' sections of the SAP Ariba developer portal. The 'Profile' section includes 'Personal Information' (First Name, Phone) and 'Company Information' (Company Country/Region: United States, Company City: Boston). The 'Authentication' section includes 'Biometric Authentication' (with a plus icon) and 'Multi-Factor Authentication' (with sub-sections for TOTP and Web Two-Factor Authentication). Each sub-section contains explanatory text about device activation requirements.

The 'Forgot My Password' form is displayed. It includes the following text: 'If you forgot your password, please enter your credentials below and click 'Send''. Below this is a 'NOTE: If you have multiple user IDs associated with the same e-mail address, then enter the specific user ID that requires the password reset. An e-mail with further instructions will be sent. Note that the e-mail might take a few minutes to reach your inbox.' A link is provided: 'If you know your password and want to change it, please see instructions in the guide [here](#).' The form has an 'E-Mail *' label and a text input field. A '*Required' label is positioned to the right of the input field. A blue 'Send' button is located below the input field. At the bottom, the 'SAP ID Service' logo is on the left, and on the right, there is a link: 'Existing Users | One login for all accounts: [Get SAP Universal ID](#)'.

Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Initial login

The login method of user name and password is being replaced by single sign on.

- On the first login, users will enter their SAP ID or email and be redirected to the SAP Universal ID Account Manager and asked to enter their password.

The diagram illustrates the initial login process. It starts with the 'SAP Developer Portal - QA Cobalt' page, which has a 'Log On' section. This section contains a text input field for 'E-Mail, ID, or Login Name' and a 'Continue' button. A red box highlights this 'Log On' section. An arrow points from the 'Continue' button to the 'SAP ID Service' page. This page features the SAP logo and the text 'Universal ID'. Below this is a user icon placeholder. The text 'Sign in to SAP Universal ID Account Manager' is displayed, followed by the email address 'atlderek@gmail.com'. A red box highlights the 'Password' input field and the 'Sign in' button on this page. A 'Forgot password?' link is located at the bottom of the page.

Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

Two Factor Authentication Setup

Setup of Two-Factor Authentication must be enabled to proceed.

- In order to enable, the SAP Authenticator application is required.
- Links to the app on [Apple Store](#) and [Google Play](#) are shown on the page.
- Launch the app and scan the QR code (1).
- Then enter the passcode shown in the app and click continue (2).
- The user will be directed back to the developer portal and logged in.

Two-Factor Authentication

The SAP Developer Portal - QA Cobalt application requires a time-based one-time passcode as a second factor for authentication. You need to activate a mobile device to generate passcodes. No devices are currently activated.


✔ SAP Authenticator is required in order to enable two-factor authentication.

SAP Authenticator is required to enable two-factor authentication and to scan the QR code on your device. The iOS version is available in the [Apple App Store \(SM\)](#). The Android version is available in [Google Play \(TM\)](#).

Apple and iTunes are trademarks of Apple Inc. App Store is a service mark of Apple Inc. Android and Google Play are trademarks of Google Inc.

1 Scan QR Code

Your Secret Key



2 Enter passcode

E-Mail, ID, or Login Name
atderek@gmail.com

Passcode *

*Required

Continue

SAP® ID Service

Existing Users | One login for all accounts:
[Get SAP Universal ID](#)

