real world technology solutions

AD Management — User Guide

Real World Technology Solutions

June 2026

Contents

real world technology solutions

Getting started

Welcome to AD Management

AD Management is a simple, web-based way to do everyday Active Directory jobs — finding people, resetting passwords, creating and offboarding accounts, and managing group membership — without needing the full Active Directory consoles.

WHAT YOU CAN DO HERE

- **Find people** quickly by name, username or email.
- **See an account at a glance** — status, location, group membership.
- **Do the common jobs** from one place: reset a password, enable or disable an account, edit details, manage groups, create a new user, offboard a leaver.

Which of these you see depends on what you've been given permission to do, and in which parts of the directory. If something below isn't visible to you, that's expected — see Why some things are hidden.

WHAT THIS TOOL IS NOT

It manages your on-premises Active Directory. It is **not** the Microsoft 365 / Entra admin centre — mailbox settings, licences and cloud-only accounts are managed there. Changes you make here flow to Microsoft 365 through your directory sync on the usual schedule, so a change may take a few minutes to appear in cloud services (see My change isn't showing yet).

WHERE TO START

- New here? Read Finding your way around.
- Need to do something now? Jump to Find a user — almost every job starts by finding the person.

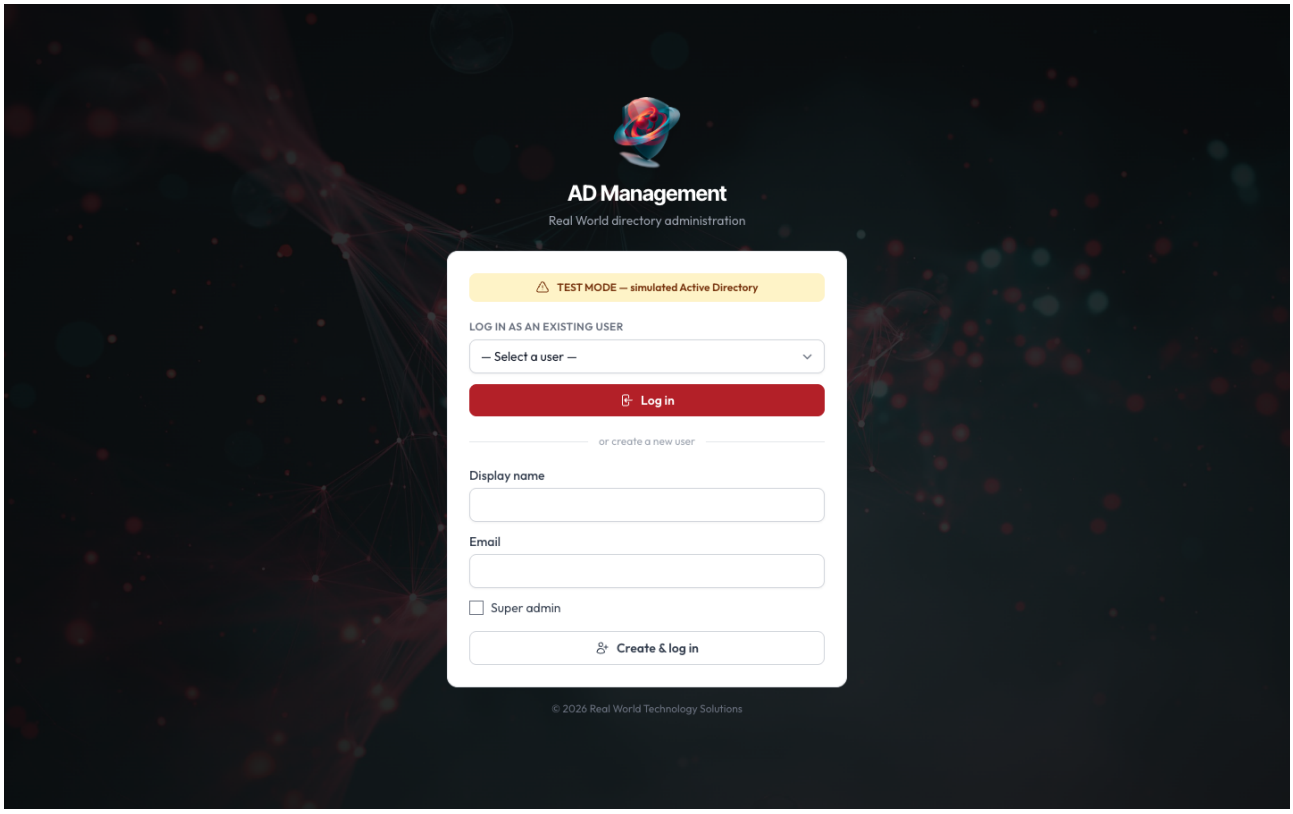
> Tip: the **?** in the top bar always opens the help for the screen you're on.

Signing in

Sign in whenever you need to manage accounts in Active Directory.

HOW TO SIGN IN

This tool uses single sign-on. Click **Sign in** and you'll be taken to your organisation's normal login page — the same one you use for Microsoft 365 and other work systems. There is no separate username or password for this tool.



Once you authenticate successfully, you'll land on the search screen and can start working straight away.

IF YOU SEE "ACCESS DENIED"

Authenticating successfully doesn't automatically grant access. Your account must also be authorised to use this tool — most staff aren't, by design.

If you reach an access-denied page after signing in, your credentials were accepted but your account hasn't been given a role here yet. Contact your administrator and ask them to assign you access. See Access denied after signing in for more detail on what that page means.

SIGNING OUT

Select **Logout** in the top bar. You'll be signed out of this tool immediately.

> Tip: closing the browser tab does not sign you out. Always use **Logout** on a shared or public machine.

Finding your way around

Use this article to get your bearings the first time you open the tool.

real world technology solutions

THE TOP BAR

The top bar is present on every screen. It holds:

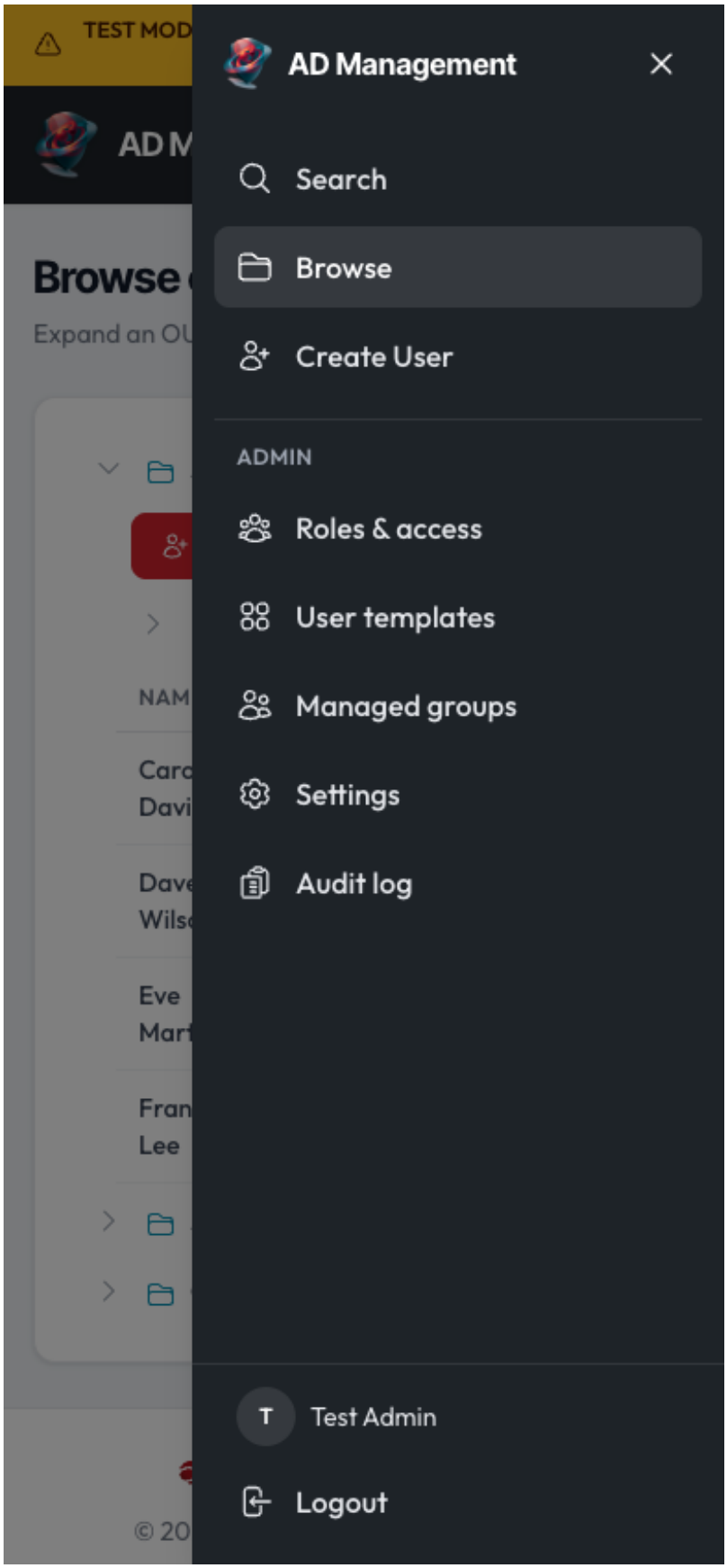
- **Search** — jump straight to a name, username, or email search.
- **Browse** — explore the directory tree by organisational unit.
- **Create User** — start a new account (only shown if you have permission).
- **?** — opens context-sensitive help for the screen you're on.
- **Logout** — signs you out.
- **Admin** — appears only if you're an administrator.

THE HOME SCREEN

The home screen is the search screen. Finding someone is always one step away from wherever you are — just click **Search** in the top bar.

ON A PHONE OR NARROW SCREEN

On smaller screens the navigation collapses into a slide-in drawer. Tap the menu button in the top right to open it.


TEST MOD
AD M
Browse
Expand an OU
NAM
Caro
Davi
Dave
Wilso
Eve
Mart
Fran
Lee
© 20
AD Management
Search
Browse
Create User
ADMIN
Roles & access
User templates
Managed groups
Settings
Audit log
T
Test Admin
Logout

THE USER ACTION HUB

Open any user's detail page and you'll see every action available to you for that person gathered in one place — reset password, enable or disable, edit details, manage group membership, and more. See View a user for a walkthrough.

THE TEST MODE BANNER

If an amber **TEST MODE** banner appears at the top of the screen, you're connected to a simulated directory. Actions you take won't affect any real accounts.

> Tip: can't find a button you expect? See Why some things are hidden.

Locations and technical details

This article explains how the app displays directory locations and where to find the underlying technical identifiers when you need them.

