
# Security in Confirmit Software - Individual User Settings





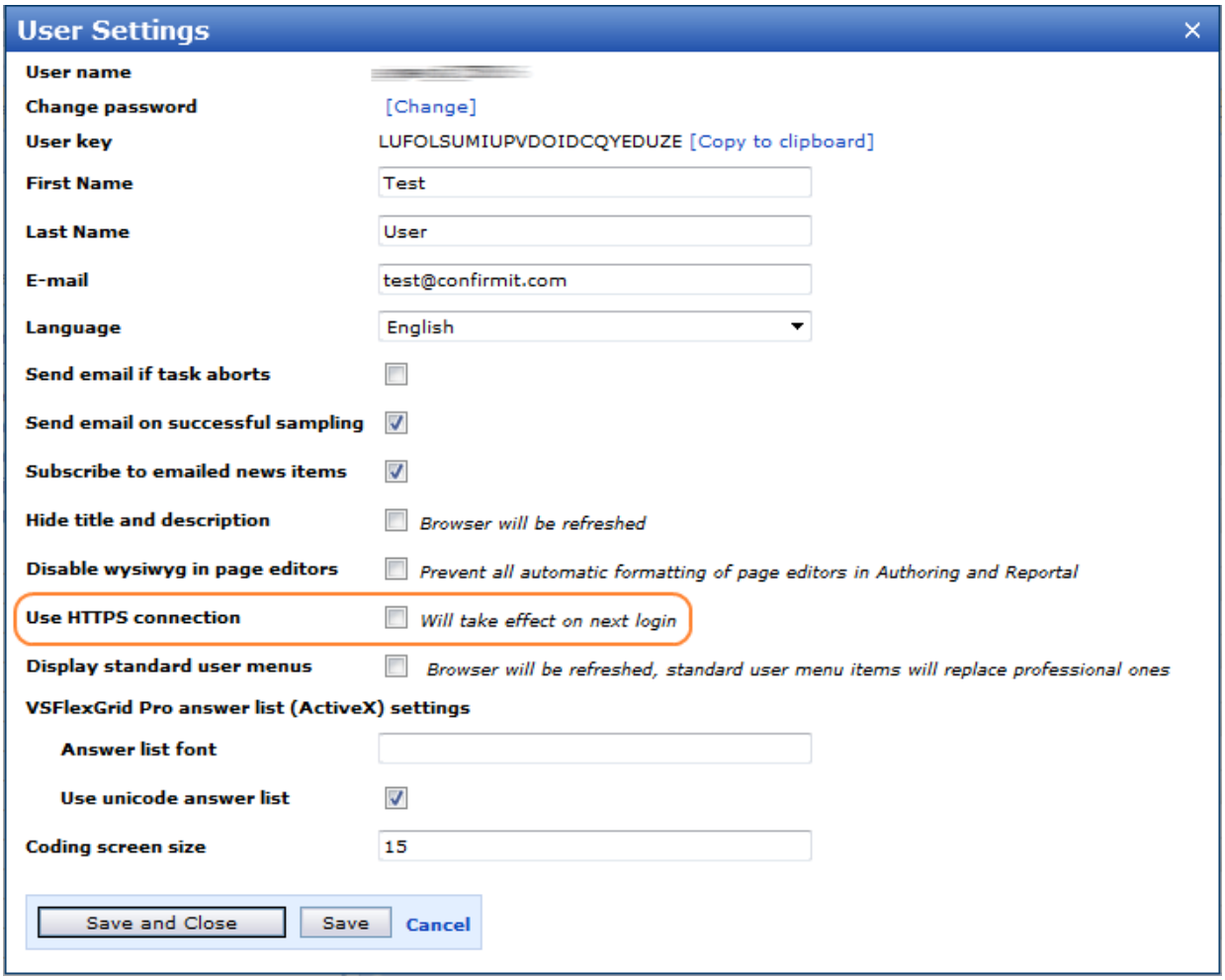
Revised: 2019-10-15

# 1 Using HTTPS in Confirmit Horizons

HTTPS is enforced for all requests to our hosted Confirmit Horizons environments, allowing all users to encrypt their sessions by using HTTPS instead of plain-text HTTP when connecting to the hosted platform. HTTPS protects your session against network eavesdropping (sometimes referred to as "packet sniffing") by ensuring the traffic between the client computer and the server is encrypted.

