

Identity and Access Management — End-user Guide

Full account, access administration, configuration, RBAC/ABAC, governance and audit procedures.

Use the current tenant, profile and permitted actions. Screenshots illustrate the application; example records and date fields may differ in your environment.

Contents

1. Using the IAM user manual
2. Detailed operating model and record lifecycles
3. Decision branches and exception handling
4. Component crosswalk for this module
5. The terms users and administrators need
6. Architecture and ownership boundaries
7. Use the standard screens, grids and record pages
8. Applicant requests an account and verifies email
9. Maker classifies; checker independently approves
10. Enroll credentials and complete the first sign-in
11. Admin-created versus subscribed-user journey
12. Maker creates the account
13. Inspect Progress and activate the account
14. Maker proposes the domain and profile
15. Independent checker reviews the originating record
16. Verify enrollment delivery and hand over to the user
17. Sign in, select a profile and work safely
18. Read account progress, personal information and settings
19. Verify sensitive actions, change credentials and recover access
20. Change, expire, revoke, suspend and restore access
21. Use this dependency order
22. Create the Domain
23. Create the Role
24. Create the Profile
25. Create a Permission or select an existing one

26. Map Domains ↔ Profiles
27. Map Profiles ↔ Roles
28. Grant Permissions to the Role
29. Maintain Menu Access and role/menu actions
30. Map Permissions ↔ Menus and inspect the screen bridge
31. Maintain Axis screens, fields and labels
32. Screen ownership mappings and presentation changes
33. Map control permissions and field restrictions
34. Configure and verify ABAC conditions
35. Field security: hidden, read-only, editable and masked
36. Review changes on the originating IAM record
37. Administer client approval rules
38. Verify dynamic navigation and RBAC/ABAC
39. Control menu availability windows
40. Maintain governed record details and inactive records
41. Configure and verify federated sign-in
42. Delegate access for a bounded period
43. Apply separation of duties and timed exceptions
44. Run an access-review campaign
45. Use just-in-time and emergency access
46. Investigate sign-ins, failures and sessions
47. Trace creation, approval and first use
48. Open notifications and review their current outcome
49. Troubleshooting administration and access
50. Resolve registration, enrollment and sign-in problems
51. Understand the states before moving to the next step
52. Table linkage and architectural reference
53. Complete IAM screen directory and entry points
54. Worked case · Build and diagnose the complete account-to-screen authorization chain
55. New domains start with no linked profiles
56. Use the named Kernel Super Administrator exception

Using the IAM user manual

Use this end-user guide for daily tasks. Choose a task below to open its operating procedure. The remaining chapters explain field meanings, lifecycle, approvals, exceptions and related components.

Task route	Open procedure
Set up the access masters and mappings	Start this route
Create a user as an administrator	Start this route
Onboard a self-registered user	Start this route
Operate and govern existing access	Start this route

Administer user onboarding, accounts, domains, profiles, roles, permissions, menus and the IAM-to-Axis bridges. Use the task chapters for subscription and administrator-created account flows, then governance, security and audit operations.

Sign in with an assigned account, choose the intended tenant/domain and effective profile, and use the authorized menu or screen search. A profile name alone does not establish access. The server rechecks permissions, current context, record state and relevant attributes.

Use a different eligible identity for independent review. Switching profiles on one account does not create a second person. Review the exact submitted revision; changes after review may require a new preview and decision.

Observation	Action
Menu missing	Check effective domain/profile, role-to-menu/permission mappings and menu-to-Axis screen bridge.
Screen visible but read denied	Check the screen read permission and current ABAC context; menu visibility alone is insufficient.
Action hidden or disabled	Inspect assigned permission, record state, ownership and independent-review eligibility.
Form loaded then session expired	Sign in again and reload the saved record. Inspect whether the last submission succeeded before repeating it.

Detailed operating model and record lifecycles

Use the master screens to define identities and the mapping actions to relate them. Domain, Profile, Role, Permission and Menu remain separate masters. A new mapping enables a relationship; it should not be mistaken for editing the target master. Record the master ID and mapping ID separately when comparing reviews.

The effective profile determines the role closure used for access. The presence of another profile on the same account does not automatically union all its roles into the selected context. The menu is an authorized navigation link to an Axis screen; data read, controls and mutations still need their own permission and ABAC checks.

There are four different decisions in a normal journey: the account may sign in, the selected tenant/domain/profile may be used, the screen may be read, and the proposed business action may execute on that record. Testing only menu visibility misses the last two. A hidden button and a backend denial are complementary controls.

CHAPTER 3

Decision branches and exception handling

Situation	Check / next action	Reason / expected effect
Menu missing	Check selected profile role closure, menu linkage, active/effective mappings and screen bridge	Do not insert a static sidebar item to hide an authorization gap.
Menu visible but 403 on the screen	Check screen-read permission and current ABAC context	Menu visibility is not proof that the read endpoint is authorized.
Checker sees pending row but no approve action	Check exact action grant, assignment, record state, subject separation and freshness	Switching profile does not change the submitting subject identity.
Field visible but read-only	Inspect control permission and field policy	A display format change in Axis will not grant update authority.
500 DB_EXEC_ERROR	Record route, timestamp and correlation; inspect server-side failure	A database execution failure is not fixed by repeatedly broadening permissions.

Diagnose the first failed boundary in order: session, selected context, effective mapping, screen read, field/action permission, ABAC/record state, owner execution. Keep 401, 403 and 500 distinct. Refreshing a session may be appropriate after authorized changes, but repeated refreshes do not repair missing grants or broken database functions. Support evidence should include the selected profile ID and failing operation, not passwords or cookies.

CHAPTER 4

Component crosswalk for this module

Component	Information passed	Responsibility at the boundary
Axis	Menu-to-screen and permission-to-control IAM bridges	Axis defines what is rendered; IAM constrains who may read or act.
Tenant Engine / TCP	Current tenant context and module eligibility	Tenant-level use and user-level authorization must both be satisfied.

Component	Information passed	Responsibility at the boundary
Regulix / native review owner	Review task and submitting/reviewing subject references	Task assignment does not erase independent-review or owner-state checks.
Core / application	Business identity and personal profile references	Authentication identity and business/KYC data have separate ownership.

Keep the source record and its current version when following an integration. A navigation link, a matching label or a technical receipt cannot substitute for the next owner's authorization and business decision.

[Open the complete Kernel platform crosswalk →](#)

CHAPTER 5

The terms users and administrators need

Term	Meaning in this application
Tenant	The customer/workspace boundary. Domain/profile operations take place within the permitted tenant context.
Domain	An organization, provider or business-responsibility context. It is not an email domain.
Access profile	The selectable responsibility bundle with eligible domains and roles. It is not the person's name/contact profile.
Role	A reusable job-function bundle of functional permissions. A name such as Maker does not establish permission by itself.
Permission	A definition tied to a registered resource/action; a role needs an effective grant for it.
Menu	A registered navigation entry whose access requirements are evaluated by IAM.
Screen / control	Axis rendering definitions: screen metadata and its fields, buttons and actions. IAM controls authorized use.
Assignment	The link giving one user an eligible profile in its tenant/domain context, subject to state and dates.
Maker / Checker	The proposer and an eligible independent reviewer. Two profiles on one account do not create two independent people.
RBAC / ABAC	Role-based permission checks / contextual policy checks. Both can matter for the same operation.
Approved / effective / published	A decision, currently usable access, and published rendering are distinct checkpoints.
Active / is_active / expiry	Availability and lifecycle controls. An active flag alone does not establish a valid assignment, current credentials or permission.

Architecture and ownership boundaries

Relationship	Cardinality / ownership	What to explain
Domain ↔ Profile	M:M · IAM	Where a profile is eligible; does not assign it to a user
Profile ↔ Role	M:M · IAM	The role bundle inherited by an assigned user context
Role ↔ Permission	M:M · IAM	Functional grants, including registered operations and effects
Permission ↔ Menu	M:M · IAM	Requirements for navigating to and using a registered menu
Role ↔ Menu access view	IAM administration projection	Maintain allowed screen actions; effective access still depends on permissions and conditions
User Account → Profile assignment	IAM · within tenant/domain context	The explicit assignment and its validity
Menu ↔ Axis Screen	1:1 bridge owned by IAM	Link to the published screen identity; do not move authorization into Axis
Permission ↔ Screen Fields / Controls	M:M bridge owned by IAM	Apply requirements to controls, actions and fields
Axis Screen → Controls / Fields	1:M · Axis	Layout, labels, format and presentation metadata
Personal/business user profile ↔ User Account	Application boundary · distinct from access profile	Names, contact/KYC are not the role bundle selected for authorization

The selected effective assignment supplies the tenant/domain/profile context. IAM resolves its roles and grants, evaluates applicable RBAC and ABAC, returns permitted navigation and enforces protected operations. Axis supplies the published screen/control metadata. Account, assignment, master and menu availability and validity windows remain relevant.

Use the standard screens, grids and record pages

1. Confirm the domain and selected profile in the header before making a change. Use the sidebar search to locate an authorized screen.
2. Search the grid for the intended code or User ID. Clear filters before concluding that a record is missing. Inspect the pagination and result count.
3. Open the View action to inspect details; use the row's More actions for offered changes and relationship mappings. Expand linked records where available.

- 4. Keep master details and relationship changes separate. For example, editing a role name is different from granting a permission to that role.
- 5. For a change, complete required fields and a meaningful Business Reason. Use the displayed Save, Review changes or Submit for approval action. Read the receipt and resulting state.
- 6. Use Back or Cancel to leave. Resolve an unsaved-changes prompt by intentionally saving or discarding. Do not assume that leaving a screen saved the form.
- 7. Return to the originating record and inspect its pending change/review action. A new master may still be visible only as a pending proposal until approved.
- 8. After a confirmed decision, refresh the relevant grid and verify the effective values. Recheck the user’s selected context when using the access outcome.

UI element	How to use it
View A–E, where offered	Choose a record presentation. It changes the arrangement of information, not privileges or data scope.
Search / filters / columns	Narrow and organize permitted records. Search scopes and export scope follow the current screen; inspect the result count.
Disabled or absent action	Check profile, permission, record state, scope, review eligibility and required assurance. Do not infer a defect solely from a hidden action.
Export Data	Use only the authorized export action. A security-report export is the loaded page; governed exports may require purpose, scope and other policy checks.
Displayed dates	Use the form’s stated timezone/date semantics. Re-enter live dates; screenshot dates are illustrative.

Expected result

You can distinguish a proposed change from applied values and explain which actor must act next.

CHAPTER 8

Applicant requests an account and verifies email

Task context	Details
Screen / entry	Portal → Sign in → Request an Account
Who acts	Applicant, signed out

User: Applicant, signed out

Open: Portal → Sign in → Request an Account

Verify: Collect identity/contact information and establish ownership of the email address, without granting access.

1. Open the portal in the applicant's separate browser profile. Select **Request an Account**.
2. Enter First Name, optional Middle Name, Last Name, the requested Username and Email Address. Use a real user-controlled inbox for the user walkthrough. Add an optional note explaining the business need.
3. Submit once. Record the confirmation. This is an access request, not an active login.
4. Open the latest verification email in the applicant's inbox. Follow its link; do not copy its token into slides or the shared demo script.
5. Select **Verify Email**. Show the **Email Verified — Awaiting Approval** confirmation. The administrator can now classify the request.
6. Return to Sign in to explain that email verification alone has not created approved access or completed credential setup.

SCREEN 1

Public account request form

Application screen with illustrative data · click to enlarge

The screenshot shows a web application for Kernel Health. The background is dark green with a large white 'K' logo. On the left, the text reads 'Kernel Health · ENTERPRISE PLATFORM' and 'MediFlex Medicaid Operations, Connected.' Below this, it says 'Supporting Medicaid Operations—from provider enrollment to claims oversight.' and 'For state agencies, providers and the teams serving Medicaid members.' In the top right corner, there is a 'MEDICAID OPERATIONS' button. The main content is a white modal titled 'YOUR MEDIFLEX ACCOUNT' and 'Request an Account'. It asks for 'Request access to MediFlex.' and includes fields for 'First Name' (Alex), 'Middle Name (Optional)' (Middle Name), 'Last Name' (Demo), 'Username' (alex.demo), and 'Email Address' (alex.demo@example.invalid). There is an optional note field with the placeholder 'Add a note (optional)'. Below the form, there is a 'Submit Request' button and a 'Back To Sign In' link. At the bottom of the modal, there is a small disclaimer: 'After submission, open the verification link in your email. No OTP is entered on this page. Already requested access? Use the link in your latest subscription email; submitting again does not resend it.'

KERNEL HEALTH
HEALTH

MEDICAID OPERATIONS

KERNEL HEALTH · ENTERPRISE PLATFORM

MediFlex Medicaid Operations, Connected.

Supporting Medicaid Operations—from provider enrollment to claims oversight.

For state agencies, providers and the teams serving Medicaid members.

YOUR MEDIFLEX ACCOUNT

Request an Account

Request access to MediFlex.

First Name **Middle Name (Optional)** **Last Name**

Alex Middle Name Demo

Username **Email Address**

alex.demo alex.demo@example.invalid

Note (Optional)

Add a note (optional)

After submission, open the verification link in your email. No OTP is entered on this page. Already requested access? Use the link in your latest subscription email; submitting again does not resend it.

Submit Request

Back To Sign In

Kernel Health · MediFlex

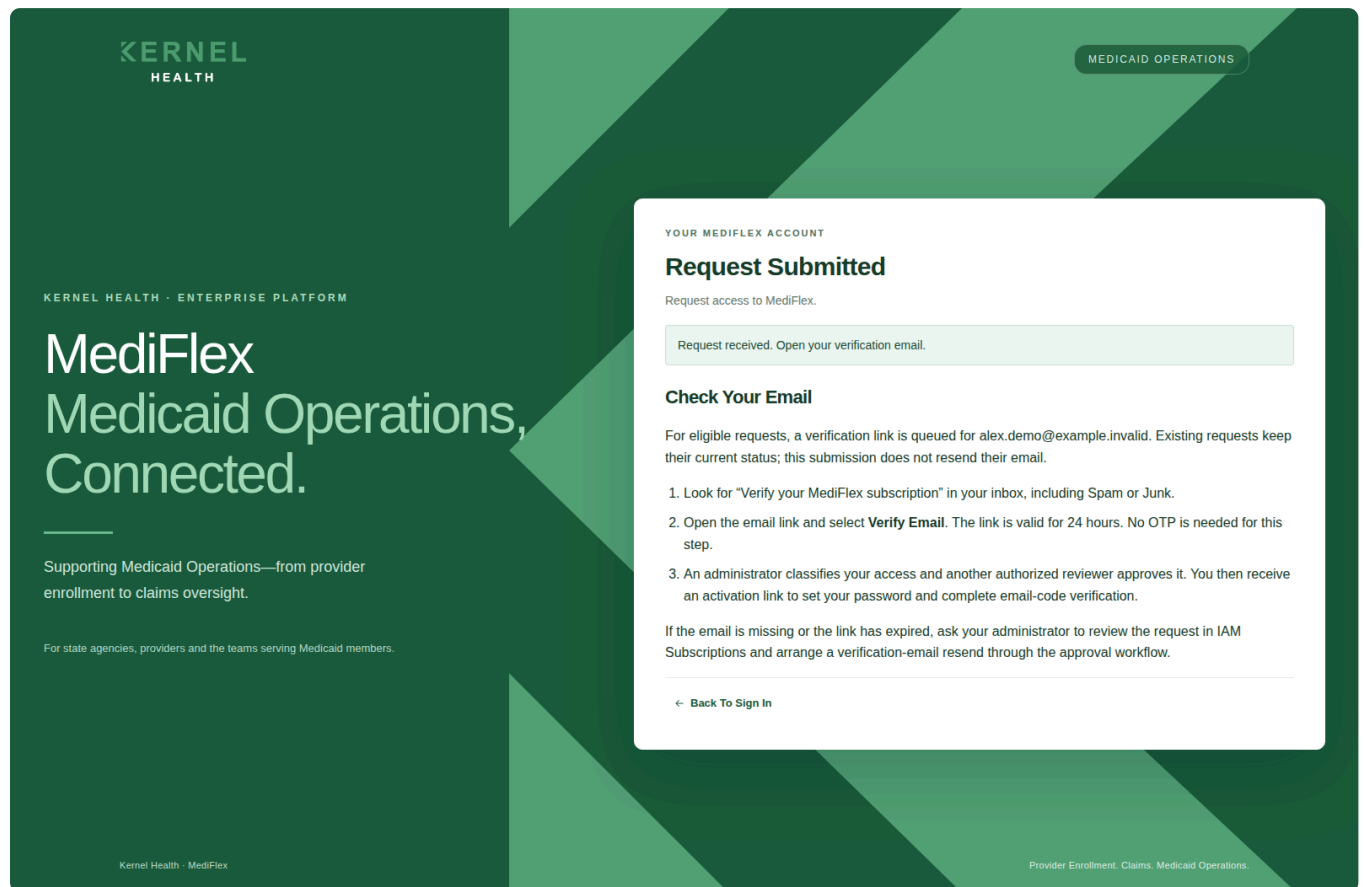
Provider Enrollment, Claims, Medicaid Operations.

- Point to the structured name fields, username and email.
- No domain, profile or administrator role is self-selected on this public form.
- The optional note explains the request; it is not an authorization rule.

SCREEN 2

Submission confirmation and next steps

Application screen with illustrative data · click to enlarge

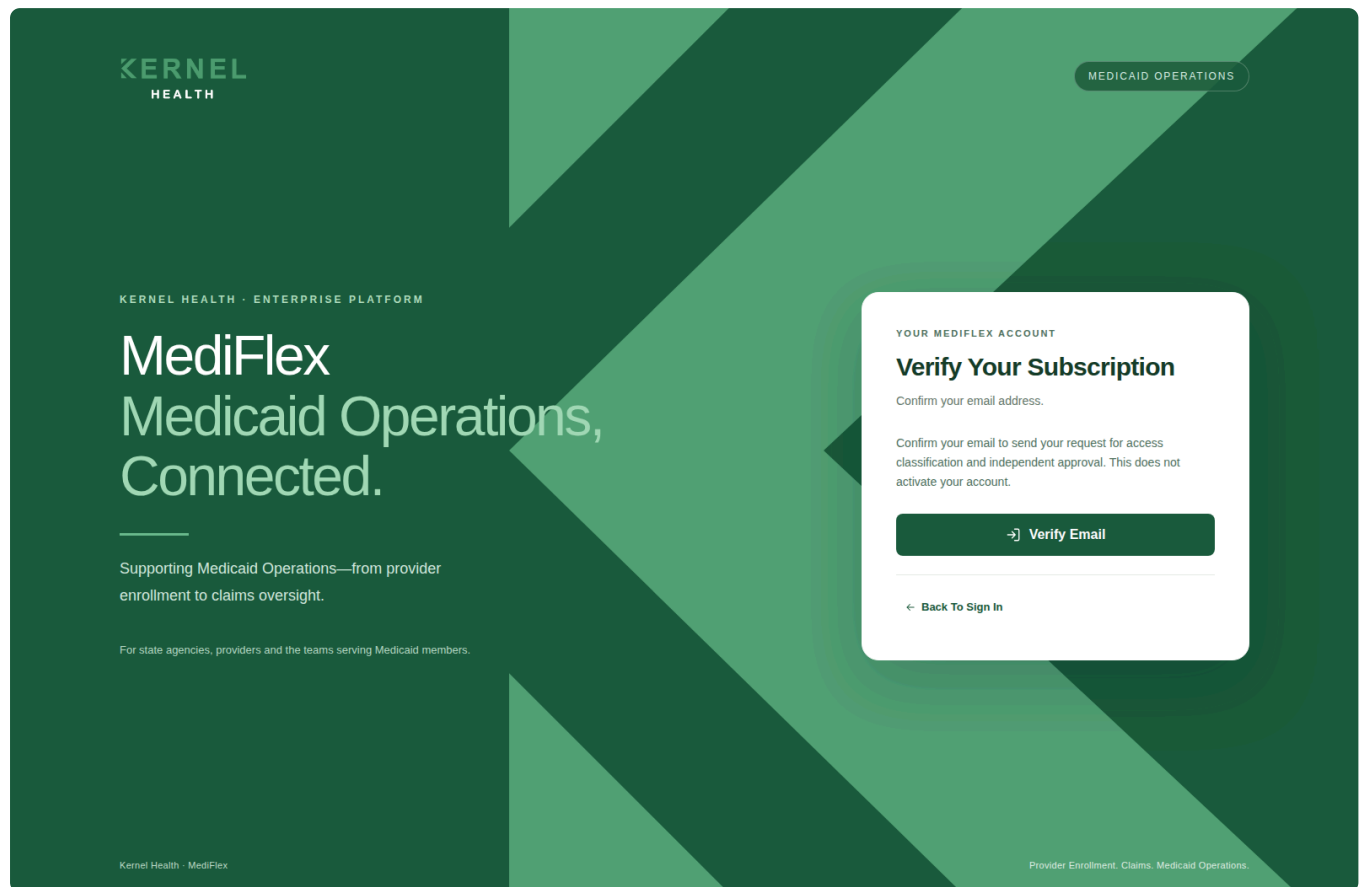


- The applicant is directed to the verification email.
- Submitting again is not a substitute for an authorized email resend.

SCREEN 3

Email ownership confirmation

Application screen with illustrative data · click to enlarge

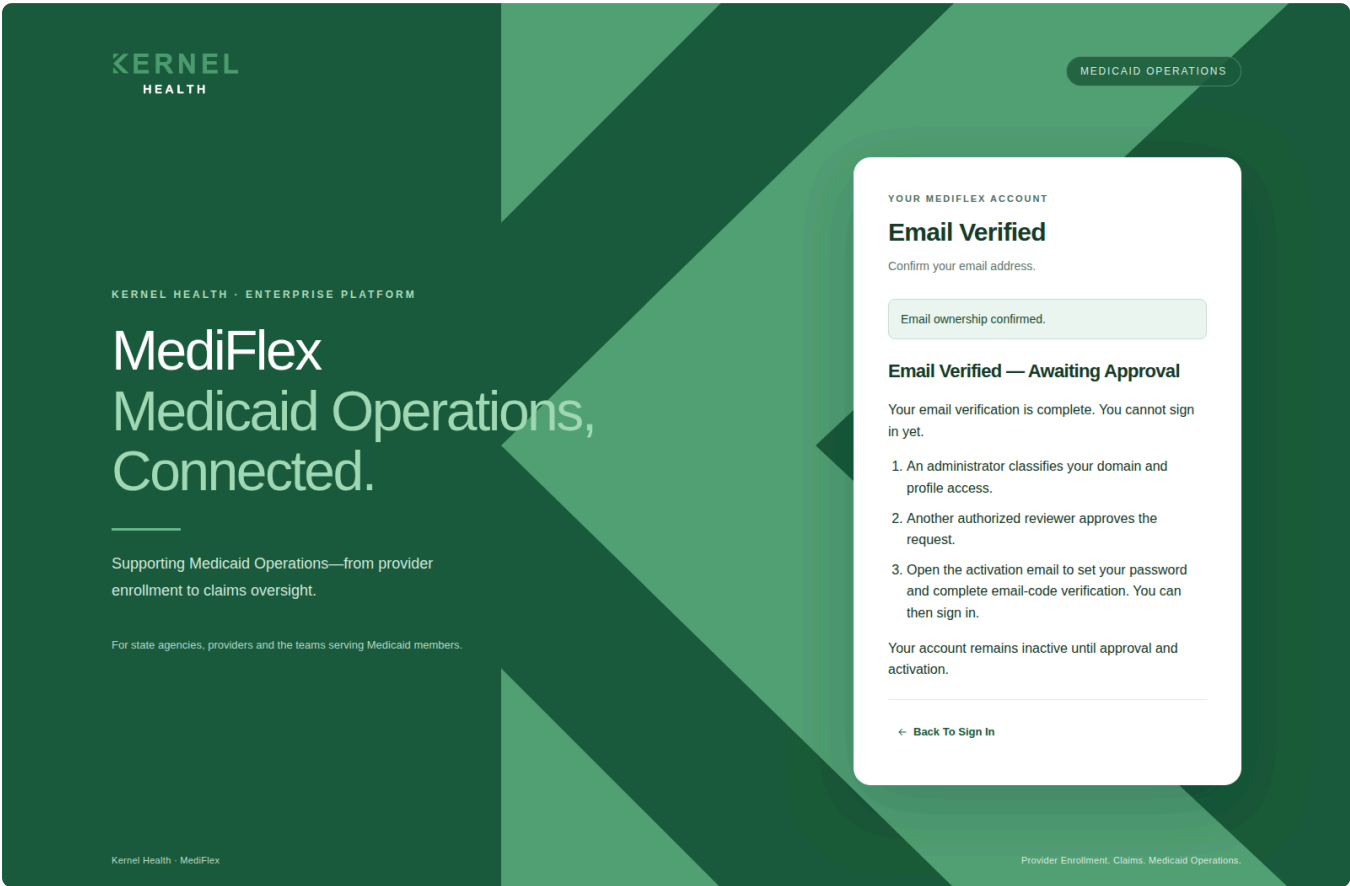


- This page is reached using the latest private verification link.
- No OTP is entered at this particular verification-link step.

SCREEN 4

Verified request awaiting classification and review

Application screen with illustrative data · click to enlarge



- Verified email is a prerequisite; it is not approved access.
- Classification, review and credential activation remain distinct.

State / stage	Who acts next	What exists
EMAIL_PENDING · Awaiting email verification	Applicant follows the email link	A registration request; access has not been granted.
REVIEW_PENDING · Awaiting maker classification	Authorized maker chooses domain/profile	Verified request; no effective new account access.
REVIEW_PENDING · Awaiting checker approval	Independent authorized checker	A pending classification proposal; current access is unchanged.
APPROVED · Awaiting activation	Applicant opens activation invitation	Approved account/access created and activation mail queued.
ACTIVATED · Registration completed	User signs in and selects an available context	Credential enrollment completed; runtime authorization still applies.

Expected result

The verified request appears under User Accounts → Registration Requests. The user cannot gain access by requesting a protected profile in the note or changing the URL.

CHAPTER 9

Maker classifies; checker independently approves

Task context	Details
Screen / entry	User Administration → User Accounts → Registration Requests
Who acts	Maker, then independent Checker

User: Maker, then independent Checker

Open: User Administration → User Accounts → Registration Requests

Verify: Choose eligible domain/profile access and review the inherited roles before approval.