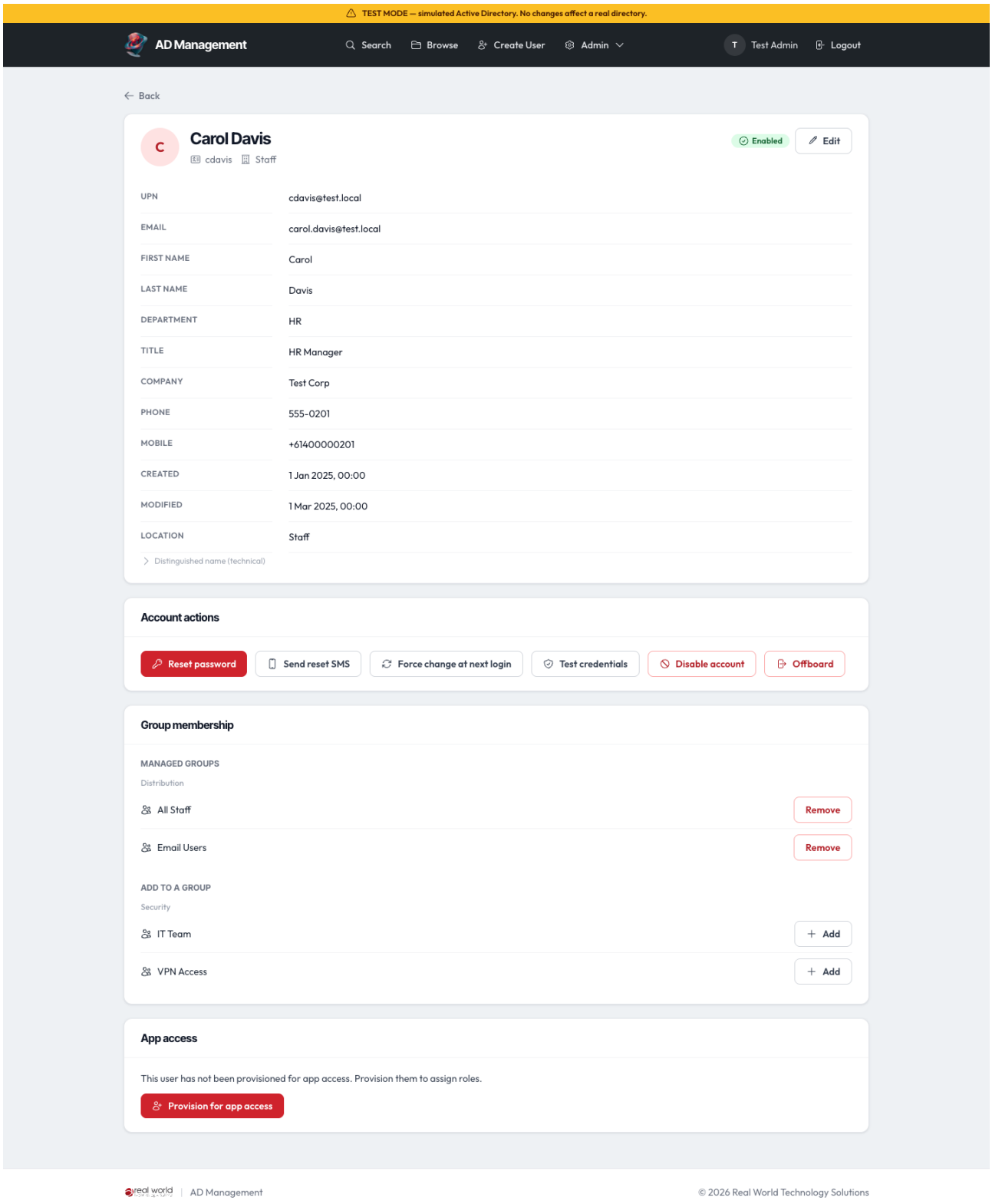
FRIENDLY LOCATION PATHS

Throughout the app, a person's or group's location in the directory is shown as a readable path — for example, **Staff › Management** — rather than raw LDAP notation. This makes everyday screens easy to scan without needing to know how LDAP structures work.

You'll see these paths on search results, the user detail page, and when browsing the directory. See Browse the directory to navigate by location.

TECHNICAL DETAILS

The exact technical identifier for any record — the Distinguished Name (DN) — is still available whenever you need it. On a user or group record, expand the **Technical details** section to see the full DN and copy it to the clipboard.


TEST MODE — simulated Active Directory. No changes affect a real directory.
AD Management
Search
Browse
Create User
Admin
Test Admin
Logout
Back
C
Carol Davis
cdavis
Staff
Enabled
Edit
UPN
cdavis@test.local
EMAIL
carol.davis@test.local
FIRST NAME
Carol
LAST NAME
Davis
DEPARTMENT
HR
TITLE
HR Manager
COMPANY
Test Corp
PHONE
555-0201
MOBILE
+61400000201
CREATED
1 Jan 2025, 00:00
MODIFIED
1 Mar 2025, 00:00
LOCATION
Staff
Distinguished name (technical)
Account actions
Reset password
Send reset SMS
Force change at next login
Test credentials
Disable account
Offboard
Group membership
MANAGED GROUPS
Distribution
All Staff
Remove
Email Users
Remove
ADD TO A GROUP
Security
IT Team
Add
VPN Access
Add
App access
This user has not been provisioned for app access. Provision them to assign roles.
Provision for app access
AD Management
© 2026 Real World Technology Solutions

DATES

Dates from the directory (such as account creation or last logon) are displayed in a readable format rather than the raw numeric value stored in Active Directory.

> Tip: if you need to paste a DN into another tool or a support request, the **Technical details** section is the place to get it — it's always current, read directly from the directory.

Why some things are hidden

Use this article when something you expect to see isn't there.

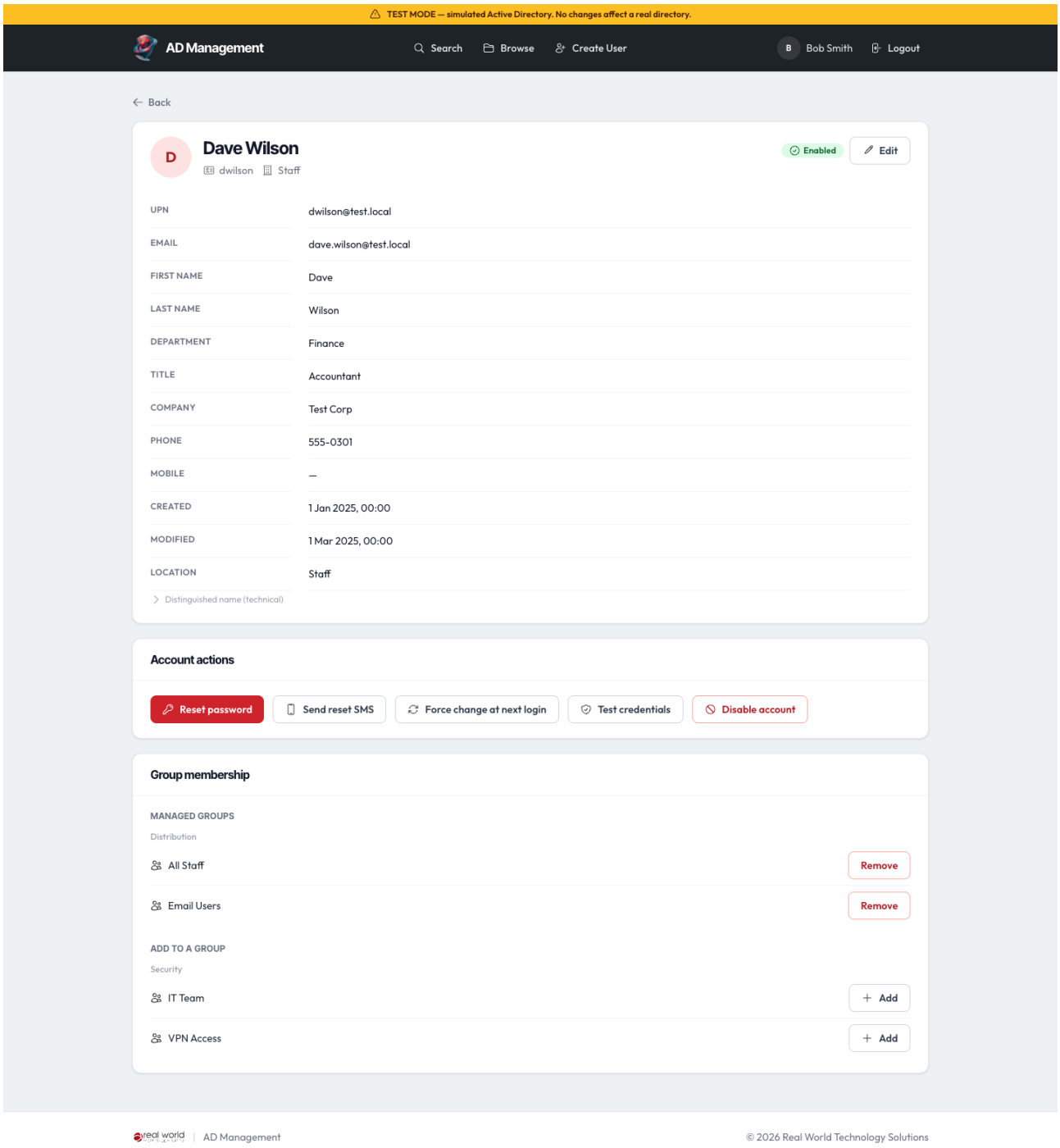
YOU ONLY SEE WHAT YOU'VE BEEN AUTHORISED TO SEE

The tool shows you only the actions you've been granted permission to perform, and only the parts of the directory that fall within your assigned scope. This is by design — it keeps each person to the work their role actually covers.

Nothing is hidden because of a fault or a bug. If it's not visible, you haven't been given access to it.

COMMON EXAMPLES

- **No Admin menu** — you're not an administrator. That's normal for most users.
- **A button is missing on a user's page** — you don't have permission for that action, or the user is outside your scope.
- **A user or OU doesn't appear in search or Browse** — they may be in a part of the directory you haven't been given access to.



WHAT TO DO

If you genuinely need access to something that's hidden, ask your administrator to review your role and scope. They can widen your permissions if it's appropriate.

For specific situations, see:

- A button I expected isn't there

- I can’t see a user or an OU

> Tip: if you’re unsure whether something should be visible to you, check with your administrator before assuming it’s a technical problem.

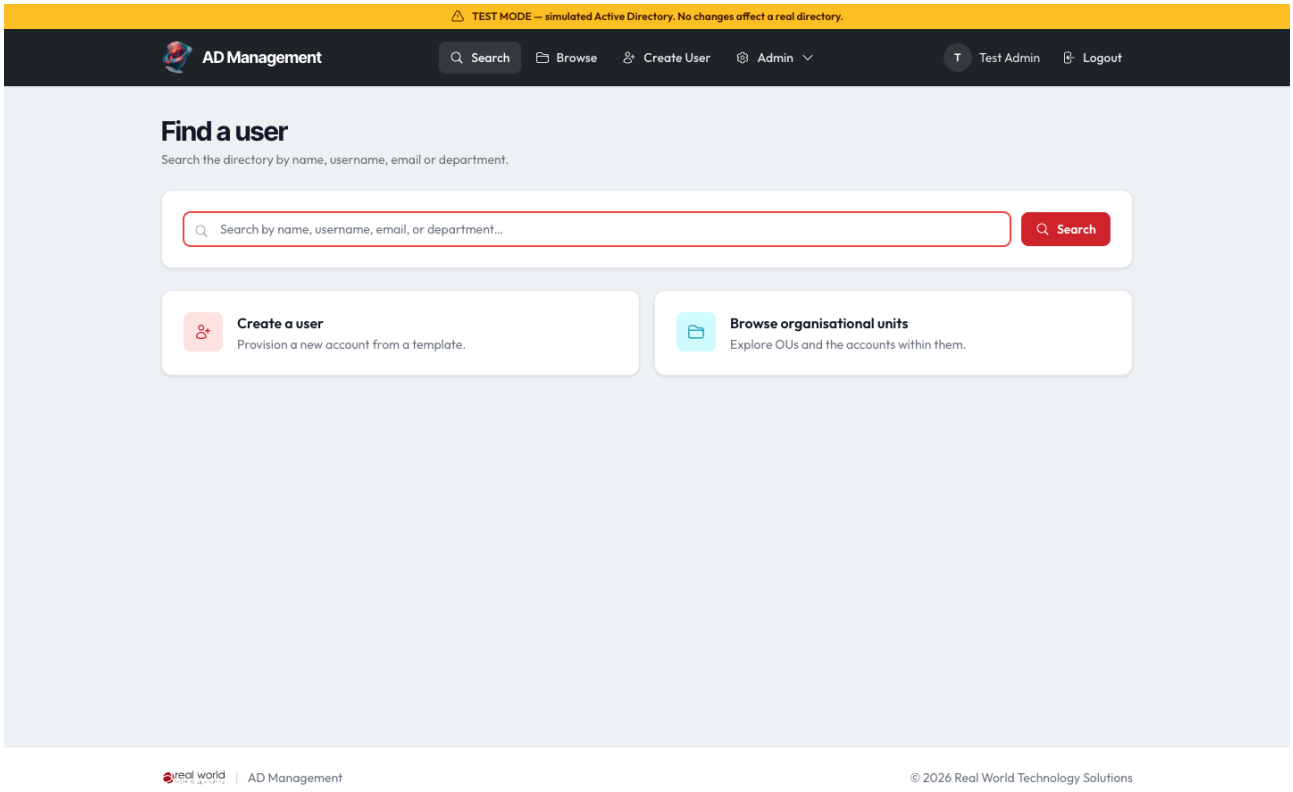
Everyday tasks

Find a user

Do this whenever you need to look someone up — almost every task starts here.

