Shared: SAP Concur Password Policy Settings

Setup Guide

Last Updated: November 15, 2023

Applies to these SAP Concur solutions:

- ☒ Expense
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Travel
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Invoice
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Request
  - ☒ Professional/Premium edition
  - ☒ Standard edition

Table of Contents

Revision History

Date	Notes/Comments/Changes
November 15, 2023	Removed phase 1 information.
November 9, 2023	Added permissions information.
November 3, 2023	New guide.
October 18, 2023	New guide in DRAFT status.

NOTE: Multiple SAP Concur product versions and UI themes are available, so this content might contain images or procedures that do not precisely match your implementation. For example, when SAP Fiori UI themes are implemented, home page navigation is consolidated under the SAP Concur Home menu.

SAP Concur Password Policy Settings

Section 1: Overview

A company administrator can define the password policy for SAP Concur solutions on the **Sign-In Settings** page. The **Sign-In Settings** page enables admins to configure the following requirements and parameters:

- Password length and character requirements
- Password expiration and reset requirements
- Account lockout parameters
- Inactive user session timeout parameters
- First sign in password change requirement
- Visibility of username reset link
- Email Address requirement for 2FA

Until the administrator manually changes the default policy settings through the **Sign-In Settings** page, the default password policy is in effect for their users.

Section 2: Accessing the Sign-In Settings Page

A Concur Administrator with the required permissions can navigate to the **Sign-In Settings** page and configure the login policy for their SAP Concur solutions.

Professional Edition

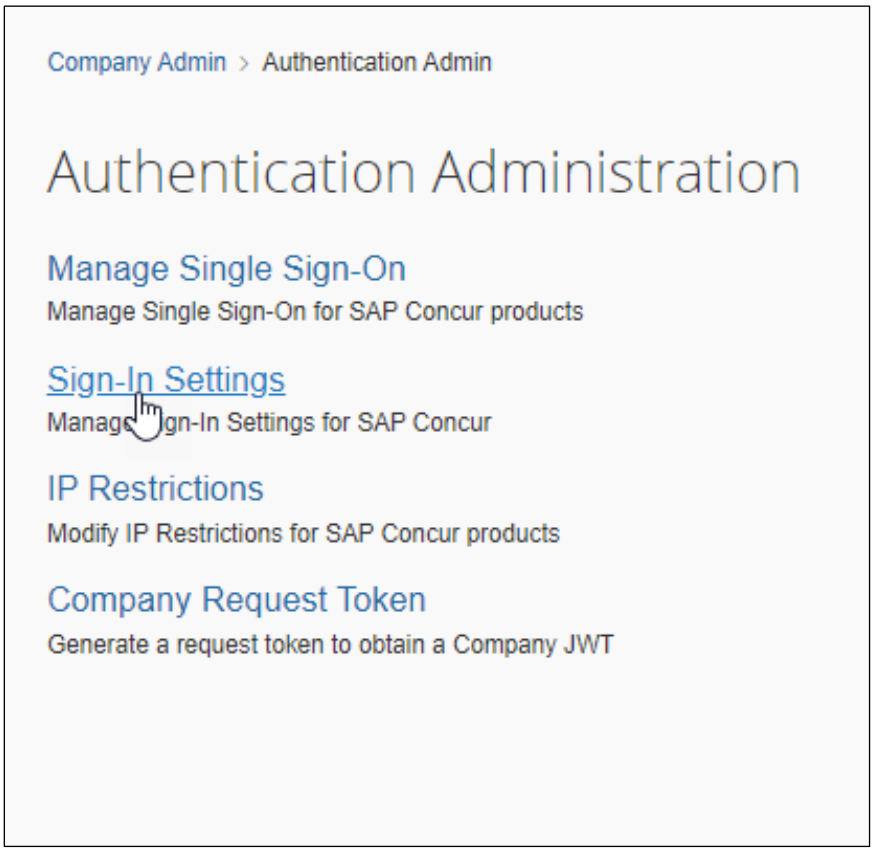
PERMISSIONS

To access **Sign-in Settings** in Professional Edition, a user must have either the **Company Administration** permission or the **Password Manager** permission assigned to them. In Professional Edition, a user with the **Permission Administrator** or **Company Administration** permission can assign the **Password Manager** permission to a user who needs access to **Sign-in Settings**.

ACCESSING SIGN-IN SETTINGS

On the on the **Administration** menu, click **Authentication Admin,** and then click **Sign-In Settings.**

NOTE: The other options available on the **Authentication Administration** page vary depending on your company's configuration.