1. As Maker, open **User Accounts → Registration Requests**. Find Alex by username or email. Inspect Workflow Stage and Email Delivery.
2. For a verified, unclassified request select **Classify Access**. If the request already awaits review, open its existing proposal instead of submitting a duplicate.
3. Choose **Operations** as Domain and **Reference data reader** as Profile. The profile must be eligible for that domain. Set Access ends if the demo is time-limited.
4. Inspect Profile Access Preview where available. Inspect the roles and configured business actions, then submit. Use a client approval rule that requires independent review for this scenario.
5. Show the pending status and record the request reference. Do not describe submission as access being granted.
6. Switch to the checker's browser. Open the matching pending request from its available record review action or **originating screen's Changes & Approvals**. Compare the exact registration, requester, domain, profile, inherited roles and expiry.
7. Approve with a review note, or reject with a meaningful reason. Refresh the source registration record. Approved access should create the account/assignment and queue the activation invitation; rejection must not grant the proposed access.

SCREEN 5

Registration requests within User Accounts

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker
IAM demonstration maker

Your Workspace

Find a screen...

Business journeys

My Dashboard

User Administration

User Accounts

Account Settings

SSO Providers

SSO Identities

Credential Recovery

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

System Access

Screens

Screen Controls / Fields

Field Access Policies

Reports

User Audit

Sign-In History

Failed Sign-In Attempts

Active Sessions

MediFlex > User Administration > User Accounts

View A B C D E Overview

Back

Identity & access

Registration Requests

After email verification, use Classify access to select the domain and profile and submit the request. A different authorized reviewer completes any required approval. Approval creates the account and queues its activation email. Email Delivery identifies which message was sent.

Search records...

🗑️

🔍

Refresh

Export Data

	Name	User ID	Email Address	Workflow Stage	Email Delivery	Actions
☐	Alex Demo	example_user_01	e***@example.invalid	Review registration	Not queued	👁️ ✓ ✖ ⋮

Showing 1-1 of 1

⏪ ⏩ Page 1 / 1

- Workflow Stage identifies whose action is next.
- Email Delivery identifies the message type and transport status.
- Classify Access belongs to an authorized maker.

SCREEN 6

Registration classification form

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

Quick Links

DM

Demo Maker

IAM demonstration maker

Your Workspace

Find a screen...

Business journeys

My Dashboard

User Administration

User Accounts

Account Settings

SSO Providers

SSO Identities

Credential Recovery

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

System Access

Screens

Screen Controls / Fields

Field Access Policies

Reports

User Audit

Sign-In History

Failed Sign-In Attempts

Active Sessions

MediFlex > User Administration > User Accounts

View A B C D E Overview

Back

Classify Registration

Find more options

Another authorized person must approve this proposal before access changes.

Registration

Alex Demo

Domain *

Operations

Profile *

Reference data reader

Access ends

MM/DD/YYYY hh:mm AM/PM

Profile Access Preview

Roles: Reference data reader role

Search loaded records...

Screen / Business Function

Country

Configured Actions

View

Showing 1-1 of 1

Page 1 / 1

Configured role grants only. Account status, domain, dates and access conditions are checked at sign-in and on each operation.

Note (Optional)

Enter note

Cancel

Submit For Approval

- Domain and Profile are separate choices.
- Profile eligibility limits the available options.
- The form states when another authorized person must approve.

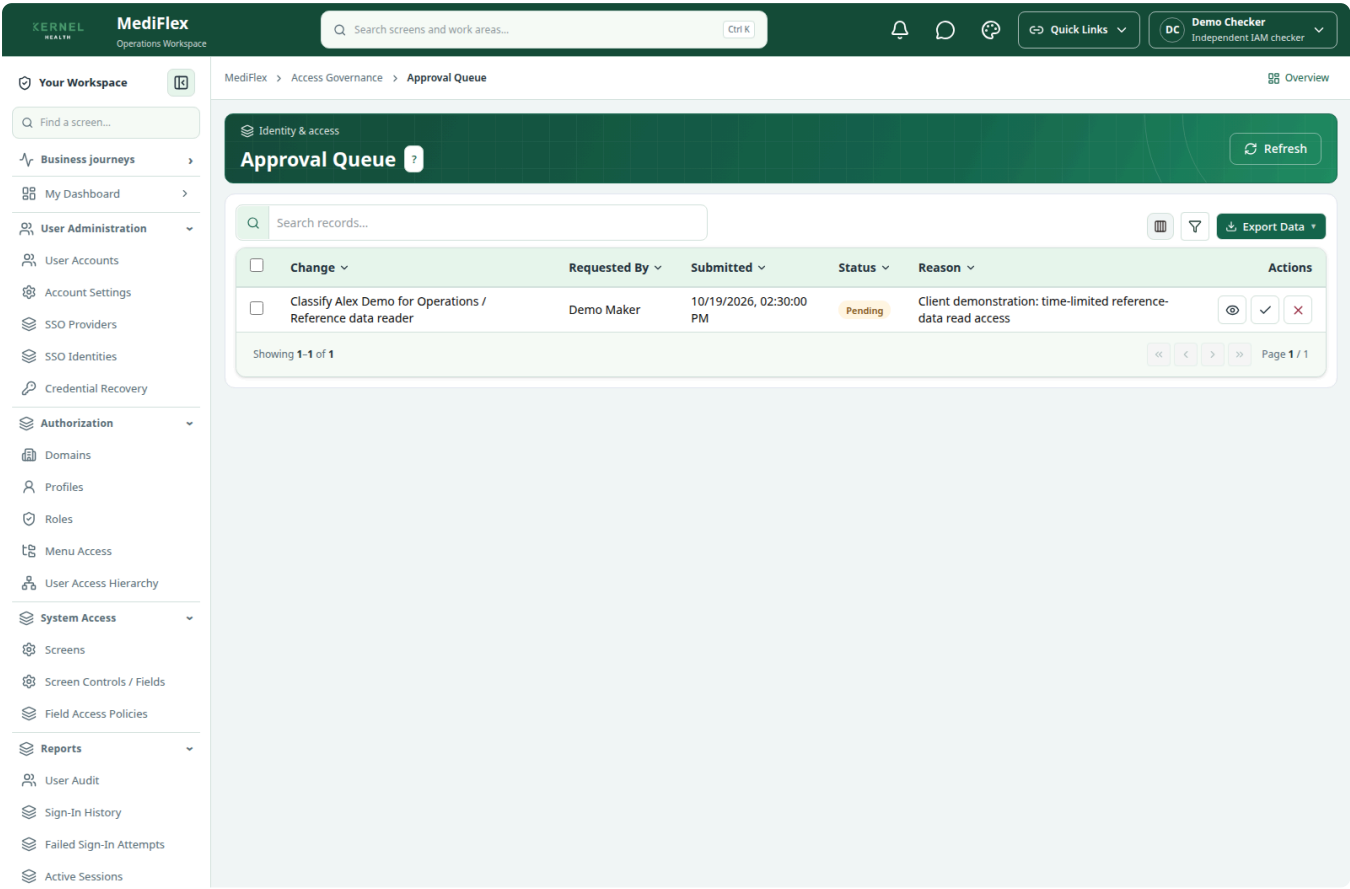
Kernel · User guide

15 / 100

SCREEN 7

The checker locates the pending registration proposal

Application screen with illustrative data · click to enlarge

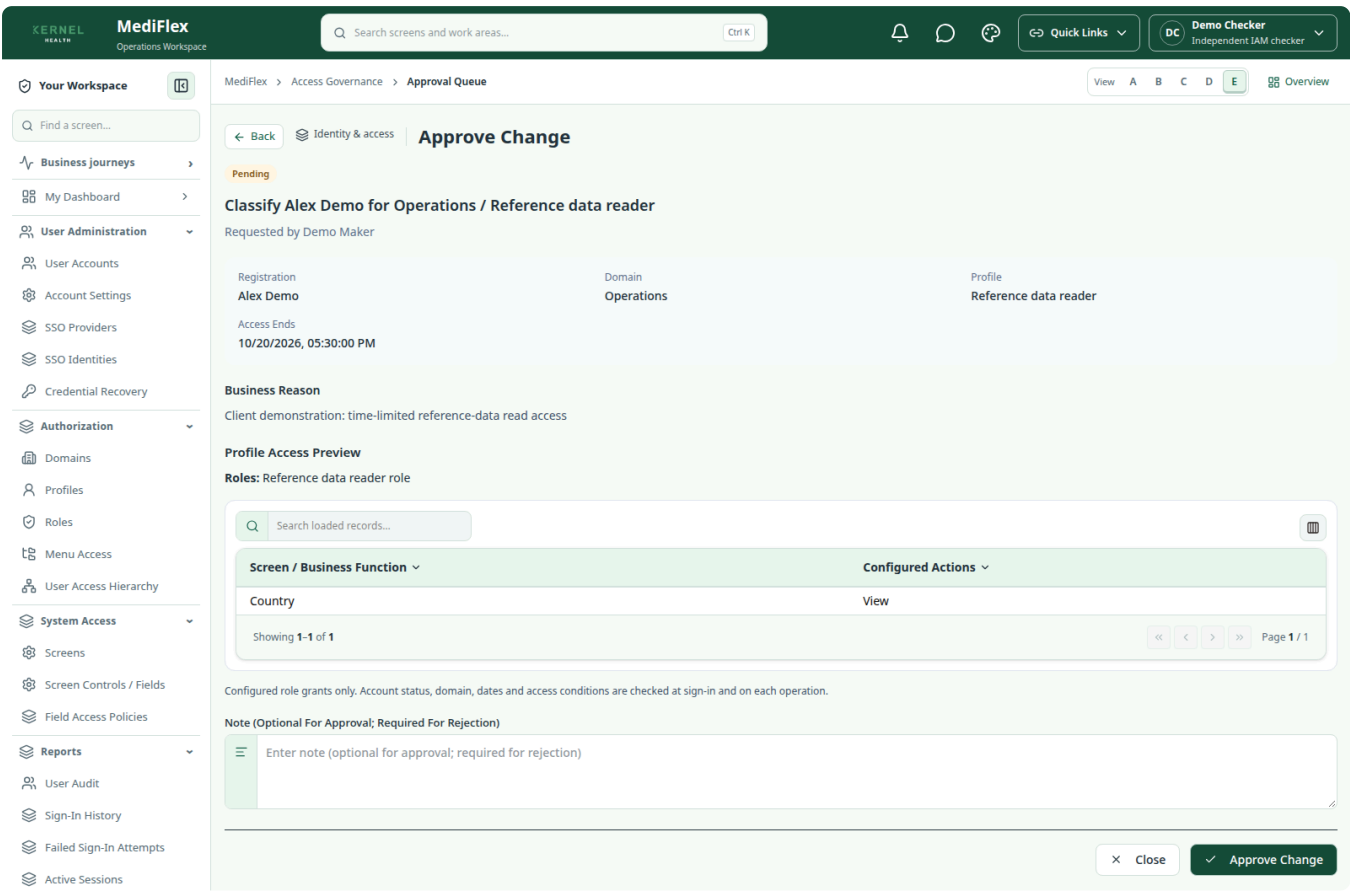


- The requester and the intended domain/profile are visible in the pending change.
- The checker uses their own authorized session.

SCREEN 8

Review the exact registration classification

Application screen with illustrative data · click to enlarge



- Compare domain, profile, effective end date and reason before deciding.
- Approval and rejection controls follow the reviewer’s permissions.

What the checker says and verifies

Review item	Acceptance question
Applicant	Is this the intended person and verified email?
Domain	Is the business context correct?
Profile and roles	Is the requested access proportionate to the stated work?
Dates	Is the start/expiry appropriate and in the expected timezone?
Independence	Is the reviewer a different authorized account from the requester, with any beneficiary restrictions satisfied?
Decision	Does the decision apply only to this exact, current proposal/version?

The generic operation identifier APPROVE_SUBSCRIPTION is used for the maker's classification proposal. It does not mean the maker has independently approved their own request. Also, if the configured Client Approval Rule permits automatic application, the UI may show that path; choose a review-required rule for the example.

Expected result

Pending access remains ineffective until the configured decision is complete. A provider-accepted activation message is not proof that it reached the applicant's inbox.

CHAPTER 10

Enroll credentials and complete the first sign-in

Task context	Details
Screen / entry	Latest activation email → Set Up Your Account → Sign in
Who acts	Applicant

User: Applicant

Open: Latest activation email → Set Up Your Account → Sign in

Verify: Finish credential enrollment and enter the approved workspace.

1. Open the newest activation invitation addressed to the applicant. Use the actual invitation supplied by the system; do not construct a URL from an account ID.
2. On **Set Up Your Account**, choose and confirm a unique password that meets the form's policy. Do not project or record the password.
3. Select **Set Password**. Read the current verification code from the applicant's inbox and enter it on **Verify Your Email Code**. The verification link and this email code are different stages.
4. Complete enrollment. At Sign in, use the requested username and enrolled credentials, then complete the configured factor.
5. Select an available domain/profile when prompted. Show the active profile in the application header.
6. Open the permitted Country screen or the chosen walkthrough screen. Note that account activation, effective assignment, role grants and policies all still matter.

SCREEN 9

Account activation: choose credentials

Application screen with illustrative data · click to enlarge

KERNEL HEALTH

MEDICAID OPERATIONS

KERNEL HEALTH · ENTERPRISE PLATFORM

MediFlex Medicaid Operations, Connected.

Supporting Medicaid Operations—from provider enrollment to claims oversight.

For state agencies, providers and the teams serving Medicaid members.

Kernel Health · MediFlex

Provider Enrollment, Claims, Medicaid Operations.

YOUR MEDIFLEX ACCOUNT

Set Up Your Account

Sign in to continue to your workspace.

Password

Enter your password

Confirm Password

Re-enter new password

→ Set Password

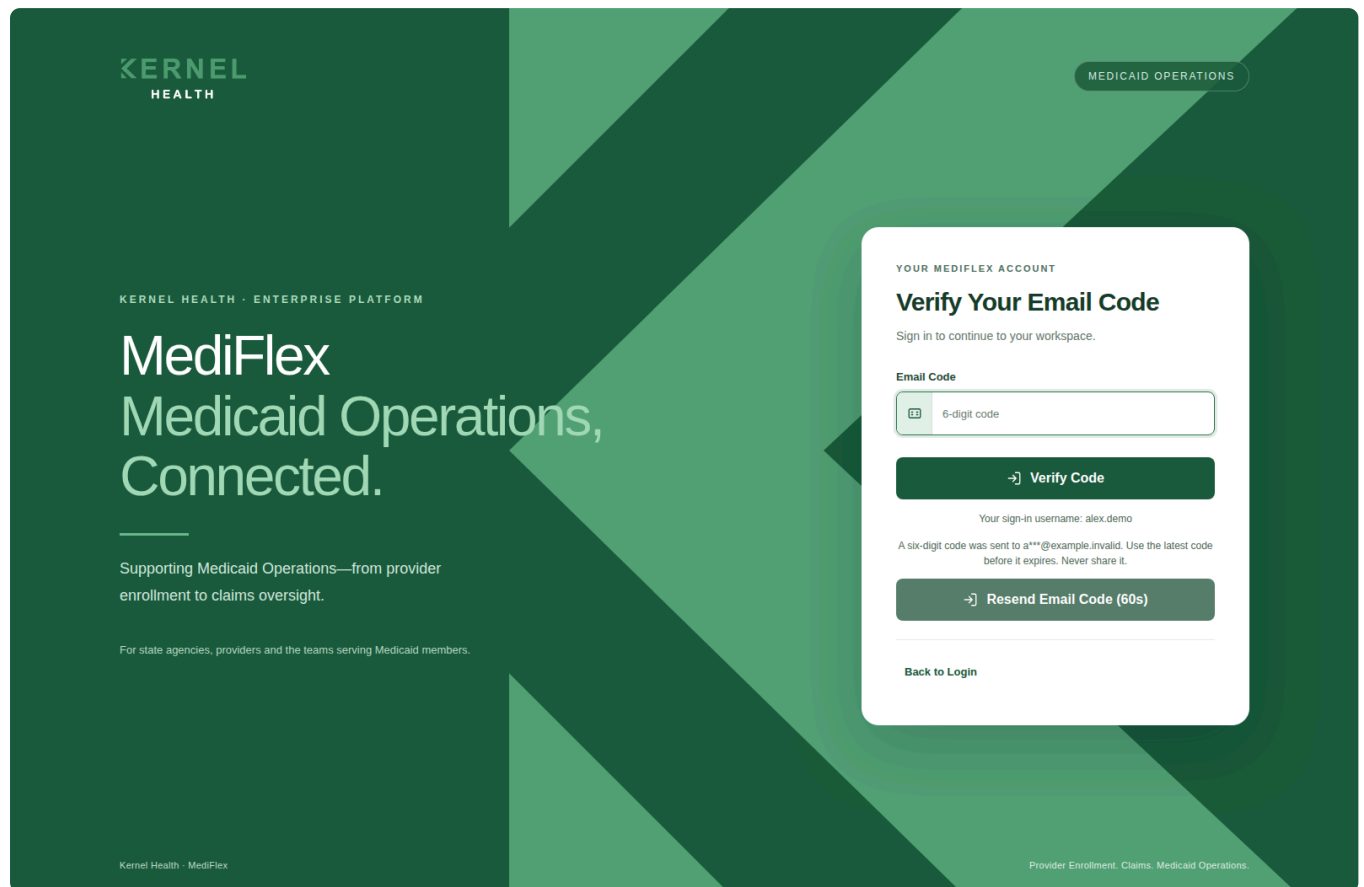
Choose a unique passphrase of at least 15 characters. Next, verify the code sent to your registered email.

- This is the invitation-led setup screen.
- The illustration contains no usable production invitation or password.

SCREEN 10

Account activation: email-code verification

Application screen with illustrative data · click to enlarge

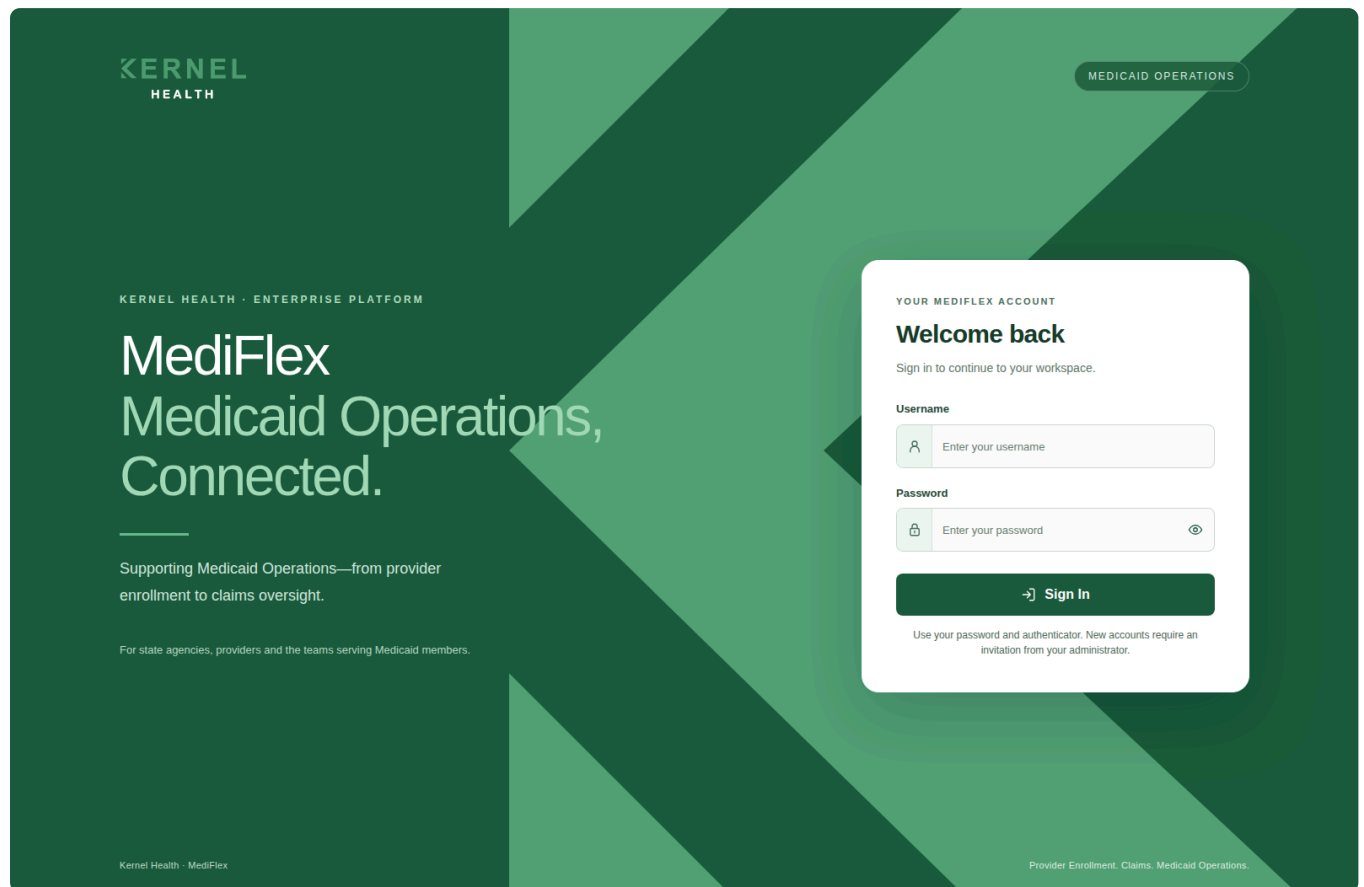


- The code is sent to the account's bound email address.
- Use the latest code and the appropriate resend action if necessary.

SCREEN 11

Native sign-in after enrollment

Application screen with illustrative data · click to enlarge



- Use the enrolled username and password, then the configured verification step.
- An enabled federated sign-in route can be verified separately.

Expected result

Registration becomes completed/activated, and the user enters an effective approved context. A suspended account, expired assignment or unpermitted screen must still be blocked.

This invitation-led enrollment procedure is also used after an eligible administrator-created account receives its enrollment email. Native enrollment and federated SSO sign-in are separate paths.

CHAPTER 11

Admin-created versus subscribed-user journey

Stage	Admin-created route	Subscribed-user route
Starts with	Authorized administrator selects Create user.	Person selects Request an Account while signed out.
Initial data	Administrator enters identity/contact and required account metadata.	Applicant enters requested identity/contact details.
First stored result	A PENDING account and linked onboarding details.	A registration request; no approved account access yet.
Email ownership before classification	Admin entry alone does not verify ownership; enrollment verifies the bound mailbox.	Applicant follows the verification email before maker classification.
Access preparation	Activate account, then Assign Profile in a domain.	Maker uses Classify Access on the verified registration.
Review policy	Client rule for initial user access assignment; this example uses independent review.	Separate client rule for subscription onboarding.
Approval result	Effective eligible assignment on the already created account; enrollment email queued.	Approved account/access is created and the activation email is queued.
Credentials and first login	User follows invitation, chooses password, verifies email code and signs in.	The same enrollment and sign-in handoff after approved onboarding.
Common runtime checks	Selected effective context, RBAC, ABAC, menu/screen/control access.	The same authorization boundaries apply.

CHAPTER 12

Maker creates the account

Task context	Details
Screen / entry	User Administration → User Accounts → Create user
Who acts	Maker

Who: Maker

Open: User Administration → User Accounts → Create user

1. Search for the intended User ID and email first so that the demo does not create a duplicate identity.
2. Select **Create user**. The full-page create form opens with a Back action.

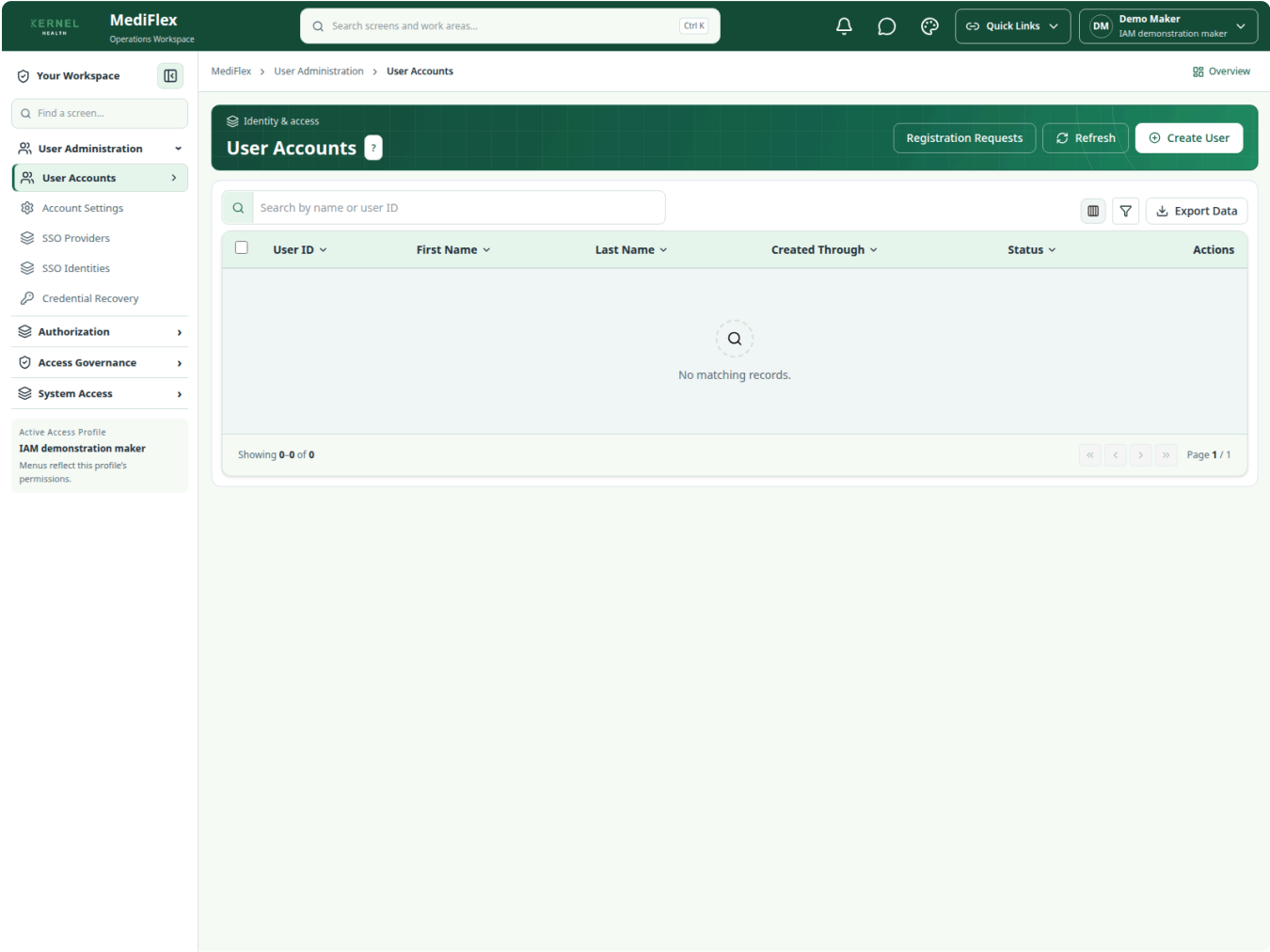
3. Enter the values below. Leave optional dates empty if the account should start immediately and no account-level end date is required. Use a future **assignment expiry** later to bound this example's access.
4. Select **Save** once. Wait for a confirmed receipt and the account workspace. Record the User ID.
5. Read the confirmation: access assignment and approval still follow, and the enrollment email has not been queued yet.