SEARCH FOR THE PERSON

1. Go to the home screen — the search box is there waiting for you.
2. Type part of the person's name, username or email address.
3. Press **Enter**.



ABOUT YOUR RESULTS

Results are limited to the locations you're permitted to see. If some matches fall outside your scope, a note tells you how many are hidden — see I can't see a user or an OU if you need access to those locations.

OPEN A PERSON'S RECORD

Click any result to open their details page, where you can see their account at a glance and take action.

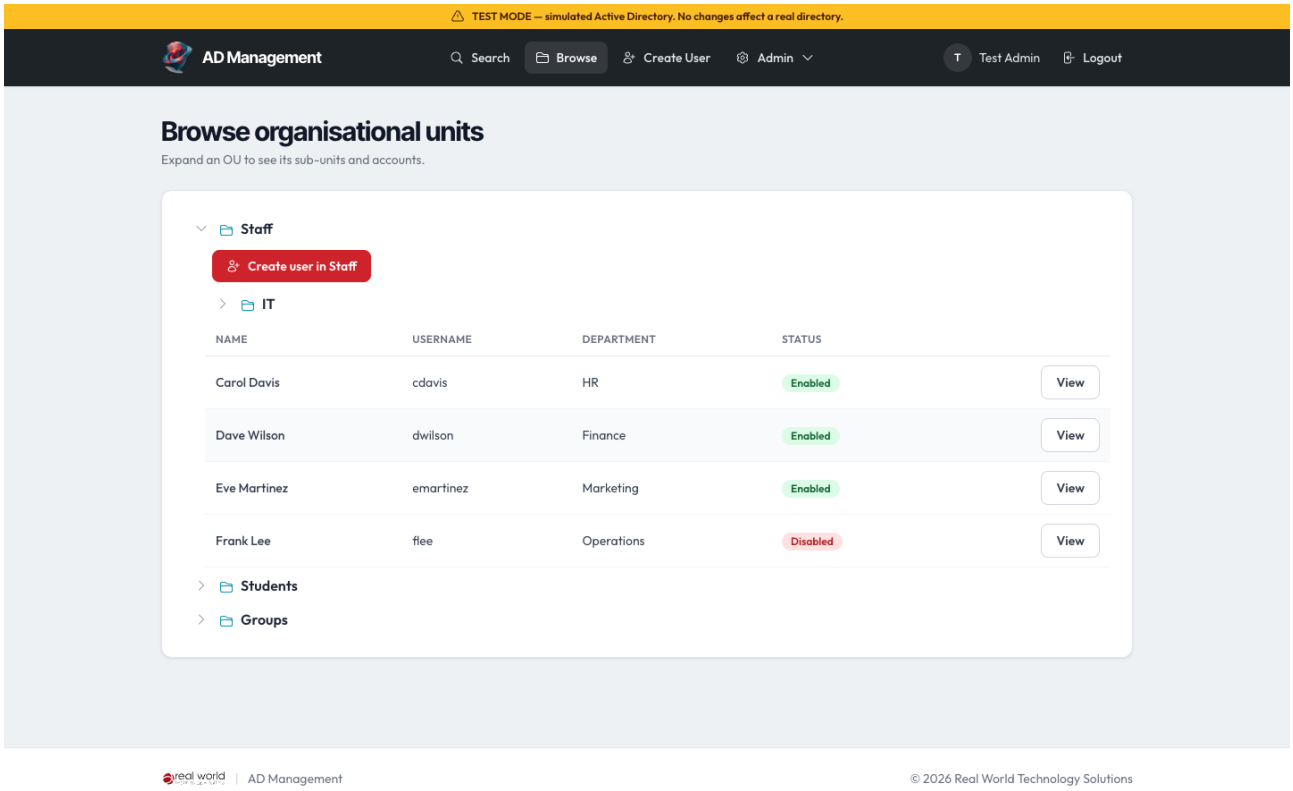
> Not sure which location a person is in? Try Browse the directory to explore the tree and spot them that way.

Browse the directory

Do this when you want to explore a part of your organisation's directory rather than search for a specific person.

NAVIGATE THE TREE

1. Open the **Browse** view from the main navigation.
2. Expand a branch to see its sub-units and the people inside them.
3. Keep expanding until you reach the location you need.



ABOUT WHAT YOU CAN SEE

You only see the branches you've been permitted to access. Branches outside your scope are not shown.

WORK FROM WITHIN A LOCATION

Each branch offers a shortcut to Create a new user already placed in that location — handy when you know exactly where a new starter should go.

Click any person in the tree to open their details page.

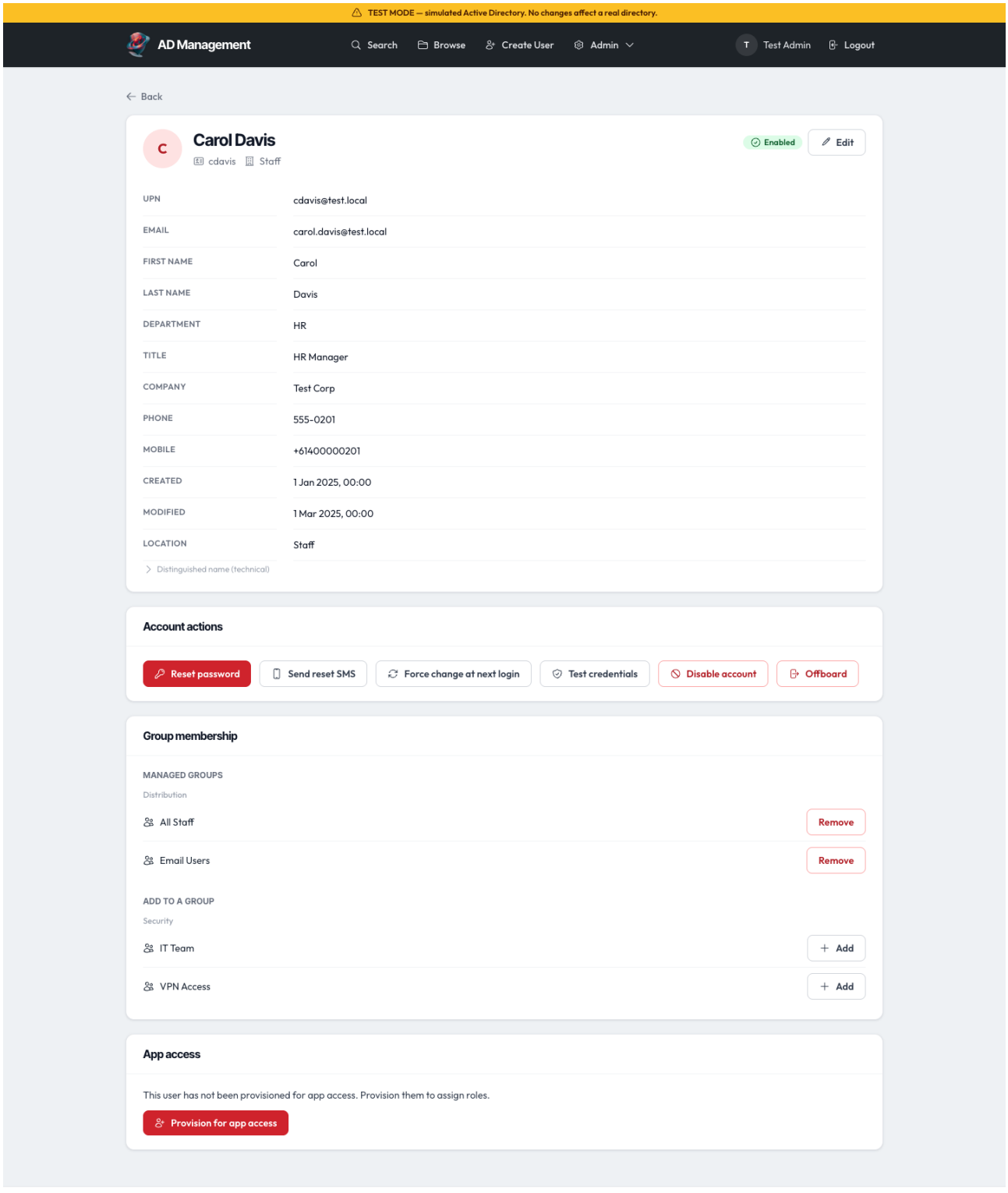
> Need to find a specific person quickly? Search is usually faster than browsing.

View a user's details

Do this to check someone's account status, location or group memberships, or to reach any action for that person.

real world technology solutions

WHAT YOU SEE



At the top, an identity header shows the person's name, avatar and a status badge indicating whether their account is **enabled** or **disabled**.

Below that, you'll see:

- Their **location** in plain, friendly language (not the raw technical path — expand **Technical details** if you need the full DN).
- **Created** and **Modified** dates in a readable format.
- An **action toolbar** with every action you're allowed to perform on this person — reset their password, edit their details, enable or disable the account, manage their groups, and more. Only the actions you have permission to use are shown.

Further down, the page groups the person's **group memberships** and any application or proxy-address details into sections.

> If an action you expect isn't visible, see Why some things are hidden.

