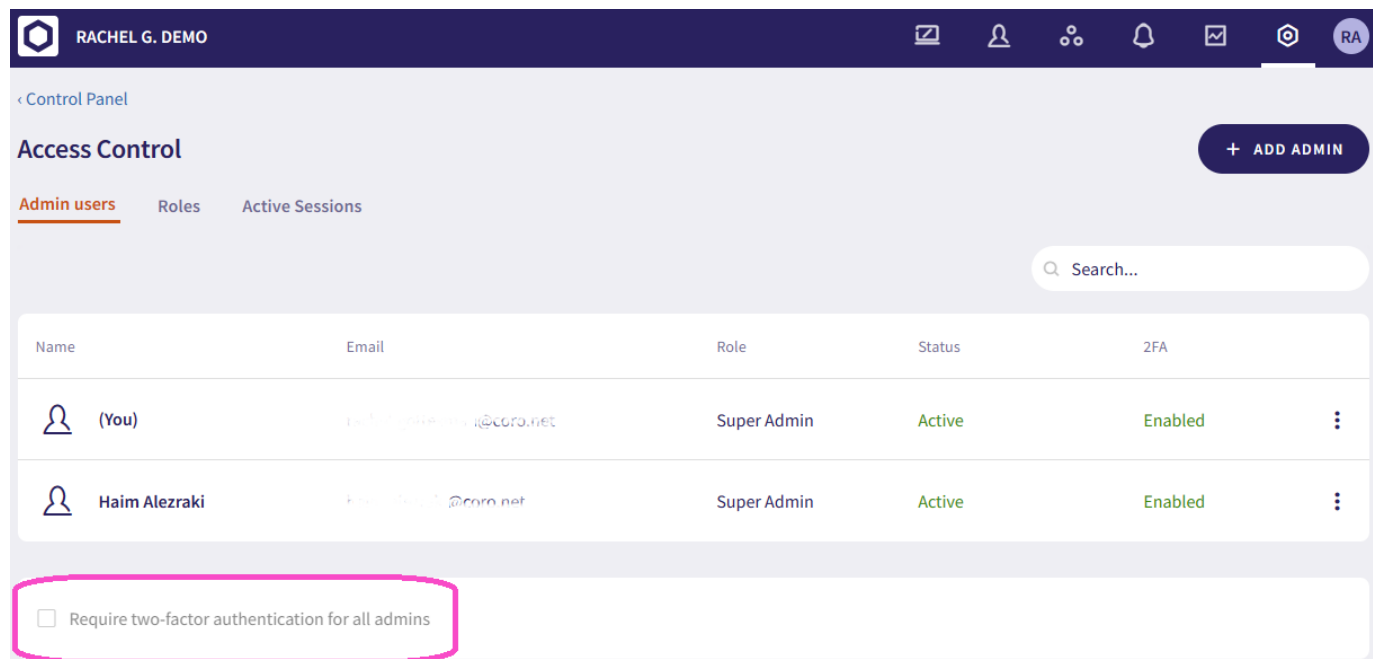


Configure 2FA

Two-Factor Authentication (2FA) is a common method to reduce the risk of unauthorized service access.

You can now enforce 2FA for admin users by selecting **Require two-factor authentication for all admins** from **Control Panel > Access Control > Admin users**:



The screenshot shows the 'Admin users' page in the Control Panel. The page has a dark blue header with the user's name 'RACHEL G. DEMO' and various navigation icons. Below the header, there's a breadcrumb trail: 'Control Panel > Access Control > Admin users'. The 'Access Control' section has a '+ ADD ADMIN' button. Underneath, there are tabs for 'Admin users', 'Roles', and 'Active Sessions'. A search bar is present. A table lists the admin users:

Name	Email	Role	Status	2FA
(You)	rachel.g.demo@coro.net	Super Admin	Active	Enabled
Haim Alezraki	haim@coro.net	Super Admin	Active	Enabled

Below the table, there is a checkbox labeled 'Require two-factor authentication for all admins', which is highlighted with a pink box.

Note

You can use whichever mobile authenticator you choose. Popular 2FA apps include, but are not limited to, Google Authenticator and OneLogin. You must have one of these installed to use Coro's 2FA protection.

To manage your own account's 2FA code, navigate to your account page (top-right account avatar icon) and select **My Account > Two Factor Auth**.