Field	Required?	Demo value / explanation
Last Name	Yes	Demo
First Name	Yes	Alex
Middle Name	No	Leave blank
Email Address	Yes	Actual controlled mailbox for the live run
User ID	Yes	Unique ID, 3–64 characters starting with a letter
User Category	Yes	State in this example; category does not itself grant roles
Owner Reference	No	Use a known external owner identifier only when relevant
Start Date / End Date	No	Account validity; dates take effect at midnight in the local timezone
Account Remarks / Remarks	No	Short business context, without credentials
Note	No	Admin-created user walkthrough; approved reference data access only

SCREEN 12

User Accounts: start administrative onboarding

Application screen with illustrative data · click to enlarge



- Create user is the administrator-led entry point.
- Created through distinguishes Admin-created from Self-registered accounts.

SCREEN 13

Complete the administrator's create form

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker

IAM demonstration maker

Your Workspace

Find a screen...

User Administration

User Accounts

Account Settings

SSO Providers

SSO Identities

Credential Recovery

Authorization

Access Governance

System Access

Active Access Profile

IAM demonstration maker

Menus reflect this profile's permissions.

MediFlex

User Administration

User Accounts

View

A

B

C

D

E

Overview

← Back

Identity & access

Create User

Enter the user's details. Next, activate the account and select its domain and profile. The client approval rule determines whether initial access needs independent review. The enrollment email follows approved access.

First Name *

Middle Name (Optional)

Last Name *

User ID *

Email Address *

User Category *

Owner Reference

Account Remarks

Remarks

Start Date

End Date

Note (Optional)

×

Cancel

Save

- Names, email, User ID and User Category are required.
- The administrator does not enter the new user's password here.

Expected result

The created account is PENDING. The person/contact details are linked for onboarding. There is no approved profile assignment or enrolled credential merely because Save succeeded.

CHAPTER 13

Inspect Progress and activate the account

Task context	Details
Screen / entry	User Accounts → Alex Demo → Progress

Task context	Details
Who acts	Maker

Who: Maker

Open: User Accounts → Alex Demo → Progress

1. Open Alex's account if the create form did not already navigate there. Inspect the header User ID and pending status.
2. Show the six stages: Registration, Personal information, Account activation, Domain and profile, Independent approval and Sign-in readiness.
3. Check why Registration is complete even for an admin-created account: the account has been recorded; Alex did not submit a public registration request.
4. Select **Activate account**. Review the account name and current status, add an optional note and confirm **Activate account**.
5. The workspace opens the access-assignment stage. Confirm ACTIVE, then continue to domain/profile assignment.

SCREEN 14

A newly created account still needs activation and access

Application screen with illustrative data · click to enlarge

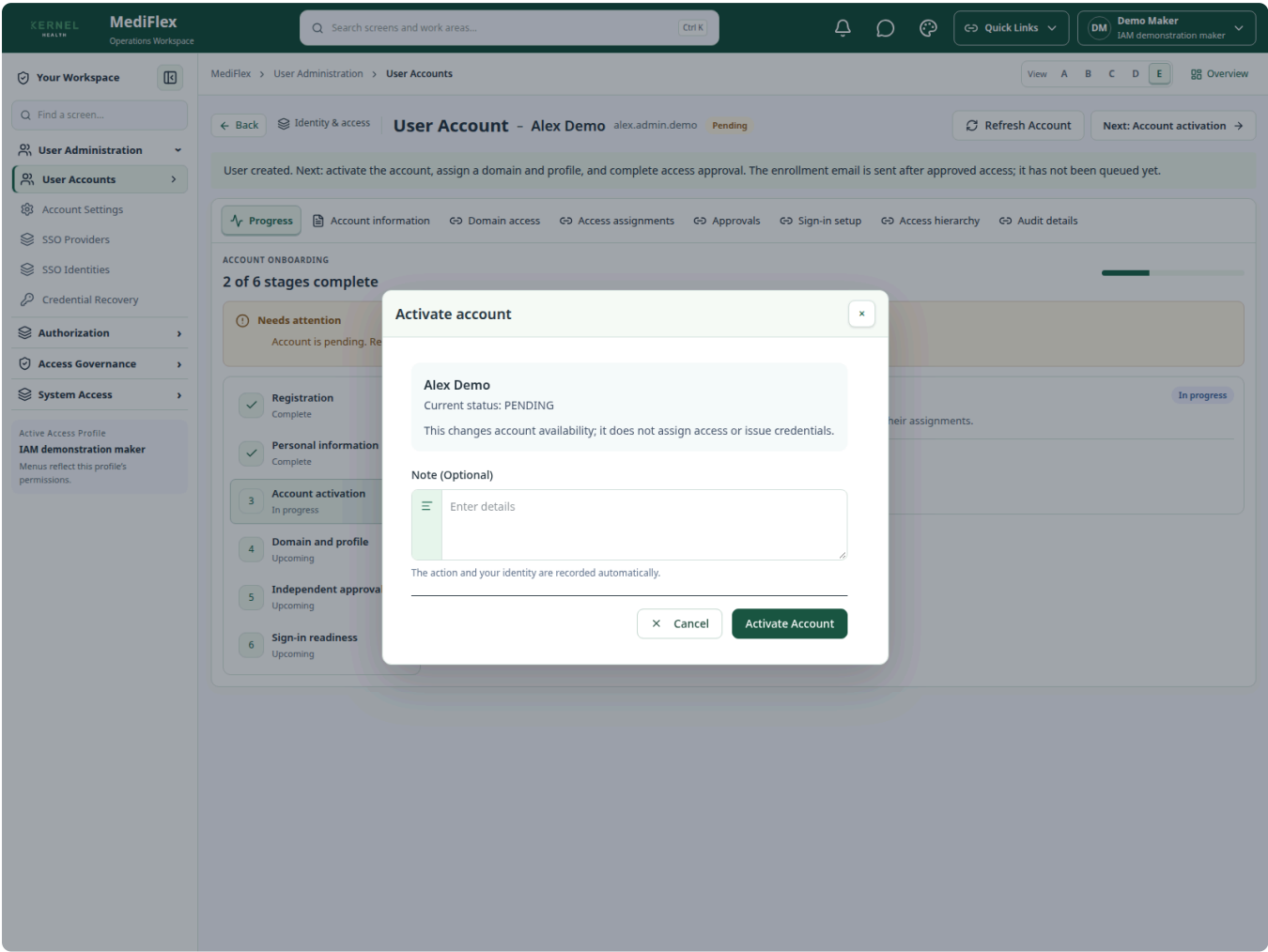
The screenshot displays the MediFlex Operations Workspace interface. The top navigation bar includes the Kernel Health logo, a search bar, and a 'Demo Maker' button. The left sidebar shows a 'Your Workspace' section with a search bar and a list of navigation items: User Administration, User Accounts, Account Settings, SSO Providers, SSO Identities, Credential Recovery, Authorization, Access Governance, and System Access. The main content area is titled 'User Account - Alex Demo' and shows the account's status as 'Pending'. A progress bar indicates '2 of 6 stages complete'. The stages are: 1. Registration (Complete), 2. Personal information (Complete), 3. Account activation (In progress), 4. Domain and profile (Upcoming), 5. Independent approval (Upcoming), and 6. Sign-in readiness (Upcoming). A 'Needs attention' banner states: 'Account is pending. Recorded assignments do not grant sign-in access.' The 'Account activation' section includes instructions to activate the account before proposing access, a responsible party of 'Authorized account administrator', and an 'Activate account' button. A 'Next: Account activation' button is also visible.

- Completed identity stages are separate from sign-in readiness.
- Use the next action to progress through the same account workspace.

SCREEN 15

Confirm account activation

Application screen with illustrative data · click to enlarge



- Verify the target account before confirming.
- Activation changes account availability; it does not issue credentials or assign business access.

Expected result

The account becomes ACTIVE. It still needs an effective domain/profile assignment and credential enrollment before sign-in readiness can complete.

CHAPTER 14

Maker proposes the domain and profile

Task context	Details
Screen / entry	Alex Demo → Access assignments → Assign Profile

Task context	Details
Who acts	Maker

Who: Maker

Open: Alex Demo → Access assignments → Assign Profile

1. Select **Assign Profile**. The current user should be carried into the form; verify it is Alex.
2. Choose **Operations**. Choose **Reference data reader** from the profiles eligible in that domain.
3. Review the inherited role and business-access preview. The intended walkthrough is read-only access to the prepared reference screen.
4. Optionally set **Access ends** to a future date/time after the demo. This is assignment validity, distinct from account validity.
5. Add the demo note. Select the form's submission action and wait for its receipt. With the review-required rule, the message should say the proposal was submitted for independent approval.
6. Return to Access assignments. Show the pending proposal on the corresponding row. Current effective access remains unchanged while it is awaiting review.

SCREEN 16

Select the domain and eligible profile

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker
IAM demonstration maker

Your Workspace

Find a screen...

User Administration

User Accounts

Account Settings

SSO Providers

SSO Identities

Credential Recovery

Authorization

Access Governance

System Access

Active Access Profile
IAM demonstration maker
Menus reflect this profile's permissions.

MediFlex

User Administration

User Accounts

View

A

B

C

D

E

Overview

← Back

Identity & access

User Account - Alex Demo

alex.admin.demo

Active

Refresh Account

Activate account completed and audited.

Assign Profile

← Back To Account

Find more options

Another authorized person must approve this proposal before access changes.

User Account

Alex Demo

Domain *

Operations

Profile *

Reference data reader

Access ends

10/27/2026, 05:30:00 PM

Profile Access Preview

Roles: Reference data reader role

Search loaded records...

Screen / Business Function

Country

Showing 1-1 of 1

Configured Actions

View

Page 1 / 1

Configured role grants only. Account status, domain, dates and access conditions are checked at sign-in and on each operation.

Note (Optional)

Client demonstration: time-limited reference-data read access

Cancel

Submit For Approval

- Check the account, domain, profile and role preview together.
- Use a future access expiry for the actual meeting.

Kernel · User guide

30 / 100

SCREEN 17

The proposed access remains with its originating account

Application screen with illustrative data · click to enlarge

The screenshot shows the 'User Account - Alex Demo' page in the MediFlex Operations Workspace. The page is titled 'User Account - Alex Demo' with the username 'alex.admin.demo' and status 'Active'. A green banner at the top states: 'Submitted for independent approval. Current access stays unchanged until approved.' Below this, a navigation bar includes 'Progress', 'Account information', 'Domain access', 'Access assignments' (highlighted), 'Approvals', 'Sign-in setup', 'Access hierarchy', and 'Audit details'. The 'Access Assignments' section features a search bar, a table of assignments, and an 'Assign Profile' button. The table has columns for Domain, Profile, Roles, Review, Profile Availability, and Actions. One assignment is shown: 'Proposed domain' with profile 'Assign Reference data reader to Alex Demo', role 'Pending approval', review status '1 pending', and profile availability 'Awaiting independent approval'. A footer note states: 'A user can hold several profiles across domains, and each profile can be assigned to several users. Availability permits profile selection; permissions and policies are checked for each action.'

- The pending item can be reviewed from its own access row.
- A recorded proposal is not an effective assignment.

Client Approval Rules can allow automatic application of initial access. If the configured rule allows that and the receipt is APPROVED, explain that the rule applied the assignment automatically; do not claim a human checker approved it. Later assignments and other IAM operations may have different review requirements.

Expected result

The intended assignment is pending under the chosen review-required rule. The user cannot select it as effective access yet, and the initial enrollment email remains dependent on approved access.

Independent checker reviews the originating record

Task context	Details
Screen / entry	User Accounts → Alex Demo → Access assignments
Who acts	Different Checker account

Who: Different Checker account

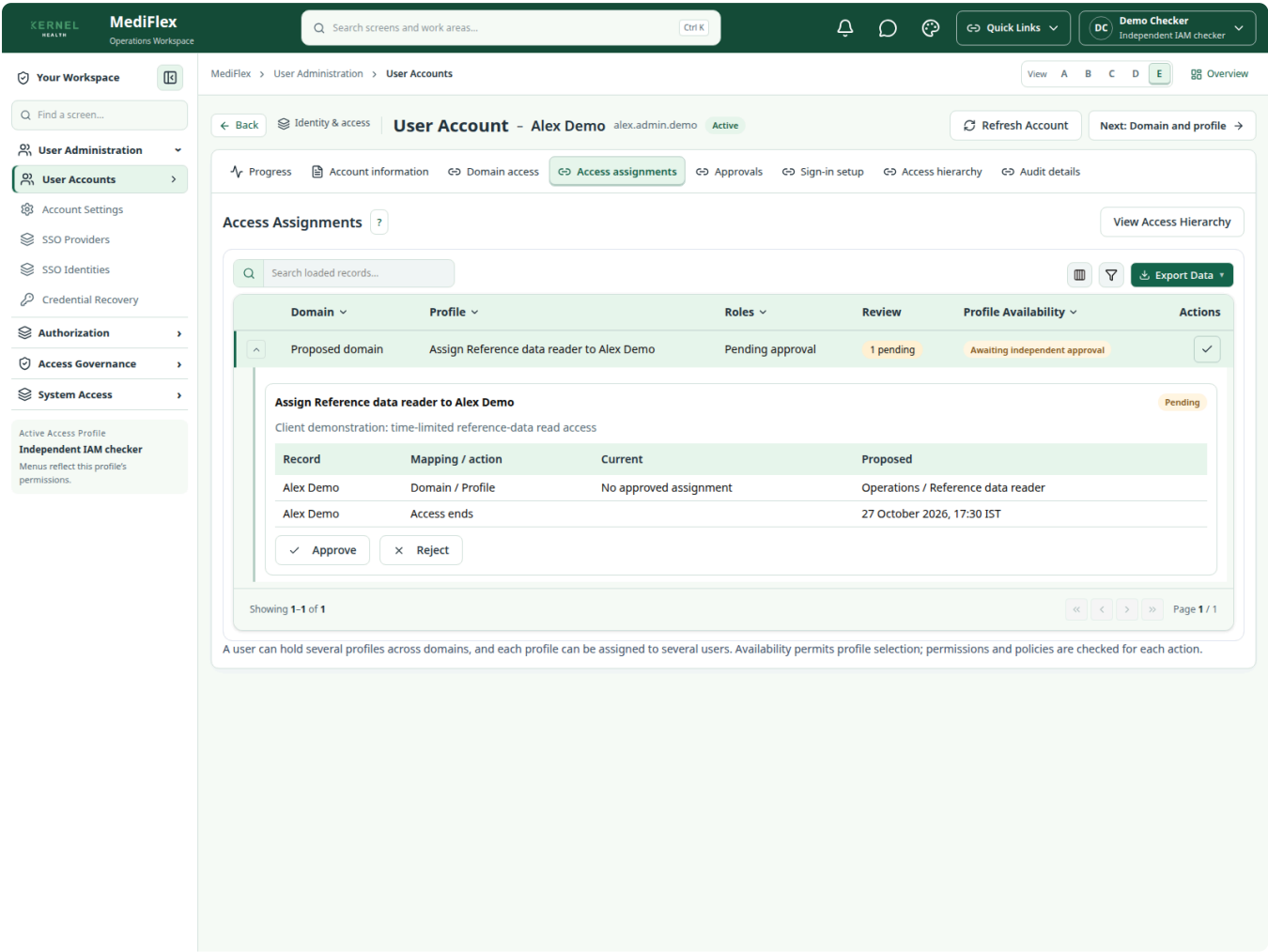
Open: User Accounts → Alex Demo → Access assignments

1. Use the checker's separate signed-in browser. Verify both the person's account identity and selected checker profile.
2. Find Alex and open **Access assignments**. Use the row's Review action or expand the pending row.
3. Compare the before/after values, maker's reason, domain, profile, inherited role bundle and expiry. Open the account's **Approvals** tab if you need the account-filtered request list.
4. Select **Approve**, add an optional approval note and select **Confirm approval** in the inline review. On the alternative Approvals detail page the final action is **Approve Change**.
5. Refresh the account. Confirm the assignment is active/available, the proposal has a completed decision and Sign-in setup shows the enrollment-email state.
6. For a rejection walkthrough, use a separate new proposal and enter a meaningful rejection reason. Rejection must not grant the requested assignment.

SCREEN 18

Review access directly within the account row

Application screen with illustrative data · click to enlarge

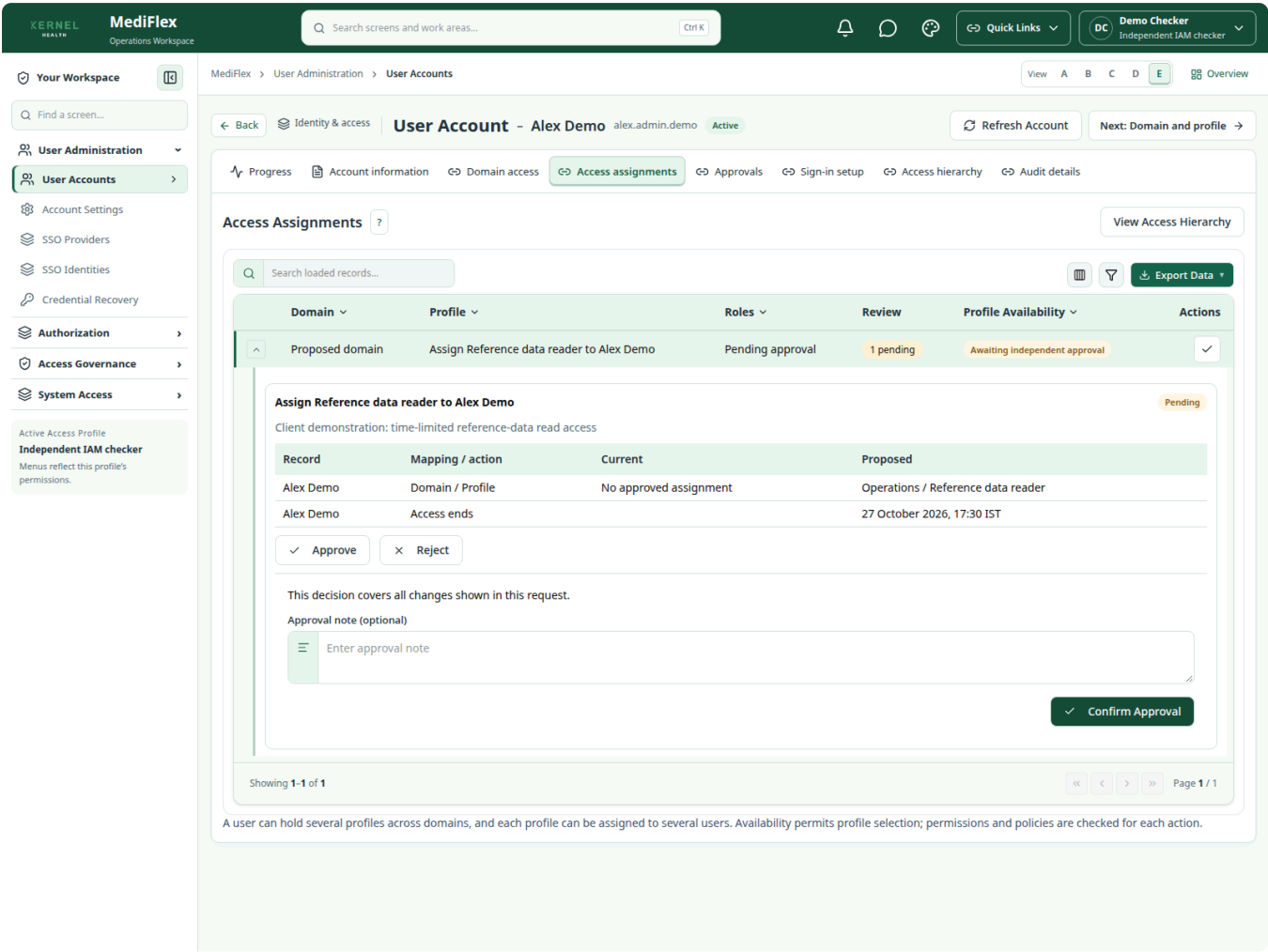


- The proposed change and decision controls stay with the relevant record.
- The illustration uses a separate checker identity in the isolated fixture.

SCREEN 19

Record the checker's decision

Application screen with illustrative data · click to enlarge



- Approval applies to the exact request and version.
- An approval note helps explain why the requested access is appropriate.

If the action is unavailable

Check

Same underlying account submitted the proposal

A different authorized account is required; changing the profile is insufficient.

Checker can view but cannot approve

Inspect eligibility, action permission, proposal state and applicable separation-of-duties restrictions.

Request already decided or stale

Refresh the record and inspect its latest version; avoid duplicate decisions.

Profile is protected or checker is an affected party

Use an eligible authorized reviewer; do not bypass the restriction.

Expected result

Approved eligible access is recorded and the enrollment email is queued once. Until the new user enrolls, Sign-in readiness still remains incomplete.

CHAPTER 16

Verify enrollment delivery and hand over to the user

Task context	Details
Screen / entry	Alex Demo → Sign-in setup → Refresh account
Who acts	Maker or authorized reader

Who: Maker or authorized reader

Open: Alex Demo → Sign-in setup → Refresh account

1. Open **Sign-in setup** after access approval. Read Account status, Sign-in setup and Enrollment email together.
2. Refresh to observe the transport state. Do not treat Queued or Accepted by email provider as proof that Alex has finished enrollment.
3. Have Alex open the newest activation/enrollment message in the real controlled inbox. Check junk/spam if the provider accepted it but it is not visible.
4. Use the actual private link from that message. Do not construct an invitation URL from the account ID.
5. If the invitation has expired or delivery needs a new attempt, use **Request Enrollment Email** when offered and complete its approved resend workflow. Credential recovery is for accounts that already enrolled.

SCREEN 20

Approved access has queued the enrollment message

Application screen with illustrative data · click to enlarge

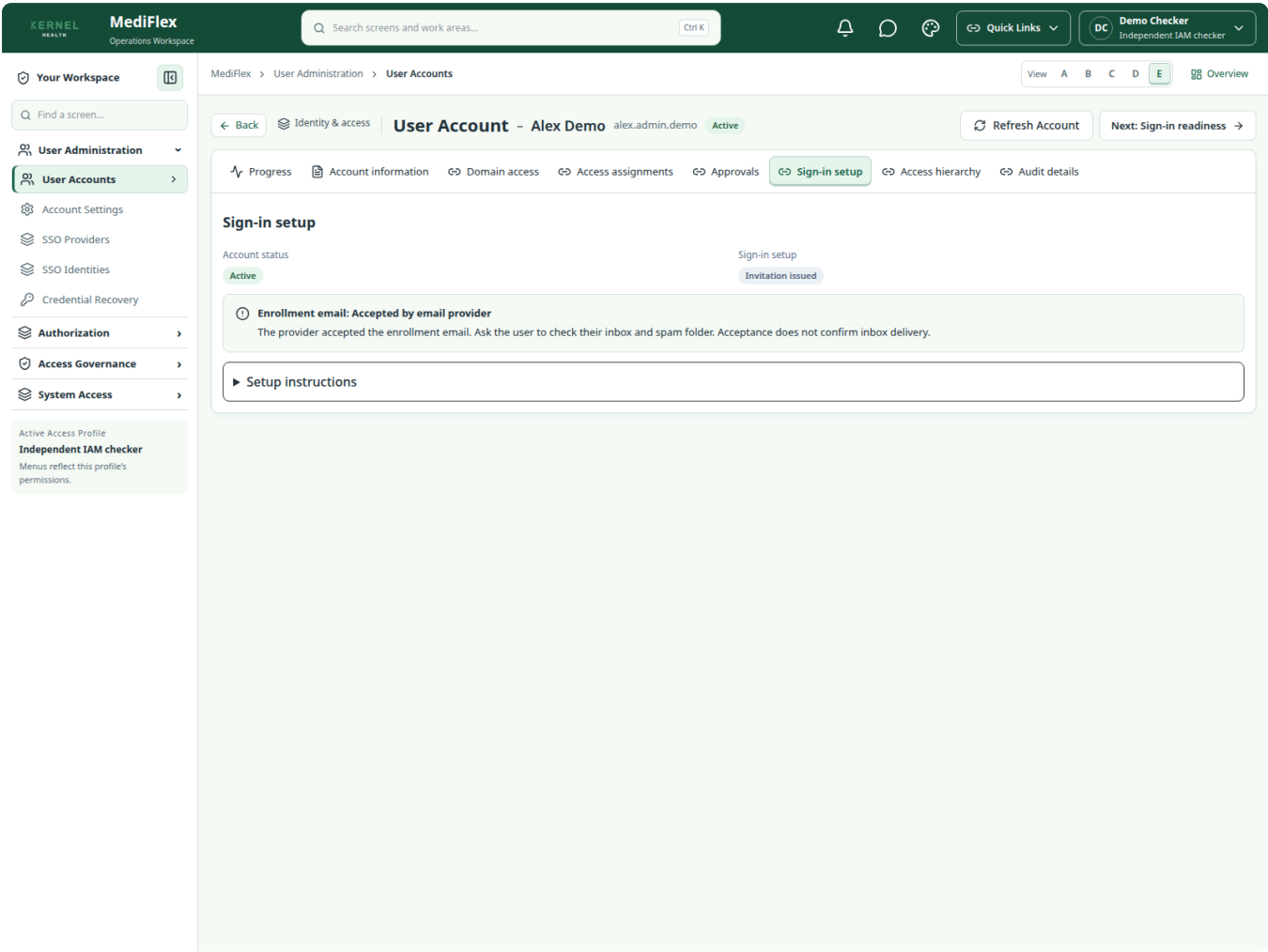
The screenshot displays the MediFlex Operations Workspace interface. The top navigation bar includes the 'MediFlex' logo, a search bar, and a 'Demo Checker' button. The left sidebar shows a 'Your Workspace' section with a search bar and a list of navigation items: 'User Administration', 'User Accounts', 'Account Settings', 'SSO Providers', 'SSO Identities', 'Credential Recovery', 'Authorization', 'Access Governance', and 'System Access'. The main content area is titled 'User Account - Alex Demo' and shows the 'Sign-in setup' section. The account status is 'Active', and the sign-in setup status is 'Enrollment incomplete'. A message states: 'Enrollment email: Queued. The enrollment email is queued for delivery. Use Refresh account to check its progress.' There is a 'Refresh Account' button and a 'Next: Sign-in readiness' button. A 'Setup instructions' section is also visible.

