

Optus Wireless IP VPN

Customer Management Interface (CMI)

Multi-Factor Authentication (MFA) Setup Guide

September 2025

V 1.0

OPTUS

This guide will help you set up Multi-Factor Authentication (MFA) for your Optus Wireless IP VPN Customer Management Interface (CMI) Admin account. MFA adds an extra layer of security to keep your account and business services safe.

When this is happening

Between **12/11/2025 – 31/01/2026**, MFA will be introduced for all CMI accounts through a simple self-enrolment process.

- At your first login with your existing username, password and authentication details, you'll be asked to register a valid email address and an optional Australian mobile number.
- Once validated, every future login will require MFA to keep your account secure.

Key Dates

- **MFA self-enrolment opens:** 6:00 AM, 12 November 2025
- **MFA setup deadline:** 11:00 PM, 31 January 2026

Any accounts not set up with MFA by the deadline may be permanently deleted. If you need access after this date, please contact the Optus Enterprise & Business Service Centre on **134 315** (or your dedicated 1300 number).

How to set up MFA

1. Open your preferred web browser and go to: <https://wirelessip.optus.com.au>.
2. Log in with your existing CMI username, password, and authentication type (APN or Realm), then select **Login**.
 - o *Tip: If you've forgotten your login details, see the help section below.*
3. Enter your email address and (optionally) your mobile number, then select **Generate One-Time Code**.
4. Enter the code sent to you and select **One-Time Code Login**. This registers your MFA details and completes your login.
 - o *Codes are valid for 3 minutes. If your code expires, log in again to request a new one.*
 - o *If you don't see the code in your inbox, please check your junk or spam folder.*

From now on, MFA will be required every time you log in.

The screenshot shows the 'Login' page of the Optus Wireless IP VPN Customer Management Interface (CMI). The page has a teal header with the 'yes OPTUS' logo on the left and 'Administrator Guide' on the right. Below the header, the title 'WIRELESS IP VPN' is displayed. A welcome message states: 'Welcome to the Wireless IP VPN Customer Management Interface (CMI). CMI is an optional service designed to manage and deliver user authentication and static IP allocation. CMI may only be accessed by the IT Manager(s) nominated by your organisation.' Below this is a login form with fields for 'Username / Email', 'Password', and 'APN'. There are radio buttons for 'Authentication type' with 'APN' selected and 'Realm' unselected. A 'Login' button is at the bottom of the form, with a link for 'First Time Login / Forgot Password' below it. The footer contains the copyright notice '© Optus Administration Pty Ltd 2025'.

The screenshot shows the 'Multi-factor Authentication Required' page of the Optus Wireless IP VPN Customer Management Interface (CMI). The page has a teal header with the 'yes OPTUS' logo on the left and 'Administrator Guide' on the right. Below the header, the title 'WIRELESS IP VPN' is displayed. A welcome message states: 'Welcome to the Wireless IP VPN Customer Management Interface (CMI). CMI is an optional service designed to manage and deliver user authentication and static IP allocation. CMI may only be accessed by the IT Manager(s) nominated by your organisation.' Below this is a message: 'To help keep your services secure, we've introduced Multi-Factor Authentication (MFA) for all users of the Optus Customer Management Interface (CMI). Please provide your Email Address and optionally your Australian Mobile Number (in '04XXXXXXX' format) to be used for MFA when logging in.' Below this is a form with fields for 'Email Address *', 'Mobile Number', and 'One-Time Code'. There is a 'Generate One-Time Code' button next to the 'Mobile Number' field. At the bottom of the form are 'Cancel' and 'One-Time Code Login' buttons. The footer contains the copyright notice '© Optus Administration Pty Ltd 2025'.

Help with login details

- **If your organisation has another active CMI Superuser:** An admin can log in to confirm usernames, authentication details, or reset passwords.
- **If your organisation doesn't have another active CMI Superuser:** Please contact the Optus Enterprise & Business Service Centre on 134 315 (or your dedicated 1300 number).

Need more help?

For more detail, see the administrator guide at <https://wirelessip.optus.com.au> or call our Enterprise & Business Service Centre on **134 315** (or your dedicated 1300 number). Our team is here to help make MFA setup easy and straightforward.

