Managing admin users

Admin users with sufficient permissions handle configuration, monitoring, and ticket remediation. When you sign up for the Coro service, you receive an initial admin user account with super admin permissions to **sign into the Coro console**. You can add additional admin users through the console.

To view the admin users page, select **Control Panel > Access Control > Admin users**:

Cor	RO				ম	٥		0	RG
< Control Panel									
Access Control							+	ADD ADI	MIN
Admin users Roles Active Sessions									
					Q Sear	ch			
Name		Email	Role	Status			2FA		
2	R G(You)	Handler of the second se	Super Admin	Active			Disabled		:
<u>R</u> .	Test22223333 Test2		Super Admin	Active			Disabled		:
<u>}</u>	a a		Viewer	Invited on	Feb 1, 2024		Disabled		:
<u></u>	AO	areastingenoveling one-convention	Super Admin	Active			Disabled		:
<u>८</u>	Anton Admin		Super Admin	Active			Disabled		:
٨			Super Admin	Active			Disabled		:
Δ	Ben barkhoff		Super Admin	Active			Disabled		:

From the Admin users tab, admin users with sufficient permissions can:

- Create a new admin user account. For more information, see add a new admin user.
- Enable two factor authentication (2FA) for all admin users. Select **Require two-factor authentication for all admins** from the bottom of the page.
- View a list of current admin users, and manage them from the three-dot menu of the row of the relevant user:
 - Edit the name, email address, or role of an admin user. Select Edit admin user.