BridgeLink Advanced Access Control + MFA Plugin: User Guide

For BridgeLink WebAdmin

Table of Contents

About This Guide

The Advanced Access Control plugin (internal name **Role-Based Access Control**, or RBAC) lets a BridgeLink administrator define named roles with a permission level for every feature area, assign those roles to users, and optionally restrict a role to a specific set of channels. The same plugin also adds Multi-Factor Authentication (MFA), which requires a one-time code from an authenticator app at login. This guide is for BridgeLink administrators who configure roles, assign roles and MFA to users, restrict channel access by role, and troubleshoot access problems. By the end of this guide you will be able to create and manage roles, scope a role to specific channels, assign roles and MFA to users, and resolve the most common access issues.

Requirements

- BridgeLink 26.6.0 or later
- A BridgeLink server with the Advanced Access Control plugin (internal name **Role-Based Access Control**) installed and enabled
- A valid license for **Role-Based Access Control**, installed on the **License Manager** tab under **Settings** (see Installation and Activation)
- For Multi-Factor Authentication: each user who will use MFA needs a TOTP-based authenticator app, such as Google Authenticator or Authy

Key Concepts

Roles

A role is a named permission profile. Each role specifies a permission level for every feature area in BridgeLink, plus an optional Channel Scope. Create as many roles as your organization needs, such as `Administrator`, `Support`, or `Interface Engineer`.

Permission Levels

Most feature areas support three permission levels:

- **No Permission**: the feature is hidden entirely. It does not appear in the sidebar or in Settings.
- **View**: read-only access. The user can see the feature and its data but cannot make changes.
- **Editor**: full access. The user can view the feature and create, edit, and delete within it.

Dashboard and **Lookup Manager** only offer **View** and **Editor**; they cannot be hidden with **No Permission**.

Channel Scope

Channel Scope controls which channels a role's users can see and act on, separately from the **Channels** permission level. Every role defaults to **All channels**. Setting Channel Scope to **Selected only** restricts the role to a chosen set of channel groups and individual channels. See Channel Scope for the full procedure.

User Assignment

Each BridgeLink user can be assigned one role. Users with no role assigned (**No Role**) retain full access to every feature; this keeps existing users working the same way after you install the plugin.

Installation and Activation

1. Sign in to **WebAdmin** as an administrator.
2. Click **Extensions** in the sidebar.
3. Confirm **Role-Based Access Control** appears in the extension list and is enabled. Enable it if it is not already enabled.
4. Click **Settings** in the sidebar, under the **Administration** group, then click the **License Manager** tab.
5. On the **Installed Licenses** sub-tab, click **Install License** and choose the Role-Based Access Control license file, a `.json` file supplied by Innovar Healthcare.
6. Review the **Install License** dialog, which previews the license's **Customer**, **Products**, **Issued**, **Expires**, and **Server match**, then click **Install**. A confirmation toast reads "License installed." Restart BridgeLink when prompted; a banner reads "License changes will take effect after restarting BridgeLink."
7. Click the **License Status** sub-tab and confirm the **Role-Based Access Control** row shows **Active** under **Status**.
8. Click the **Access Control** tab to open the plugin's settings.

Configuration

Accessing Access Control Settings

Click **Settings** in the sidebar, then click the **Access Control** tab across the top. The tab has two sub-tabs: **Role** and **User Configuration**.

Access to this tab is controlled by the **Access Control** row under the Settings sub-permissions (see Feature Areas and Permission Mapping): **No Permission** hides the tab entirely, **View** opens it read-only, and **Editor** grants full access to create, edit, and save roles and user assignments. Typically, only full administrators should have **Editor** here.

