

CONTRACT EXPRESS

How to

Set up two-factor authentication

Overview

In Contract Express 8.1 you can enable two-factor authentication for your license space.

Enabling this feature will strengthen login security for forms based authenticated users by requiring the entering of a secondary code from a pre-established smartphone app, in addition to the standard email and password. Users that use SSO in the same environment will be unaffected.

1. Enable two-factor authentication

Admins can choose from 3 enforcement levels for their forms-based authenticated users.

In the admin section 'Features', enable 'Two-factor authentication', and select one of the following;

User choice

Two-factor authentication is not mandatory for any user. Individual users have the ability to decide if they would like the second layer of security every time they log in or when they log in with an unrecognized browser.

This selection is a good choice for environments that would like the administrators only to use two-factor authentication, or for specific subsites.

Users can enable this in My Accounts, by selecting 'ENABLE TWO-FACTOR AUTHENTICATION'.

When this option is enabled, users have the ability to disable their personal authenticator if they choose to.

Enforce when a new browser is used

All forms based authenticated users will be forced to use two-factor authentication when they sign into Contract Express with an unrecognized browser. By selecting 'Remember this browser', the user will not be prompted for a verification code again until their cookies are cleared or they log on with a different browser.

Existing users will be prompted to set up their authenticator the next time they sign into Contract Express. New users will be prompted along with their initial set up.

Enforce every time a user logs in

All forms based authenticated users will be forced to use two-factor authentication when they sign into Contract Express every time they log in.

Existing users will be prompted to set up their authenticator the next time they sign into Contract Express. New users will be prompted along with their initial set up.



We suggest before enforcing two-factor authentication; start by selecting 'user choice' for a specified amount of time. Distribute materials to all users which authenticator apps you recommend and how to set it up within Contract Express. This way when you switch to an enforced option, the users will not be prevented logging in until set up is complete.

2. Choosing an Authenticator

Users can connect to any authenticator that is a 'time-based one time password' authenticator. Administrators cannot enforce which authenticator their users can choose. However, recommending an authenticator and providing steps for the users will help with user adoption of the company-desired authenticator.

In Contract Express when user is prompted for authenticator set up, the on screen steps can be followed. Depending on the chosen authenticator, they will either need to use their smartphone's camera for QR code scanning, or are given the ability to type the Contract Express Key into the key field.



Most popular authenticators

Google Authenticator

For information or to download the Google Authenticator please visit <http://www.google.com/2step>

Microsoft Authenticator

For information or to download the Microsoft Authenticator visit <https://www.microsoft.com/en-us/account/authenticator>

Authy

For information or to download the Authy authenticator please visit <https://authy.com/>

Symantec VIP

For information or to download the Symantec VIP authenticator please visit <https://vip.symantec.com/>