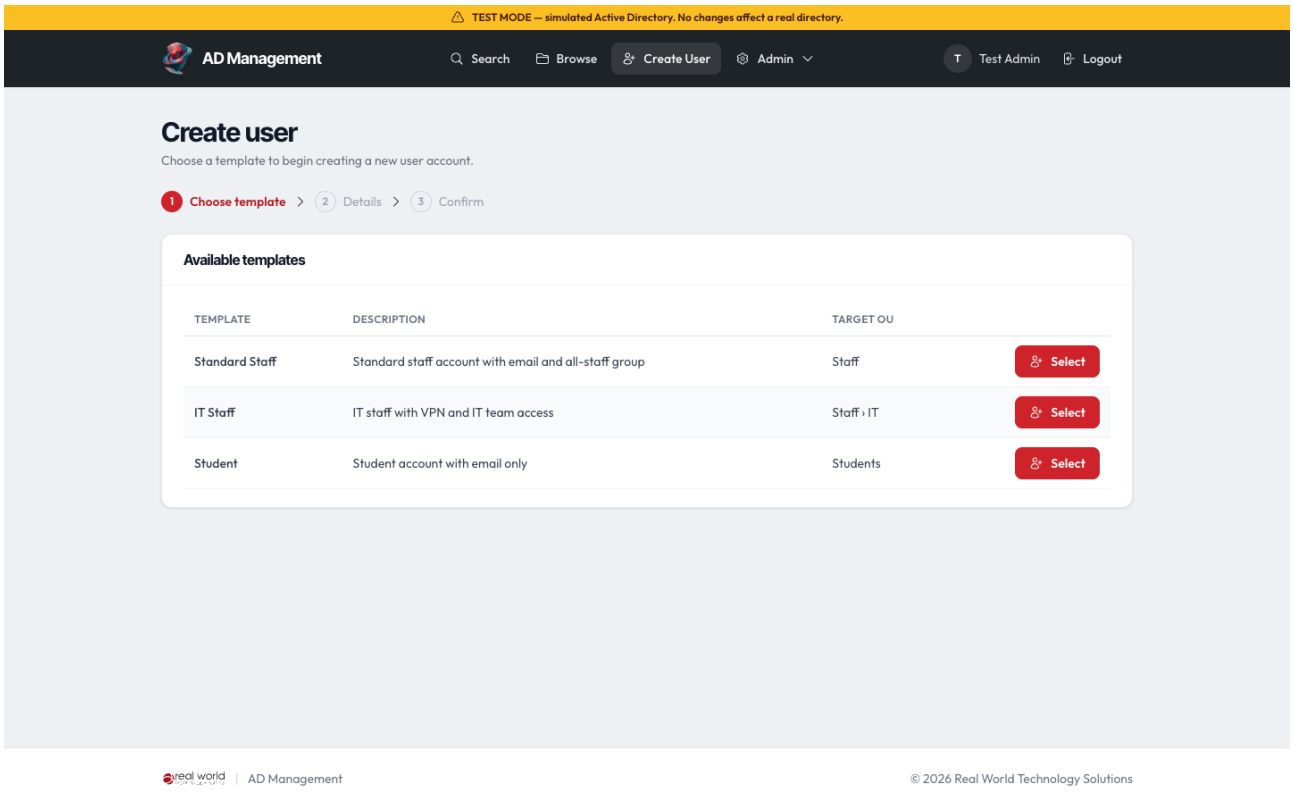
Create a new user

Do this when onboarding a new starter who needs an Active Directory account.

THE THREE-STEP WIZARD

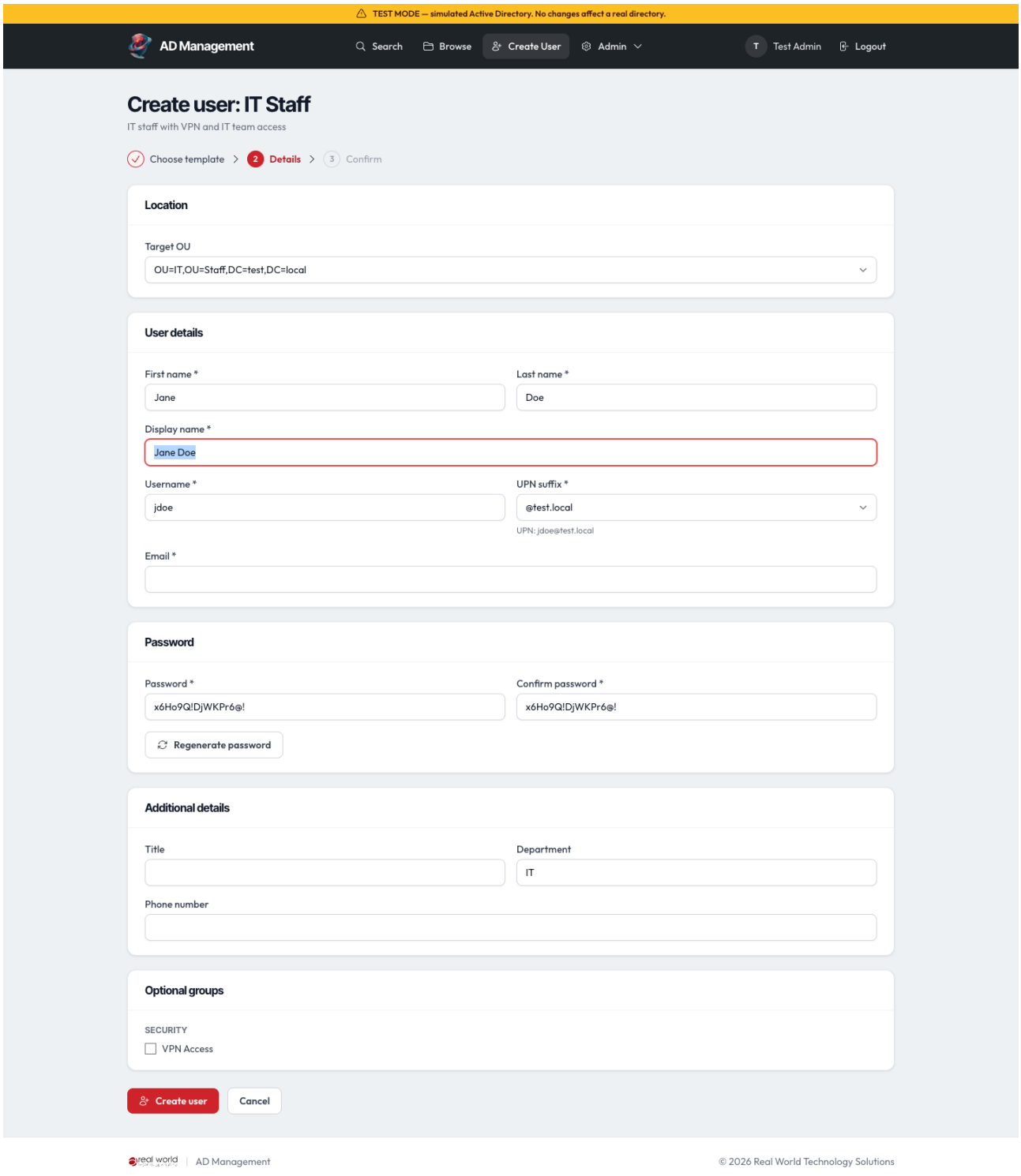
Step 1 — Choose a template

Select a user template for the new account. The template determines which organisational unit (location) the account will be created in and which groups it will receive by default. Choose the template that best matches the person's role.



Step 2 — Enter the person's details

Type the person's name. As you type, the wizard suggests a username, sign-in name (UPN) and email address for you — review these and edit them if needed.



Step 3 — Review and create

Check everything on the summary screen, then confirm to create the account.

SET THE FIRST PASSWORD

You can set the first password as part of, or immediately after, creation — see Reset a password for how the password reset screen works.

START FROM A LOCATION

If you already know where the new user should go, open that location in Browse and use the shortcut there — the wizard will open with the correct location pre-selected.

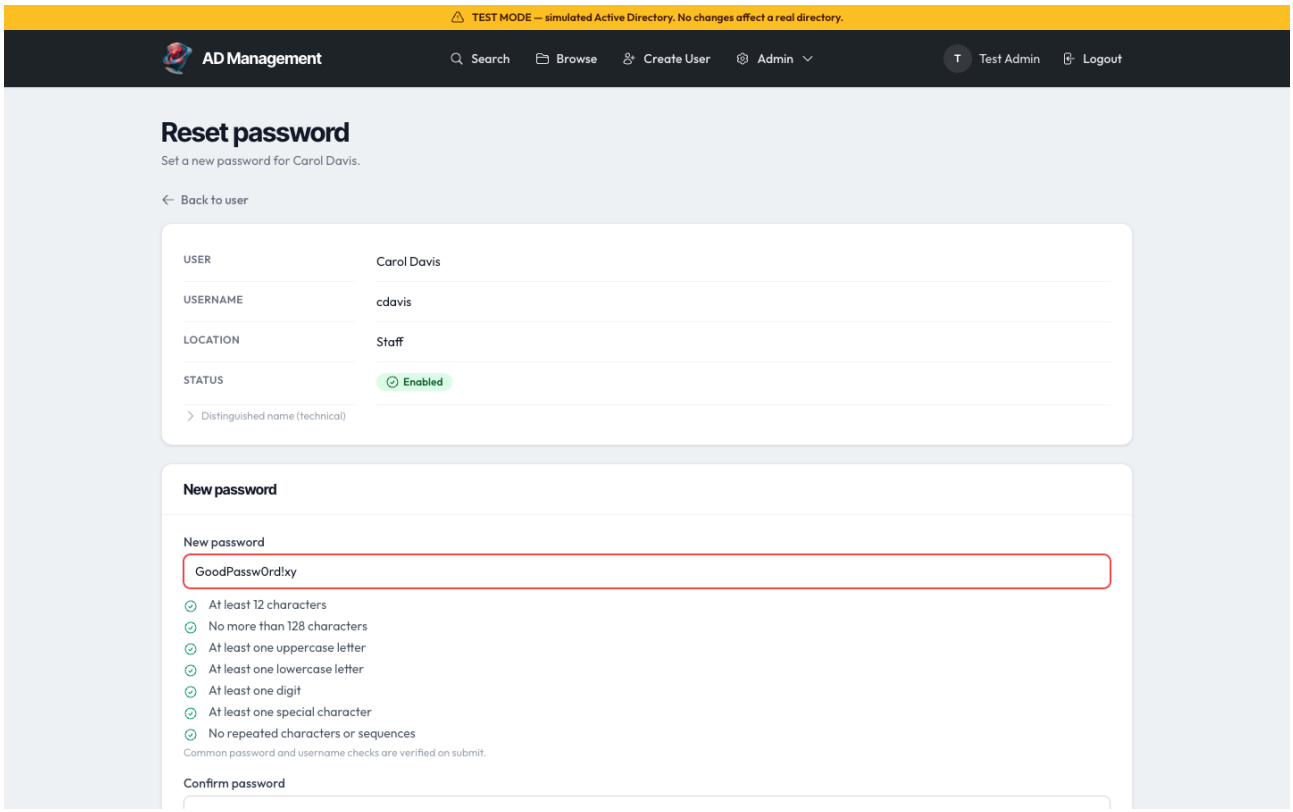
> Need to change which groups the account gets? That's controlled by the template — see User templates.

Reset a password

Do this when someone is locked out, has forgotten their password, or you're setting up a new starter.

RESET THE PASSWORD

1. Find the user and open their details page.
2. On the action toolbar, choose **Reset password**.
3. Either:
   - click **Generate** to create a strong random password that meets the policy, or
   - type a new password yourself — the strength meter shows whether it meets the policy.
4. Leave **Require the user to change their password at next sign-in** ticked unless you have a reason not to (recommended for any password you've seen).
5. Choose **Reset password**.



SHARE IT SAFELY

Read a generated password to the person directly or send it over a separate channel from their username — never email both together. Because **change at next sign-in** is on, the temporary password only gets them through the first login.

> Prefer not to handle the password at all? Send a reset link by SMS so the user sets their own.

IF IT DOESN'T WORK

- The account may be **disabled** rather than locked — see Locked vs disabled.
- If you don't see **Reset password**, you haven't been granted it for that user's location — see Why some things are hidden.

Send a password reset by SMS

Do this when you'd rather the user set their own password — you never see it at all.

SEND THE SMS

1. Find the user and open their details page.
2. On the action toolbar, choose to send a reset SMS.
3. If no mobile number is on file, enter one — it will be saved to the directory in full international format.
4. Confirm to send the message.

