Activation of JAGGAER Supplier Identity Management & Multi-Factor Authentication

Announcement: To improve security, your supplier user account will be upgraded to a JAGGAER Supplier Identity Management (IDM) account, and Multi-Factor-Authentication will be activated. This document outlines the changes supplier users will experience when using the JAGGAER solution, once Supplier IDM has been activated.

Who is JAGGAER?

JAGGAER is a global leader in enterprise procurement and supplier collaboration, and the procurement platform of choice for your customer(s).
To learn more, visit: https://www.jaggaer.com/.

What is JAGGAER Supplier Identity Management?

Supplier Identity Management (IDM) is JAGGAER'S solution for creating, maintaining and managing the **supplier users' digital identities.** Suppliers can easily authenticate to all JAGGAER modules and any integrated external applications using a **single set of credentials**, while reducing the risk of fraud via **Multi-Factor Authentication**.

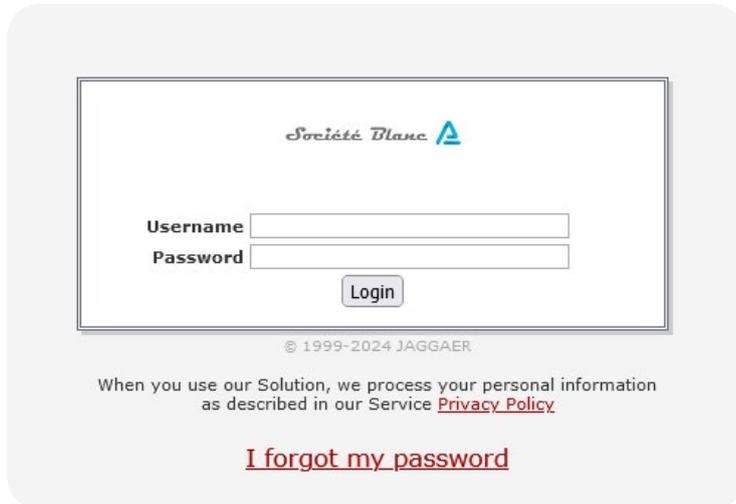## What is 2-factor (or multi-factor) authentication (2FA, MFA)?

With the activation of JAGGAER Supplier IDM, supplier users will go through a 2-step verification process when they access their account: in the first step, you will have to provide your e-mail address and password, and in the second step, you will have to provide a one-time password that is generated automatically for you and sent to you using a method of your choice: your email address or a mobile authenticator application.

NOTE: Some customers may provide only one of the methods. JAGGAER may add other MFA methods of verification in the future.

Summary of Changes

Current login page

Supplier users currently use this option to log in to JAGGAER with a username and password they created:

Future login page

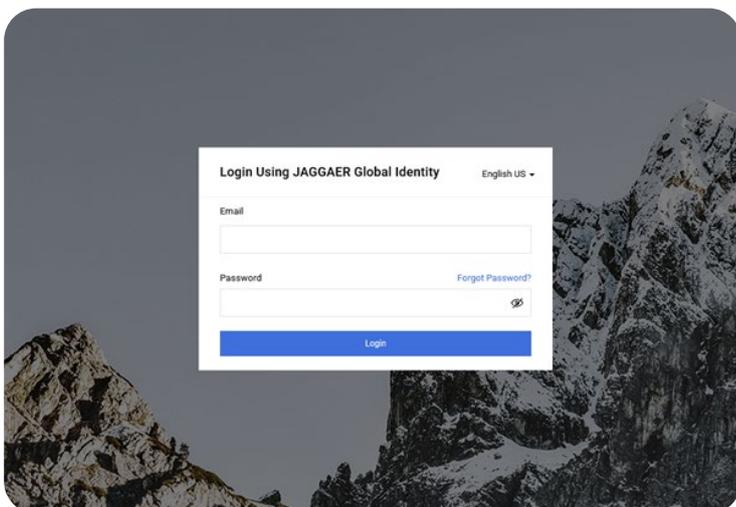After activation of JAGGAER Supplier Identity Management, supplier users will login with their e-mail address and a new password, as well as a one-time code that will be sent via a verification method of their choice (either their e-mail address or a mobile authenticator app):

NOTE: The login page may look differently, depending on the customer's configuration, but the behavior should be the same.

Instructions for setting up JAGGAER Supplier Identity Management and Multi-Factor Authentication

Before you begin

Please ensure your supplier user account complies with the following best practices:

1. The e-mail address used in the JAGGAER solution should ideally belong to a single person (e.g. john.doe@acme.com instead of contact@acme.com), since any sensitive email communication about credentials (password reset, one-time codes for authentication, etc.) will be sent to this address.

2. If additional colleagues need to be involved in the collaboration with your customer, it is recommended to create a supplier user account for each person, instead of sharing the same account.