On-Premise customers who have enabled installed SSL certificates will enforce the HTTPS protocol for all login pages in Confirmit Horizons, i.e. for Professional users, Express users, Translators, Reportal users, and panelists. Exchanges of authentication credentials between the client and server are therefore always secured with SSL encryption. If the site or company is not set to enforce HTTPS the users are then redirected back to regular, unencrypted HTTP once the server has successfully authenticated the login request. However, it is possible to enforce SSL encryption for the entire session when working in Confirmit Horizons.

As a logged on user, you can access your user settings by clicking on your user name in the top right area of the screen in Professional Authoring (you can also use the Home > User > Settings menu selection to open the same page). This will bring up an overlay screen which will contain the setting 'Use HTTPS connection' if HTTPS is not enforced sitewide:




If the checkbox is selected, Confirmit will always keep your session secured with HTTPS, even if you open windows to Confirmit Express, Reportal or Translator. If HTTPS is enforced sitewide then the checkbox will not be displayed.

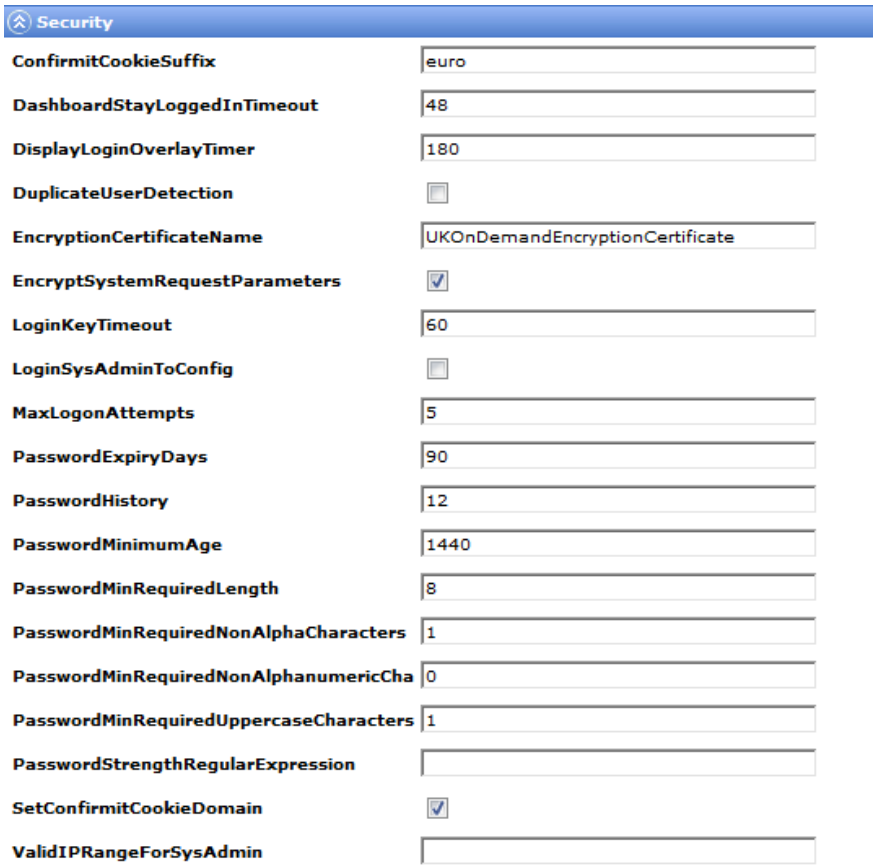



Revised: 2019-10-15

# 2 Password / Account Security

Passwords in Confirmit Horizons must comply with the minimum requirements configured on the system. As seen in the below screenshot, these settings include:

- Locking of accounts after 5 consecutive failed login attempts.
- Lock screen displayed after 60 minutes inactivity (Password required to unlock).
- Sessions logged off after 3 hours unless unlocked.
- Passwords must be changed after 90 days.
- Passwords cannot be reused (history of last 12 passwords stored on the system).
- Passwords cannot be changed more than once per day (to prevent circumvention of password history).
- Passwords cannot be found in lists of breached passwords or can only be found a configurable number of times in lists of breached passwords (depending on company setting).
- Minimum requirements for passwords: 8 characters in length, at least one uppercase character and one numeric/symbol character.




Passwords are not stored in clear text in the database, instead they are encrypted using one-way hashing technique (using the PBKDF2 key derivation function) with a unique salt value for each account, and the output hash value is stored in the database. The authentication mechanism will perform the same hash function on a password submitted from the login page and will try to match this against the hash value that is stored in the database for the user account, rather than verifying the actual password itself.