The user receives a link and uses it to set their own password directly.

IF THE MESSAGE DOESN'T ARRIVE

Check that the mobile number is correct, then see The reset SMS didn't arrive for further steps.

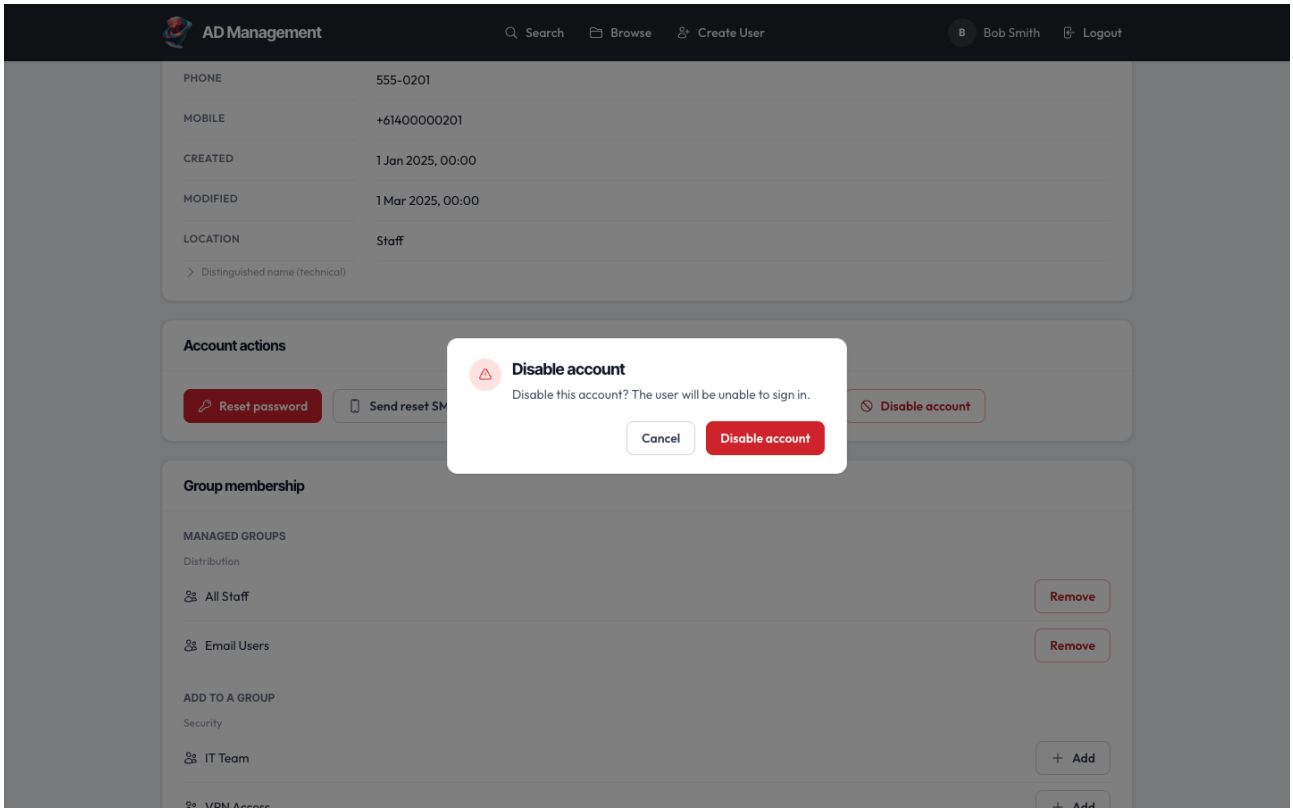
> Prefer to set the password yourself? Use Reset a password instead.

Enable or disable an account

Do this to immediately block or restore a person's access to the system.

DISABLE AN ACCOUNT

1. Find the user and open their details page.
2. On the action toolbar, choose **Disable**.
3. Confirm the action when prompted.



The account is blocked straight away — the person cannot sign in. Use this for a leaver, a suspected compromise, or any situation where access needs to stop immediately.

ENABLE AN ACCOUNT

1. Find the user and open their details page.
2. On the action toolbar, choose **Enable**.

The account is restored and the person can sign in again. Disabling is fully reversible.

DISABLING IS NOT OFFBOARDING

Disabling an account blocks sign-in, but it does not remove group memberships or run any leaver workflow. For a proper leaver process, use Offboard a leaver instead.

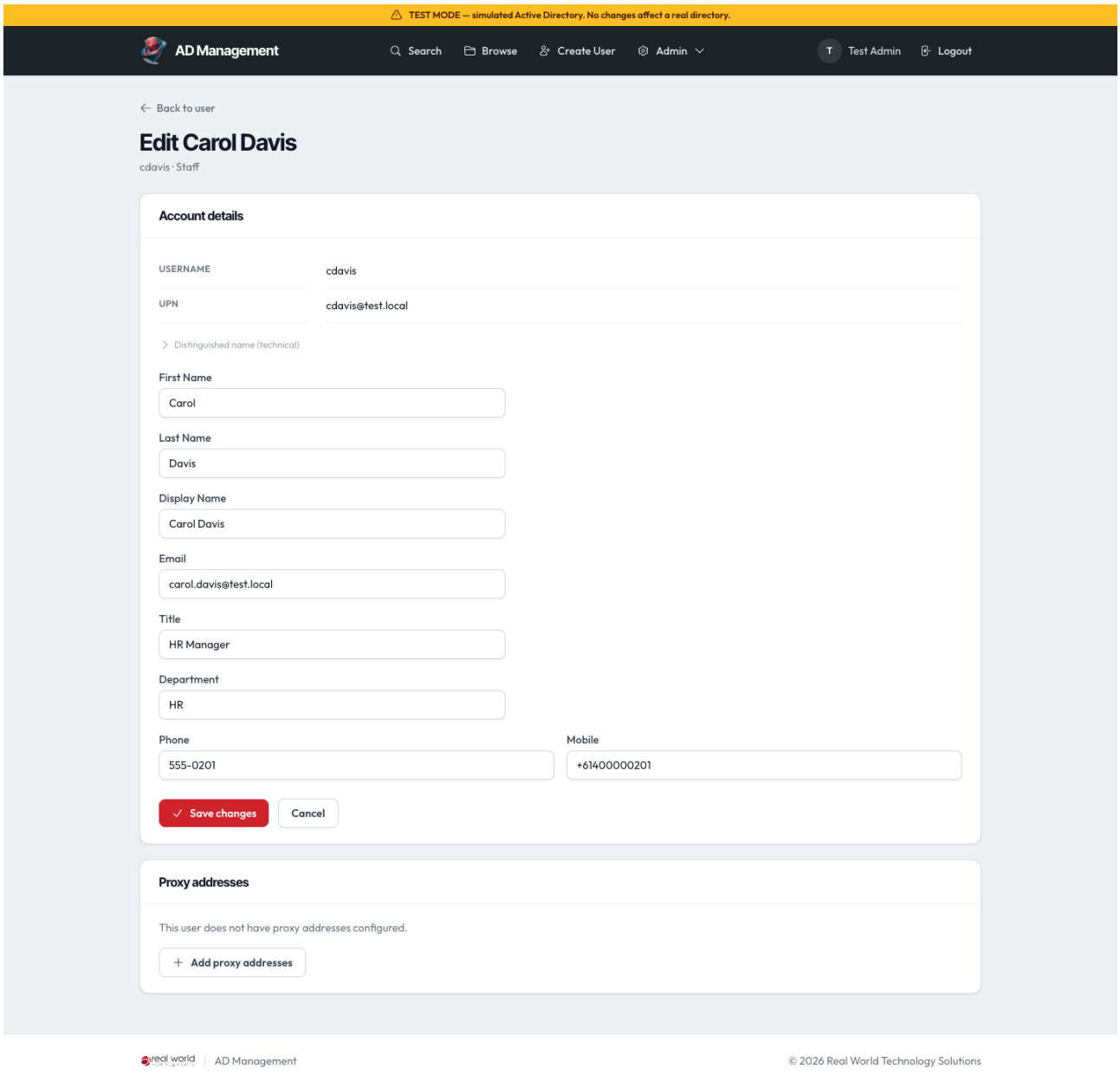
> Not sure whether an account is locked or disabled? See Locked vs disabled.

Edit a user's details

Do this when a person's name, contact details or proxy addresses need updating in the directory.

EDIT THE DETAILS

1. Find the user and open their details page.
2. On the action toolbar, choose **Edit**.
3. Update the fields you need to change — such as names, contact details, and the proxy-address list.
4. Save your changes.



Changes are written to the directory straight away.

CLOUD SERVICES TAKE A MOMENT TO CATCH UP

Microsoft 365 and other cloud services pick up changes on their next directory sync, so an update may not appear in those services immediately. See My change isn't showing yet if you need to understand why.

> Only the fields you're permitted to edit are shown. If a field you need is missing, speak to your administrator.

Manage group membership

Do this when a person needs access to a resource, system or distribution list that is controlled by a group.

ADD OR REMOVE A GROUP

1. Find the user and open their details page.
2. Scroll to the membership section.
3. Groups you're allowed to manage have **Add** or **Remove** controls next to them. Click the appropriate one.

The change takes effect in the directory straight away.

ABOUT READ-ONLY GROUPS

Some groups are shown without controls — these are groups the tool isn't configured to manage. You can view them but cannot change them here.

You can only add or remove a user from groups that an administrator has placed on the managed groups list. If a group you need isn't there, ask an administrator to add it.

> Not sure why a group has no controls? See Why some things are hidden.

Offboard a leaver

Do this when someone leaves the organisation and their account needs to be properly wound down.

RUN THE OFFBOARDING WORKFLOW

1. Find the user and open their details page.
2. On the action toolbar, choose **Offboard**.
3. Tick the steps you want to run — for example, disabling the account and removing group memberships according to policy.
4. Start the run.
5. Watch the status page as each step completes.

IF A STEP FAILS

You can retry any failed step individually without re-running the ones that already succeeded. See An offboarding step failed for more detail.

OFFBOARDING VS SIMPLY DISABLING

Offboarding runs a full leaver workflow — removing group memberships and any other configured steps — not just blocking sign-in. Simply disabling an account is quicker but less thorough; see Enable or disable an account if that's all you need.