- The account and assignment are ready for the user's credential setup.
- Refresh account follows delivery progress.

SCREEN 21

The provider accepted the message

Application screen with illustrative data · click to enlarge



- Confirm the message in the actual recipient inbox during the live demo.
- Provider acceptance and completed enrollment are different results.

Displayed state	Meaning / next action
Not queued — activate account	Complete account activation first.
Not queued — approve access	Assign the profile and finish required access review.
Queued / Sending	The delivery service is handling the message; refresh.
Accepted by email provider	Transport accepted it; verify the inbox separately.
Delivery failed / Delivery canceled	Inspect email, account and access state; use the authorized resend process.
Invitation expired	Request a new invitation; use only the latest unexpired link.
Verification in progress	The user needs to finish email-code verification.

Displayed state	Meaning / next action
Enrollment complete	The user finished credential enrollment; runtime access checks still apply.

Continue with [Enroll credentials](#) and [complete the first sign-in](#). The invited user completes the setup; the administrator does not select or distribute that person's password.

Expected result: The approved account shows a traceable enrollment message and its actual delivery stage. The intended person uses the latest eligible invitation; provider acceptance is not proof that it was read.

CHAPTER 17

Sign in, select a profile and work safely

Task context	Details
Screen / entry	the portal's Sign in page
Who acts	Authorized operator / eligible independent reviewer as specified below

1. Open the portal's Sign in page. Use the native route if native credentials were enrolled, or the enabled federated provider linked to the account. Complete the verification steps offered by that route.
2. If the workspace selector appears, choose Organization Or Provider, then Access Profile. These are available assignments returned for this user. With a single choice the context may resolve directly.
3. Read the active domain and profile in the header. Open a permitted screen from the dynamic sidebar or authorized search result.
4. To change responsibility, open the top-right profile menu → Switch profile. Select the other offered assignment. Wait for the new context and navigation to load.
5. Before changing a record, confirm the new profile and its permitted actions. Permissions from all assigned profiles are not combined simply because the account can select them.
6. Use the application Back action to return from record pages. A direct bookmark still needs access in the current context.
7. When finished, use the profile menu → Sign out. On a shared machine, close the browser window after sign-out.

What you see	Meaning / next action
No available context	Ask an authorized administrator to check account/membership status, approved assignment, domain eligibility, profile selectability and effective dates.

What you see	Meaning / next action
Menu list changes after switching	The selected profile has a different effective permission set or context. This is expected.
You can see a menu but cannot read the screen	Navigation and protected read requirements must both succeed. Record the exact error and selected context for the administrator.
Session expired	Sign in again. If an in-progress submission may have succeeded, inspect the record/proposal receipt before submitting a duplicate.

Expected result

The header, available menus and permitted operations agree with the selected effective assignment.

CHAPTER 18

Read account progress, personal information and settings

An authorized administrator opens User Accounts and the person's View action. A normal business user receives only the account screens their profile permits; this guide does not assume universal self-edit permission.

Account area	Use
Progress	Track Registration, Personal information, Account activation, Domain and profile, Independent approval and Sign-in readiness. Complete each outstanding prerequisite using its offered action.
Account information	Inspect identity/lifecycle, category, owner reference and validity. Pending changes do not replace effective values before approval.
Personal information	Inspect the linked name, email addresses and phone numbers. Only edit fields permitted by IAM; masked/read-only fields stay constrained.
Domain access	Inspect where the account belongs and the related profile assignments. Membership alone does not grant every profile.
Access assignments	Inspect profile/domain assignments, validity and pending proposals.
Approvals	Review pending and decided account-related access changes in the permitted scope.
Sign-in setup	Check enrollment, invitation/delivery state and eligible lifecycle or recovery actions.
Access hierarchy	Trace effective assigned profiles to roles and permissions.
Audit details	Read record metadata; use decision and sign-in reports for their separate evidence.

- 1. For a permitted personal-information update, open the relevant section and choose the existing name/contact record. Change only the intended field.
- 2. Respect the form’s required fields, masking and linked-reference restrictions. Read-only references should be reviewed at their owning source.
- 3. Save using the offered action, inspect any governance notice and reload to confirm the resulting state.
- 4. Use Account Settings only for its offered account type and authentication realm administration. It is not the profile-role mapping screen.

Person/contact or KYC data belongs to the application boundary; an IAM access profile is a role bundle. The target separation is explained here without claiming that every legacy personal-data migration has been completed.

CHAPTER 19

Verify sensitive actions, change credentials and recover access

Task context	Details
Screen / entry	Verify sensitive actions, change credentials and recover access
Who acts	Authorized administrator / reviewer

- 1. Choose the task that matches the problem: verify a sensitive action, replace native credentials, recover an account or recover at the external identity provider.
- 2. Start from the screen named in the table below and complete the required current identity verification.
- 3. Follow only that task’s setup, confirmation or independent-review path. Use the latest eligible code/invitation and inspect its outcome before requesting another.
- 4. Sign in through the resulting supported path and check the selected domain/profile. If you cancel, return to the workspace and confirm that no incomplete replacement is being treated as completed.

Task	Steps	Successful checkpoint
Verify sensitive actions	Profile menu → Verify sensitive actions. Complete the current trusted verification flow and return to the requested workspace action.	The protected action rechecks the session’s current assurance. A successful normal login alone may be insufficient.
Change native credentials	Profile menu → Change credentials. This routes through sensitive-action verification before replacement setup. Follow the offered setup and email-confirmation steps.	Use the replacement credentials on a new sign-in; confirm the stated session effects.

Task	Steps	Successful checkpoint
Leave the verification/replacement flow	Use the page's offered return/cancel action. If the session is no longer usable, return through the portal sign-in and select your assignment.	The user can resume permitted work without assuming an incomplete credential replacement succeeded.
Administrative recovery	Both administrators verify sensitive actions. The maker opens Credential Recovery or the account's Sign-in setup recovery action, selects the account, records Identity verification performed and the Business Reason, and submits for independent review.	Approval immediately revokes old credentials and sessions. Only the approving reviewer can use Issue Recovery Invitation. They deliver the short-lived, one-use link privately to the verified person. Issuing another link invalidates the previous one.
Expired invitation or code	Use the supported resend/request-enrollment action after checking eligibility and the latest delivery status. Use the newest invitation/code.	Enrollment completes once; an old link is not treated as evidence of access.
Federated password problem	Use the configured identity provider's account-recovery process; ask an authorized administrator to check the internal identity link if sign-in cannot resolve the account.	External authentication and internal IAM assignment both succeed.

Do not put passwords, OTPs, recovery links or invitation tokens in the shared demo evidence. Recovery is not a way to create a new role grant. If a flow returns DB_EXEC_ERROR, preserve its correlation ID and check whether a request already exists before retrying.

Expected result: The selected credential or recovery path completes its required verification and confirmation. A subsequent authorized sign-in succeeds; no new role grant is inferred from credential recovery.

CHAPTER 20

Change, expire, revoke, suspend and restore access

Task context	Details
Screen / entry	the intended test or business account and inspect current status and effective assignments.
Who acts	Authorized operator / eligible independent reviewer as specified below

1. Open the intended test or business account and inspect current status and effective assignments.

2. Select the needed lifecycle action from the table below. Check whether it affects an assignment, the account or existing sessions.
3. Record the business reason and obtain the independent decision when required. Preserve the original account and assignment references.
4. Reopen the account and verify the effective result from the affected user context. Restoration must not recreate an expired or revoked grant.

Scenario	Procedure	Checkpoint
Add a second business profile	Maker proposes another eligible assignment; a different checker completes required review.	The existing assignment remains unchanged while the new request is pending. After approval, the user can choose the new available context.
Reject an inappropriate request	Submit a separate prepared proposal; checker rejects with a reason.	The proposed access does not become effective.
Revoke an assignment	From the permitted assignment action, propose revocation with a reason and complete required review.	After application, refresh/reselect context and verify that revoked assignment is unusable.
Suspend the demo account	An authorized lifecycle operator opens Sign-in setup and selects Suspend Account with a reason.	The UI states existing sessions are revoked immediately; verify the actual browser/session outcome.
Restore, when eligible	Use Restore account with the permitted operator.	Restoration does not recreate an expired/revoked assignment or eliminate ordinary authorization checks.
End the walkthrough	Use approved expiry/revocation/suspension appropriate for this example user; preserve audit history.	Do not hard-delete records or close a reusable demo account. Closure is terminal.

Use only the newly prepared demo account for these operations. Do not suspend the operator or checker account. Verify the action on the UI and verify the resulting state; a status badge alone is insufficient evidence that an old session has stopped working.

Expected result: The requested assignment/account change is reflected in the effective user context and session behavior. Original requests, decisions and history remain available.

CHAPTER 21

Use this dependency order

Order	Action	Complete before moving on
0	Select an existing published screen, registered actions and its baseline permission keys	The screen and menu/control identities exist
1	Create Domain	Independent approval; domain available
2	Create Role	Independent approval; role available
3	Create Profile with Initial Domain	Independent approval; inspect initial domain eligibility
4	Create a permission when needed, or reuse registered permissions	Definition is approved and tied to the intended action
5	Confirm Domain ↔ Profile; add further links if needed	Approved eligibility with compatible access scope
6	Map Profile ↔ Role	Approved role bundle
7	Grant Role ↔ Permissions and configure role/menu actions	Required read permissions effective; write permissions absent
8	Inspect Permission ↔ Menu and Menu ↔ Screen	Required registered dependencies preserved
9	Configure control requirements and field restrictions if needed	Approved IAM changes referencing the correct Axis controls
10	Optionally verify Axis ownership/experience revisions	Approval and publication are distinguished
11	Apply and review a prepared ABAC rule	Approved rule with a reproducible positive/negative case
12	Assign the business user to the domain/profile	Approved, currently effective assignment
13	Select that profile; prove navigation, read, write denial and ABAC	Runtime results and audit captured

Do not try to finish every mapping while its source master is still awaiting approval. Refresh the lookup after the checker's confirmed decision. An approved definition, an effective assignment and a published presentation are separate checkpoints.

CHAPTER 22

Create the Domain

Task context	Details
Screen / entry	Authorization → Domains → Create Domain
Who acts	Maker

Who: Maker

Open: Authorization → Domains → Create Domain

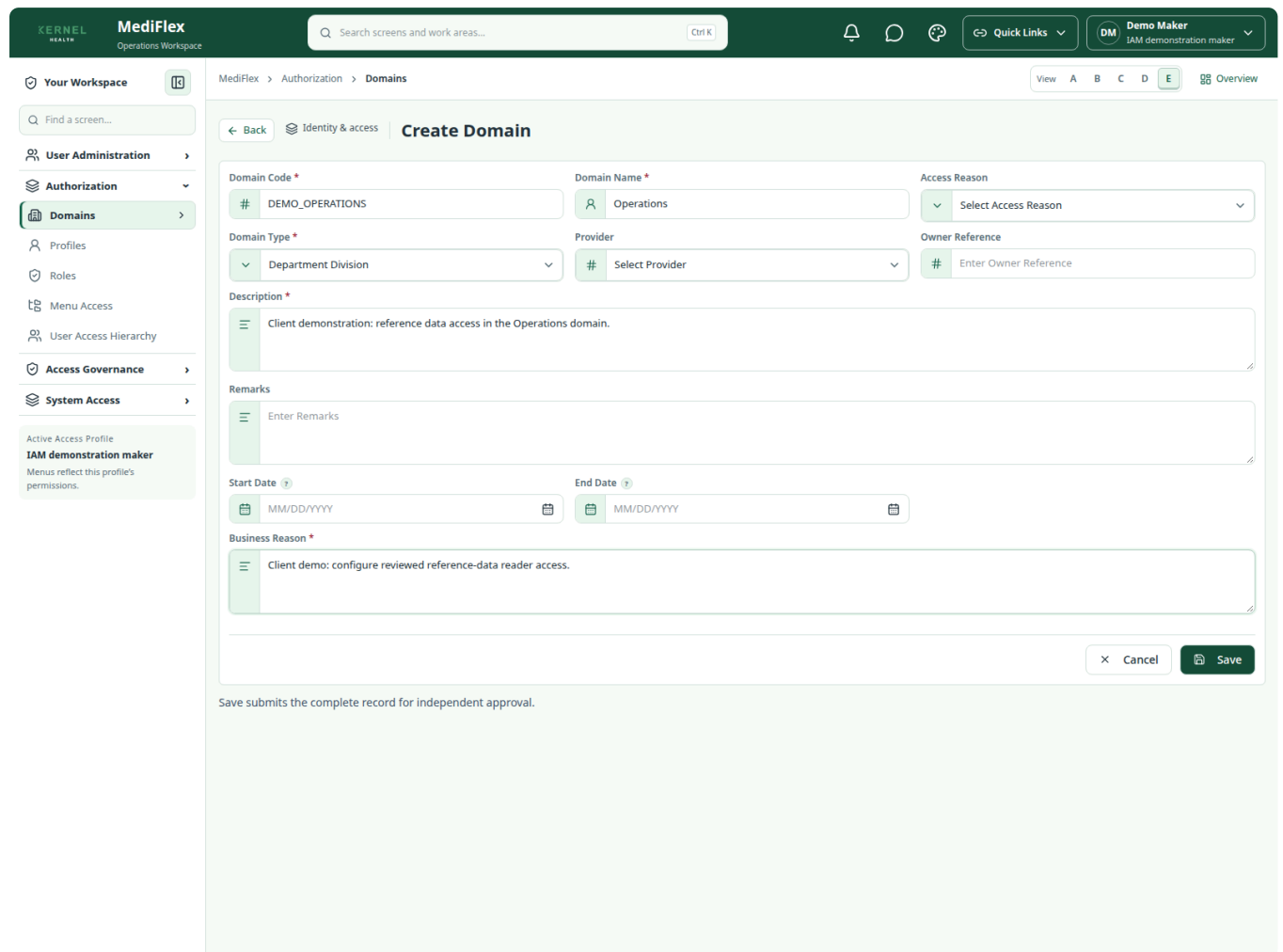
1. Search for DEMO_OPERATIONS or the chosen suffixed code. Reuse only an intentionally prepared example record.
2. Select **Create Domain**. Enter the following values in the full-page form.
3. Choose the appropriate offered access reason if your setup requires it. For Department Division, do not invent a Provider reference.
4. Use future or current validity dates appropriate to the live run; blank dates and date limits follow the configured form rules.
5. Select **Save**. On the metadata-backed form, Save submits the complete record for independent approval. A fallback form can label the action Submit for Approval.
6. Record the proposal reference. Have the independent Checker review the creation as described in the review chapter, then refresh Domains.

Field	Example / instruction
Domain Code	DEMO_OPERATIONS
Domain Name	Operations
Domain Type	Department Division
Description	Reference-data setup: reference data access in the Operations domain.
Provider / Owner Reference	Only when relevant and offered for the selected domain type
Access Reason / Remarks	Use approved catalog reason when applicable; short explanatory remarks
Start Date / End Date	Business validity; the form describes local-midnight handling
Business Reason	Reference-data setup: configure reviewed reference-data reader access.

SCREEN 22

Create Domain: complete the actual master form

Application screen with illustrative data · click to enlarge



MediFlex Operations Workspace

Search screens and work areas... Ctrl K

Quick Links

Demo Maker IAM demonstration maker

Your Workspace

Find a screen...

User Administration

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

Access Governance

System Access

Active Access Profile: IAM demonstration maker
Menus reflect this profile's permissions.

MediFlex > Authorization > Domains

View A B C D E Overview

Back Identity & access Create Domain

Domain Code * DEMO_OPERATIONS

Domain Name * Operations

Access Reason Select Access Reason

Domain Type * Department Division

Provider Select Provider

Owner Reference Enter Owner Reference

Description * Client demonstration: reference data access in the Operations domain.

Remarks Enter Remarks

Start Date MM/DD/YYYY

End Date MM/DD/YYYY

Business Reason * Client demo: configure reviewed reference-data reader access.

Cancel Save

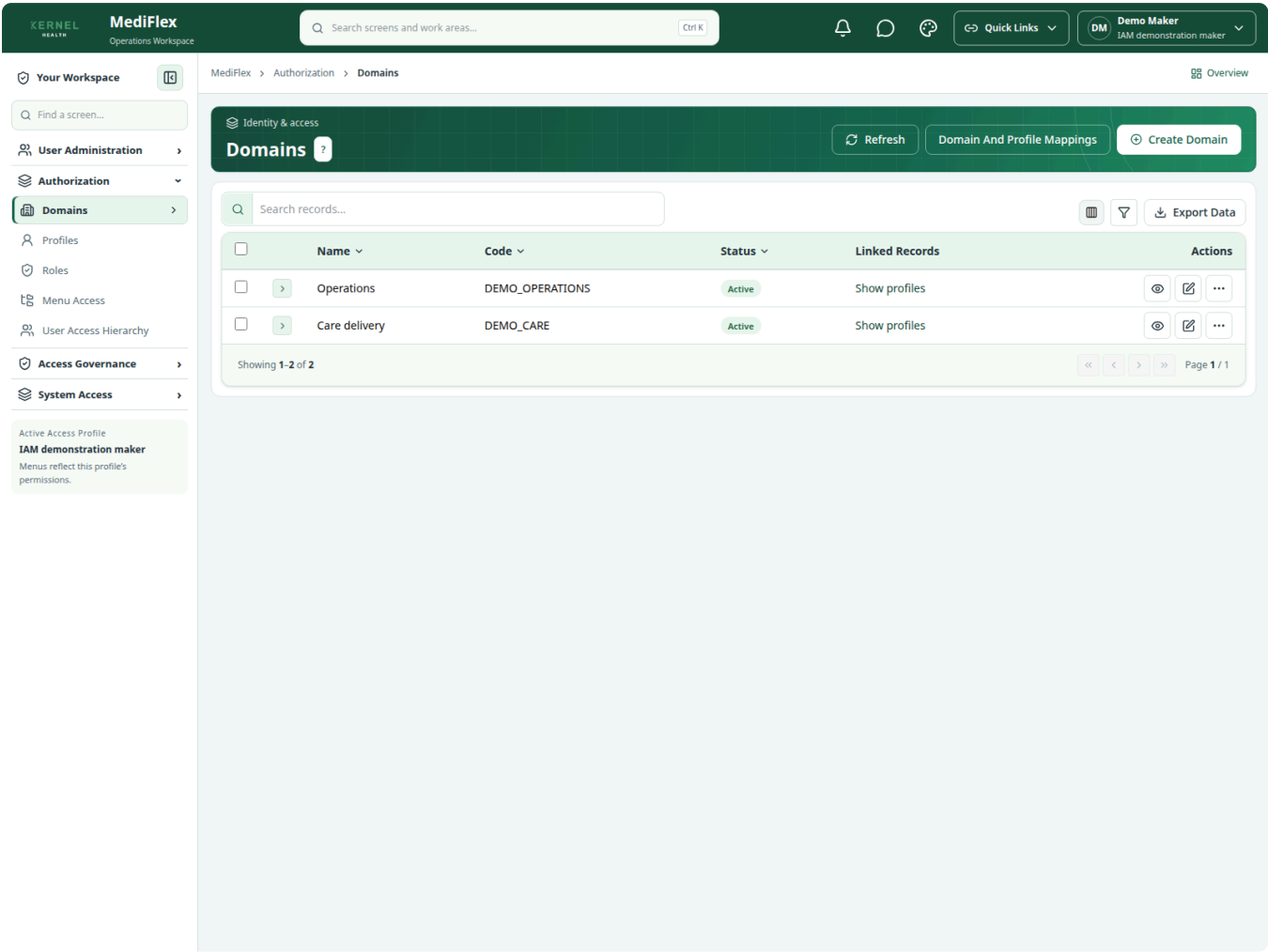
Save submits the complete record for independent approval.

- Domain Type and Description are part of the master definition.
- Save creates an approval proposal, not an immediate universal access grant.

SCREEN 23

Domain master after an illustrative approved setup

Application screen with illustrative data · click to enlarge



- The master grid remains a master grid.
- Relationship actions add eligibility without replacing the domain definition.

Expected result

After a confirmed approval, the domain is available for eligible profile setup. Creating it does not add users, roles or permissions.

CHAPTER 23

Create the Role

Task context	Details
Screen / entry	Authorization → Roles → Create Role

Task context	Details
Who acts	Maker

Who: Maker

Open: Authorization → Roles → Create Role

1. Select **Create Role**.
2. Enter Role Code DEMO_READ_ROLE and Role Name Reference data reader role.
3. Select **Role Type: Regular** for this business walkthrough. Enter Description: Read approved reference data without maintaining it.
4. Complete dates, catalog reason and remarks only as applicable. Add a Business Reason.
5. Select Save and obtain the independent creation decision. Refresh Roles and locate the approved role.
6. Open its details. Note that a role without permission grants cannot perform the intended business actions.

SCREEN 24

Create a regular business role

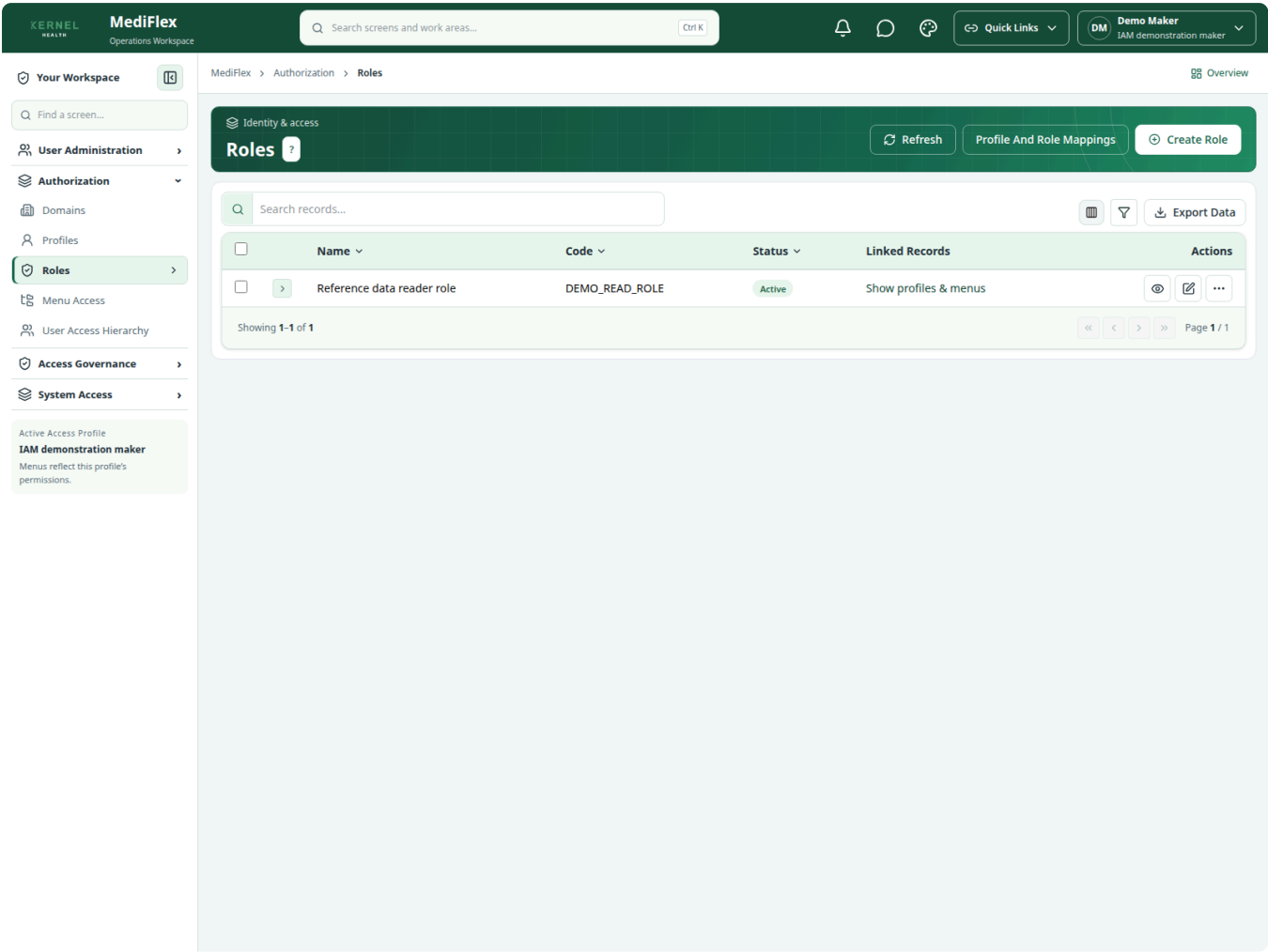
Application screen with illustrative data · click to enlarge

- The role definition and its later permission grants are different changes.
- System/Regular classifies the role; it is not an administrator-access shortcut.

SCREEN 25

Role master and relationship entry points

Application screen with illustrative data · click to enlarge



- Use the role's record details for Role Permissions.
- Use row mappings/Menu Access for relationships to profiles and screen actions.