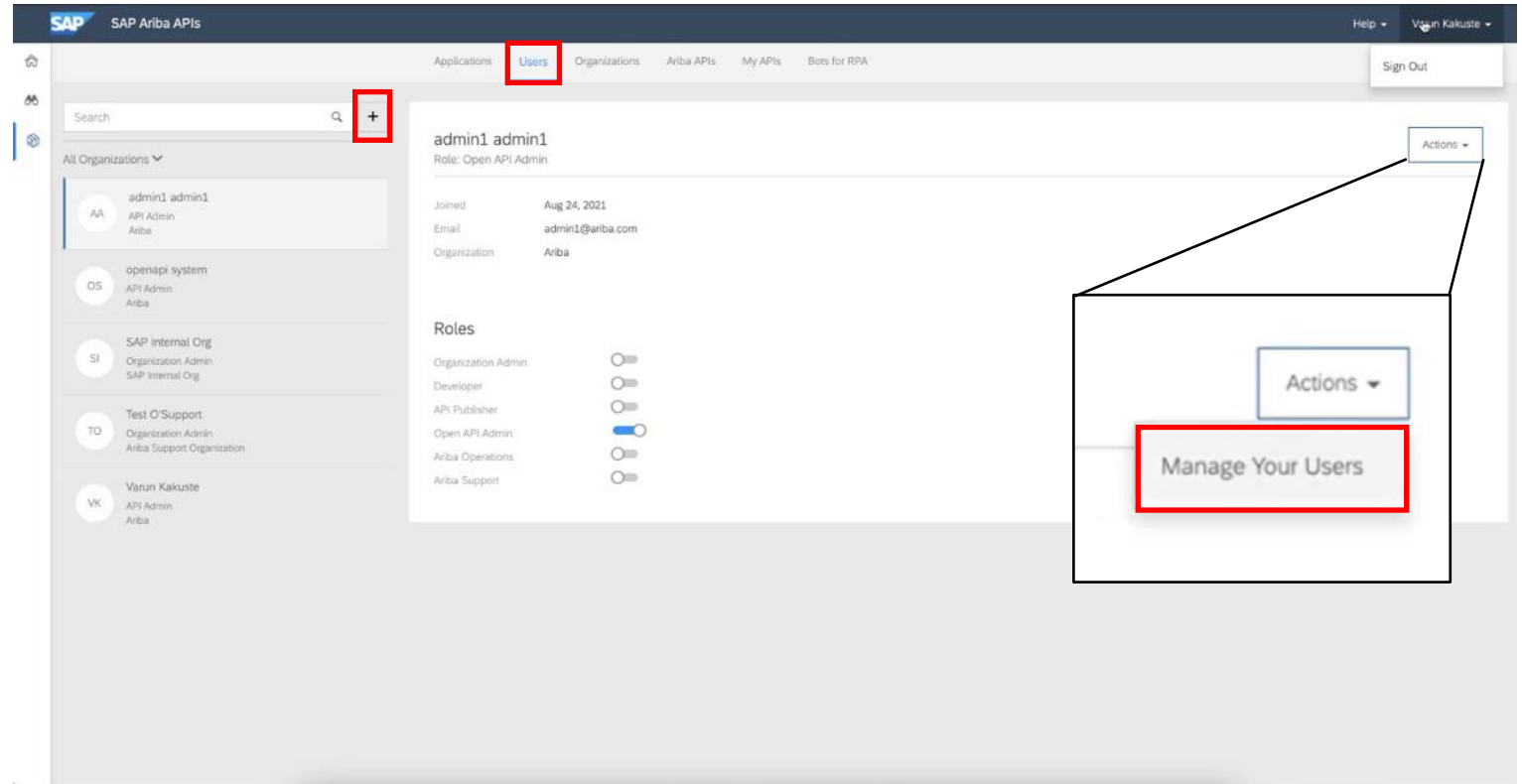
Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

User Administration

The Users tab allows for user administration.

- Users can be added by clicking the plus icon (+), or clicking the **Actions** menu and selecting **Manage Your Users**.
- User roles may be assigned, including:
 - Organization Admin
 - Developer
 - API Publisher
 - Open API Admin
 - Ariba Operations
 - Ariba Support



Feature at a Glance

Introducing: Enabling multi-factor authentication for the SAP Ariba developer portal

User Administration

- Users can be added by clicking the plus icon (+) or clicking the **Actions** menu and selecting **Manage Your Users**.
- User roles may be assigned, including:
 - Organization Admin
 - Developer
 - API Publisher
 - Open API Admin
 - Ariba Operations
 - Ariba Support
- Both options will bring you to the **User Management** page on SAP Launchpad, shown here.