Solving a problem

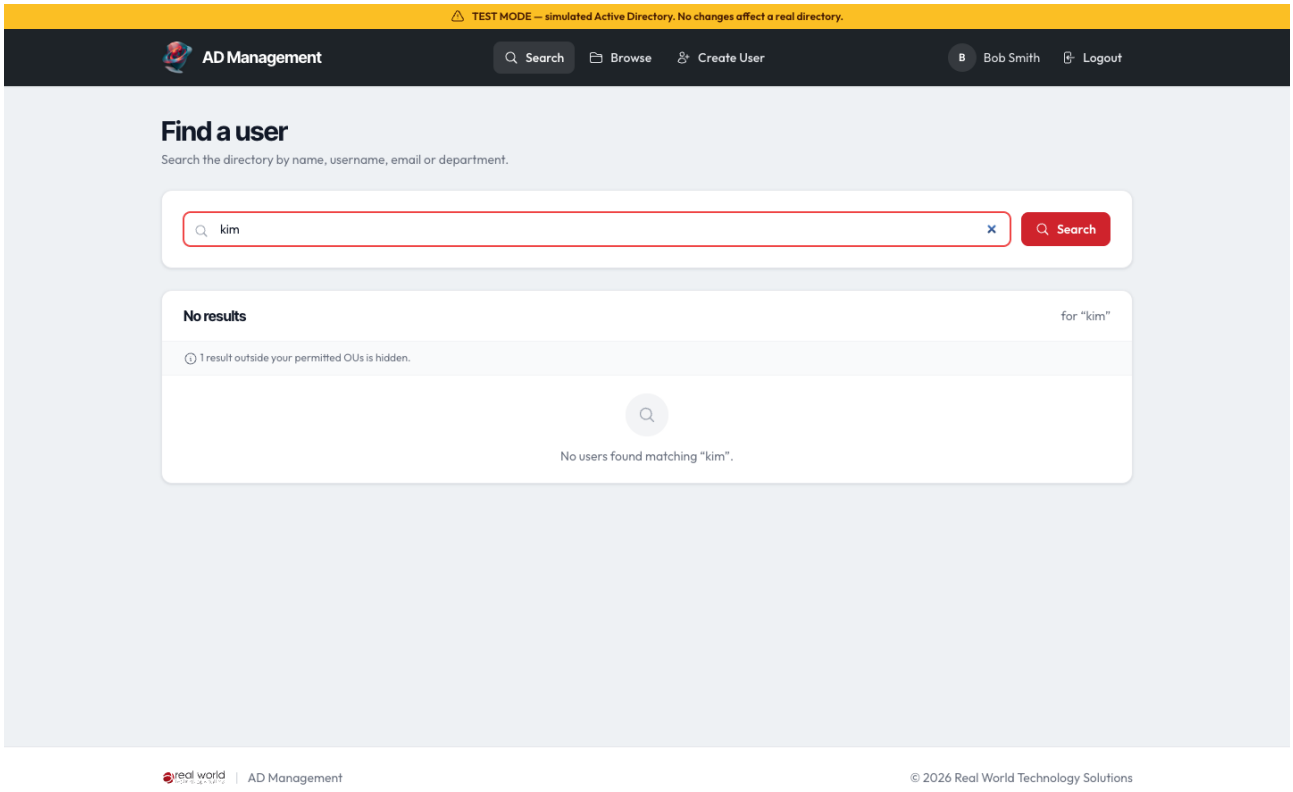
I can't see a user or an OU

If you can't find someone in search results or can't see a particular OU while browsing, it's most likely because that person or location sits outside the part of the directory you've been granted access to.

WHY THIS HAPPENS

Both Search and Browse are limited to the locations you've been given permission to work in. If a search finds matches elsewhere, it shows you a count of how many it has hidden rather than revealing them — that's intentional, not a bug.

See Why some things are hidden for more on how scoping works.



WHAT TO DO

- **Check your scope first.** The person may genuinely sit in a part of the directory you don't manage. That's expected.
- **Try a broader search term.** A middle name or partial username sometimes produces different results.
- **Ask your administrator to widen your scope** if you do need to manage people in that location. They can add the relevant OU to your role.

> If you can see the user but can't take an action, see A button I expected isn't there.

A button I expected isn't there

If a button you expected — such as **Reset password**, **Offboard**, or **Edit details** — is missing from the action toolbar on a user's page, nothing is broken.

WHY THIS HAPPENS

The toolbar only shows actions you're authorised to perform for that particular user's location. A missing action means one of two things:

- You haven't been granted that permission for the OU the person sits in, or
- The action is administrator-only and isn't available to your role.

The app doesn't show greyed-out or locked buttons — it simply doesn't show actions you can't take. See Why some things are hidden for the full explanation.

WHAT TO DO

- **Check you're looking at the right person.** If the user is in a different OU than you expect, their toolbar will reflect permissions for that location.
- **Contact your administrator** if you need the permission. Let them know which action you need and for which part of the directory.

The reset SMS didn't arrive, or a mobile won't save

If a reset SMS didn't reach the user, or you're having trouble saving a mobile number to their account, here's what to check.

SMS DIDN'T ARRIVE

- **Verify the number is correct.** Open the user's details and confirm the mobile field contains the right number in full international format (e.g. `+61 4xx xxx xxx`).
- **Check for delays.** Delivery can occasionally take a minute or two depending on the carrier.
- **Try a direct reset instead.** As a reliable fallback, you can reset the password directly and share the new password with the user over a separate channel.

MOBILE NUMBER WON'T SAVE

If saving a mobile number fails, the app will show a warning — it no longer fails silently. The most common causes are:

- **You don't have permission** to write that field for the user's location.
- **A cloud sync is overwriting on-prem changes** — your directory sync may be pushing the old value back from Microsoft 365.

In either case, contact your administrator to investigate the sync configuration or grant the necessary write permission.

"Access denied" after signing in

If you signed in successfully but the tool shows an "Access denied" message, your account authenticated with your organisation but hasn't been authorised to use this tool.

WHY THIS HAPPENS

Authentication (proving who you are) and authorisation (being allowed to use the tool) are separate steps. Most staff will authenticate just fine but won't have a role assigned in AD Management — that's expected, because most people don't administer the directory.

WHAT TO DO

1. **Confirm you're signing in to the right tool.** Check the URL matches the one your IT team gave you.
2. **Contact your administrator.** Ask them to assign you a role in AD Management. Let them know what you need to do (for example, reset passwords for a specific department).

Once a role is assigned, sign out and back in — see Signing in if you need a reminder of how that works.

An offboarding step failed

If a step in an offboarding run shows a failure, don't worry — the status page tells you exactly what went wrong, and other steps in the same run may have completed successfully.

WHY THIS HAPPENS

Common causes include:

- A **directory-permission issue** preventing the required change.
- A **group or attribute that had already been changed** before the offboarding ran — for example, someone manually removed a group membership earlier.

WHAT TO DO

1. **Read the error shown on the status page.** It describes what failed and often points to the cause.
2. **Address the underlying issue** — fix the permission, or confirm whether the change had already been made manually.
3. **Use Retry on the failed step.** Once the cause is resolved, retry brings that step back into line without re-running the steps that succeeded.
4. **If it keeps failing**, copy the error message and pass it to your administrator to investigate.

See Offboard a leaver for the full offboarding workflow.

real world technology solutions

Locked vs disabled — what's the difference?

If a user can't sign in, check the status badge on their details page — it tells you whether the account is **locked** or **disabled**, which matters because the fix is different for each.

LOCKED

A locked account usually means too many failed sign-in attempts triggered a lockout policy. It will often clear on its own after a short waiting period, or you can reset the password — a successful reset typically lifts the lockout at the same time.

DISABLED

A disabled account was deliberately switched off. It won't become usable on its own — someone has to explicitly turn it back on. See Enable or disable an account for how to do that.

QUICK GUIDE

STATUS	CAUSE	FIX
Locked	Too many failed sign-in attempts	Wait, or reset the password
Disabled	Manually switched off	Explicitly re-enable the account

If you're not sure which applies, the status badge on the user's page makes it clear before you take any action.

My change isn't showing yet

If you've made a change in AD Management but it isn't reflected in Microsoft 365 or Entra yet, that's normal — give it a few minutes.

WHY THIS HAPPENS

This tool writes to your on-premises Active Directory immediately. However, Microsoft 365 and Entra pick up changes on a directory sync schedule, which typically runs every few minutes. The delay is on Microsoft's side, not ours.

WHAT TO DO

- **Wait and refresh.** Allow the sync cycle to run — usually a few minutes is enough. Refresh the relevant Microsoft 365 page or application afterwards.
- **Check you changed the right thing.** Some settings — mailbox configuration, licences and cloud-only accounts — are managed in the Microsoft 365 admin centre, not here. If the change you need isn't available in this tool, that's why.

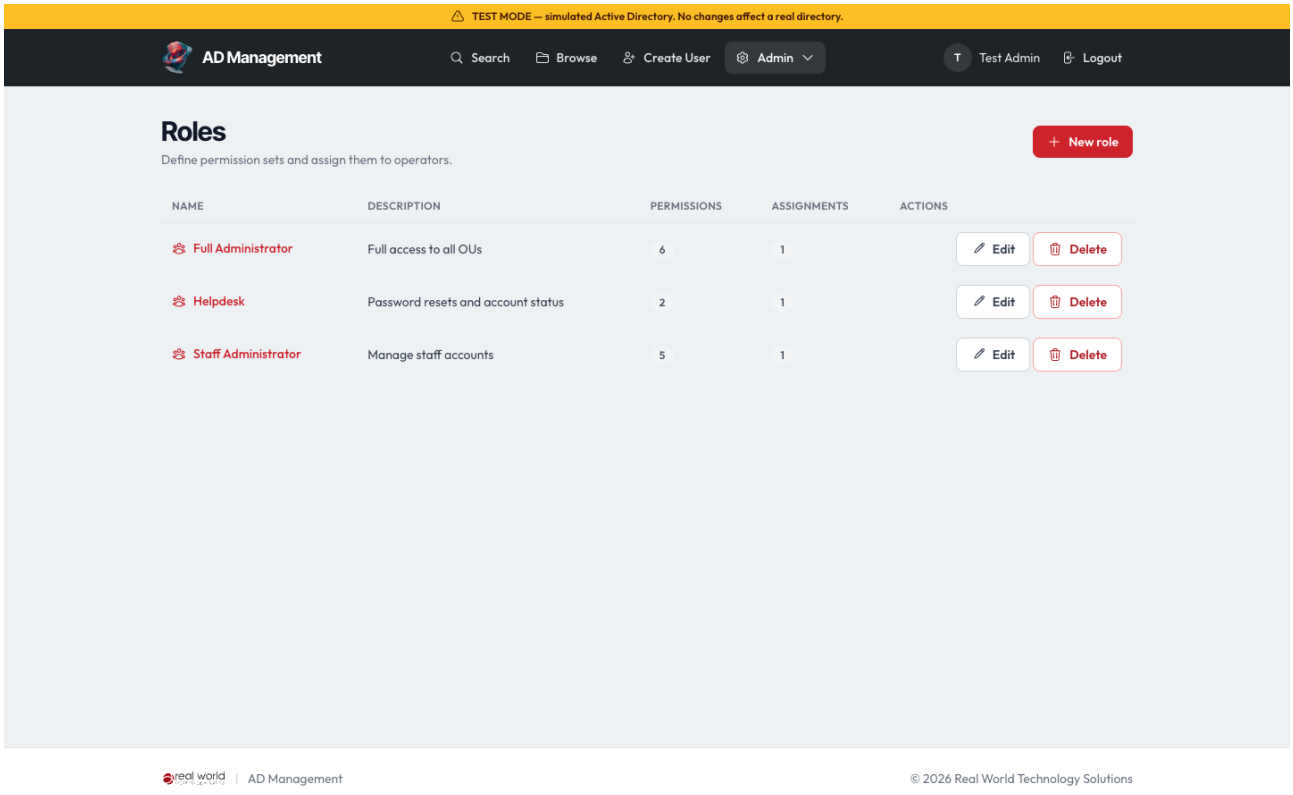
See Welcome to AD Management for a clear picture of what this tool manages and what belongs in Microsoft 365.

> If you changed a user's details here and the field has reverted, a cloud sync may be overwriting on-prem changes. Contact your administrator to investigate the sync configuration.

For occasional admins

Roles & access

A role is the unit of access in AD Management — it bundles a set of permitted actions and ties each one to one or more locations (organisational units) in the directory. Operators see only the features they've been given permission to use, and only for the users whose OU falls within their allowed scope.