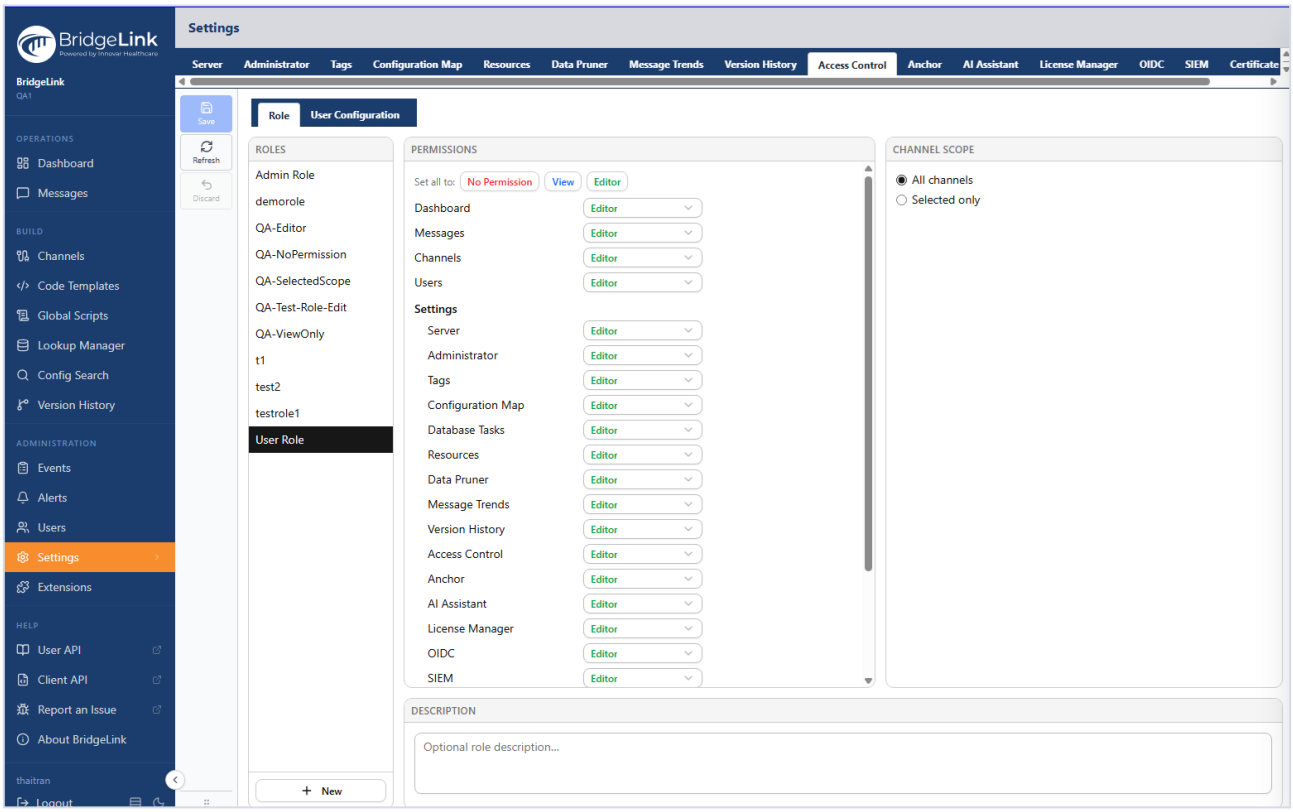

Figure 1: The Role tab, showing the Roles list, Permissions grid, Channel Scope panel, and Description field.

Creating a Role

1. On the **Role** tab, click **New** at the bottom of the Roles list.
2. In the **New Role** dialog, enter a name in **Role name** (for example, `Support` or `Read-Only Viewer`).

Figure 2: The New Role dialog.

3. Click **Create**.
4. The new role is added to the Roles list and selected automatically. Every permission defaults to **View**.
5. For each row in the Permissions panel, use the dropdown to choose **No Permission**, **View**, or **Editor**.
6. Optionally, click **No Permission**, **View**, or **Editor** under **Set all to:** to set every permission at once, then adjust individual rows as needed.
7. Under **Channel Scope**, leave **All channels** selected to give the role access to every channel, or choose **Selected only** to restrict it (see Channel Scope).
8. Optionally, enter notes in the **Description** field.
9. Click **Save** in the task panel on the left.