3. Do not ignore any e-mail communication coming directly from JAGGAER, since information about the supplier's credentials will be sent directly by JAGGAER (i.e., not in the customer's name).

4. Please check the Spam or Junk folders of your inbox and make sure these e-mails are not blocked by any firewalls in your company's network.

Upgrading your existing credentials to the new JAGGAER Supplier Identity Management (IDM) credentials.

1. Navigate to your customer's Supplier Portal. (typically, the address follows this pattern: app11.jaggaer.com/portals/{customer_name}, but the URL may vary, depending on your customer's setup)

2. If this is the first time you are accessing your customer's supplier portal after the activation of JAGGAER Supplier Identity Management, you need to click on the "Forgot Password" page, in order to define a new password.

JAGGAER

3. On the "Forgot Password" page, enter the e-mail address associated with your JAGGAER account and click Submit:
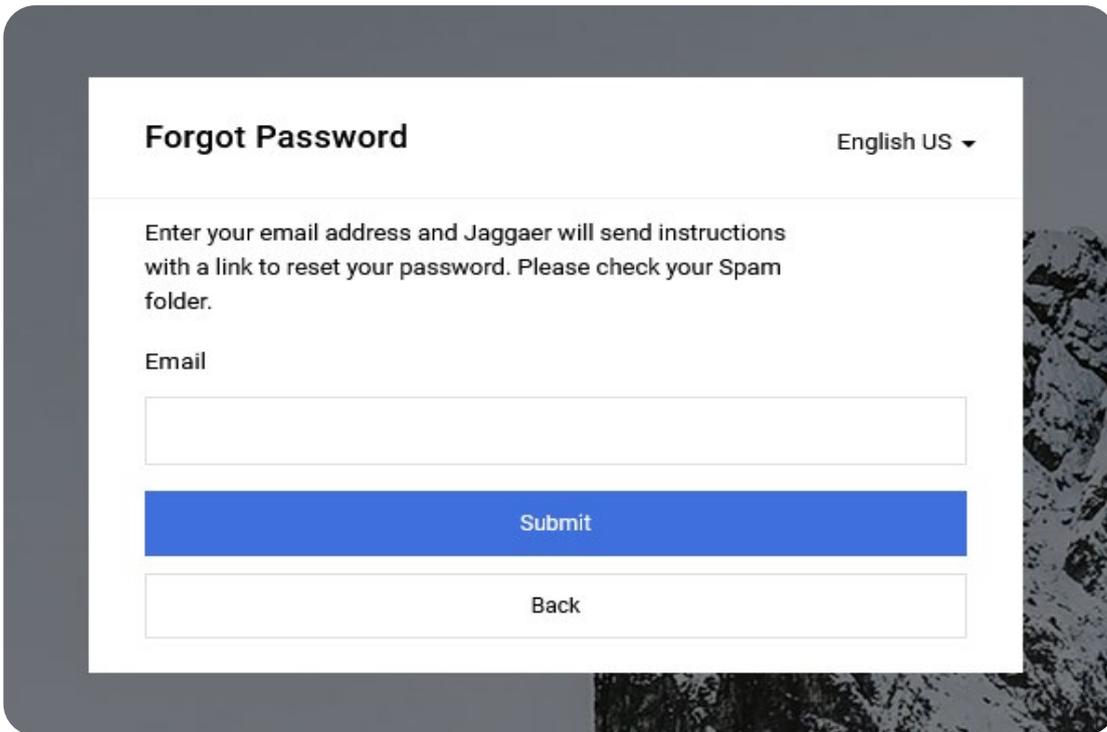
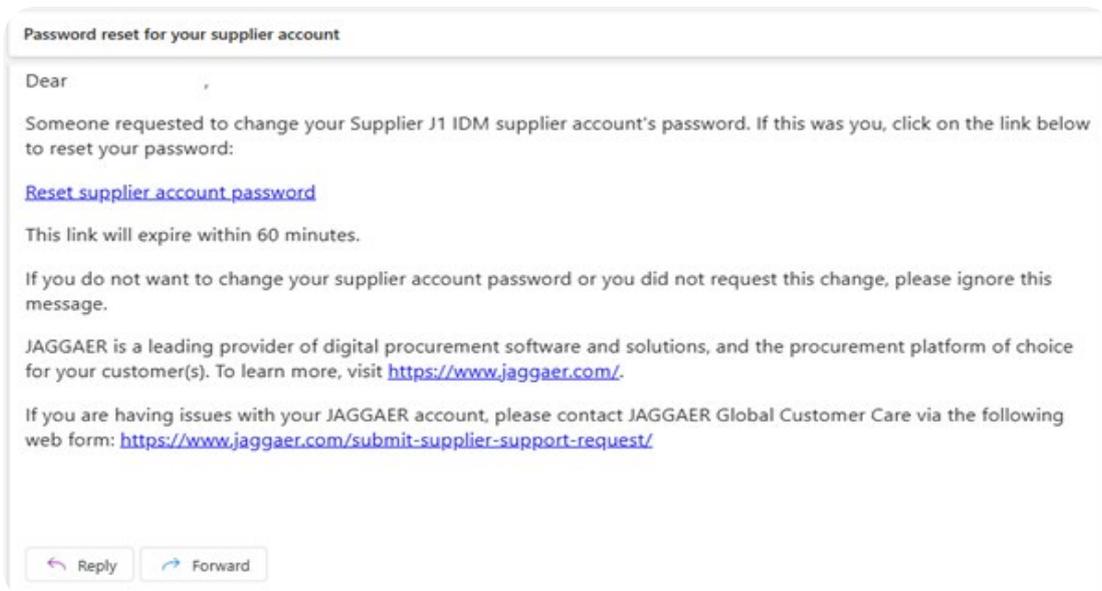4. Go to your e-mail inbox and search for an email message from JAGGAER with the subject line "Password reset for your supplier account":