Expected result

The role exists after approval. It still needs the intended effective permission grants and a profile relationship.

CHAPTER 24

Create the Profile

Task context	Details
Screen / entry	Authorization → Profiles → Create Profile

Task context	Details
Who acts	Maker

Who: Maker

Open: Authorization → Profiles → Create Profile

1. Select **Create Profile**. Enter Profile Code DEMO_READER and Profile Name Reference data reader.
2. Choose **Initial Domain: Operations**. The domain must be available and permitted to this operator.
3. Select **Profile Type: Regular**. Enter the required Description. Set **Available for Profile Selection: Yes** for the intended interactive user.
4. Complete any required catalog values, dates and Business Reason, then Save.
5. Obtain independent approval and refresh Profiles.
6. Expand the approved profile's linked records. Inspect Domains and Roles. Verify the initial domain relationship before attempting to add a duplicate.

Create Profile with its initial domain and selectable setting

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker

IAM demonstration maker

Your Workspace

Find a screen...

User Administration

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

Access Governance

System Access

Active Access Profile

IAM demonstration maker

Menus reflect this profile's permissions.

MediFlex

Authorization

Profiles

View

A

B

C

D

E

Overview

Back

Identity & access

Create Profile

Find more options

Profile Code *

#

DEMO_READER

Profile Name *

👤

Reference data reader

Initial Domain *

▼

Operations

▼

Access Reason

▼

Select Access Reason

▼

Profile Type *

▼

Regular

▼

Profile Category

T

Enter Profile Category

Available For Profile Selection *

▼

Yes

▼

Description *

≡

Client demonstration: reference data access in the Operations domain.

Remarks

≡

Enter Remarks

Start Date

📅

MM/DD/YYYY

📅

End Date

📅

MM/DD/YYYY

📅

Business Reason *

≡

Client demo: configure reviewed reference-data reader access.

Cancel

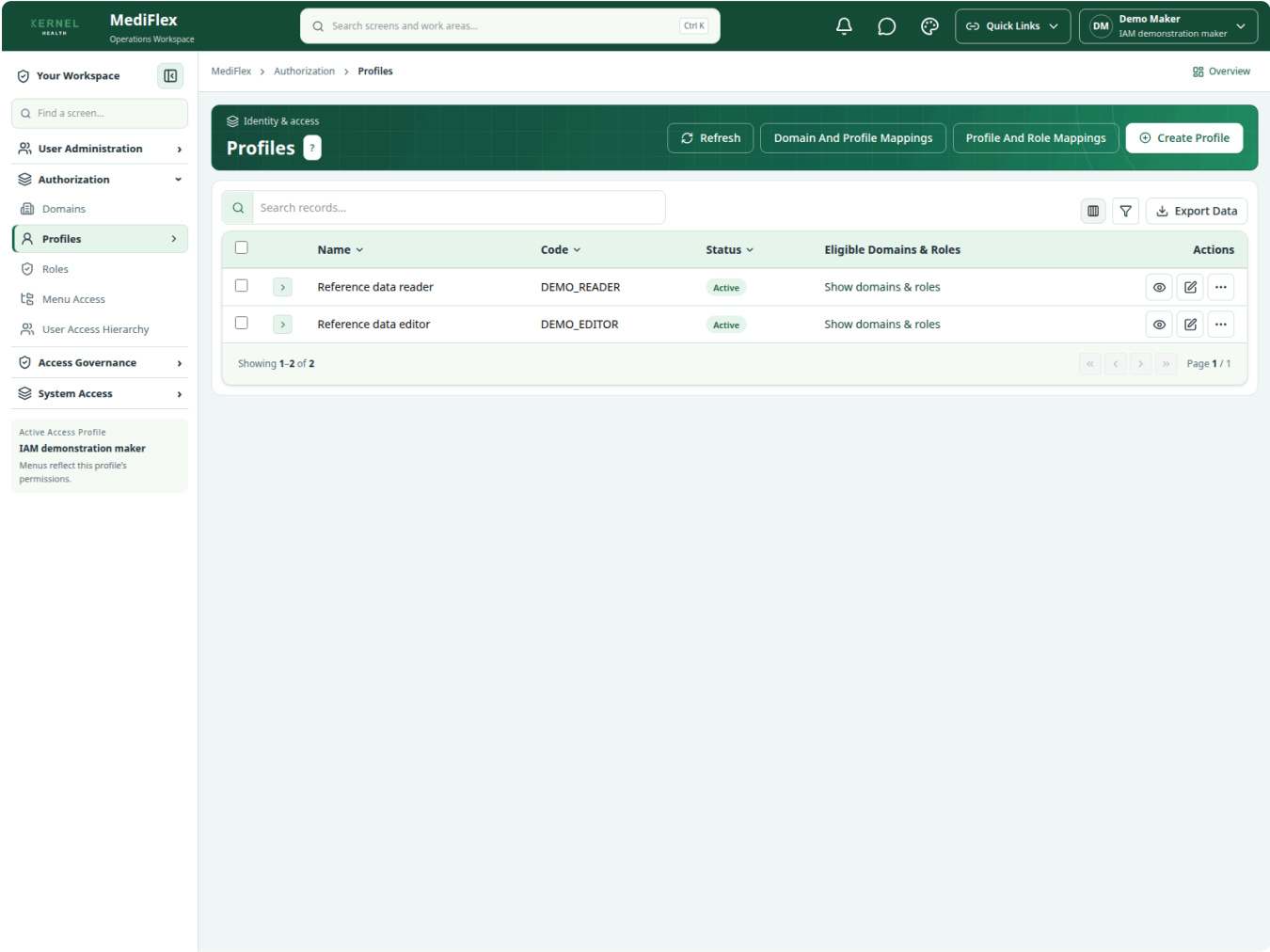
Save

Save submits the complete record for independent approval.

- Profile creation can establish the initial domain association.
- A selectable profile still requires user assignment, effective dates and role grants.

Profiles remain separate master records

Application screen with illustrative data · click to enlarge



- Master details describe the profile.
- Domain and role relationships are administered through additional mapping actions.

Expected result

The approved profile is eligible in the intended domain. A user does not receive it merely because it is marked available for selection.

Create a Permission or select an existing one

Task context	Details
Screen / entry	Advanced Configuration → Permission Catalog → Create Permission

Task context	Details
Who acts	Maker

Who: Maker

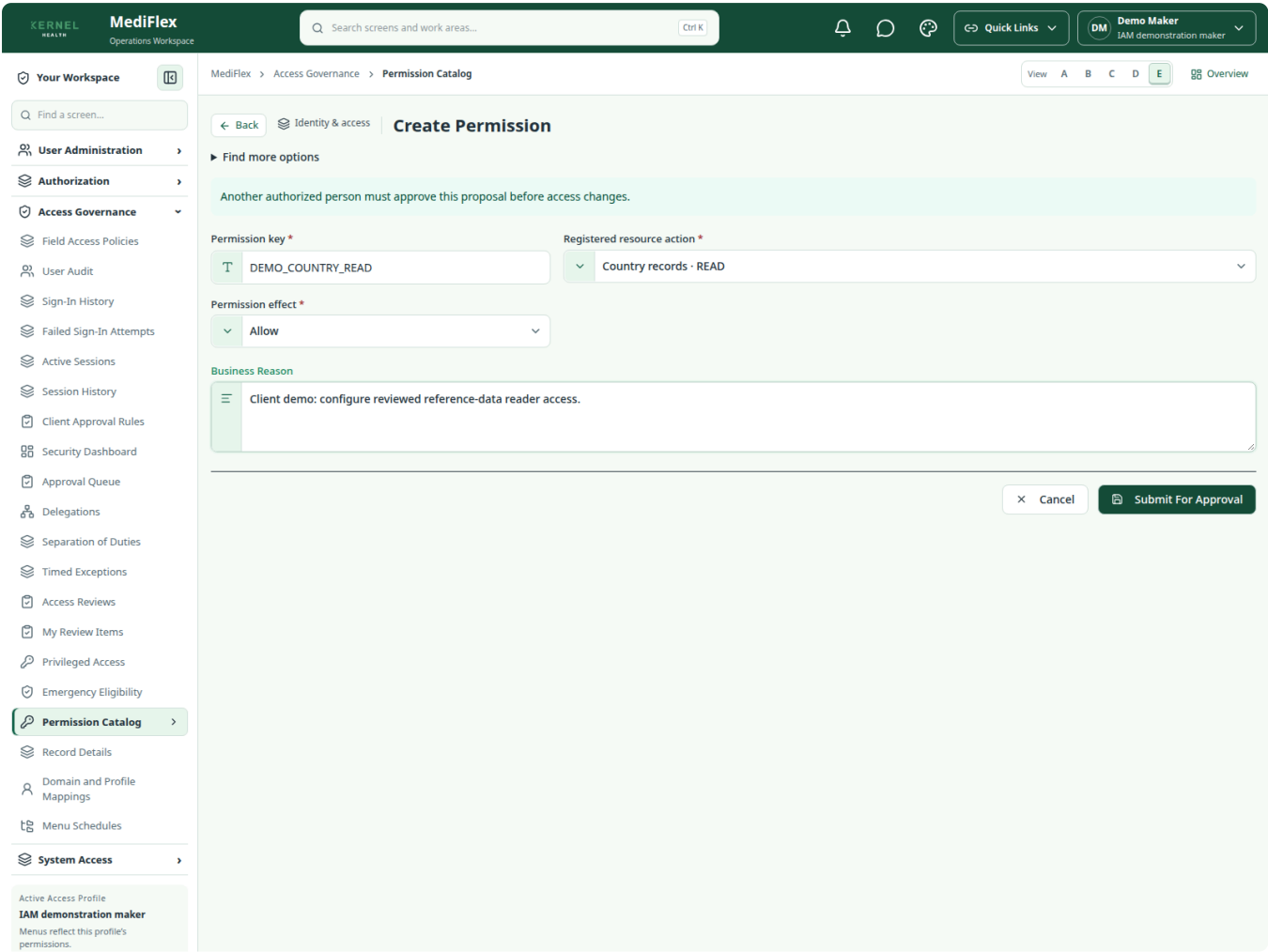
Open: Advanced Configuration → Permission Catalog → Create Permission

1. Inspect the existing published permission keys for the target screen and read API. Prefer the matching existing permission when it already exists.
2. For the creation exercise, select **Create Permission**. Enter a unique Permission key such as DEMO_COUNTRY_READ.
3. Choose the exact offered **Registered resource action** representing the demo read operation. The illustration uses Country records · READ; use the actual entry in your deployment.
4. Choose **Permission effect: ALLOW**. Supply the Business Reason and select Submit for Approval.
5. Have the Checker validate the registered action, effect and purpose, then approve. Refresh the Permission Catalog.
6. Before using the new key in a live flow, confirm that the relevant published menu/control requirements reference it, or verify it only as an additional requirement in the isolated demo setup.

SCREEN 28

Create Permission against an existing registered action

Application screen with illustrative data · click to enlarge



- The operation must already exist in the resource-action catalog.
- Creating an ALLOW definition does not grant it to any role.

SCREEN 29

Permission Catalog: inspect action, effect and status

Application screen with illustrative data · click to enlarge

MediFlex Operations Workspace

Search screens and work areas... Ctrl K

Quick Links Demo Maker IAM demonstration maker

Your Workspace 10

Find a screen...

User Administration

Authorization

Access Governance

Field Access Policies

User Audit

Sign-In History

Failed Sign-In Attempts

Active Sessions

Session History

Client Approval Rules

Security Dashboard

Approval Queue

Delegations

Separation of Duties

Timed Exceptions

Access Reviews

My Review Items

Privileged Access

Emergency Eligibility

Permission Catalog

Record Details

Domain and Profile Mappings

Menu Schedules

System Access

Active Access Profile
IAM demonstration maker
Menus reflect this profile's permissions.

MediFlex > Access Governance > Permission Catalog Overview

Published permission meanings are immutable. Create a new permission or propose changes to a role's grants. RBAC grants remain subject to backend policy checks.

Identity & access

Permission Catalog ?

Refresh Menu Permission Mappings Create Permission

Search records...

Export Data

	Name	Code	Status	Linked Records	Resource	Actions
☐	Read countries	country.read	Approved	Show menus	Country records	

Showing 1-1 of 1

Page 1 / 1

- The permission key must match the required binding.
- A similarly named permission is not a substitute for an exact published key.

Three different actions: creating a permission defines it; granting it to a role assigns it; adding it as a menu/control requirement constrains access. A new name alone does not satisfy an existing screen's required permission keys. A DENY definition is not a weaker ALLOW; only use one in a specifically rehearsed policy example.

Expected result

An approved permission definition exists. No user gains access until the appropriate role grants and runtime bindings are effective.

Published permission meanings are immutable in the inspected administration flow. Create a new permission definition or propose a change to a role's grants instead of silently changing the meaning of a permission already in use.

CHAPTER 26

Map Domains ↔ Profiles

Task context	Details
Screen / entry	Domains → Operations row → More actions → Map profiles
Who acts	Maker, then Checker

Who: Maker, then Checker

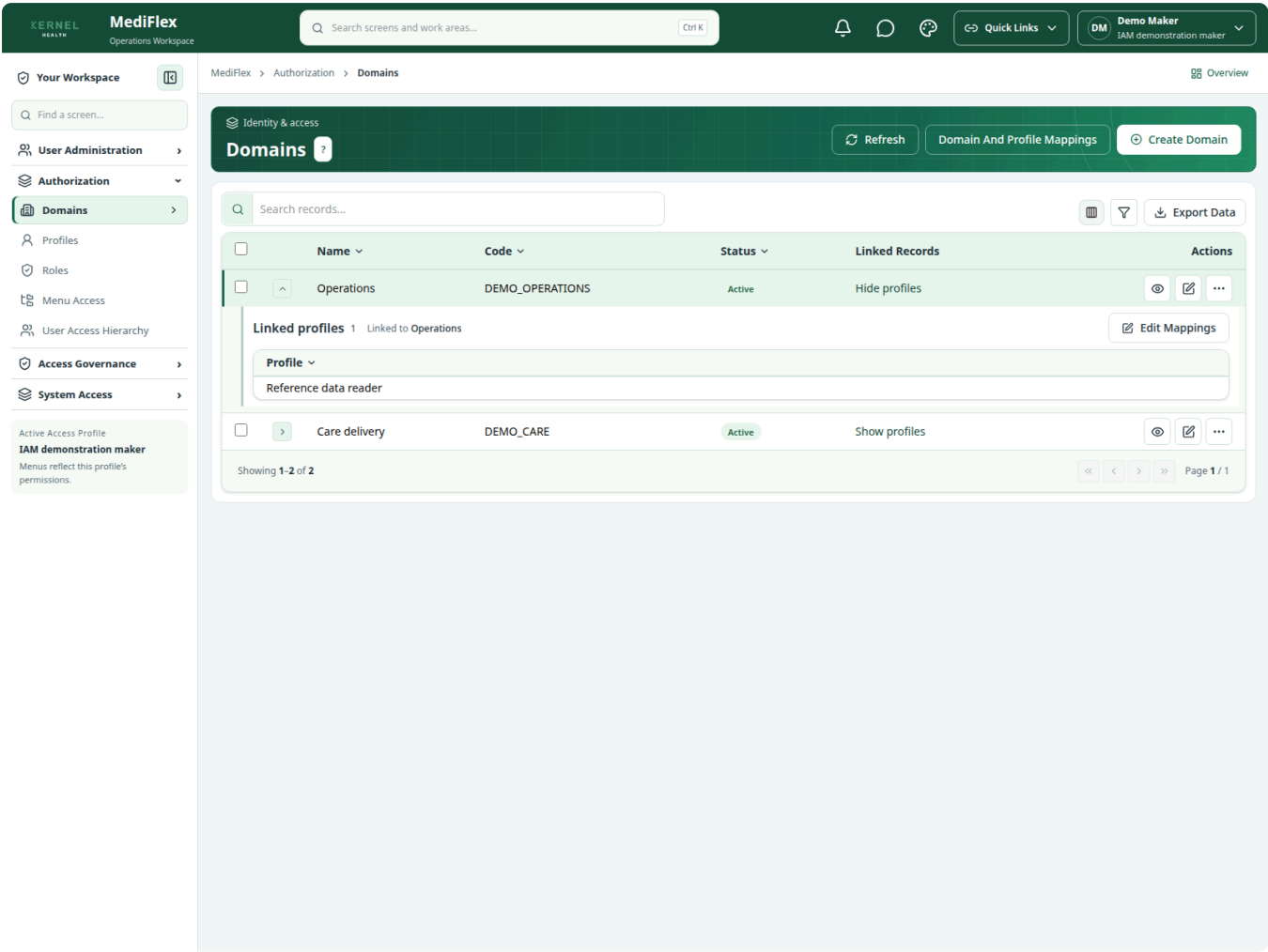
Open: Domains → Operations row → More actions → Map profiles

1. Expand the Operations row first to show the currently linked profiles.
2. If Create Profile already established Operations ↔ Reference data reader, leave that link intact and explain the initial association. To verify an additional change, use a second prepared eligible profile or domain.
3. Select **Map profiles** or the header's **Domain and profile mappings**, then **Edit mappings**.
4. Choose the source record if it was not carried from the row. Select the intended additional counterpart. Existing links must remain selected unless removal is intended.
5. Select **Review changes**. Inspect every addition/removal and enter the reason. Select **Submit for approval**.
6. On the affected record, show the pending Mapping changes. As the independent Checker, inspect the same proposal, approve and confirm.
7. Refresh and expand the domain. Show the resulting profiles. Open Profiles → the profile → **Map domains** to verify the reverse view.

SCREEN 30

Domain row expanded to show profile relationships

Application screen with illustrative data · click to enlarge



- Eligibility can be viewed from either side.
- A second link demonstrates many-to-many behavior without duplicating the initial association.

Expected result

The approved relationship is visible from both domain and profile views. It does not automatically assign every domain member to the profile.

Access-scope compatibility and protected-record restrictions still apply. Do not change a domain/profile scope merely to force a failed mapping through. Review the stated restriction.

CHAPTER 27

Map Profiles ↔ Roles

Task context	Details
Screen / entry	Profiles → Reference data reader row → More actions → Map roles
Who acts	Maker, then Checker

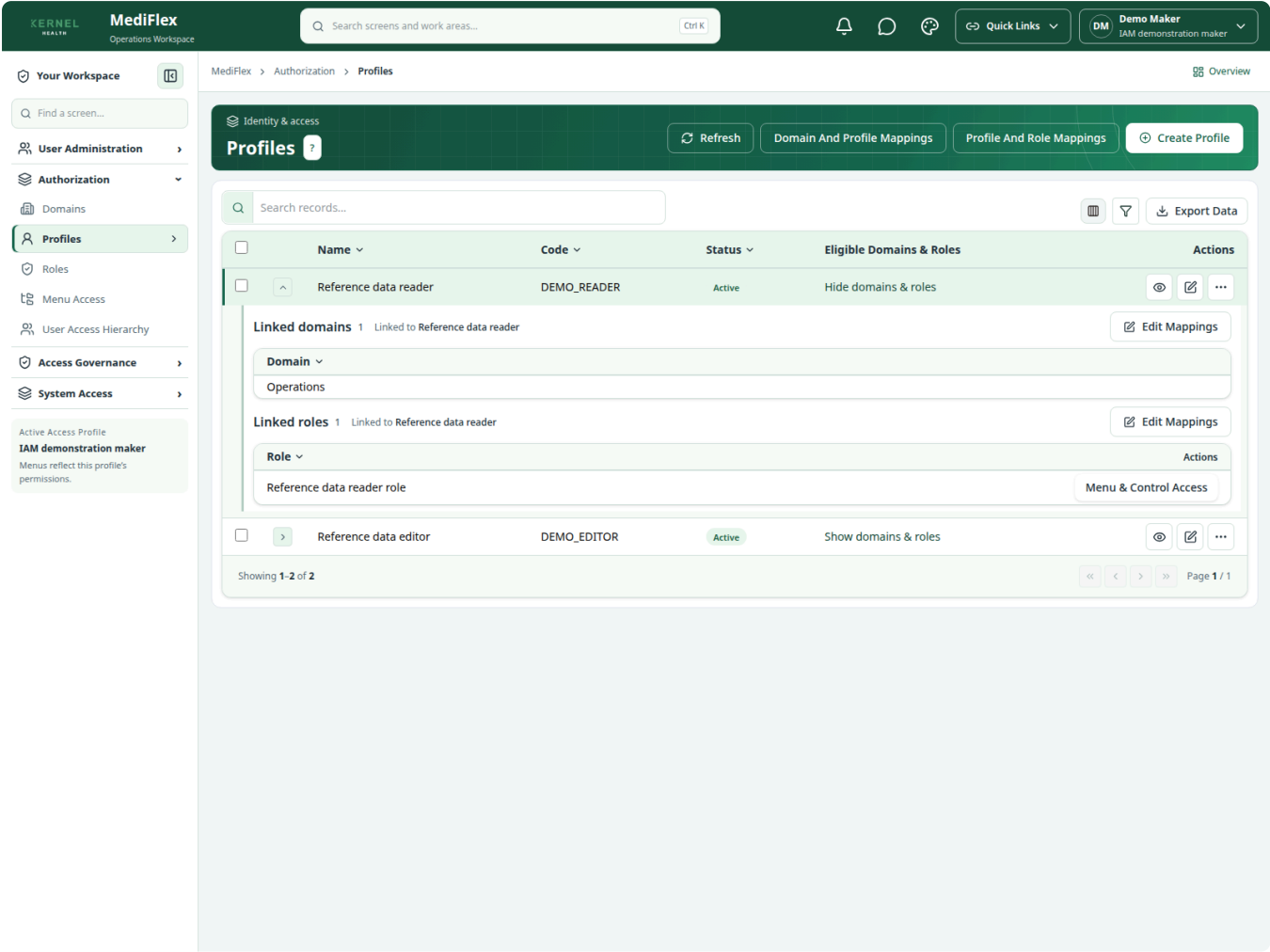
Who: Maker, then Checker

Open: Profiles → Reference data reader row → More actions → Map roles

1. Open **Map roles**, or use **Profile and role mappings** from Profiles or Roles.
2. Keep Reference data reader as the source profile. Select Reference data reader role.
3. Review changes, add a Business Reason and submit for approval.
4. Have the independent Checker inspect the affected row's proposal and confirm the decision.
5. Refresh and expand the profile: the approved role appears under Roles.
6. Inspect the reverse relationship from Roles → Reference data reader role → **Map profiles**. Note that additional approved roles can be bundled into a profile and a role can be reused by multiple profiles.

Profile relationships: domain eligibility and role bundle

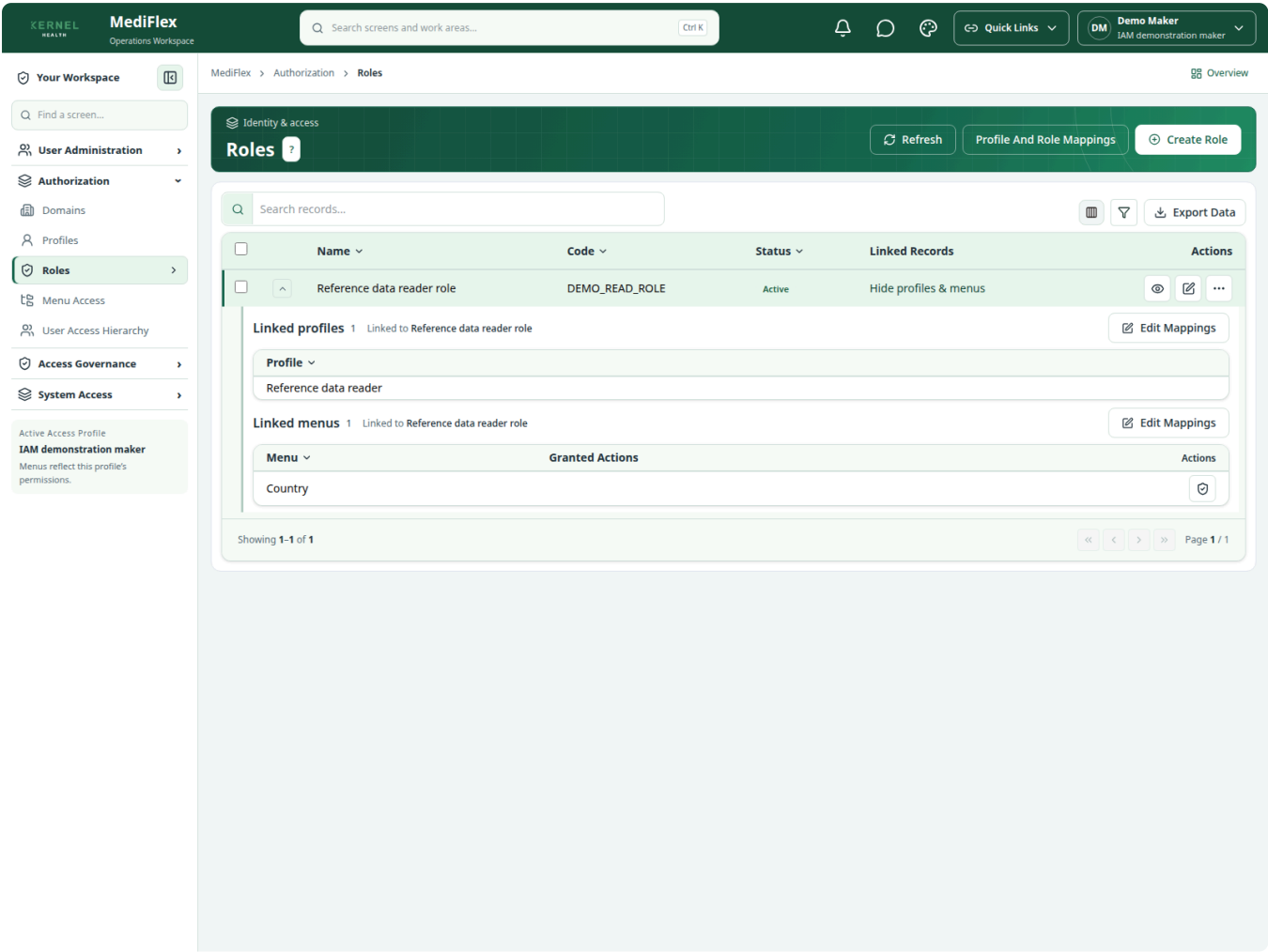
Application screen with illustrative data · click to enlarge



- The profile's domains and roles are separate relationships.
- Changing a shared role can affect several profiles and assigned users.

