

Vistara™: How to Use Multi-Factor Authentication with HST Connect®

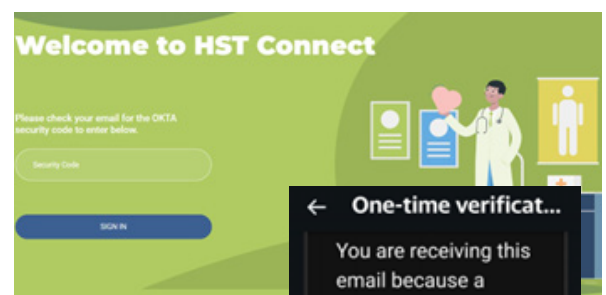
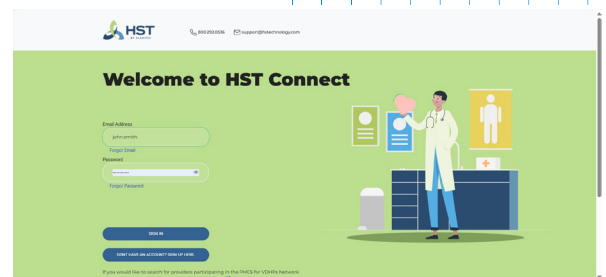
Tightening state regulations now require financial and insurance services organizations like ours to use multifactor authentication (MFA) for access to any non-public information. We're committed to keeping our systems and your data secure, so we've enhanced the security of our client-facing applications, including Vistara's HST Connect.

MFA, sometimes referred to as two-step verification, requires users to log in to a system with another method in addition to their username and password.

Using MFA

Registering for HST Connect automatically enrolls you in MFA. There is no need to download any other applications. HST Connect uses Okta Verify, which works much like many other websites: you'll be emailed a one-time, temporary code to enter as part of the login process.

- Once you enter your log-in credentials, a message will appear asking you to check your email for an Okta security code.
- The email from Okta will be sent to the address you used to register for HST.
- If you don't receive the code within a couple of minutes, check your spam folder. Once you enter the code, you will be able to use HST Connect.
- Please note that you will be prompted to enter a new code during login every 24 hours per our security policy.



This is an example code