5. In the e-mail, click on the link labeled "Reset supplier account password".
    NOTE: The subject or the contents of the e-mail may be different for your customer.

JAGGAER

6. You will be required to change your password. Please enter a password that meets the requirements on the screen:
   - a. Minimum of 12 characters
   - b. Minimum of 1 uppercase letter
   - c. Minimum of 1 lowercase letter
   - d. Minimum of 1 special character.
   - e. Minimum of 1 number
   - f. Email must be different from password

NOTE: The password rules for your customer may be different. Please follow the instructions on the screen.

7. Select "Set Password" when done.

8. You will see a confirmation message that the upgrade was successful:

You have now successfully upgraded your credentials, and you can start using them on your customer portal.

NOTE: Please note that your username will change to your e-mail address (i.e. jdoe@acme.com instead of john_doe). For specific customer setups, your username may remain unchanged. If you are unsure about your username, please ask your customer representative.

Using Multi-Factor Authentication

The new JAGGAER authentication uses a 2-step verification process, which relies on a one-time code that is valid for 20 minutes. You can use either e-mail or an authenticator mobile application as the method of receiving the one-time code, with e-mail being the default.
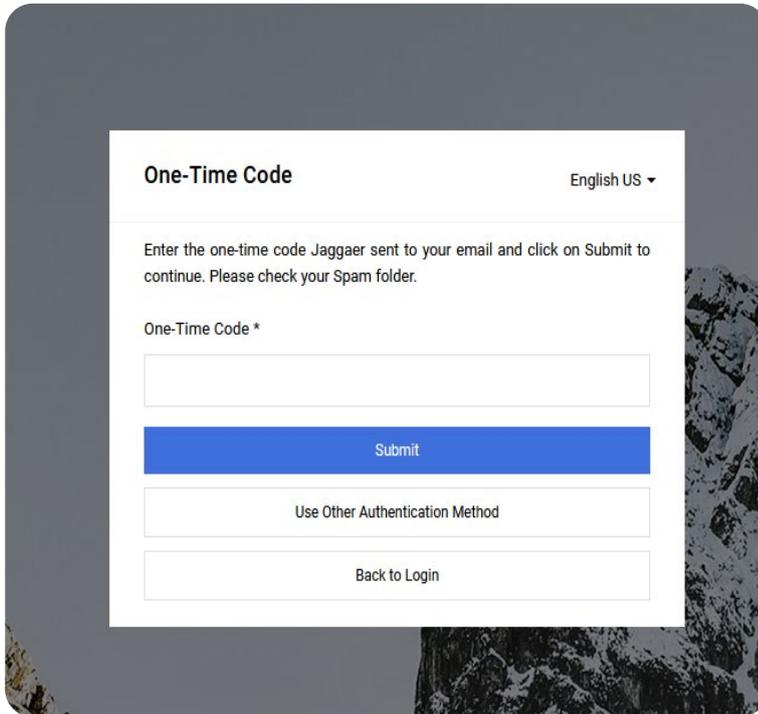**NOTE:** Your customer may provide only one of the methods above for Multi-Factor Authentication.

