



**SAP Fieldglass** 

**PUBLIC**

SAP Fieldglass

2025-10-31

# **SAP Fieldglass Two-Factor Authentication Configuration Guide**

# Content

- 1     **SAP Fieldglass Two-Factor Authentication Configuration Guide. . . . . 3**
- 2     **Enabling Two-Factor Authentication. . . . . 4**
- 2.1   Configurable Parameters. . . . . 5

# 1 SAP Fieldglass Two-Factor Authentication Configuration Guide

Provides an overview of SAP Fieldglass two-factor authentication security.

Two-factor authentication standards mandate that a system require a user to provide two means of authenticating themselves before they gain access to the system. SAP Fieldglass requires one authentication: a username and password. In certain cases, a buyer's business process may dictate two-factor authentication for certain users.

Two-factor authentication methodologies generally require a user to use information from:

1. Something the user knows, such as username/password, passcode, or answer to a question.
2. Something the user has, such as a phone, a device, or an email.

SAP Fieldglass two-factor authentication will require a user to enter:

1. The user's username and password, and
2. A onetime passcode that is emailed to the email address on the user's SAP Fieldglass user profile. This passcode is emailed after the user successfully enters their username and password, and is entered on a secondary authentication page that displays for the user.

Administrators are always required to use two-factor authentication if the company is enabled for two-factor. Other users must use two-factor authentication if their roles are configured for *require\_two\_factor\_auth\_flag*.

## Considerations

- If a user accesses SAP Fieldglass using single sign on, the user will be directed to the secondary authentication page and must enter their passcode before being granted access.
- The method of using a onetime passcode is referred to as TOTP, or Time based One Time Passcode. Purely from a usability and ease of use perspective, SAP Fieldglass has relaxed the onetime usage restriction and allows the same passcode to be leveraged for up to eight hours. The system will only generate and require a new passcode if it is eight or more hours since the last time a passcode was generated for the user.

## Related Information

[Enabling Two-Factor Authentication \[page 4\]](#)

[Configurable Parameters \[page 5\]](#)

## 2 Enabling Two-Factor Authentication

Describes how to enable two-factor authentication for a buyer or supplier company, selected roles, and workers.

Two-factor authentication can be enabled for either SSO or password authentication.

### Enabling for a Buyer or Supplier Company

To enable two-factor authentication for a buyer or supplier company:

1. Select the [Edit Configuration](#) link for a buyer or supplier company.
2. In the [Company Configuration](#) section, select the appropriate option(s):
  - [2-factor authentication for all users](#): Select this option if you want every user—regardless of how they sign in (SSO, username/password, or both)—to be required to use two-factor authentication.
  - [2-factor authentication for SSO or both \(SSO and username/password\)](#): Select this option if you want users who sign in using SSO or a combination of SSO and username/password to use two-factor authentication. Users who sign in using only username and password will not be required to use two-factor authentication.
  - [2-factor authentication for username/password](#): Select this option if you want users who sign in using only a username and password to be required to use two-factor authentication.
3. After entering a reason for the change, select [Save](#).

### Enabling for Select Roles

Two-factor authentication can be enabled for select roles, but not through Company Configuration.

SAP Fieldglass will set the [require\\_two\\_factor\\_auth\\_flag](#) for each of the customer's applicable roles.

### Enabling for Workers

To enable two-factor authentication for a worker:

1. Select the [Edit Configuration](#) link for the company.
2. In the [Worker](#) section, select the [2 factor authentication for workers](#) configuration.
3. After entering a reason for the change, select [Save](#).

#### Note

In the event a worker works for more than one company, if at least one company has two-factor authentication enabled for workers, the worker will always have to use two-factor authentication.

## Related Information

[Configurable Parameters \[page 5\]](#)

## 2.1 Configurable Parameters

The following CompanySysEnv variables can be used.

CompanySysEnv Parameters



Parameter	Description	Default
TWO_FACTOR_AUTH_PASSWORD_LEN	The length of the one-time-password to be generated.	6 alphanumeric characters
TWO_FACTOR_AUTH_TTL_HOURS	If not zero, do "two-factor" for every login.	By default (0), only do "two-factor" every 12 hours, or set by "TWO_FACTOR_AUTH_TTL_HOURS"
TWO_FACTOR_AUTH_PASSWORD_POLICY	If not zero, do "two-factor" for every login.	By default (0), only do "two-factor" every 12 hours, or set by "TWO_FACTOR_AUTH_TTL_HOURS"
TWO_FACTOR_AUTH_EMAIL_SUBJECT	If not zero, do "two-factor" for every login.	Password to complete your required secondary authentication
TWO_FACTOR_AUTH_EMAIL_BODY	The body text of the email.	Please enter the following password to complete your required secondary authentication: #oneTimePassword#

# Important Disclaimers and Legal Information

## Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

## Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

## Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

## Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

## Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.



© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.

**Material Number: 2019-04-09**