Standard Edition

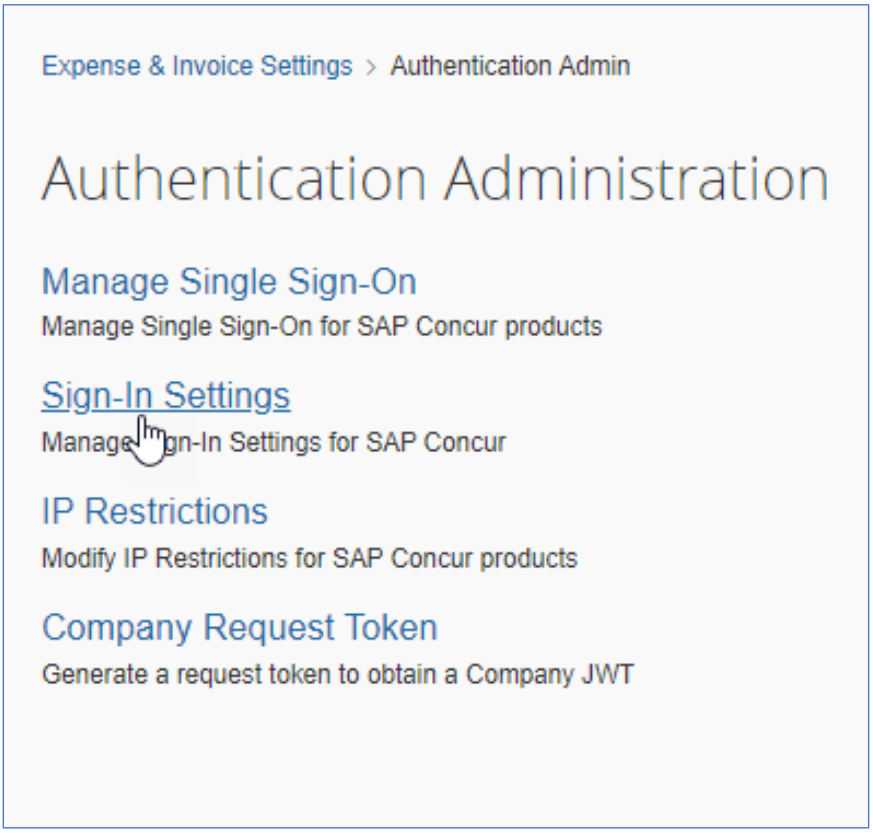
PERMISSIONS

To access the **Sign-In Settings** page in Standard Edition, a user must have the **Can administer**, **Travel-Only administrator**, or **Expense and Travel administrator** check box selected on their user account page. In Standard edition, the client administrator can select **Can administer**, **Travel-Only administrator**, or **Expense and Travel administrator** on the desired user's user account page to enable the user to access **Sign-In Settings**.

NOTE: The other options available on the **Authentication Administration** page vary depending on your company's configuration.

ACCESSING SIGN-IN SETTINGS

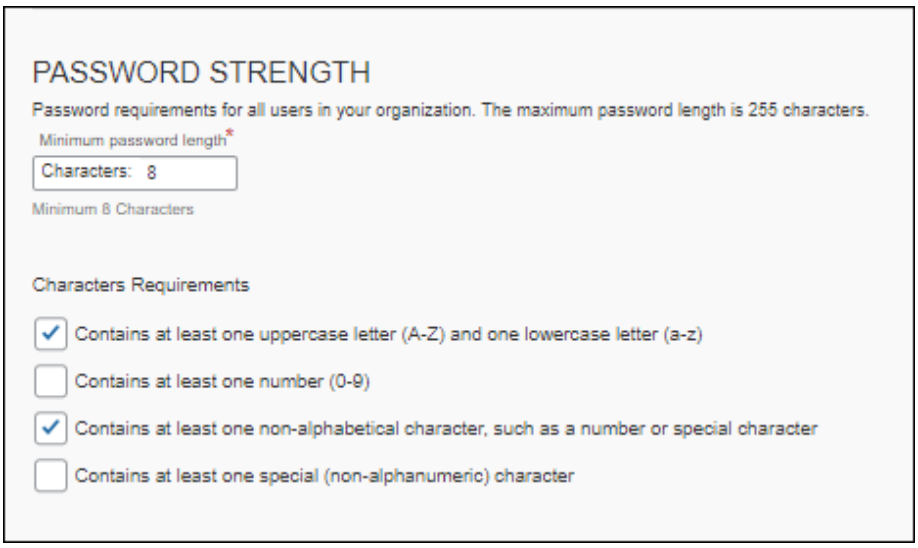
To access the **Sign-In Settings** page in SAP Concur Standard Edition, on the **Administration** menu, click **Company > Authentication Admin.** On the **Authentication Administration** page, click **Sign-In Settings.**