1. If using e-mail (the default), go to your inbox and look for an e-mail with the subject line "Verification code for supplier authentication". Please make sure you also check your Spam or Junk e-mail folders. Below is a sample e-mail:
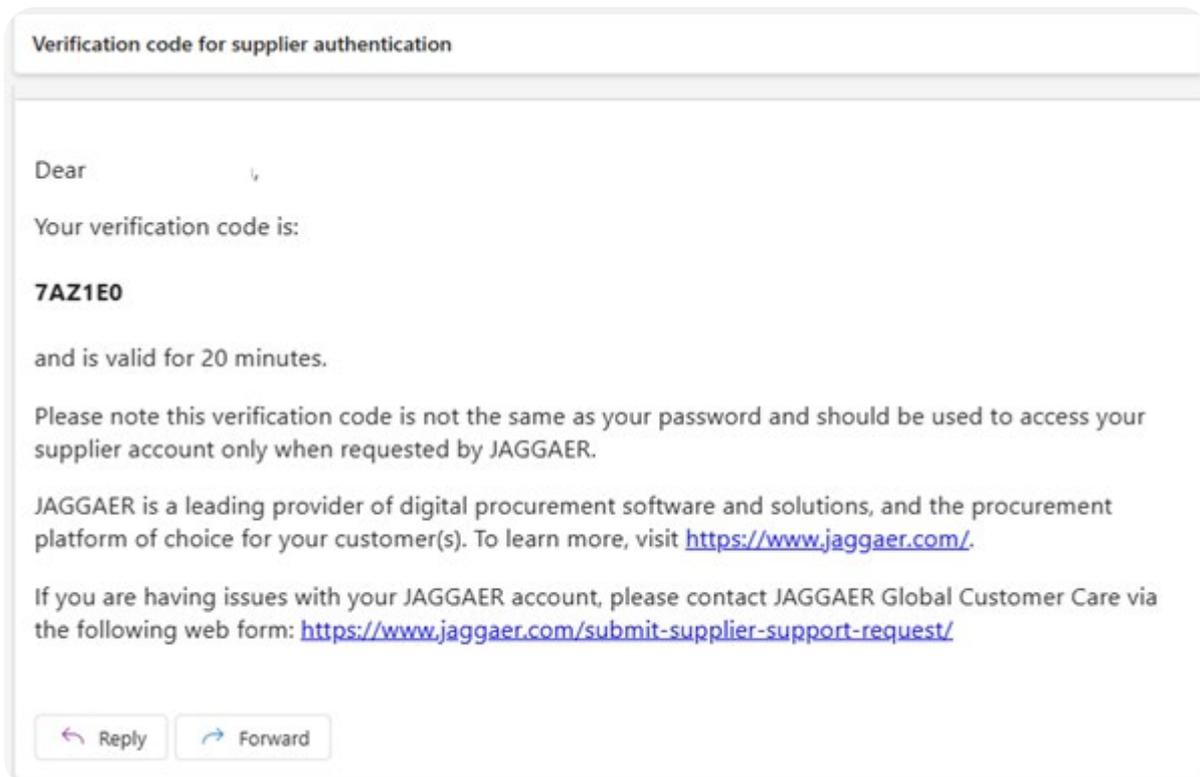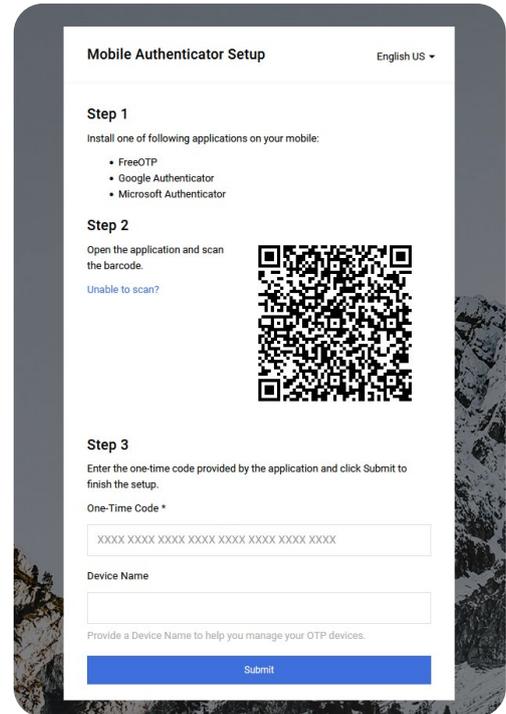

NOTE: The subject or the contents of the e-mail may be different for your customer.

2. Enter the verification code from the e-mail message above into the interface below, by either using copy-paste or manually typing the code.

3. If using the mobile authenticator method to receive this code, please make sure Google Authenticator, Microsoft Authenticator or FreeOTP mobile apps are installed on your smart phone.

4. Open any of the the above authenticator apps, and scan the QR code on the screen.

5. Enter the one-time code generated by the authenticator app in the interface below, and click "Submit":

You should now be successfully authenticated to your customer's Supplier Portal. Please note that the one-time code will only be required again when you:

    a. Access the customer portal after more than 10 days of inactivity.
    b. Access the customer portal after loging out.
    c. Access the customer portal from a different device and/or browser.

Need Assistance?

If you are still having trouble setting up your JAGGAER Supplier IDM credentials and/or 2-step verification, please contact JAGGAER Global Customer Care using the following web form: https://www.jaggaer.com/submit-supplier-support-request/

JAGGAER