Reverse inspection from the Role master

Application screen with illustrative data · click to enlarge



- The role remains a master record.
- Linked profiles and menus provide navigation to related access administration.

Expected result

The profile contains the approved role. Runtime privileges still depend on that role’s effective permissions and all applicable conditions.

Grant Permissions to the Role

Task context	Details
Screen / entry	Roles → open Reference data reader role → Role Permissions

Task context	Details
Who acts	Maker, then Checker

Who: Maker, then Checker

Open: Roles → open Reference data reader role → Role Permissions

1. Open the role's record using its View action. Expand **Role Permissions** if collapsed.
2. Select **Grant permission**. Verify the carried role and choose an approved permission from the offered catalog.
3. For the working reader walkthrough, grant the actual registered navigation, screen read, data read and required field/control permissions identified during preparation. A screen may need more than one permission.
4. Add the reason and submit. The permission grant/removal proposal remains attached to its permission row until an independent decision.
5. As Checker, open the same role, inspect the proposed permission row and select its Review/Open proposal action. Read the before/after change. Approve, then Confirm approval.
6. Return as Maker or Business user and refresh the relevant access view. Verify the effective grant.
7. Leave Create, Update, Delete and approval permissions ungranted for this reader example. Rehearse the resulting write denial later.

Item	Walkthrough result
Permission definition	Exists and references the correct registered action
Role permission grant	Reviewed link to Reference data reader role
Profile role link	Reader profile inherits the role
User assignment	Only assigned eligible users can select that profile
Control/menu requirement	Must match the permission keys actually evaluated at runtime

Expected result

The role's permission rows show the approved read grants. Pending changes do not yet alter effective access.

Maintain Menu Access and role/menu actions

Task context	Details
Screen / entry	Authorization → Menu Access
Who acts	Maker, then Checker

Who: Maker, then Checker

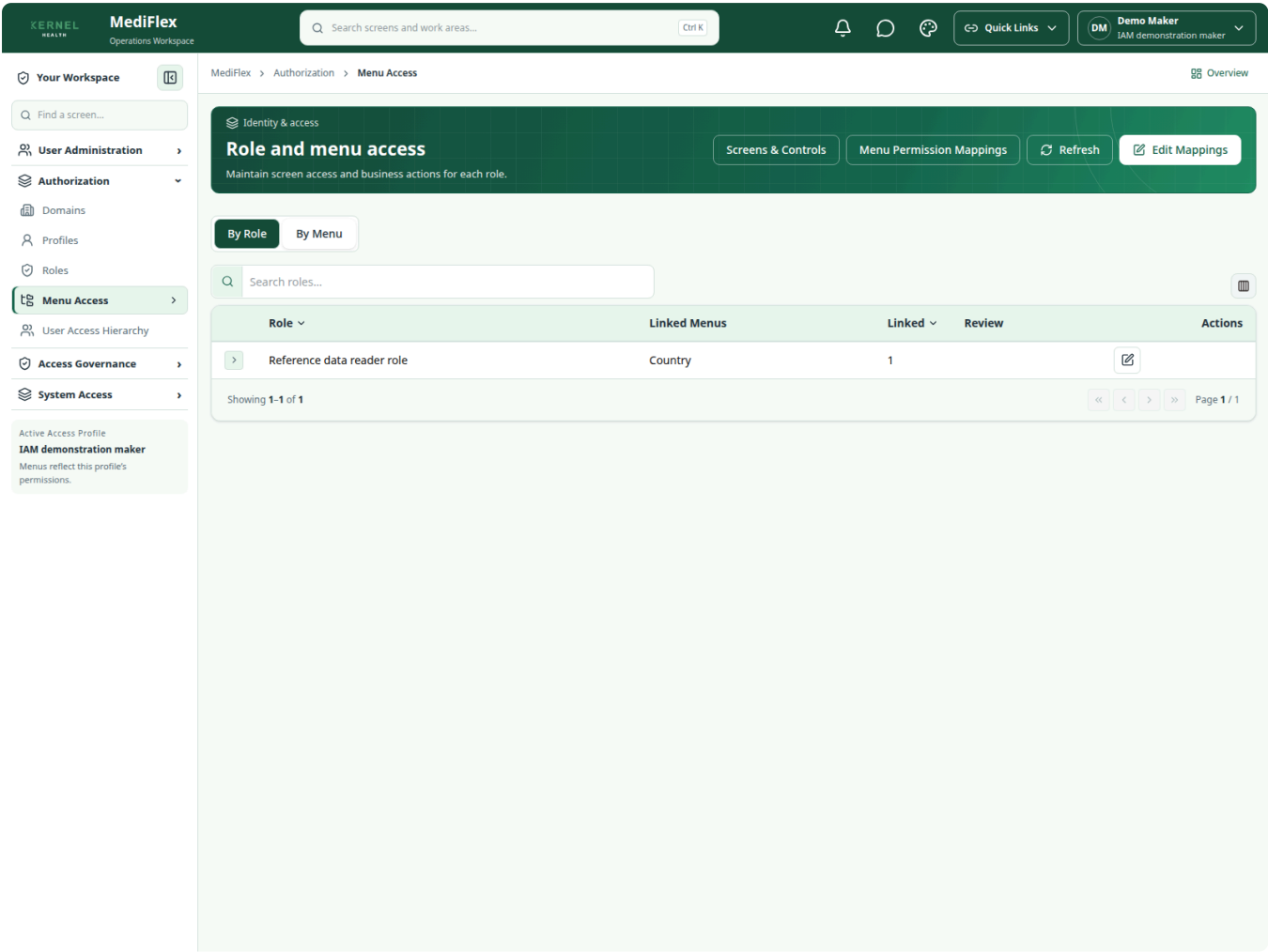
Open: Authorization → Menu Access

1. Open Menu Access. The relationship workspace shows **Role and menu access**; switch back to it if Menu permission mappings is selected.
2. Select Reference data reader role, then Edit mappings. Locate the registered Country menu.
3. Inspect its action choices. Configure only the intended View/read-related access for the example. Review any automatically included view dependencies.
4. Select Review changes and check the displayed permission/action effects. Add the reason and Submit for approval.
5. Have the independent Checker decide the proposal from the affected row. Refresh to inspect the effective action state.
6. Use **Screens & controls** to inspect the target screen and its detailed security requirements.
7. Later sign in as the business user with Reference data reader selected. Verify the sidebar is the result of that effective context. Do not infer runtime access from the administrator’s menu alone.

SCREEN 33

Menu Access: role/menu administration

Application screen with illustrative data · click to enlarge



- This workspace maintains access to registered navigation entries.
- The role/menu view translates business screen actions into governed access changes.

There is an IAM menu master in the data model. The inspected Menu Access UI is a mapping workspace; it is not an arbitrary new-menu creation form. The effective permission path remains authoritative. A visible menu is not permission to execute every operation on that page.

Expected result

The approved role/menu configuration agrees with the role’s actual permission grants. The user’s authorized navigation reflects the selected effective profile and policy context.

Map Permissions ↔ Menus and inspect the screen bridge

Task context	Details
Screen / entry	Permission Catalog → permission row → Map menus; or Menu Access → Menu permission mappings
Who acts	Maker for changes; either authorized operator for inspection

Who: Maker for changes; either authorized operator for inspection

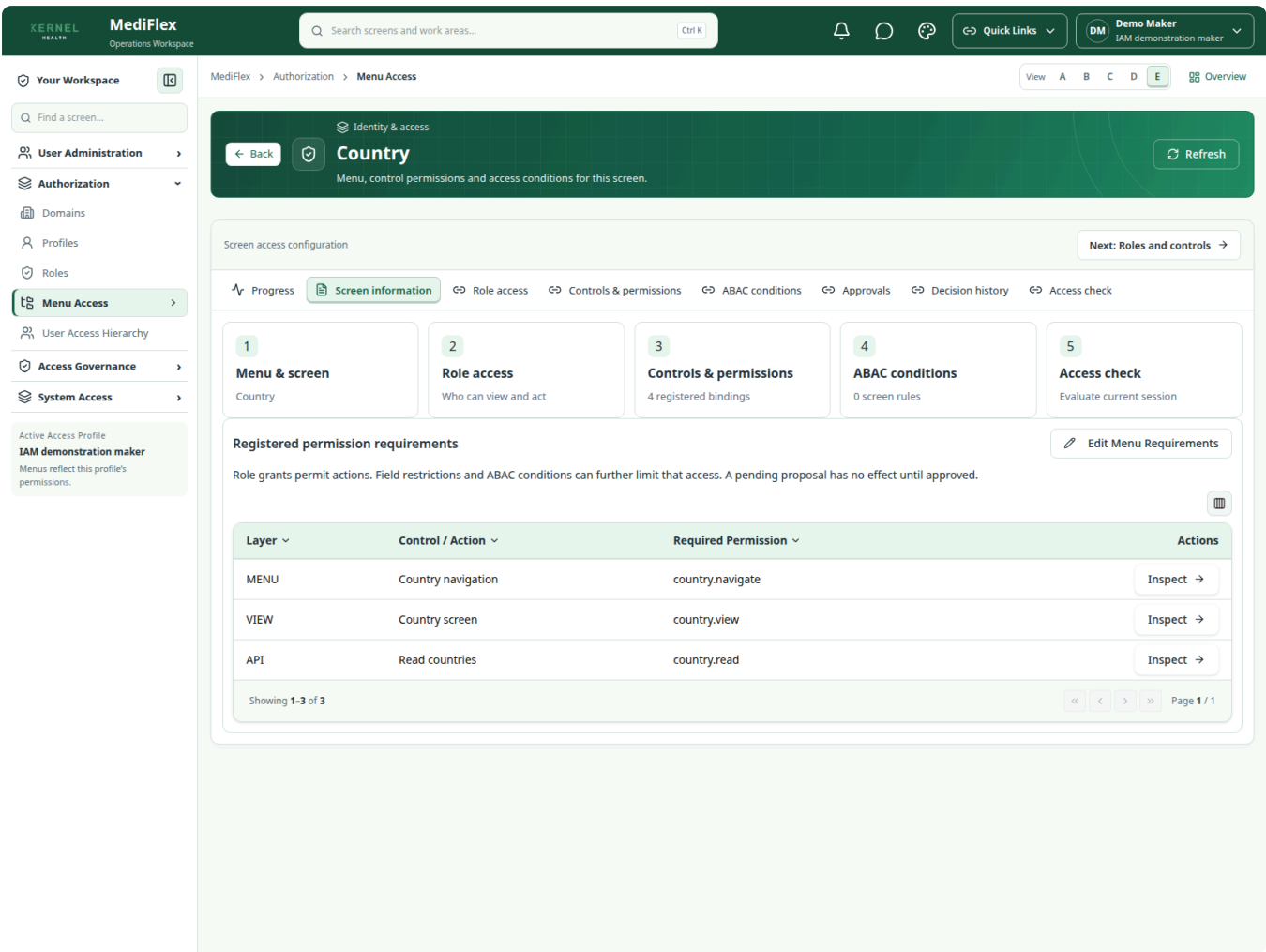
Open: Permission Catalog → permission row → Map menus; or Menu Access → Menu permission mappings

1. Open the relationship from a permission’s **Map menus** action, or select **Menu permission mappings** in Menu Access.
2. Choose the registered menu or permission as the source. Inspect linked entries and their Applies to/Binding information.
3. Distinguish locked **Required dependency** entries from editable **Additional requirement** entries. Do not remove baseline dependencies.
4. If using an additional restriction, choose the prepared permission in the isolated demo setup. Review changes, reason and submit; obtain the independent decision.
5. Open **Screens & controls**, select Country and use **Screen information**. Identify the menu/screen relationship and applicable registered requirements.
6. Confirm the Axis inventory contains the matching screen and controls. Publication and IAM bridge identity must agree before treating the route as ready.

SCREEN 34

Screen information: connect the menu to its registered screen

Application screen with illustrative data · click to enlarge



- Inspect the screen and registered security layers.
- This is a verification step, not a claim that a new bridge can be typed into this page.

Expected result

Permission/menu requirements and the registered screen identity are traceable. An additional requirement narrows access; it does not grant that permission to a role.

CHAPTER 31

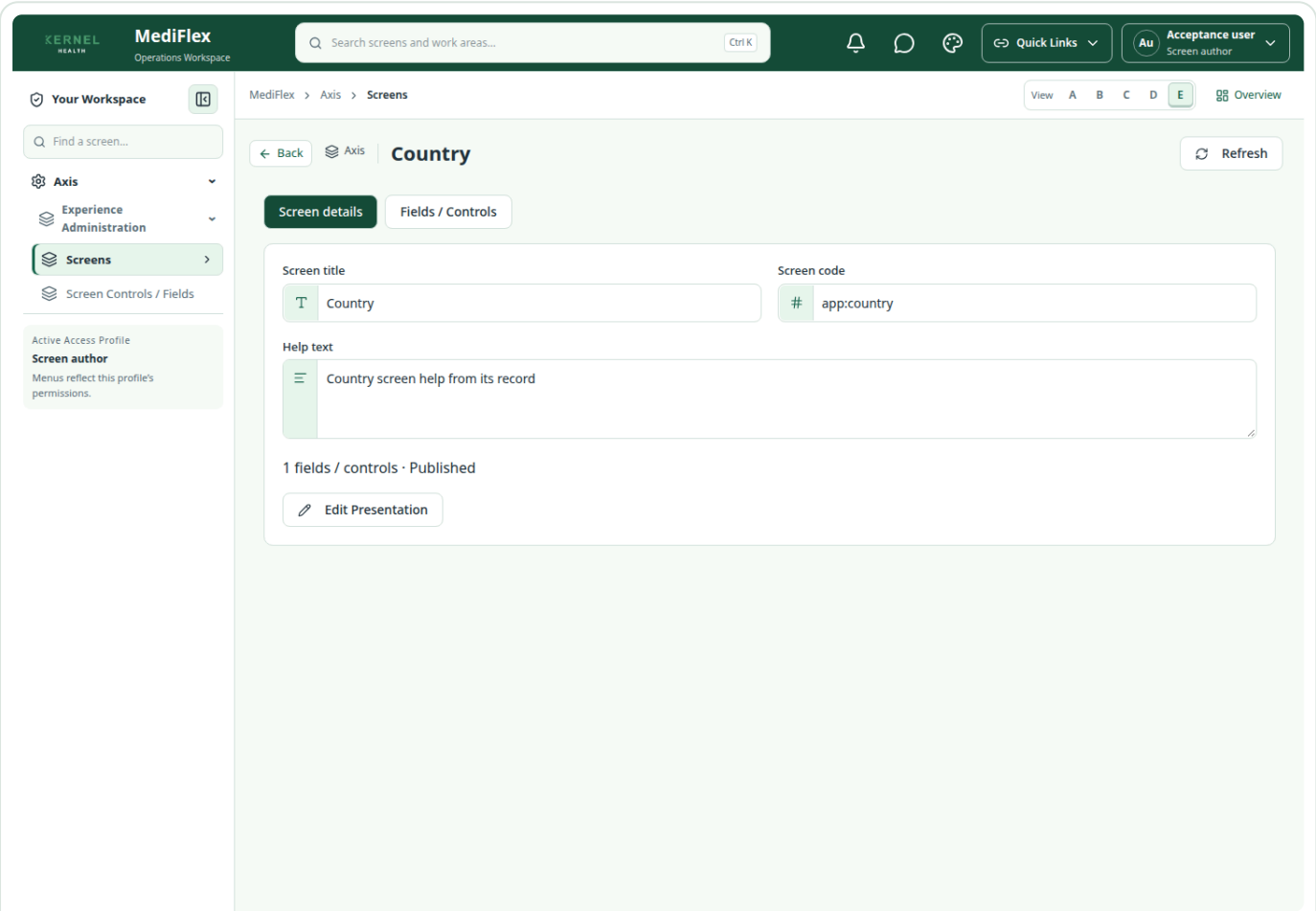
Maintain Axis screens, fields and labels

Current screen model: open a screen record first, then use **Screen details** and **Fields / Controls** within that record. The Controls entry lists owning screens before showing their controls. Existing registered screens and newly authored screens are managed through the same screen workspace.

1. **Open the owning screen.** Go to System Access → Experience Administration → Screens. Search for an approved example such as Country. Select Open screen on that row. Confirm the title and Screen code before changing anything.
2. **Inspect screen presentation.** In Screen details read Screen title and Help text. Select Edit Presentation, enter the proposed values and a clear Change / decision reason, then submit for review. Pending values must not immediately replace the approved title or help.
3. **Inspect its controls.** Select Fields / Controls. Only this screen's fields and actions should appear. Open the intended row with Edit presentation; inspect its stable code, kind and current presentation.
4. **Propose the control change.** Edit Control label, Help text and the offered display format. Enter the reason and submit. Remain in the same screen context; its row shows the pending control change.
5. **Review on this record.** The eligible checker opens this screen and the pending control row, inspects before/after and the exact revision, enters the decision reason and selects Approve or Reject. Standard contributors cannot approve their own proposal.
6. **Verify the result.** Refresh the original screen. Confirm the approved label/help and retained history. Refresh or reopen the original business screen to verify the resulting presentation. Back returns to the owning screen list; refresh preserves the selected screen.

Field	What to enter / expected behavior
Screen code	Unique technical code for a newly authored screen. It becomes fixed after the first save. Existing screen codes identify the published owner; do not rename them to change a title.
Screen name / Screen title	The business-facing heading. For an existing screen, change Screen title through Edit Presentation and submit a reason.
Screen header help text	Multiline screen-level guidance shown behind the question mark beside the header. It saves through the existing screen description metadata and becomes effective after approval. A control's Help text belongs to that control.
Layout	Table displays the configured fields as columns; Record details displays them as a record. This selects a renderer for an authored screen; it does not change the entire application theme.
Navigation section	The parent sidebar section for the authored screen, for example Operations. Use the agreed business section consistently.
Menu group	Optional subgroup beneath the section, for example Reference data. Leave empty when no subgroup is needed. It does not grant access.
Registered business source	An approved server operation supplying records and its declared fields. Choose a source appropriate to the task. This is not a connection string or a place to enter SQL. The source's owner still enforces access.
Source field	Declared field from the selected business source. Changing the source clears incompatible field bindings.

Field	What to enter / expected behavior
Control label / Help text / Display format	Presentation values for the selected owning screen's control. Use its stable identity; a renamed label does not create a new permission.
Change / decision reason	Explain the business reason for saving, submitting or deciding the exact revision.
IAM Access Mapping	Select existing authorized navigation, page and field/control permission references. Defining a screen does not create role grants.
Active / Include inactive	Inactive configuration remains available for permitted historical inspection. Approval state and active state are separate.



Owning screen details and controls tabs · application rendered with illustrative test records; select to enlarge.

Screen ownership mappings and presentation changes

Who: Axis Maker → eligible owner/reviewer → publisher

Open: Screens → selected registered screen → Create Screen Mapping

1. Use an eligible unmapped demo screen or an existing demo draft. Select **Create Screen Mapping** from the screen's available actions; use **Revise Screen Mapping** when revising a current draft.
2. Select **Responsible Role** and enter **Change Reason** of at least eight characters. The registered screen/source identity is carried by the UI. Save the draft.
3. Open **Screen Mapping Drafts**. Inspect the current revision and ownership state. Use **Confirm Mapping Ownership** when available to the eligible owner. Its decision is **Confirm Ownership** or **Return for Revision**.
4. Use **Submit Mapping for Review** when offered for the eligible revision, supplying a reason.
5. An eligible independent reviewer uses **Review Screen Mapping** for that exact revision and chooses **Approve for Publication** or **Return for Revision**.
6. Note that **approved for publication is not yet published**. Complete publication through the established authorized process before using a runtime presentation change.

Responsible Role records ownership. It does not grant that role screen access. This Axis ownership/revision flow is separate from the IAM relationship proposal workflow; its stages must not be presented as extra approval rounds for each role grant.

Optional presentation example: label and read-only setting

1. From an eligible mapping record, open **Create Experience Version**.
2. Select the intended **Profile** for this example; leaving it blank targets all profiles in the tenant. Choose the actual **Locale** and existing **Control**.
3. For example, set Label Text to Country display name. Use Visibility: Inherit the screen setting and Editability: Read Only if using a narrower presentation.
4. Use only settings supported for that selected control: default, position, placeholder, field guidance, column width, theme or spacing as offered. Enter the reason and save.
5. Follow the version's applicable review/publication process. Reopen the screen under the target profile and verify the published label and presentation.
6. Confirm that changing an Axis label or presentation setting has not created a new IAM permission or broadened backend access.

Expected result

Ownership and presentation changes are versioned and distinguishable from permission grants. Verify runtime changes only after actual publication.

Map control permissions and field restrictions

Task context	Details
Screen / entry	Menu Access → Screens & controls → Country → Controls & permissions
Who acts	Maker, then Checker

Who: Maker, then Checker

Open: Menu Access → Screens & controls → Country → Controls & permissions

1. Select the role being inspected. Locate the prepared Country name field/control. Read its Type, Role grant, Field restriction and Additional requirements.
2. Use **Edit permission requirements** for an editable additional-requirement change. Select only the intended permission, inspect shared-screen impact and submit the proposal.
3. Use the control's More actions → **Grant control permission** or Revoke control permission when administering a role grant. This is a different operation from adding a requirement.
4. To verify data-field protection, choose **Edit field access** for the selected role and field. Pick the offered read-only setting for this example. Use masking only for fields that expose a supported masking option.
5. Review before/after values and submit. Have the independent Checker review and decide the proposal on its corresponding control row.
6. Refresh, then test the actual business user. Verify both rendering behavior and protected-operation enforcement. A disabled field alone is not proof of a backend denial.

SCREEN 37

Controls & permissions: inspect each authorization layer

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

Quick Links

Demo Maker

IAM demonstration maker

Your Workspace

Find a screen...

User Administration

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

Access Governance

System Access

Active Access Profile

IAM demonstration maker

Menus reflect this profile's permissions.

MediFlex

Authorization

Menu Access

View

A

B

C

D

E

Overview

Identity & access

Country

Menu, control permissions and access conditions for this screen.

Refresh

Screen access configuration

Next: Roles and controls

Progress

Screen information

Role access

Controls & permissions

ABAC conditions

Approvals

Decision history

Access check

Find role

Enter find role

Search loaded records...

Role for field and control access

Reference data reader role

Previous Roles

More Roles

Control / Field	Type	Role Grant	Field Restriction	Review	Actions
Country name	Field	Granted	Inherit role permissions		
Country navigation	Menu	Granted			
Country screen	Screen	Granted			
Read countries	Server operation	Granted			

Showing 1-4 of 4

Page 1 / 1

- Role grant and additional requirements answer different questions.
- Shared-screen information matters before changing a reused permission.

Field access: propose a read-only restriction

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker

IAM demonstration maker

Your Workspace

Find a screen...

User Administration

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

Access Governance

System Access

Active Access Profile: IAM demonstration maker

Menus reflect this profile's permissions.

Reference data reader role

Previous Roles

More Roles

Control / Field	Type	Role Grant	Field Restriction	Review	Actions
Country name	Field	Granted	Inherit role permissions	1 pending	✎ ✕ ⋮

Country name

Proposed changes and decisions

Require reference-data review for Country name

Demonstration: limit sensitive field maintenance

Record	Mapping / action	Current	Proposed
Country	Country name requirements	No additional requirement	Review reference data

Required permission

country.name.use

Action

USE

Additional permission requirements

0

Linked to Country name

Permission

No linked records.

Also used by

1

Linked to Country name

Screen

State

Open

Country name · Reference data reader role

Field restrictions apply to this role across the field's registered screens. Edit access remains subject to the role's permissions.

Field access

Read only

✕ Cancel

✓ Review Changes

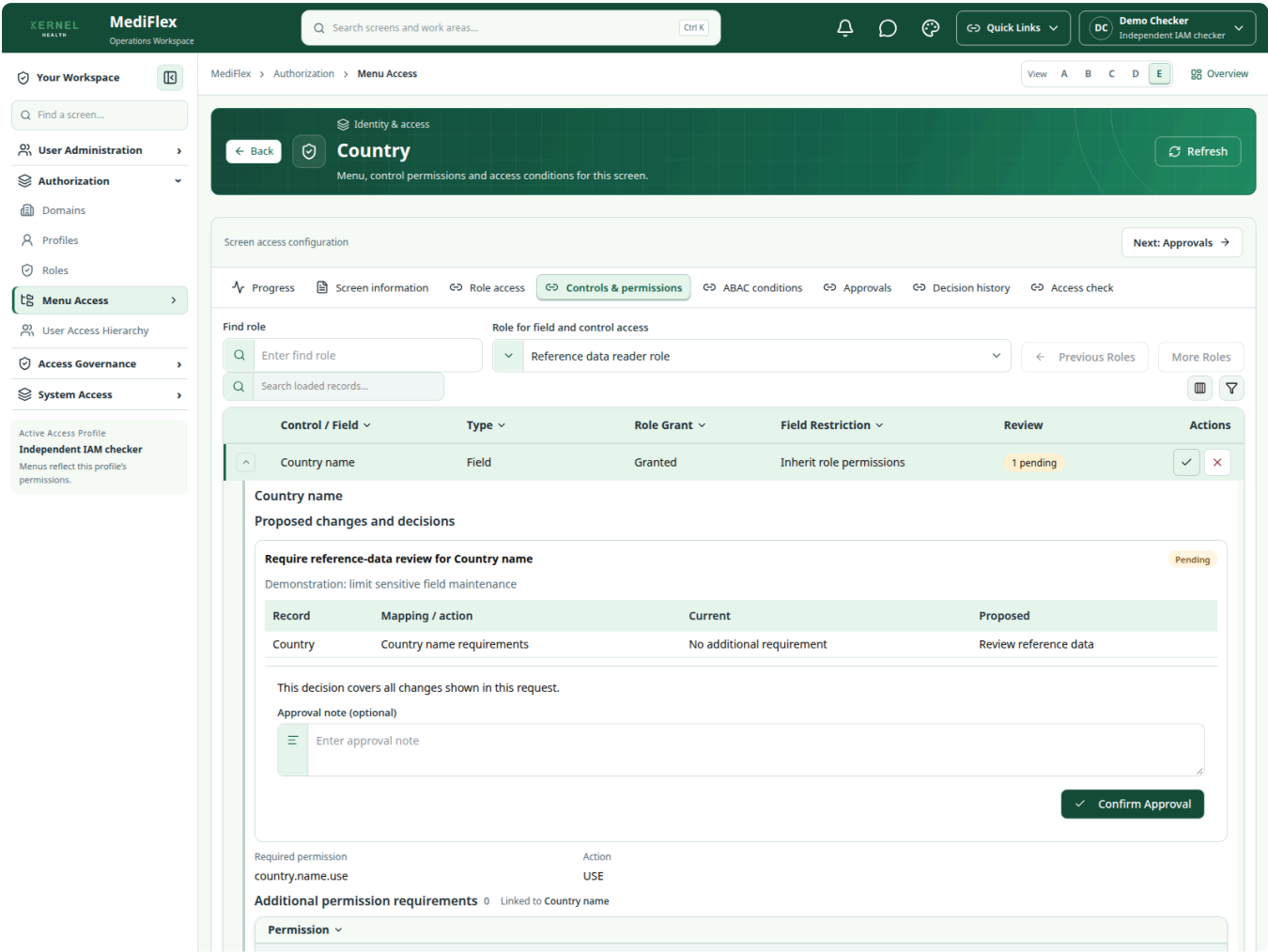
- Choose a role and registered field.
- The saved proposal requires an eligible decision before becoming effective.