WHAT A ROLE CONTAINS

Each role carries any combination of these permissions:

- **Create user** — provision new accounts
- **Reset password** — set or force-reset a password
- **Edit user** — update account attributes
- **Enable / disable account** — toggle account status
- **Manage groups** — add and remove users from managed groups
- **Offboard user** — run the offboarding workflow

Every permission is scoped to specific OUs. An operator with "Reset password" in `OU=Helpdesk,DC=…` cannot reset passwords for users in any other part of the directory.

ASSIGNING ACCESS

Open a role and use the **Assign** tab to give an operator that role. You can only grant permissions you hold yourself — the tool prevents self-escalation.

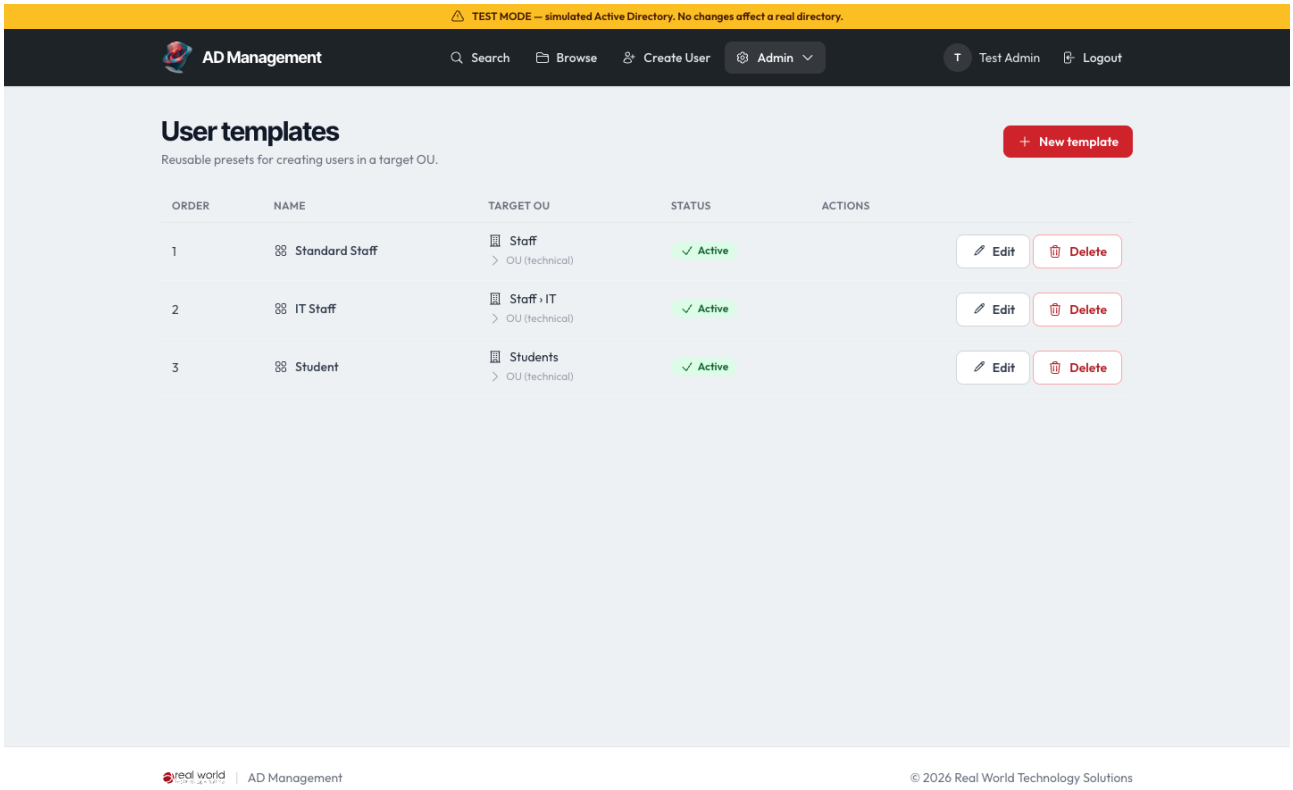
Super-administrators bypass all scoping and can do everything, regardless of OU.

RELATED ARTICLES

Not sure why a control is missing for a user? See Why some things are hidden.

User templates

A user template is a reusable starting point for the create-user wizard. When an operator picks a template, it pre-fills the destination location and the group assignments for the new account, so they don't have to configure those details from scratch every time.



WHAT A TEMPLATE SETS

- **Location** — the organisational unit (OU) the new account will be placed in.
- **Default groups** — groups automatically added to every account created from this template. The operator cannot remove these during creation.
- **Optional groups** — groups offered as tick-box choices during creation. The operator can include or exclude them as appropriate.

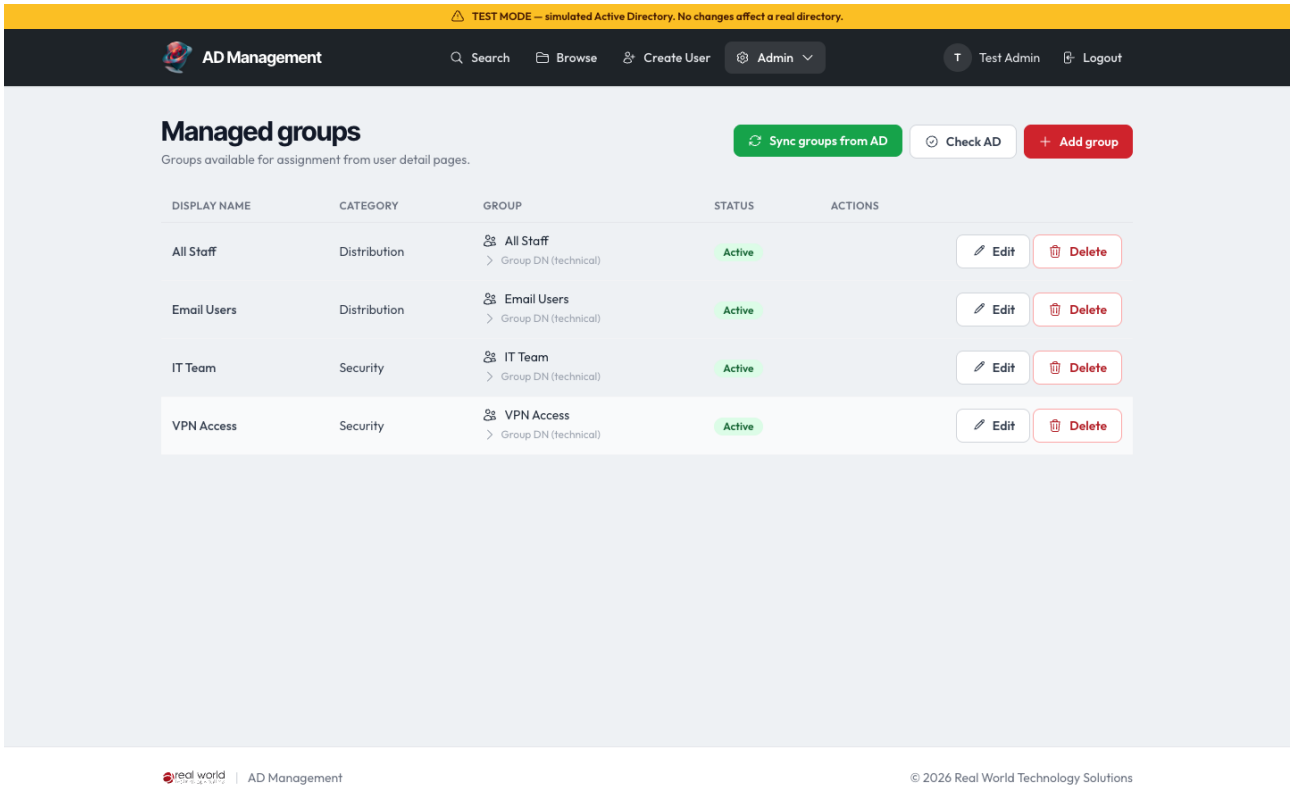
KEEPING TEMPLATES USEFUL

Aim for one template per common type of starter — for example, one for full-time staff in a given department, one for contractors, one for service accounts. That way operators simply pick the right template and the sensible defaults follow automatically.

If your organisation adds a new team or location, add a template for it so operators always have a correct starting point and new accounts consistently land in the right place with the right groups.

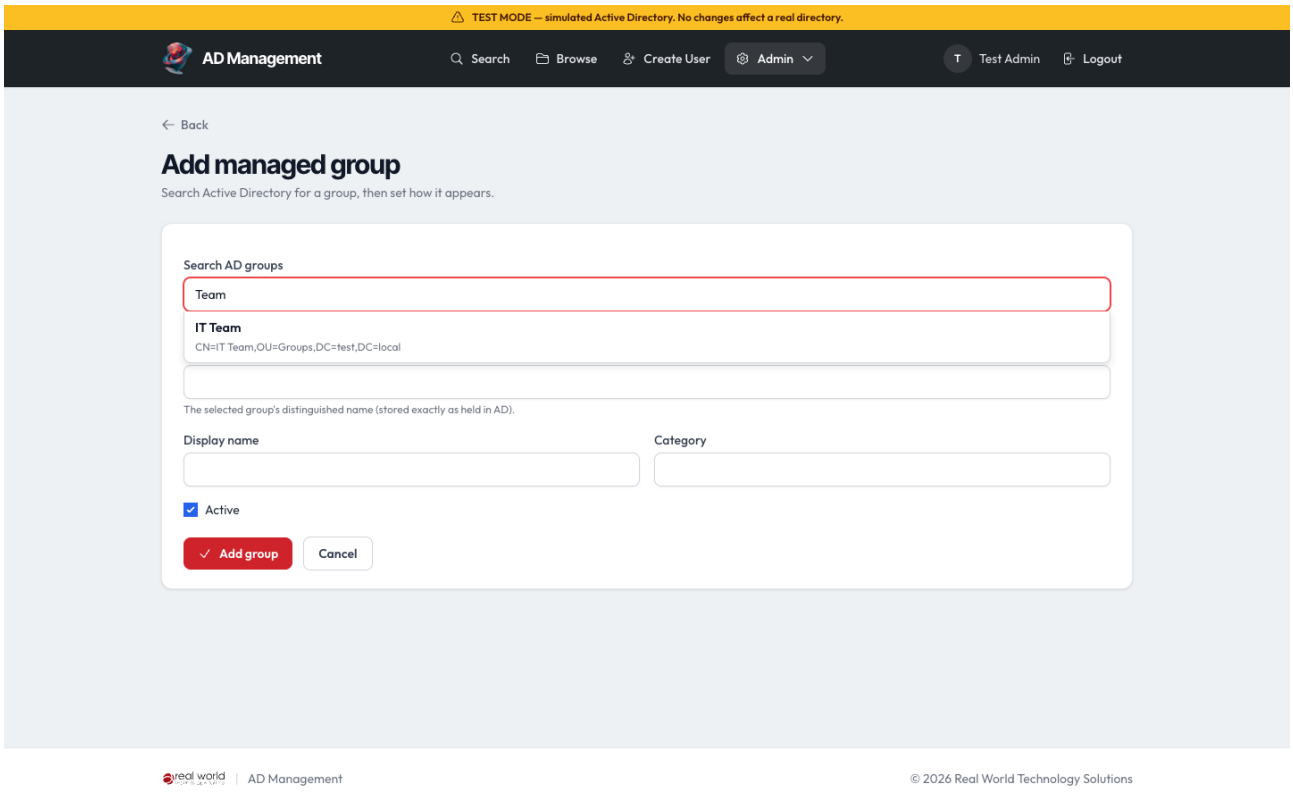
Managed groups

Only groups on the managed list can be changed from a user's detail page. This keeps operators from accidentally adding or removing membership from groups the tool isn't supposed to touch.