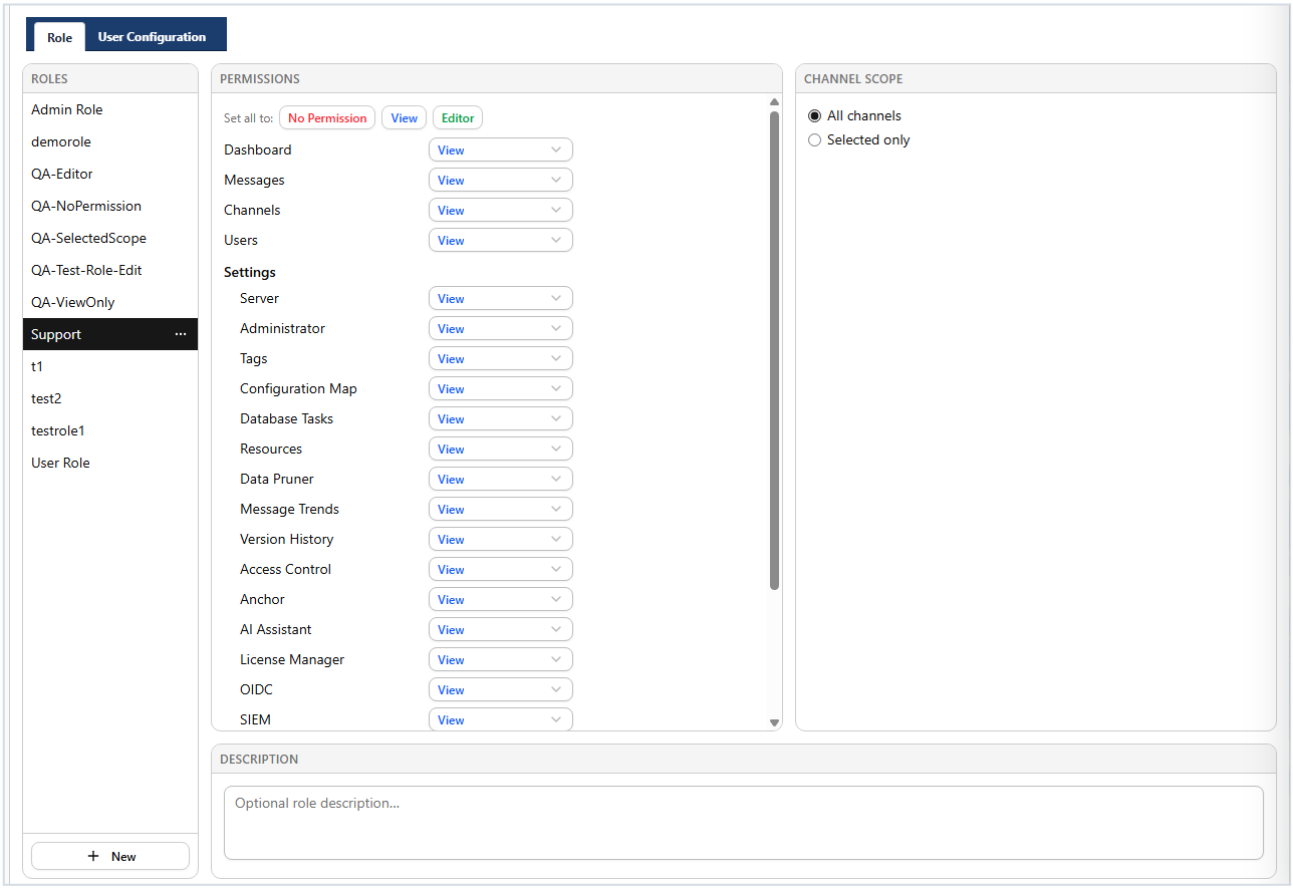

Figure 3: A configured role with every permission set to View.

Editing, Duplicating, and Deleting Roles

1. On the **Role** tab, hover over a role in the Roles list. A small options icon appears next to its name.
2. Click that icon to open the menu.

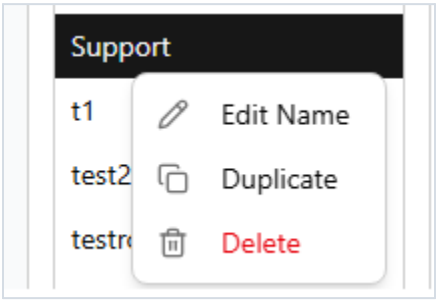

Figure 4: The options menu for a role, showing Edit Name, Duplicate, and Delete.

- **Edit Name**: renames the role. Enter the new name and click **Rename**. The role's permissions, Channel Scope, and user assignments are unchanged.
- **Duplicate**: copies the role, including all of its permissions and Channel Scope. Edit the prefilled name (`Copy of <role name>`) if needed and click **Duplicate**.

- **Delete**: removes the role. Users assigned to the deleted role revert to **No Role**, which grants full access to all features; reassign those users to another role promptly.

Creating, renaming, duplicating, and deleting a role, and any change to its permissions, Channel Scope, or description, is staged locally. Click **Save** in the task panel to write the changes to the server, or **Discard** to revert to the last saved state.