Kernel · User guide

71 / 100

Independent review on the originating control row

Application screen with illustrative data · click to enlarge



- The reviewer sees the specific control change and before/after values.
- Confirm approval applies to the whole displayed proposal, not unrelated configuration.

Expected result

The approved control requirement, role grant and field rule can each be explained and verified independently. They reference Axis controls through IAM-owned security bindings.

Configure and verify ABAC conditions

Task context	Details
Screen / entry	Menu Access → Screens & controls → Country → ABAC conditions

Task context	Details
Who acts	Maker → Checker → Business user

Who: Maker → Checker → Business user

Open: Menu Access → Screens & controls → Country → ABAC conditions

1. Use a prepared isolated demo screen/policy, so the condition does not unexpectedly affect other users of a shared screen.
2. Select **Add policy**. Enter Policy name: Country access in Operations domain.
3. Choose the intended Applies to target. Select **Require all conditions** for this example.
4. Choose the offered attribute **Selected domain**, operator **is**, value **Operations**. Use the actual offered values, not typed claims about the user.
5. Keep the policy enabled, provide the reason and submit. Have the independent Checker review the before/after condition and approve.
6. Select the Business user's valid Operations / Reference data reader context. Run the access check and perform the authorized read.
7. For a genuine ABAC-negative walkthrough, use a second approved context that has the same required RBAC read grants but fails this condition. If that comparison context is not prepared, explain the negative case rather than pretending a missing-role denial proves ABAC.

SCREEN 40

ABAC conditions alongside inherited policies

Application screen with illustrative data · click to enlarge

Kernel

MediFlex

Operations Workspace

Search screens and work areas...

Ctrl K

🔔

💬

🔄

Quick Links

DM Demo Maker
IAM demonstration maker

Your Workspace

Find a screen...

User Administration

Authorization

Domains

Profiles

Roles

Menu Access

User Access Hierarchy

Access Governance

System Access

Active Access Profile:
IAM demonstration maker
Menus reflect this profile's permissions.

MediFlex

Authorization

Menu Access

View

A

B

C

D

E

Overview

Identity & access

Country

Menu, control permissions and access conditions for this screen.

Refresh

Screen access configuration

Next: Roles and controls

Progress

Screen information

Role access

Controls & permissions

ABAC conditions

Approvals

Decision history

Access check

Use conditions based on the selected profile, domain, sign-in assurance and other server attributes.

Search loaded records...

Add Policy

Policy

Applies To

Rule

Conditions

Review

Actions

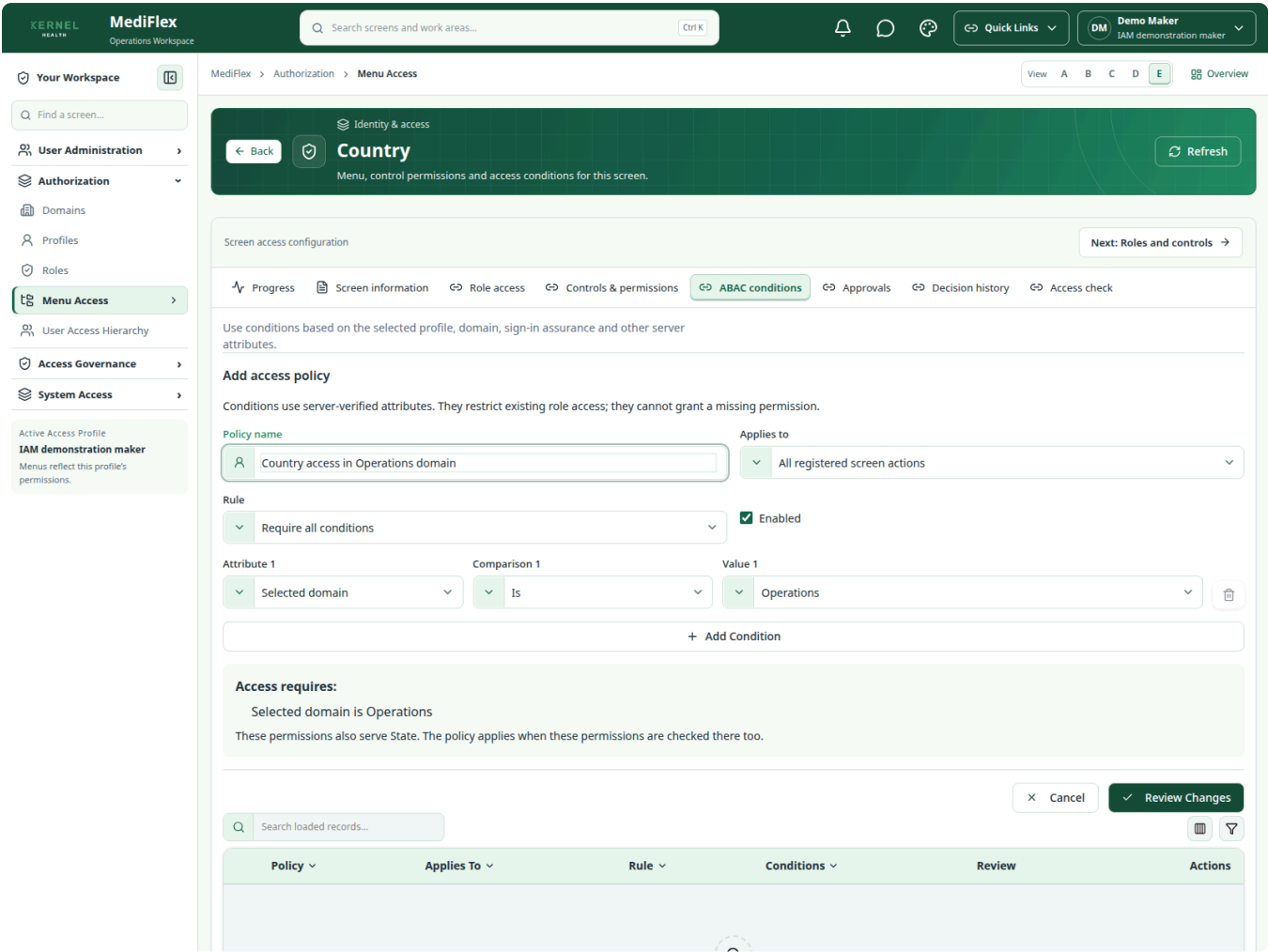
No records found

Applicable platform policies (0)

- Policies supplement the effective role/permission result.
- Inspect inherited/baseline conditions as well as the edited screen policy.

Define a condition using registered runtime attributes

Application screen with illustrative data · click to enlarge



- Require all conditions means the configured requirements must match.
- Deny when matched has a different meaning and should not be selected for this example.

Expected result

RBAC grants the intended operation and ABAC permits it only in the matching trusted context. A matching condition cannot create a missing role grant.

The role selector in the administration workspace inspects configuration. It does not impersonate a business user. Access check evaluates the signed-in selected context; use the actual user’s session for the final runtime proof.

Field security: hidden, read-only, editable and masked

User: IAM Maker → Checker → Reader/Editor

Open: Screen Access → Controls & permissions → control menu → Edit field access

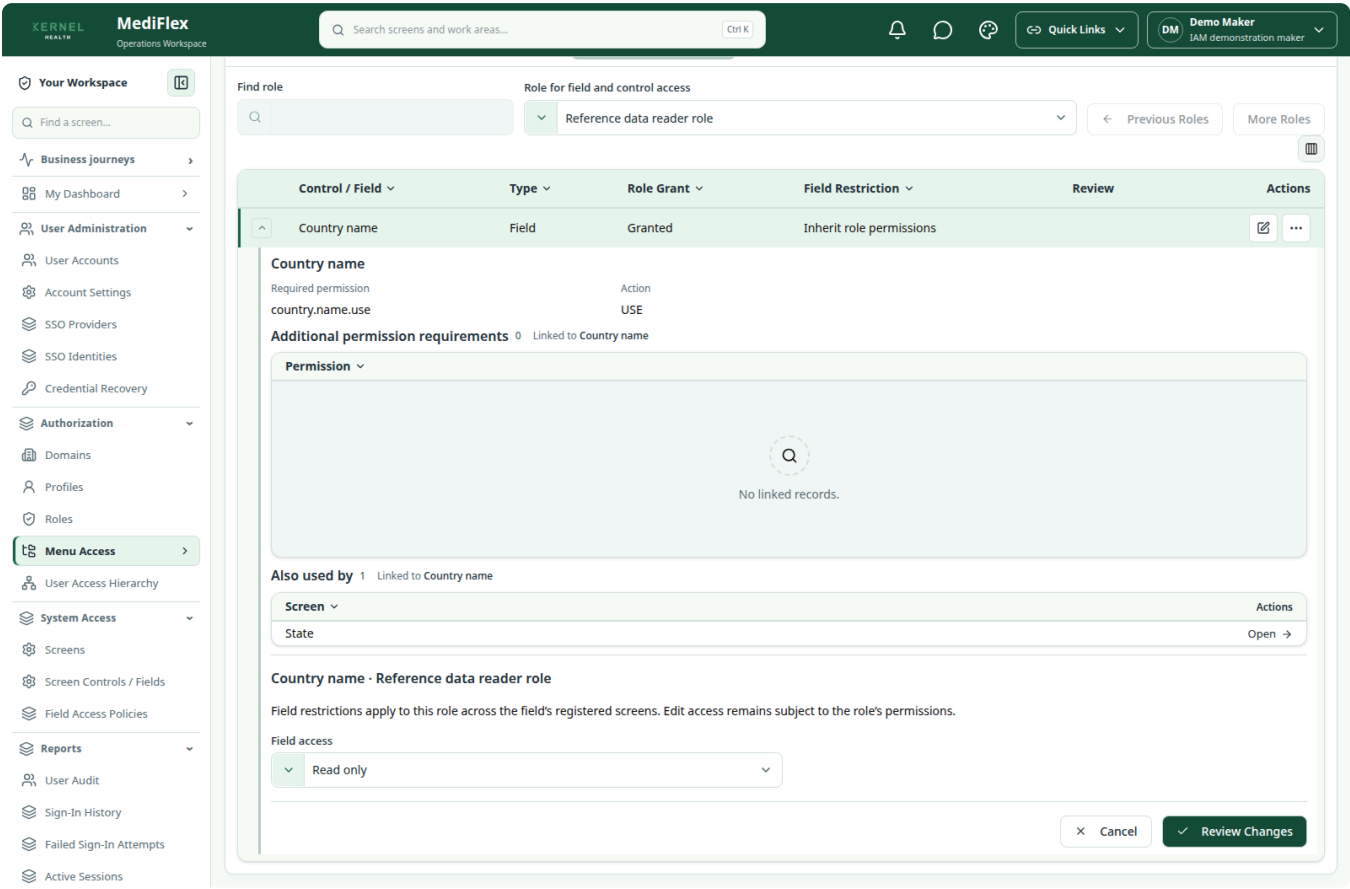
Verify: Verify controlled rendering and data protection for a specific registered field.

1. Choose a synthetic field with a registered IAM binding. For masking, use a field explicitly marked maskable and an available masking policy.
2. Select the role being configured. Open **Edit field access** from the control's row menu.
3. Choose the supported rule, inspect the affected control and any shared impact, then submit the proposal.
4. The checker reviews the affected row, including before/after rule, and approves or rejects.
5. Re-open the screen in the affected business-user session. Show the intended hidden, read-only, inherited or masked behavior.
6. For data exposure, inspect the authorized server response during recorded test. A masked display alone does not prove the raw value is absent from the response.
7. Verify an unauthorized write remains denied even if a user changes the browser DOM or constructs a request.

SCREEN 42

Configure a read-only field restriction

Application screen with illustrative data · click to enlarge



- The selected role and field identify the scope of this proposal.
- Read only narrows editing capability; independent review and server enforcement remain required.

Code	UI meaning	Walkthrough
N	No access	The governed field is not exposed to that context.
R	Read only	The user can inspect the permitted value but cannot modify it.
E	Edit within role permissions	Editing remains subject to the underlying write permission.
F	Use role permissions	Use the role/action decision without an extra field restriction.
M	Masked	Display only the permitted masked representation for a supported maskable field.

Expected result

Field policy narrows the effective capability; it does not create a missing write grant. Verify both presentation and the backend data/operation boundary.

CHAPTER 36

Review changes on the originating IAM record

1. Open the screen that owns the change: Domains, Profiles, Roles, Permission Catalog, Menu Access or User Accounts.
2. Locate its pending proposal or Changes & Approvals action. Newly proposed records may appear as pending rows before an effective record exists.
3. Inspect requester, beneficiary, scope, current/proposed values, reason and revision. Review relationship additions and removals individually.
4. With an eligible reviewer identity select Approve or Reject on that record and supply the decision reason. If stale, reload the current revision.
5. Refresh the same record; verify effective values and audit history. A rejected proposal must leave the prior state effective.

Switching an ordinary Maker to Checker profile in the same account does not establish independence. The explicitly assigned Kernel Super Administrator profile can use its recorded administrator exception where supported; inspect the authority and audit evidence.

CHAPTER 37

Administer client approval rules

Task context	Details
Screen / entry	Administer client approval rules
Who acts	Authorized administrator / reviewer

Open Access Governance → Client Approval Rules. The screen shows Workflow, Approval Flow, Version and Managed By. These settings govern eligible initial onboarding submissions; they are not a global switch to bypass later access review.

1. Inspect the current workflow row and effective version before planning the walkthrough.
2. For an authorized configuration change, open the row and choose Checker Required or Automatic Approval. Supply a Policy Code when the form requests a new policy.
3. Select Submit Policy. Read the notice: the policy change itself is submitted for independent approval and the current setting remains effective until that decision.
4. Have a different eligible reviewer inspect the policy proposal. Refresh the rule after the confirmed decision.

5. Use a new, explicitly prepared onboarding submission to verify the effective setting. Inspect the specific proposal's policy/receipt; do not infer that old pending requests changed automatically.
6. Use Submit Retirement only when retirement is the intended configuration change and its downstream behavior has been reviewed.

Expected result

The operator can explain which onboarding rule applies, which policy version is effective and why later access changes still require their own checks.

CHAPTER 38

Verify dynamic navigation and RBAC/ABAC

Task context	Details
Screen / entry	Select Operations / Reference data reader → prepared Country screen
Who acts	Business user in a separate browser profile

Who: Business user in a separate browser profile

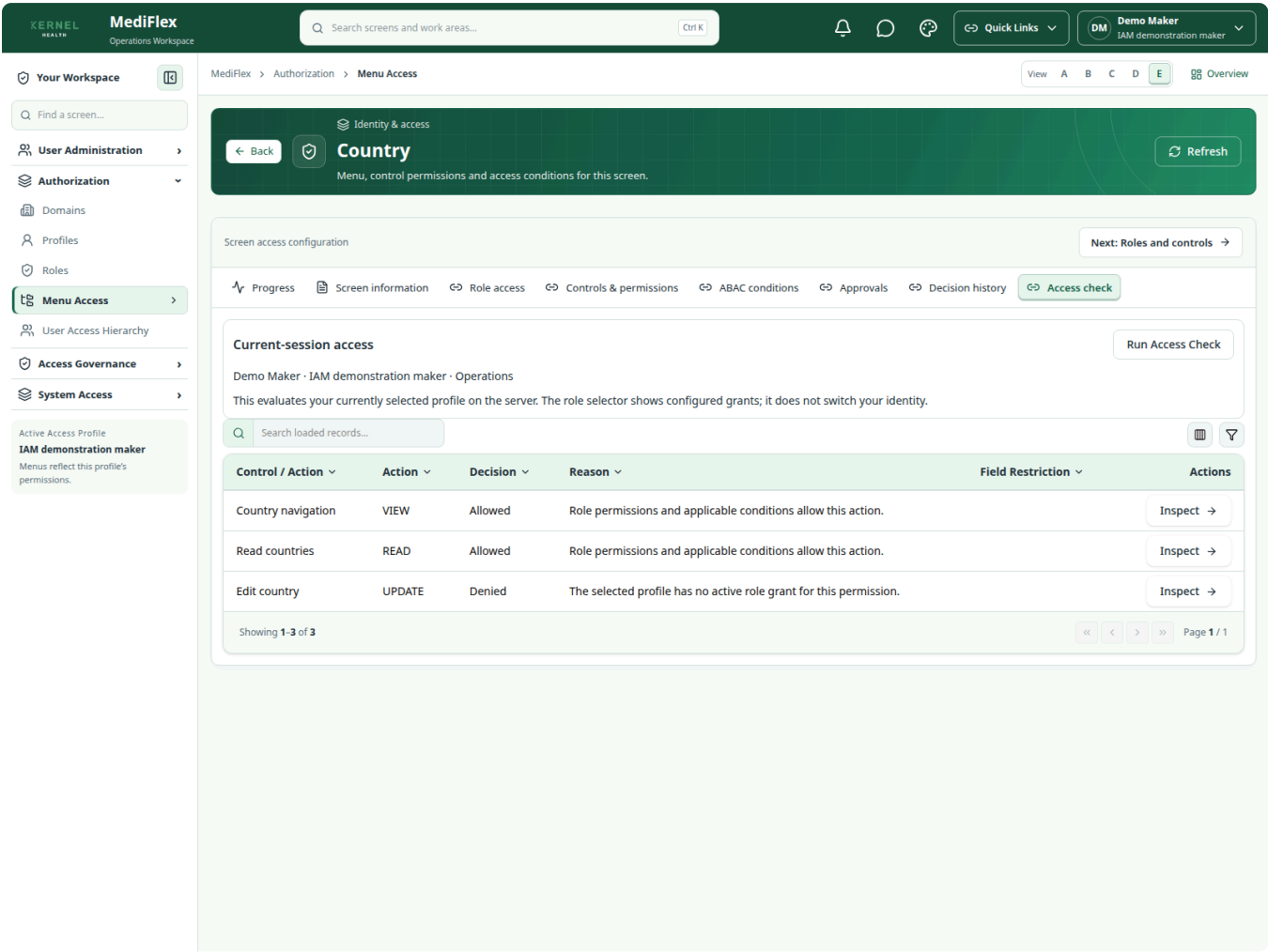
Open: Select Operations / Reference data reader → prepared Country screen

1. Show the header's selected domain/profile and the visible menus. Confirm these belong to the Business user's actual session.
2. Open Country. Read a known non-sensitive reference record and compare the result with the expected reader permissions.
3. Show that Create/Edit/Delete or approval actions are unavailable when not granted. Where a controlled authorization diagnostic is prepared, also show the server-side deny result. Do not replay a real destructive command for walkthrough.
4. Open the screen-access Access check under the same signed-in context if the user is authorized to use that diagnostic; otherwise have an authorized tester collect the equivalent runtime evidence.
5. Use the prepared ABAC comparison context and show the condition failure while required RBAC grants remain present.
6. Switch back to the intended permitted context and verify the allowed read again.
7. If using revocation, make and approve a separate removal proposal, refresh/renew context as required and verify the revoked operation is denied.

SCREEN 43

Access-check illustration: read allowed, write denied

Application screen with illustrative data · click to enlarge

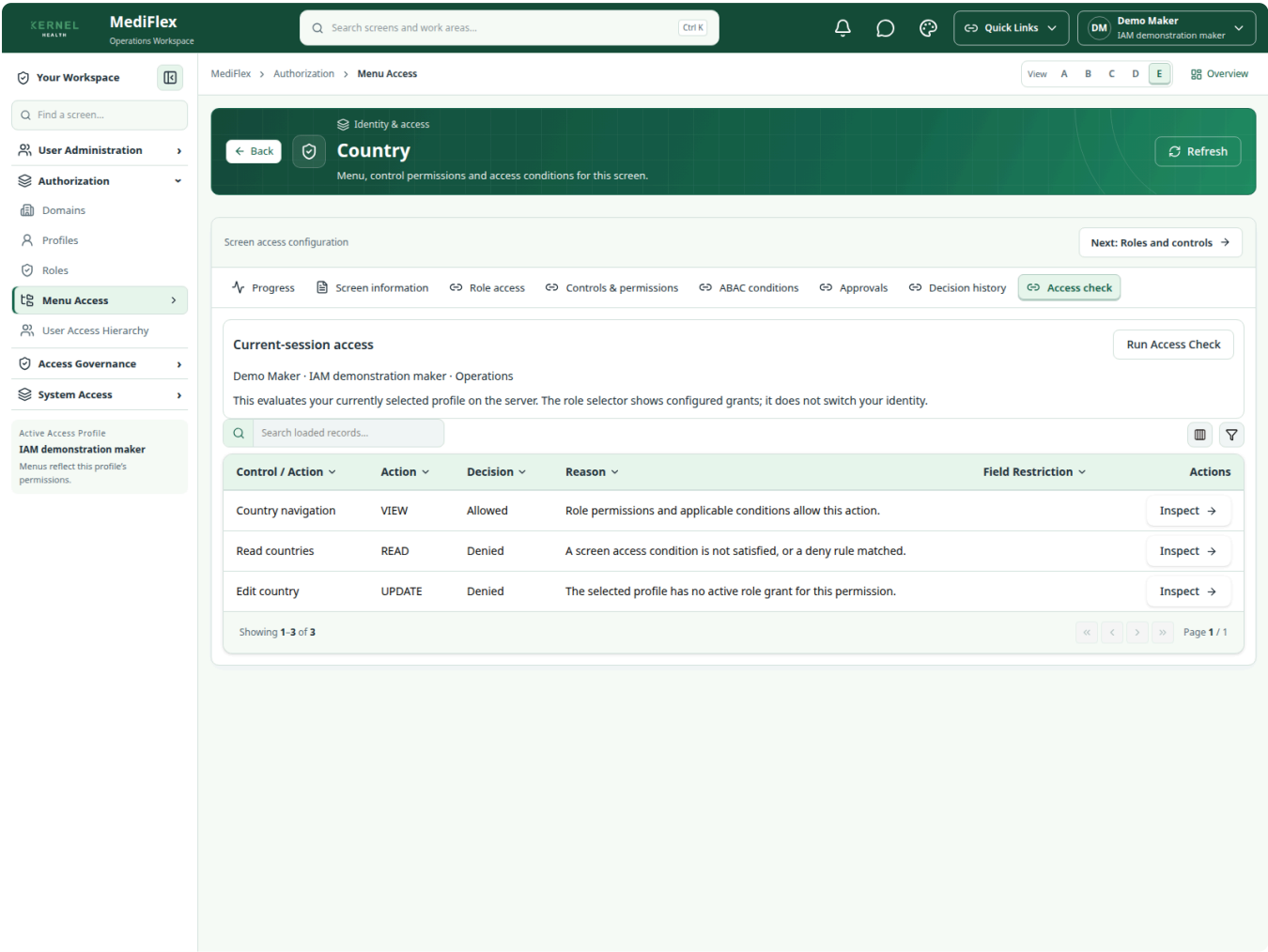


- This screenshot uses isolated example decisions.
- During the live demo, capture the actual user/context and current server result.

SCREEN 44

Access-check illustration: contextual condition denies the action

Application screen with illustrative data · click to enlarge



- A policy deny must be distinguished from missing permissions or an expired session.
- Keep the same intended operation and a valid comparison context for a meaningful test.

Check	Expected evidence
Dynamic menu	Menu shown or absent under the selected effective profile
Allowed read	Actual authorized response and visible record
Denied write	Action absent/disabled plus a controlled backend denial where verified
ABAC mismatch	Current trusted context fails the intended condition
Field restriction	Correct presentation plus enforced data/operation restriction
Revoked access	After the effective removal, the former capability is denied

Expected result

The demo proves the end-to-end chain instead of stopping at saved configuration or visible navigation.

CHAPTER 39

Control menu availability windows

Task context	Details
Screen / entry	the record, enter edit mode when authorized and set Enabled plus the intended start/end values
Who acts	Authorized operator / eligible independent reviewer as specified below

Open Advanced Configuration → Menu Schedules. This controls the availability of a registered menu. It is separate from the Enterprise Scheduler that executes business jobs.

1. Find the prepared demo menu and inspect its availability: Always Available, Disabled, Scheduled, Available or Ended.
2. Open the record, enter edit mode when authorized and set Enabled plus the intended start/end values. Use a non-critical walkthrough menu.
3. Review the exact change and submit the proposal with a reason. Complete the independent review from its record or the eligible queue.
4. Recheck the row after the decision. Under the affected user context, verify the menu and protected screen behavior inside/outside the approved window.
5. Restore the intended window through the permitted workflow after the walkthrough.

Expected result

Availability constrains an otherwise authorized menu. Making a menu available does not grant a missing permission.

CHAPTER 40

Maintain governed record details and inactive records

Open Advanced Configuration → Record Details when the specific metadata-backed administration task requires it. Continue to use Domains, Profiles and Roles as the normal master entry points.

1. Choose the offered entity and locate the exact record. Inspect its current version, availability and values.
2. Enter edit mode only if your selected profile is permitted. Change only the intended editable fields; preserve identifiers and linked records.

