Multifactor Authentication

Multifactor authentication is a two-step verification process where you are required to authenticate yourself a second time using a time-based verification code. As compared to the single step authentication process, the multifactor authentication process provides enhanced security.

If multifactor authentication is enabled for critical fields, you are required to perform the two-step verification process while attempting to update the values of critical fields such as email addresses, phone numbers, remittance information and so on. With multifactor authentication enabled for login, you are required to perform the two-step verification process to log in to SAP Business Network.

SAP Business Network administrators can now enable the following functionalities for users in their organization by selecting the desired users from a table:

- Require multi-factor authentication for critical fields
- Require multi-factor authentication for login

Note

- Only supplier administrators with the required permissions can disable multifactor authentication for login.
- SAP Business Network does not prompt newly created users to complete the multifactor authentication setup immediately after a successful login. New users are recommended to set up multifactor authentication for login after they change their initial password.

Prerequisites

When multifactor authentication is enabled for your organization, you must install an authenticator application such as SAP Authenticator from iTunes (for iOS devices) or from Google Play (for Android devices) in your hand-held devices to generate a time-based verification code (also called time-based one-time password). The time-based verification code setup is also compatible with third-party authenticators such as Google Authenticator or Microsoft Authenticator.

Enabling Multifactor Authentication for Login
Configuring Multifactor Authentication Settings
Managing Multifactor Authentication for Users
Setting Up Multifactor Authentication (Supplier User)
Setting Up Multifactor Authentication Using a New Device (Supplier User)

Enabling Multifactor Authentication for Login

For additional security, the supplier administrator can enable multifactor authentication for select users.

Procedure

1. Click the Account Settings icon, and choose Settings > Users.
2. Click Manage User Authentication.

The **Multi-factor Authentication User Setup** page is displayed.

3. Select the box **Require multi-factor authentication for login**.
4. Click **Yes** in the dialog box that appears.
5. Select the desired users by checking the boxes against their user names from the table, and click **Enable**.

> **Note**
>
> **Only the selected users are enabled for "multifactor authentication for login." If you do not select any user from the table, none of the users in your organization will be enabled for multifactor authentication.**

Configuring Multifactor Authentication Settings

The supplier administrator can configure multifactor authentication for an SAP Ariba account.

Procedure

1. Click the **Account Settings** icon, and choose **Settings** > **Users**.
2. Click **Manage User Authentication**.
3. Click **Configure MFA Settings**.

   The **Configure Multi-factor Authentication Settings** page appears.
4. Enter a value in the **Time allowed to skip multi-factor authentication setup** box.

   This field specifies the maximum number of days the user can skip the multifactor authentication setup when an administrator has enabled it for that user. The default value is 5 days.
5. Enter a value in the **Number of invalid multi-factor authentication attempts allowed** box.

   This field specifies the maximum number of invalid multifactor authentication attempts that the user can make. The default value is 5 attempts. After the number of invalid attempts specified in this field, the user account is locked. It can be unlocked only by an administrator.
6. Enter a value in the **Retry period for locked out users** box.
   - After the number of minutes (the default value is 120 minutes) specified in this field, the user account is automatically unlocked and can be re-used.
   - If the user gets locked a second time, the default value becomes 240 minutes, and the user is unlocked only after 240 minutes.
   - If the user gets locked a third time, the user account is locked for good, and can be unlocked only by an administrator.

   > **Note**
   >
   > Users can contact their administrator at any time during this period to get their account unlocked.

7. Select the **Enable the Remember me option** check box.

   This checkbox (unchecked by default) specifies if users can choose the Remember me option for multifactor authentication in the one-time password input screen. If this box is checked, an input box **Remember device for** is displayed.
8. Enter a value in the **Remember device for** box.

   This field specifies the maximum number of days the user's device and browser will be remembered, during which they will not be prompted for the multifactor authentication passcode during login. The default value is 5 days.
9. Click **Save**.

Managing Multifactor Authentication for Users

The supplier administrator can help manage multifactor authentication for users.

Procedure

1. Click the Account Settings icon, and choose Settings > Users.
2. Click Manage User Authentication.
3. Select the desired multifactor authentication check boxes.
4. Select the users (from the table) for which you want to manage multifactor authentication.
5. Click the following buttons depending on what you wish to do:
    - Enable: Enables multifactor authentication for the selected users.
    - Disable: Disables multifactor authentication for the selected users.
    - Reset: Resets multifactor authentication for the selected users. These users must either enter the secure key displayed on the user interface, or scan a new QR code during their next login session.
    - Send Email Reminder: Sends a reminder email to the selected users.
    - Unlock: Unlocks the selected users.
6. Click Save.

Setting Up Multifactor Authentication (Supplier User)

You can set up multifactor authentication after your SAP Business Network administrator has enabled the feature.

Procedure

1. Click the Account Settings icon, and choose My Account.

   The My Account page appears.

2. Below the Username text box, click the Set up multi-factor authentication link.

   The Set up Multi-factor Authentication page appears.

3. Download and install SAP Authenticator or any compatible authenticator application such as Google Authenticator or Microsoft Authenticator on your hand-held device.
4. Open the authenticator application that you have installed on your mobile device and do either one of the following:

a. Scan the QR code displayed on the page, and enter the code in the Time-based Verification Code input box, **or**

b. Enter the secure key displayed on the page in the Time-based Verification Code input box.

5. Click Done.

Setting Up Multifactor Authentication Using a New Device (Supplier User)

When you change your mobile device, you can reset the multifactor authentication that had been configured using your old device. Using the verification code from the old device, you can set up multifactor authentication on your new device.

Procedure

1. Click the **Account Settings** icon, and choose **My Account**.
2. Below the **Username** text box, click the **Reset multi-factor authentication** link.
3. Enter the verification code from your old mobile device.
4. Set up multifactor authentication again, using a new QR code on your new mobile device.
5. Click **Done**.