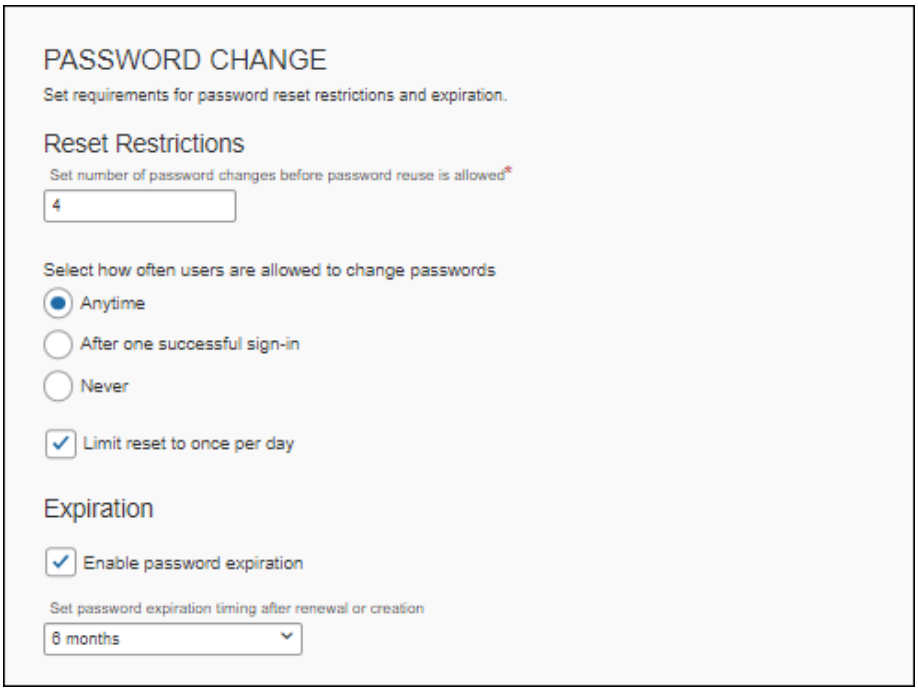
Section 3: Configuring the Password Policy

The **Sign-In Settings** page enables the administrator to define policies for the following:

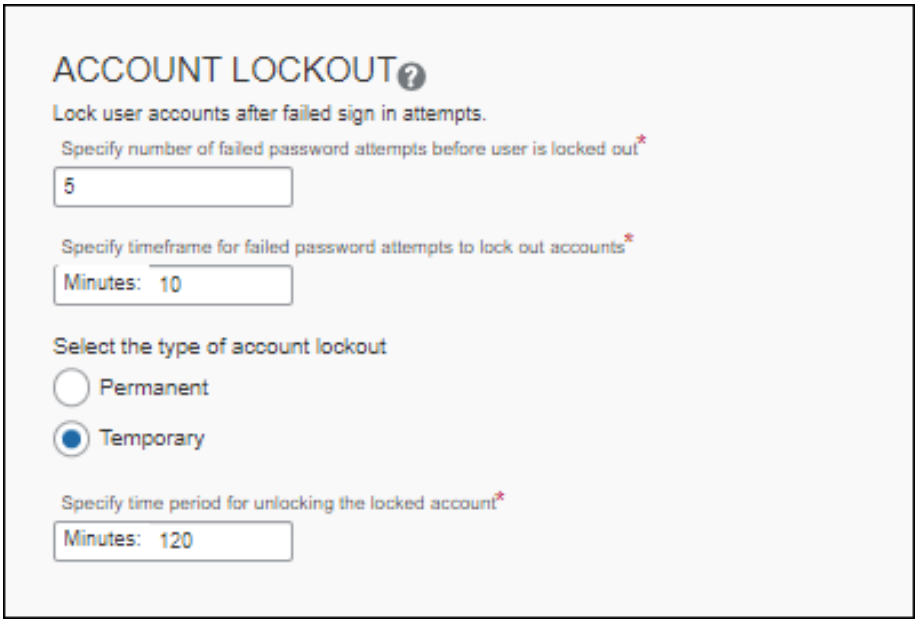
- Password Strength (required elements)



