

Concur Multi-Factor Authentication

Frequently Asked Questions

What is Multi -factor Authentication (MFA)?

Multi-factor Authentication is an authentication process that requires two different authentication factors to establish identity. This means the user will have to prove their identity in two different ways to establish access. To increase security, more software websites are requiring their users to use MFA to sign in. MFA gives your organization the ability to help safeguard your information.

Why is MFA being required to sign into SAP Concur?

MFA is a layered approach to securing your users accounts and the data they contain. When MFA is enabled, after entering the correct password, the user is prompted to provide the second factor of authentication, which could be a one-time code generated by a mobile authenticator app. This second step verifies the user's identity before the service grants the user access. MFA greatly enhances the security of online accounts and is a core component of a strong identity and access management policy. While important, usernames and passwords are vulnerable to credential stuffing, password breaches and can be stolen by third parties. Enforcing the use of an MFA significantly reduces the risk of unauthorized access and increases confidence that your accounts will stay safe from cyber criminals.

Can I opt out of using MFA?

No.

When will this change occur in SAP Concur?

Wednesday October 18, 2023

If I am using Employee Self Service to access SAP Concur, am I impacted?

No, the link in ESS automatically authenticates your login credentials.

If I am connected to the Commonwealth Network or log into VPN and use my user id and a password to access SAP Concur at www.concursolutions.com, am I impacted?

Yes. If you have CWOPA credentials, select the AZURE link to log into SAP Concur. This will use the Commonwealth of Pa's MFA process. If you do not have CWOPA credentials, you will use the Password link to log into SAP Concur and will be required to set up and use SAP Concur's MFA.

If I am using the mobile app, am I impacted?

Yes. If you have CWOPA credentials, select the AZURE link to log into SAP Concur. This will use the Commonwealth of Pa's MFA process. If you do not have CWOPA credentials, you will use the Password link to log into Concur and will be required to set up and use Concur's MFA.

What authenticator app should I use?

SAP Concur supports multiple authenticator apps, but it is recommended to use Microsoft's authenticator app.

If I already have the Microsoft Authenticator app installed on my phone, what do I need to do?

Follow the on-screen instructions from SAP Concur to link the existing app to Concur.

Does the SAP Concur MFA process support receiving a call or email with the verification code?

No. If you are using the SAP Concur MFA process, you must use an authentication app to receive the verification code.

What if I do not want to install an authentication app on my personal phone?

You will be required to use the browser extension version of the selected authentication app.

Once I have MFA, how often do I need to authenticate to sign into SAP Concur?

You will need to authenticate every time you sign in. In the event your session is timed out, you would need to input your username and password again and will need to provide your authentication code.

What if I am a delegate, will this impact my ability to switch profiles?

No