3. Review the before/after values, add a Business Reason and submit. An independently decided proposal applies the permitted change.
4. Refresh and inspect the result. A changed availability flag is only one part of effective access; status, validity dates, assignments, grants and policies still matter.

Use the record's offered deactivate, retire, revoke or lifecycle operation for that business purpose. Do not substitute direct database deletion or assume every screen exposes an identical `is_active` control. Historical decisions must remain traceable. Restoring a master does not automatically reinstate a revoked assignment.

CHAPTER 41

Configure and verify federated sign-in

Task context	Details
Screen / entry	Configure and verify federated sign-in
Who acts	Authorized administrator / reviewer

Use User Administration → SSO Providers and SSO Identities with a prepared non-production walkthrough identity or an approved existing provider.

Provider / identity field	What the administrator supplies
Provider Code / Provider Name	A unique reference and recognizable provider name.
Issuer URL	The configured identity provider's exact issuer.
Application Client ID	The registered application identifier.
Secret Reference	The configured secret reference, not a secret pasted into demo notes.
Identity Claim	The supported claim offered by the provider configuration.
SSO Provider + User Account	The provider and intended internal identity to link.
External Subject or Entra Object ID	The verified provider-issued stable subject expected by the configured claim; an arbitrary email address is not a replacement.

1. Verify the provider-side application, callback configuration and secret reference with the identity administrator before configuring sign-in.
2. Create or inspect the provider from SSO Providers. Submit any changes through the offered governed action; obtain the required independent decision.
3. From SSO Identities, propose the provider-to-account link using the verified external subject. Review the exact account and subject before approval.

4. In the business user's separate browser, select the enabled provider on Sign in and authenticate at that provider.
5. After return, select the permitted internal domain/profile. Verify its menus and a protected read operation.
6. For a lifecycle walkthrough, inspect the offered disable-provider or revoke-identity action and its scope. Do not disable the only working operator login during this task.

Expected result

The provider establishes identity; the internal account, membership, effective profile assignment and IAM policies still determine access.

The UI has provider creation, identity linking and governed disable/revoke operations. This guide does not assume that a particular provider is already configured, or that a disabled provider has a one-click re-enable action on every screen. Review its current configuration and available action before starting.

CHAPTER 42

Delegate access for a bounded period

Task context	Details
Screen / entry	Delegate access for a bounded period
Who acts	Authorized administrator / reviewer

Open Access Governance → Delegations.

1. Select Delegate Access when authorized. Choose the eligible Source assignment, Recipient user and Delegation ends time.
2. Check that the source responsibility and recipient are appropriate. Add a Business Reason and submit.
3. A different eligible reviewer inspects the source, recipient, dates and effect, then decides the proposal.
4. Inspect the resulting delegation and verify the recipient's effective context through the normal sign-in/access checks.
5. Use End Delegation when the temporary duty ends, complete required review and verify the former delegated access is no longer usable.

Expected result

The delegation remains bound to its source, permitted scope and expiry. It is not a permanent copy of an administrator's privileges.

Apply separation of duties and timed exceptions

Task context	Details
Screen / entry	Separation of Duties and define the intended domain and conflicting role pair through Separate Duties
Who acts	Authorized operator / eligible independent reviewer as specified below

1. Open Separation of Duties and define the intended domain and conflicting role pair through Separate Duties. Record the policy code and reason, submit and obtain the independent decision.
2. Use the normal access-request flow on a prepared example account to check that the conflicting combination is rejected. Preserve its denial reference.
3. If an approved business exception is needed, open Timed Exceptions and request the exact policy/user pairing with an explicit end and reason. Obtain the required review.
4. Verify only the scoped approved exception, then revoke it or verify its expiry. Confirm that the ordinary conflict restriction applies again.

Task	Operating steps
Define a conflict	Separation of Duties → Separate Duties. Supply Policy code, Domain, First role, Conflicting role and reason. Submit and complete the independent decision.
Verify enforcement	Use a prepared test account and conflicting assignment through the normal access workflow. Record the actual conflict/deny response and leave current permitted access intact.
Request an exception	Timed Exceptions → Request Timed Exception. Select the exact Policy and User Account, set Exception ends, explain the need and submit for the required review.
Verify an approved exception	Check its scope and dates, then rehearse the intended operation under that user's actual context. Other grants and policy checks still apply.
End the exception or policy	Use Revoke Timed Exception or Retire Duties Policy only for the intended record, with the required reason and decision. Confirm the resulting effective restriction.

Use an isolated prepared business conflict. An exception does not disable all duty controls, and changing profiles does not make a maker independent from their own proposal.

Expected result: The defined conflicting role combination is denied unless the exact reviewed, unexpired exception applies. Ending the exception restores the ordinary restriction.

CHAPTER 44

Run an access-review campaign

Task context	Details
Screen / entry	Access Review and supply Campaign code, Campaign name, Domain, Assigned reviewer and Review due, plus the Business Reason.
Who acts	Authorized operator / eligible independent reviewer as specified below

Use Access Governance → Access Reviews for campaigns and My Review Items for the assigned reviewer's work.

1. Open Access Review and supply Campaign code, Campaign name, Domain, Assigned reviewer and Review due, plus the Business Reason.
2. Submit the campaign action and follow its governance receipt. Inspect the resulting campaign and assigned review items.
3. As the assigned authorized reviewer, open My Review Items. Inspect the user, assignment, domain/profile and current need for access.
4. For an item that remains justified, choose Retain Reviewed Access with the reason. For an item that should end, choose Remove Reviewed Access and follow the required decision/application flow.
5. Refresh the item and verify the effective result. A submitted removal proposal alone does not establish that access ended.
6. Return to the campaign, resolve outstanding items and use Close Access Review when offered. Retain the evidence of each decision.

Expected result

The campaign has identifiable reviewed items and outcomes. Creation of a campaign is not completion of the review.

CHAPTER 45

Use just-in-time and emergency access

Task context	Details
Screen / entry	Use just-in-time and emergency access

Task context	Details
Who acts	Authorized administrator / reviewer

1. Verify sensitive actions, then open Access Governance → Privileged Access. Choose either Just-In-Time with independent approval or Emergency with existing pre-approved eligibility.
2. Select the eligible permission and permitted duration, record the business reason and submit the chosen request.
3. For JIT, obtain a different eligible reviewer's decision and use Activate when permitted. For Emergency, follow the state and action returned for the approved eligibility.
4. Perform only the authorized operation and inspect Recorded Activity. Revoke or verify expiry, then complete eligible post-use review and closure.

Open Access Governance → Privileged Access. These operations require the appropriate permissions and current trusted step-up where indicated. Verify only an eligible permission prepared for the session.

Stage	Just-in-time path	Emergency path
Prepare	Use Verify sensitive actions; confirm an eligible permission exists in the selected profile.	An authorized administrator first governs Emergency Eligibility for the user, assigned profile, permission, eligibility end and maximum duration.
Request	Request temporary access → Just-In-Time · Independent Approval. Choose Permission, duration and Business Reason.	Request temporary access → Emergency · Pre-Approved Eligibility. Choose eligible Permission, matching approved eligibility, Emergency category, duration and reason.
Decision and activation	A different eligible reviewer approves; the owner then uses Activate. Both protected transitions recheck required assurance.	Follow the returned state and offered action under the pre-approved eligibility. Do not treat Emergency as unrestricted access.
Use and monitor	Perform the permitted walkthrough operation and inspect Recorded Activity.	Inspect the same activity/expiry evidence within the emergency grant's limits.
End	Use Revoke Now, or verify expiry. Cancel a not-yet-active request when appropriate.	Revoke/expire the temporary grant; separately revoke eligibility if its future use should end.
Review and close	Eligible reviewer uses Review Usage after the grant ends, records findings and then Close Request when offered.	The same post-use review and closure controls remain important.

The inspected form caps a JIT request at 30 minutes and an emergency request at 15 minutes; server eligibility/policy can further constrain duration. Requested, Approved and Active are distinct states. The activity panel shows the latest 50 decisions, not the entire audit store.

Expected result

The permission is usable only for its authorized context and bounded lifetime, with accountable approval or pre-approved emergency eligibility and post-use evidence.

CHAPTER 46

Investigate sign-ins, failures and sessions

Task context	Details
Screen / entry	a row for details
Who acts	Authorized operator / eligible independent reviewer as specified below

Screen	Use
Sign-In History	Inspect authentication outcomes and stages for the relevant user/time range.
Failed Sign-In Attempts	Investigate failed attempts within authorized scope; a deliberate demo failure must use a prepared test account.
Active Sessions	Inspect unexpired, unrevoked sessions and their last selected domain/profile/activity.
Session History	Inspect session lifecycle and ended-session evidence.
Security Dashboard	Open the reviewed/published security dashboard configuration if available to this profile; its configuration availability is separate from raw report permissions.

1. Choose the report, search the walkthrough User ID and submit Search.
2. Use both start/end dates, or leave both blank for the default last-seven-day range. The inspected report validates ranges of up to 90 days.
3. Inspect status, authentication stage or session domain/profile, and the report's Updated time. Active means unexpired/unrevoked; it does not prove the person is presently at the keyboard.
4. Use Refresh for an immediate reload. The offered auto-refresh interval is five minutes while the page is visible.
5. Open a row for details. Export Data on these security-report screens exports the currently loaded page, which is up to 50 records. Do not call that export the complete audit history.
6. Compare the actual session result after sign-out, suspension or revocation when those are verified.

Expected result

The authorized user can distinguish authentication success, effective authorization, current session validity and historical evidence.

CHAPTER 47

Trace creation, approval and first use

Task context	Details
Screen / entry	Alex Demo → Audit details; Approvals; Access hierarchy; sign-in reports
Who acts	Authorized administrator / auditor

Who: Authorized administrator / auditor

Open: Alex Demo → Audit details; Approvals; Access hierarchy; sign-in reports

Evidence	Where to verify it	What to explain
Account identity and source	User Accounts and Account information	User ID, Admin-created source, account status and effective dates.
Person/contact information	Personal information	The linked person and contact details used during onboarding; ownership is distinct from permission grants.
Creation / update metadata	Account → Audit details	Creation/update information available for the record. Do not describe these fields as an exhaustive event ledger.
Access decision	Account → Approvals and originating access row	Requester, exact proposed values, decision, reviewer and reason; pending versus applied.
Effective access chain	Account → Access hierarchy	Assigned domain/profile and inherited role/permission chain.
Credential enrollment / delivery	Account → Sign-in setup	Enrollment and invitation/delivery status; avoid displaying tokens.
Authentication results	Reports → Sign-In History / Failed Sign-In Attempts	Successful sign-in and any deliberate failed attempt within the approved demo scope.
Session lifecycle	Reports → Active Sessions / Session History	Current session and, when exercised, its end/revocation.

1. Record the User ID, assignment/proposal reference, tenant/domain/profile, decision timestamp and reviewer for this example evidence.
2. Filter the available reports to the demo account and the meeting time range. Show only the evidence needed for this user.
3. Compare the effective access now with the originally requested assignment. Verify the intended expiry.
4. If a report or audit event is unavailable, record that gap explicitly. Do not claim that a record's Created On field proves every authentication or authorization event.

Expected result

The authorized user can trace who created the account, who proposed and approved the business access, whether enrollment completed and which sign-in/session evidence is actually available.

CHAPTER 48

Open notifications and review their current outcome

1. Open the notification bell using the account that received the item. Read its subject, current stage and offered action.
2. Select View outcome or the offered work-item action. If an email link requires sign-in, finish sign-in and select the profile responsible for the item.
3. Verify that the application opens the originating screen and the corresponding record or pending change, for example Profiles → the requested profile change. Inspect the current outcome; an old message can refer to work that has since completed.
4. Approve or reject only from the current owning record if your selected profile is eligible. Opening a notification does not decide the work item.
5. Use Mark as read separately. If Notification unavailable appears, select Try Again after verifying the account/context; use Switch Profile or Open Notifications as appropriate. If it persists, retain the notification reference and correlation identifier for support.

CHAPTER 49

Troubleshooting administration and access

Symptom	Check in this order
Master or Create button missing	Selected profile/context → screen permission → action permission → protected scope restrictions
A newly created item is absent from a lookup	Creation receipt → pending decision → approved effective state → refreshed lookup and compatible scope
Profile cannot link to domain	Current eligibility, access-scope compatibility, protected records and effective dates

Symptom	Check in this order
Role has a permission but screen is denied	Exact registered key/action → other required dependencies → menu/screen availability → ABAC → selected assignment
New permission does not affect the screen	Definition vs role grant vs published menu/control binding; check the exact key
Menu appears but page/API denies	Navigation grant is only one layer; verify page/control/data-operation requirements
Checker sees no approval action	Different identity, pending state, eligible scope, action permission, version and assurance
Mapping approval says stale	Reload the exact request/revision and re-check its current before/after values
Axis mapping approved but UI unchanged	Approval-for-publication vs actual publication, source hash, profile/locale target and refreshed presentation
Screen inventory has no Create Screen/Field	The inspected pages are inventories; use platform definition/publication for new definitions
ABAC test seems inconsistent	Actual signed-in context vs inspected role, inherited policies, missing grants, expiry or inactive records
DB_EXEC_ERROR	Record correlation ID, time and operation; confirm whether a proposal receipt exists before retrying
Selected profile cannot read this screen	Trace assignment → profile → roles → permissions/menu → published Axis screen and applicable policy; do not bypass the denial
User has profile but cannot select it	Account/membership status, assignment state/dates, profile selectability and current context choices

CHAPTER 50

Resolve registration, enrollment and sign-in problems

Symptom	Check / next action
Registration not in the main User Accounts list	Use User Accounts → Registration Requests. A request is not necessarily an effective account yet. Check email verification and classification stage.
Awaiting checker approval but only View is available	Confirm a pending proposal, different reviewer identity, selected profile, scope, decision permission and current request version. Open the proposal from its record or queue.
Active account cannot sign in	Check credential enrollment and required factor, tenant membership, effective profile assignment, validity, account state and selected realm/provider.

Symptom	Check / next action
No invitation after creation	Creation alone is insufficient. Check activation, approved eligible access and Sign-in setup delivery state. Request enrollment email only when offered and eligible.
Provider accepted email, user did not receive it	Check the intended address and latest message kind, then mail delivery/inbox filtering. Provider acceptance is not a receipt/read guarantee.
Invalid/expired link or verification code	Use the latest message and supported resend path. Do not reconstruct a private token URL or repeatedly create new requests.
Login/register form has been open a long time	Reload/reopen the public form to obtain a fresh session/form context, then submit once. Preserve the displayed reference if a previous submission may already exist.
DB_EXEC_ERROR or intermittent loading	Record operation, selected tenant/domain/profile, time and correlation ID. Determine whether a proposal was created before retry. Do not diagnose a database failure as missing permission without evidence.
SSO authenticates but internal access fails	Check enabled provider, verified external-subject link, internal account/membership and effective assignments. Provider authentication does not create internal role grants.

For support, record the screen URL with private tokens removed, time, non-secret record/proposal reference, chosen profile and exact error/correlation ID. Do not include passwords, OTPs, cookies, session storage or invitation/recovery tokens.

CHAPTER 51

Understand the states before moving to the next step

Object	State / indicator	What to do next
Registration	Awaiting email verification	Applicant verifies ownership using the latest mail.
Registration	Awaiting maker classification	Authorized maker chooses the eligible domain/profile.
Registration / access proposal	Awaiting checker approval / Pending	Different eligible reviewer inspects and decides. Existing access stays as stated by the workflow.
Registration	Awaiting activation	Applicant completes the invitation-led setup.
Admin-created account	Pending	Authorized administrator activates it and completes separate access setup.

Object	State / indicator	What to do next
Account	Active	Check approved effective assignment and credential readiness; active alone is insufficient.
Assignment	Pending / approved / expired / revoked	Use the actual state and dates. Only a currently effective permitted assignment should be selectable.
Configuration proposal	Rejected / cancelled	Requested changes do not become effective. Correct and submit a new intentional proposal if needed.
Axis change	Approved for publication / published	Confirm actual publication and target version before expecting rendering to change.
Privileged grant	Requested → Approved → Active → ended → reviewed/closed	Complete each offered eligible transition; approval is not activation.
Mail delivery	Queued / provider accepted / failed	Inspect delivery evidence and use the appropriate retry/resend process. Provider accepted is not user enrollment completed.

Labels vary with the entity and configured workflow. Use the current record's receipt, dates and available actions rather than applying one generic status sequence to every object.

CHAPTER 52

Table linkage and architectural reference

Use this appendix for technical questions after the business walkthrough. It identifies the principal implemented names; it is not a direct SQL maintenance procedure or a complete schema inventory.

Concept	Implemented table(s)	Boundary
Account identity	kh_iam.digital_subject kh_iam.user_account	IAM
Tenant membership	kh_iam.tenant_membership	IAM
Domain	kh_iam.resp_scope	IAM
Profile	kh_iam.access_profile	IAM
Domain ↔ Profile	kh_iam.access_profile_scope	IAM
Role / Profile ↔ Role	kh_iam.role kh_iam.access_profile_role	IAM

Concept	Implemented table(s)	Boundary
Permission / Role ↔ Permission	kh_iam.permission kh_iam.role_permission_grant	IAM
Registered operation	kh_iam.resource_action	IAM
User ↔ Profile in domain context	kh_iam.access_profile_asgn kh_iam.membership_scope_binding	IAM
Selected context	kh_iam.session kh_iam.session_access_profile_context	IAM
Menu master	kh_iam.menu	IAM
Permission ↔ Menu	kh_iam.menu_permission	IAM
Menu ↔ Axis Screen	kh_iam.menu_axis_screen	IAM-owned bridge
Menu availability window	kh_iam.menu_schedule	IAM
Screen / published version	kh_axis.page_def kh_axis.page_version	Axis
Screen → Controls / Fields	kh_axis.screen_control_registry	Axis
Permission ↔ Control	kh_iam.permission_axis_control	IAM-owned bridge
Field restrictions	kh_iam.field_access_rule	IAM
ABAC rules	kh_iam.policy_rule	IAM
Proposal and decision	kh_iam.access_request kh_iam.access_request_item kh_iam.access_approval_decision	IAM
Initial-access approval rule	kh_iam.client_approval_rule	IAM
Personal/business profile	Application/Core person and contact data; separate application-user-profile linkage migration	Application boundary; not access_profile

The Role and menu access screen is an administration projection over governed grants. The inspected native menu path uses role_permission_grant and menu_permission. This guide does not assert that a separate authoritative role_menu table is present. Other Axis draft/publication records and legacy metadata tables are outside this principal-table summary.

Personal/KYC boundary migration and legacy cleanup are separate from this access-configuration demo. Their presence in the target architecture is not a claim that all legacy personal-data handling has already moved.

CHAPTER 53

Complete IAM screen directory and entry points

All 32 native IAM entries in the inspected catalog are accounted for below, plus the registration subview and three related Axis entry points. Some entries are panels under a parent workspace rather than separate sidebar items. The selected profile, mapping, scope and policy determine what appears. An entry in this directory is not an entitlement.

Area / screen	Purpose / entry note
User Administration User Accounts	Create/manage accounts and open Registration Requests.
User Administration Domain Access	Account Domain access panel; canonical entry is User Accounts. Workspace owner: users
Authorization Access Assignments	Inspect/propose user profile assignments from account/hierarchy workspaces. Workspace owner: hierarchy
User Administration Account Settings	Govern account type and authentication realm.
User Administration SSO Providers	Inspect/propose configured identity providers.
User Administration SSO Identities	Link/revoke external subjects to internal accounts.
User Administration Credential Recovery	Govern native credential recovery after identity verification.
Authorization Domains	Domain master and profile eligibility mappings.
Authorization Profiles	Profile master, domain eligibility and role bundle.
Authorization Roles	Role master, permission grants and related access mappings.
Authorization Menu Access	Role/menu actions, menu requirements and screen-access inspection.
Authorization User Access Hierarchy	Trace user → domain/profile → roles/permissions.
System Access Field Access Policies	Screen/control permission requirements and field restrictions.
Reports User Audit	Authorized account/audit inspection.
Reports Sign-In History	Authentication outcomes.

Area / screen	Purpose / entry note
Reports Failed Sign-In Attempts	Failed authentication evidence.
Reports Active Sessions	Current unexpired/unrevoked session evidence.
Reports Session History	Session history.
Access Governance Client Approval Rules	Govern initial-onboarding approval policies.
Access Governance Security Dashboard	Configured security summary/report entry.
Access Governance originating screen's Changes & Approvals	Eligible pending/decided proposals, including not-yet-effective master creation.
Access Governance Delegations	Source-assignment-bound temporary delegation.
Access Governance Separation of Duties	Conflicting-role policies.
Access Governance Timed Exceptions	Time-limited exceptions to a named conflict policy.
Access Governance Access Reviews	Access-review campaigns.
Access Governance My Review Items	Reviewer work items and retain/remove decisions.
Access Governance Privileged Access	Temporary privilege requests, activation, activity and review.
Access Governance Emergency Eligibility	Pre-approved emergency eligibility.
Advanced Configuration Permission Catalog	Permission definitions and menu mappings.
Advanced Configuration Record Details	Governed metadata-backed record changes.
Advanced Configuration Domain and Profile Mappings	Domain/Profile eligibility mapping entry.
Advanced Configuration Menu Schedules	Registered-menu availability windows; not business-job scheduling.
User Administration Registration Requests	Verify/classify/decide end-user requests; canonical entry within User Accounts. Workspace owner: users

Area / screen	Purpose / entry note
Axis / System Access Screens	Registered screen inventory and existing-screen mapping actions.
Axis / System Access Screen Controls / Fields	Registered control inventory.
Axis / System Access Screen Mapping Drafts	Versioned ownership mapping proposals for existing screens.

Use live grid actions for record-specific URLs. Do not copy illustrative IDs from screenshots into production links. Source/configuration routes can be permission-controlled even when their related master menu is visible.

CHAPTER 54

Worked case · Build and diagnose the complete account-to-screen authorization chain

Use existing master screens and approved, narrowly scoped demo access. Prepare a maker and a different checker identity, an intended domain/profile and a non-sensitive walkthrough screen. Record the existing grant chain before adding mappings. Do not use one account with two profiles as evidence of independent approval.

Worked example: proposed training values, not pre-created live records. Follow the current permitted actions and owner validation. Earlier screenshots are retained illustrations; this edition does not claim a new production run.

Field / choice	Example or selection	How to decide / validation
Domain	The actual domain selected for the walkthrough	This is not interchangeable with the tenant or a verified DNS hostname.
Profile	The intended access profile	An access profile groups roles/context. It is not the user's personal KYC profile.
Role	A job function with explicit permissions	Keep maker, checker and read responsibilities distinguishable; broad profile names do not prove grants.
Permission	Registered permission identity for read/action/control	Use the permission catalog and exact supported action. A label does not create a functional permission.
Menu	A navigation entry connected to the intended Axis screen	Its approved IAM bridge supplies the screen target. Parent navigation/group visibility is not a data grant.

Field / choice	Example or selection	How to decide / validation
Screen / control	An Axis screen identity and stable field/control identity	Labels, formats and layouts belong to Axis. Permission-to-control associations belong to IAM.
Mapping validity / active state	The applicable current interval and active relationship	A master can be active while a relationship is inactive, unapproved or not yet effective.

Confirm the account and selected context

Open User Accounts and inspect the target account, lifecycle and profile assignments. Select the intended domain/profile through the account menu. Reopen the current context and note the selected profile.

Verify before continuing: The profile must be assigned and eligible now. Account activation does not create missing mappings.

Trace domain/profile and profile/role

Open Domains and Profiles, use their contextual mapping/assignment actions and inspect the existing relationships. Select the exact target records through controlled lookups. Submit any required change as a proposal, then inspect it from the originating record.

Verify before continuing: Record the approved relationship and effective interval. Do not overwrite the profile master simply to change one role association.

Trace role/permission and permission/menu

Open Roles and Permission Catalog. Compare the role's effective permissions with the Menu Access linkage. Where the implementation requires an additional role/menu relationship, inspect that constraint too.

Verify before continuing: A role label matching "Maker" is not evidence of create permission. Confirm the exact catalog identities.

Trace IAM-to-Axis bridges

Inspect the menu-to-screen bridge and the permission-to-control relationships for the selected Axis screen. Check a visible read field, an editable field and a submit/review action.

Verify before continuing: The screen owns presentation and its controls; IAM owns their authorization bridges. A label change must not alter permission identity.

Perform positive and negative checks

Using the maker, open the screen and propose a disposable change. With a reader, inspect allowed data and confirm that the mutation is unavailable/denied. With the different checker, inspect the pending row and eligible review action.

Verify before continuing: Retain actual request/decision references. Denials should preserve business data and give a usable reason or correlation reference.

Prove origin-row review and history

Decide the exact submitted revision with the independent checker. Reopen the originating record and inspect applied values, pending state and audit. If the source changed after submission, reconcile and resubmit through the supported flow.

Verify before continuing: A review page visit is not a decision. Successful approval should be supported by the decision receipt and resulting record readback.

CHAPTER 55

New domains start with no linked profiles

Approval creates the domain definition with an empty profile mapping. Creating a domain must not link legacy or default profiles. Open Domains → the domain → Mappings: Linked profiles should be zero until an explicit mapping is approved.

1. Select Edit Mappings and choose only the intended profile(s). Enter the business reason and submit.
2. Inspect the pending additions/removals on the same domain record. A pending mapping does not make a profile eligible.
3. An eligible reviewer approves or rejects the mapping. Refresh both By Domain and By Profile to verify the same exact links.
4. Assign the user to the approved domain/profile combination separately. An approved domain-profile relationship does not create a user assignment.

If unexpected profiles appear immediately after creation, retain the domain and request references and report the mapping defect; do not treat automatic access as a configured default.

CHAPTER 56

Use the named Kernel Super Administrator exception

Select Kernel Super Administrator from the profile selector only when assigned to your account and domain. The exception permits the named administrator to review their own changes in supported governed flows. It is recorded as an administrator review; ordinary Maker/Checker profiles retain their independence

restrictions.

Still checked	What to verify
Account and selected assignment	The account, session, tenant and selected profile must be current and effective.
Scope and permission	A powerful profile does not activate a parked module or enable disabled APIs.
Revision and business validation	Review the exact current revision, required preview receipts and valid state. Stale decisions remain blocked.
Audit evidence	Retain the request, decision, administrator authority and resulting version.
Return to normal duties	Select the ordinary functional profile when the exceptional activity is complete.