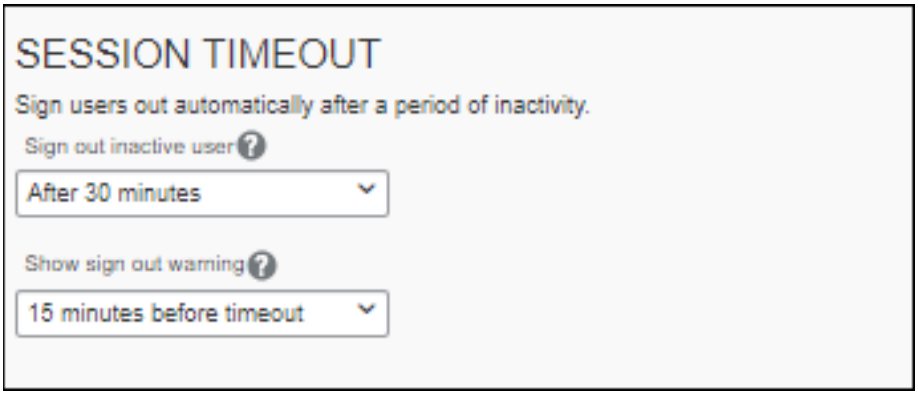
- Password Change (password reset and expiration)



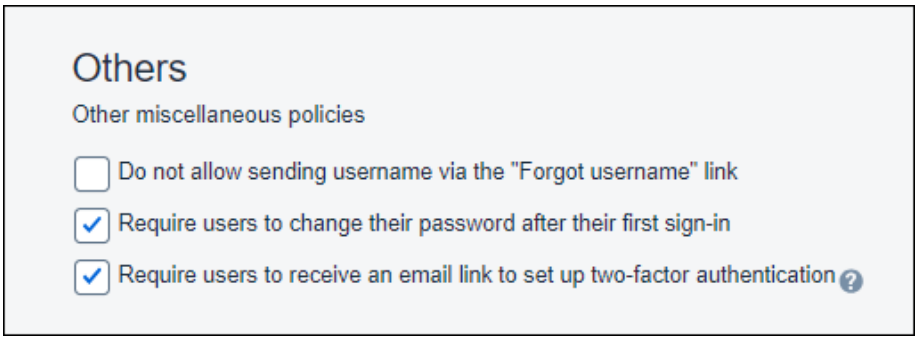
- Account Lockout (conditions for locking an account)



- Session Timeout (response to user inactivity)



- Other Settings (username reset, change password, require email link for 2FA setup)



Section 4: Default, Minimum, and Maximum Settings

To improve security for our clients, SAP Concur specifies default, minimum, and maximum password policy settings. If a company admin does not change these settings, the default settings are enforced.

For the default, minimum, and maximum values, refer to the following table:

Password Strength (required password elements)	Minimum	**Maximum**	**Default**
Password length	8	255	8
Upper (A-Z) and lower (a-z) case letters required	True/False	True/False	True
Number (0-9) required	True/False	True/False	False
Number or special (non-alphabetic) character required	True/False	True/False	True
Special (non-alphanumeric) character required	True/False	True/False	False
Password Change (password reset and expiration)	**Minimum**	**Maximum**	**Default**
How often users are allowed to change their password	Never	Anytime	Anytime
Password reset allowed once per day	True/False	True/False	True
Number of password changes required before reusing a password	4	20	4
Passwords expire	True/False	True/False	True
Period after which password expires	1 month	1 year	6 months
Account Lockout (criteria for locking an account after failed attempt(s))	**Minimum**	**Maximum**	**Default**
Number of failed sign-in attempts allowed before an account is locked	3	20	5
Sign in failure window (elapsed time before restarting the failure count)	10 min	240 min	10 min
Permanent lockout	True/False	True/False	False
Duration of account lockout	30 min	1440 min	120 min
Session Timeout (sign users out after a period of inactivity)	**Minimum**	**Maximum**	**Default**
Display sign-out warning (display a warning x minutes before user is signed out due to inactivity)	0	15	15

Sign out an idle user (number of minutes a user can be idle before being automatically signed out)	10	120	30
Other settings	**Minimum**	**Maximum**	**Default**
Hide the "Forgot Username" link	True/False	True/False	False
User must change their password on first sign in	True/False	True/False	True
Require users to receive an email link to set up 2FA	Enabled/Disabled	Enabled/Disabled	Enabled