ADDING A GROUP

Click **Add group** and start typing a name. A type-ahead autocomplete searches the directory and shows matching groups as you type — select the one you want to add.



Once added, operators with the manage groups permission will see **Add** and **Remove** controls for that group on user detail pages.

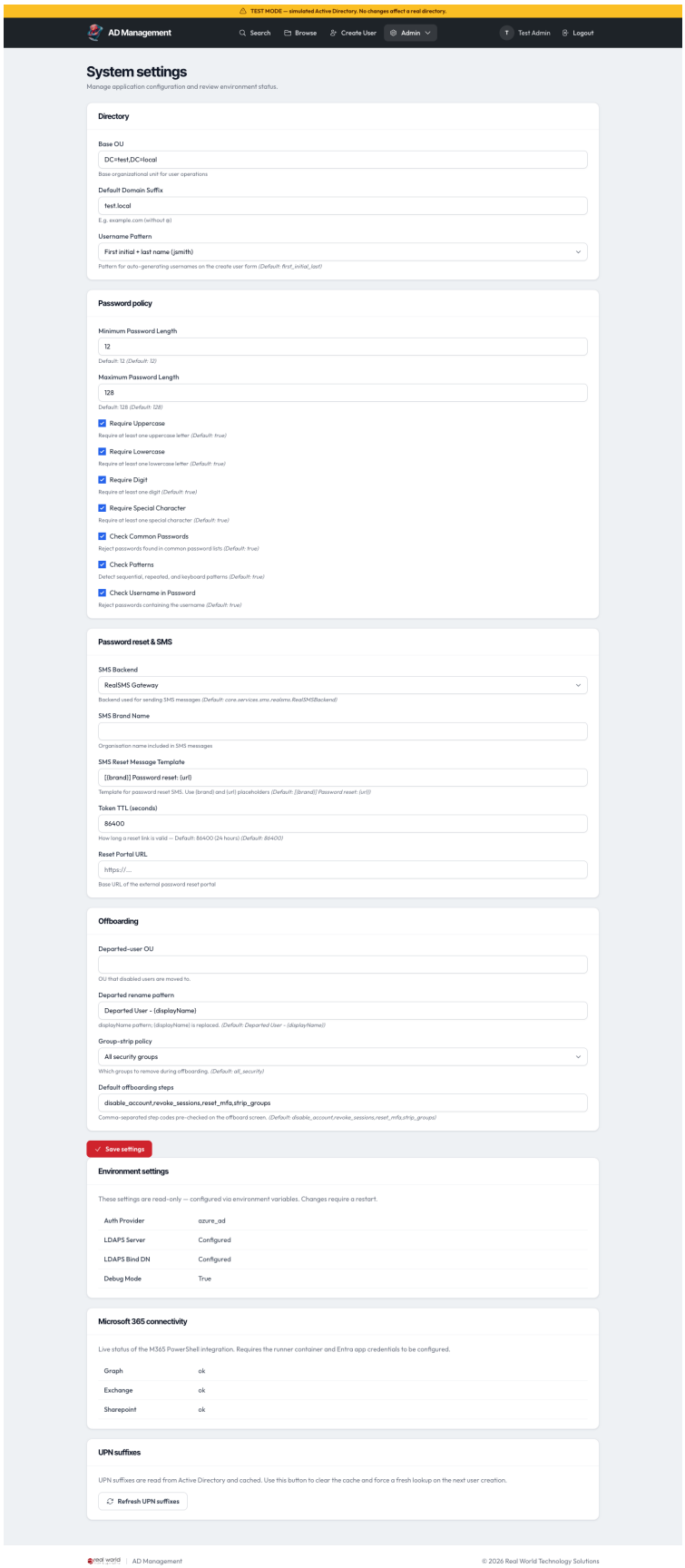
KEEPING THE LIST ACCURATE

Directory groups can be renamed, moved or deleted outside this tool. Use the **Check / sync** action to run a staleness check against the live directory — any group that no longer exists or has moved will be flagged so you can update or remove it from the managed list.

Running this check periodically keeps the managed list accurate and avoids operators seeing stale group names.

Settings

The settings page collects all configurable options in one place, organised into groups so related settings stay together.


TEST MODE — simulated Active Directory. No changes affect a real directory.
AD Management
Search
Browse
Create User
Admin
Test Admin
Logout
System settings
Manage application configuration and review environment status.
Directory
Base OU
DC=test,DC=local
Base organizational unit for user operations
Default Domain Suffix
test.local
E.g. example.com (without @)
Username Pattern
First initial + last name (jsmith)
Pattern for auto-generating usernames on the create user form (Default: first_initial_last)
Password policy
Minimum Password Length
12
Default: 12 (Default: 12)
Maximum Password Length
128
Default: 128 (Default: 128)
Require Uppercase
Require at least one uppercase letter (Default: true)
Require Lowercase
Require at least one lowercase letter (Default: true)
Require Digit
Require at least one digit (Default: true)
Require Special Character
Require at least one special character (Default: true)
Check Common Passwords
Reject passwords found in common password lists (Default: true)
Check Patterns
Detect sequential, repeated, and keyboard patterns (Default: true)
Check Username in Password
Reject passwords containing the username (Default: true)
Password reset & SMS
SMS Backend
RealSMS Gateway
Backend used for sending SMS messages (Default: core.services.sms.realsms.RealSMSBackend)
SMS Brand Name
Organisation name included in SMS messages
SMS Reset Message Template
[{brand}] Password reset: {url}
Template for password reset SMS. Use {brand} and {url} placeholders (Default: [{brand}] Password reset: {url})
Token TTL (seconds)
86400
How long a reset link is valid — Default: 86400 (24 hours) (Default: 86400)
Reset Portal URL
https://...
Base URL of the external password reset portal
Offboarding
Departed-user OU
OU that disabled users are moved to.
Departed rename pattern
Departed User - {displayName}
displayName pattern; {displayName} is replaced. (Default: Departed User - {displayName})
Group-strip policy
All security groups
Which groups to remove during offboarding. (Default: all_security)
Default offboarding steps
disable_account,revoke_sessions,reset_mfa,strip_groups
Comma-separated step codes pre-checked on the offboard screen. (Default: disable_account,revoke_sessions,reset_mfa,strip_groups)
Save settings
Environment settings
These settings are read-only — configured via environment variables. Changes require a restart.
Auth Provider
azure_ad
LDAPS Server
Configured
LDAPS Bind DN
Configured
Debug Mode
True
Microsoft 365 connectivity
Live status of the M365 PowerShell integration. Requires the runner container and Entra app credentials to be configured.
Graph
ok
Exchange
ok
Sharepoint
ok
UPN suffixes
UPN suffixes are read from Active Directory and cached. Use this button to clear the cache and force a fresh lookup on the next user creation.
Refresh UPN suffixes
AD Management
© 2026 Real World Technology Solutions

SETTING GROUPS

Directory — controls how the tool connects to and reads from your Active Directory, including the base location for searches and the default domain suffix for new accounts.

Password policy — governs the rules applied when passwords are generated or validated: minimum length, required character classes, and similar constraints.

Password reset & SMS — configures how the tool delivers temporary passwords to users, including SMS gateway settings for sending reset codes.

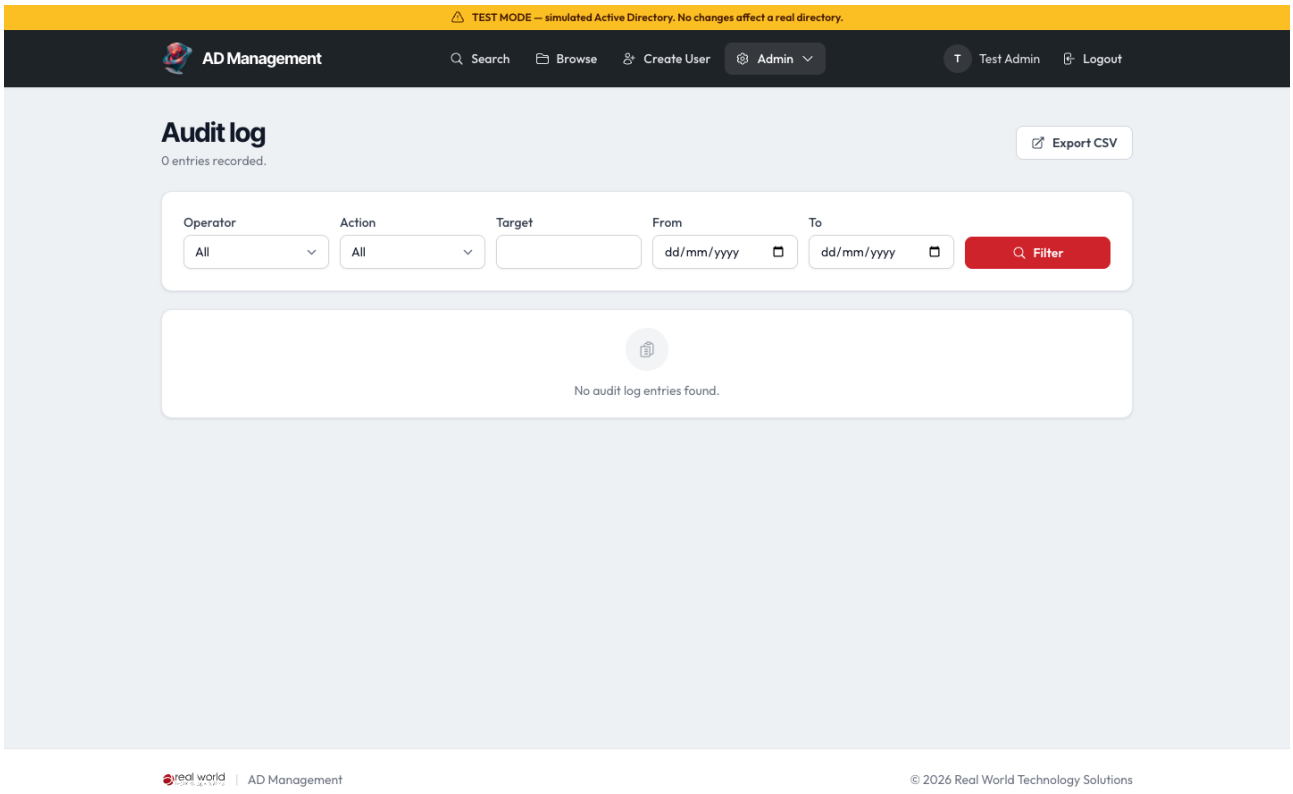
Offboarding — defines what happens when an account is offboarded: which groups to remove, whether to disable the account, and where (if anywhere) to move it.

READ-ONLY VALUES

Some settings come from the deployment environment — environment variables set at the server level — and are shown here as read-only. They can only be changed by updating the deployment configuration. The read-only label makes it clear which values fall into this category.

Audit log

Every action taken through AD Management is automatically recorded — who did it, what they did, which account was affected, and when. The audit log gives you a complete, searchable history of operator activity.



FILTERING THE LOG

Use the filter bar to narrow the view:

- **Operator** — see activity by a specific person.
- **Action** — filter to a particular action type, such as password resets or account disables.
- **Target** — find all entries relating to a specific account.
- **Date range** — restrict the view to a time window.

Filters can be combined. The results update immediately.

VIEWING ENTRY DETAIL

Click any row to expand it and see the full details recorded for that action, including any before/after attribute values captured at the time.

EXPORTING TO CSV

Click **Export CSV** to download the current filtered view as a spreadsheet. The export respects all active filters, so narrow the view first if you only need a subset of the log.