Southern Cross Health Insurance

Account dormancy FAQs

Why are accounts being locked or removed?
Southern Cross Health Society needs to ensure registered users of Provider Web have a legitimate business purpose to access the portal. To keep our user database accurate and up to date we need to remove inactive accounts on an ongoing basis.

What happens if an account is not accessed regularly?
If an account is inactive for more than 90 days, it will be locked. If it remains inactive for more than 180 days, it will be permanently removed.

Reminder emails will be sent before this happens.

What happens if I go on extended leave, for example paternity leave, will my account be locked or removed?
Yes. The same inactivity rules apply as outlined above.

How do I regain access if my account has been locked?
Contact the Affiliated Provider Relationship Management team on 0800 757 838 to have the account re-enabled.

What happens if I have not logged in for 180 days?
Accounts inactive for more than 180 days will be permanently removed.
Reminder emails will be sent on day 91 and day 151, with instructions on how to unlock the account to maintain access.
If no action is taken, a final email will be sent on day 181 confirming that access to Provider Web has been removed.

Who will receive reminder emails about inactivity?
Only the account holder will receive inactivity reminder emails.
Provider Web administrators, Affiliated Provider contract contacts or your manager will not be notified.

Once an account is removed, can it be reinstated or the same username be reused?
No. Once an account is removed, it cannot be restored, and the same username cannot be reused.

How do I get access to Provider Web if my account has been removed?
A new Provider Web user login will need to be created. Please contact your Provider Web administrator to request this. If no administrator is linked to the contract, the Affiliated Provider relationship management team can be contacted at aps@southerncross.co.nz for assistance.

What will happen when account dormancy is switched on?
Once account dormancy is switched on, the system will automatically review each user's activity history. It will look back to the last recorded login date from the time multi-factor authentication (MFA) was first set up. This date will be used as the starting point to measure

inactivity. If no login has occurred since setting up MFA, the account will be treated as inactive and will follow the dormancy process (reminders, lock, and eventual removal).

This ensures that all accounts are assessed consistently, based on verified login activity, and helps maintain the security and accuracy of the Provider Web user database.

For more information on MFA setup, please refer to the *MFA User Guide* available in Provider Web mfa_user_guide.pdf.

What should I do if I haven't received reminder emails?
Check your spam/junk folder and confirm your registered email address is correct.