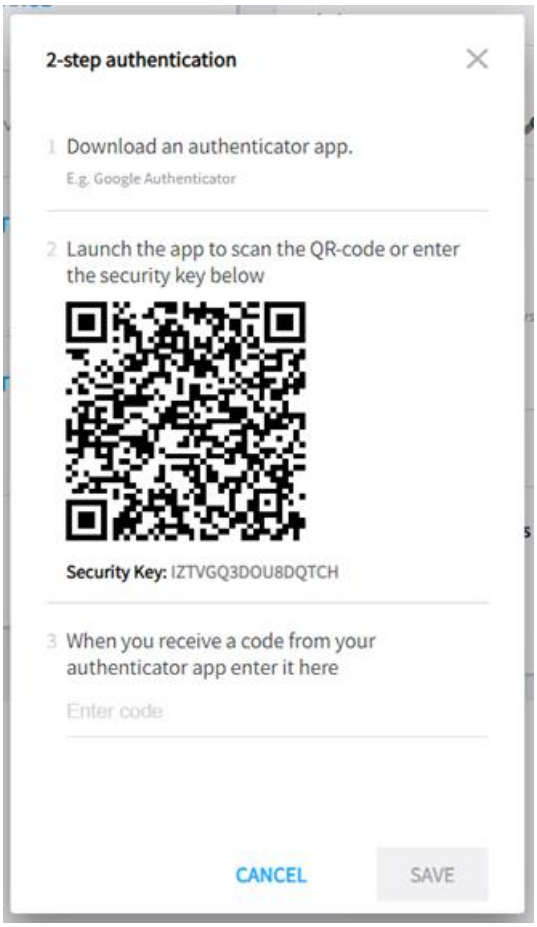
A side-effect of this is that no one, not even Confirmit's Account Management Team, can retrieve the original clear-text password from the database. Instead of retrieving existing passwords, it is possible for an account administrator to reset a user's password from the admin menu (and provide the user with the new, temporary password, which must be changed at the first subsequent login), or the user may request a password reset link to be sent to the registered email address for the account from the login page as long as they know their Confirmit Horizons user name.

# 3 Two factor authentication and backup codes

Confirmit supports 2-step verification (2-factor authentication – 2FA). When 2FA is enabled for your Confirmit account, when you log in to Horizons you will need your password and a code that is generated by an authenticator aplication. Download an authenticator app such as Authy, Duo, Google Authenticator, LastPass Authenticator or Microsoft Authenticator, into your mobile device to generate the required code. To set up the authenticator app:

1. Download the authenticator app that you wish to use onto your mobile device.

2. In Horizons, click the User menu icon to open the User Settings overlay and beside the 2-step authentication property click SETUP. The 2-step authentication overlay opens with a QR code.




3. Using your mobile device, scan the QR code. A code number is generated and presented on your mobile device.

4. Enter the number into the field towards the bottom of the overlay and click SAVE. The authenticator overlay closes and you are returned to the User Settings page. 2FA is now activated.

With the current settings you will need to generate and input a new code number every time you log in to Confirmit Horizons. You can however set the browser to be "trusted"; this you can do the next time you log in (see below). The computer and browser you use to log in to Confirmit Horizons will then allow you access for 30 days without having to input a new code. After 30 days you will need to generate and input a new code. Note that if you log in to Confirmit Horizons from any other computer or using a different browser then you will need to input a code again.

To disable 2FA, in the User Settings page click DISABLE beside the 2-step authentication option.

Note that if the mobile device providing the 2FA codes is not available for any reason, "Recovery codes" are available via the User Account Settings page, or the system administrator can access the user settings and disable the 2FA functionality.

In the User Account Settings page, the Recovery Codes section will automatically appear when 2FA is active. This property provides 10 randomly generated one-time codes which you can use to access your account in the event your 2FA code generator app is unavailable. While you have access to Horizons, make a note of these codes and store them in a safe location; they will then be available if required. There will be no indication of which codes are "spent" and which aren't, but you can regenerate a new set of codes at any time (all old codes including unused codes will then be invalid).

**Logging in to Confirmit using 2FA:**

When you log in to Confirmit Horizons, if 2FA is enabled then after entering your username and password you will be asked for a code number.

1. On your mobile device, run the Authentication app to generate a valid code and enter the code into the field.

2. If you wish to "Trust this browser", check the box. You will then be able to log in using the current browser for the next 30 days. After this time you will need to input a new code.

3. Click Verify.

Confirmit Horizons opens.

# 4 Other options

Other security options are also available, but may depend on license specific add-ons. See the separate Additional Options document for further details.





**Revised: 2019-10-15**