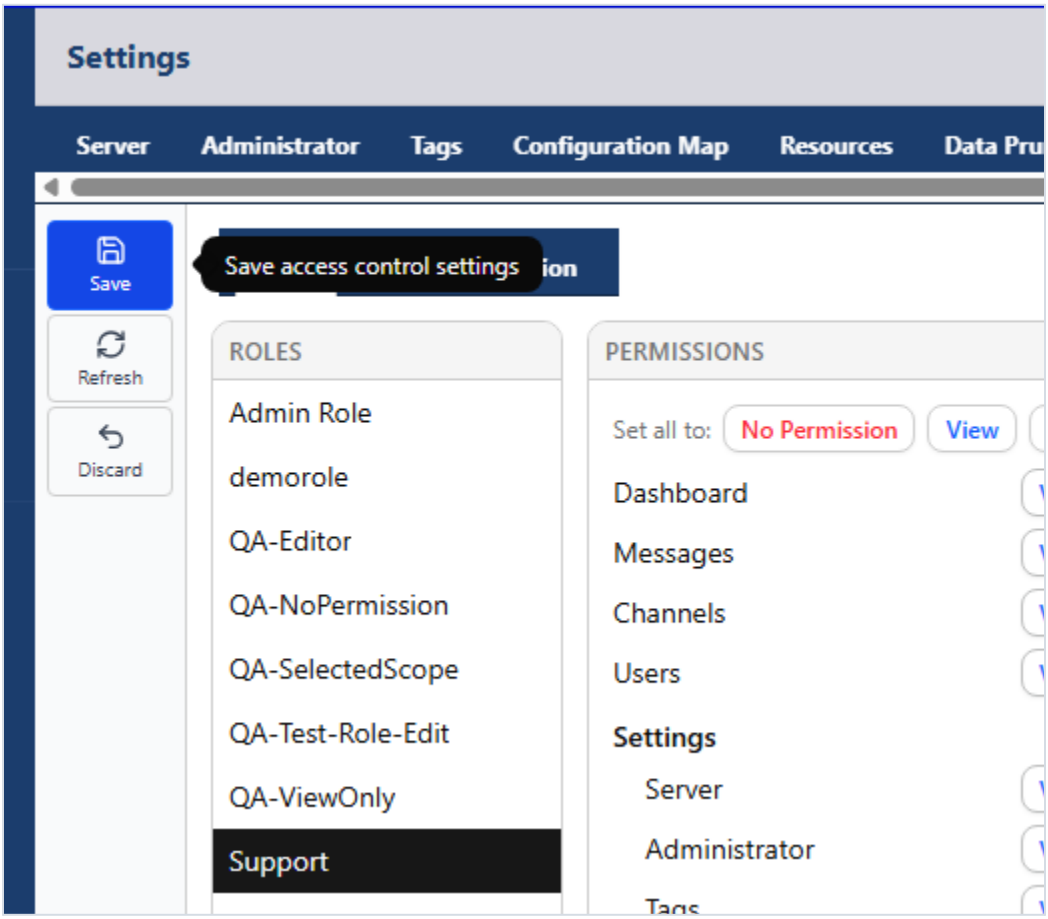

Figure 5: The task panel with Save, Refresh, and Discard.

Feature Areas and Permission Mapping

The following core features can be set independently for each role:

Feature	Permission levels available
Dashboard	View, Editor
Messages	No Permission, View, Editor
Channels	No Permission, View, Editor
Users	No Permission, View, Editor
Alerts	No Permission, View, Editor

Feature	Permission levels available
Events	No Permission, View, Editor
Extensions	No Permission, View, Editor
Lookup Manager	View, Editor

Users here is the core Users screen used to manage BridgeLink login accounts. It is separate from this plugin's own **User Configuration** tab, which assigns roles and MFA to those accounts (see Assigning Roles to Users).

Settings is expanded into one row per settings tab. The core rows are:

Settings sub-permission	Permission levels available
Server	No Permission, View, Editor
Administrator	No Permission, View, Editor
Tags	No Permission, View, Editor
Configuration Map	No Permission, View, Editor
Database Tasks	No Permission, View, Editor
Resources	No Permission, View, Editor

Additional rows appear for every other settings-panel plugin installed and enabled on the server, including this plugin's own **Access Control** row. On a server with the full BridgeLink commercial suite installed, this can also include **Data Pruner**, **Message Trends**, **Version History**, **Anchor**, **AI Assistant**, **License Manager**, **OIDC**, and **SIEM**. If every Settings row is set to **No Permission**, the **Settings** link itself is hidden from the sidebar.

Channel Scope

Channel Scope narrows a role to a specific set of channels, on top of whatever permission level the role grants on **Channels**. It is enforced by the BridgeLink server for channel-scoped actions generally, not only inside the Channels feature.

1. On the **Role** tab, select the role to scope.
2. In the **Channel Scope** panel, select **Selected only**.

Until you add at least one group or channel, the panel shows **Add at least one group or channel** and the role cannot be saved.

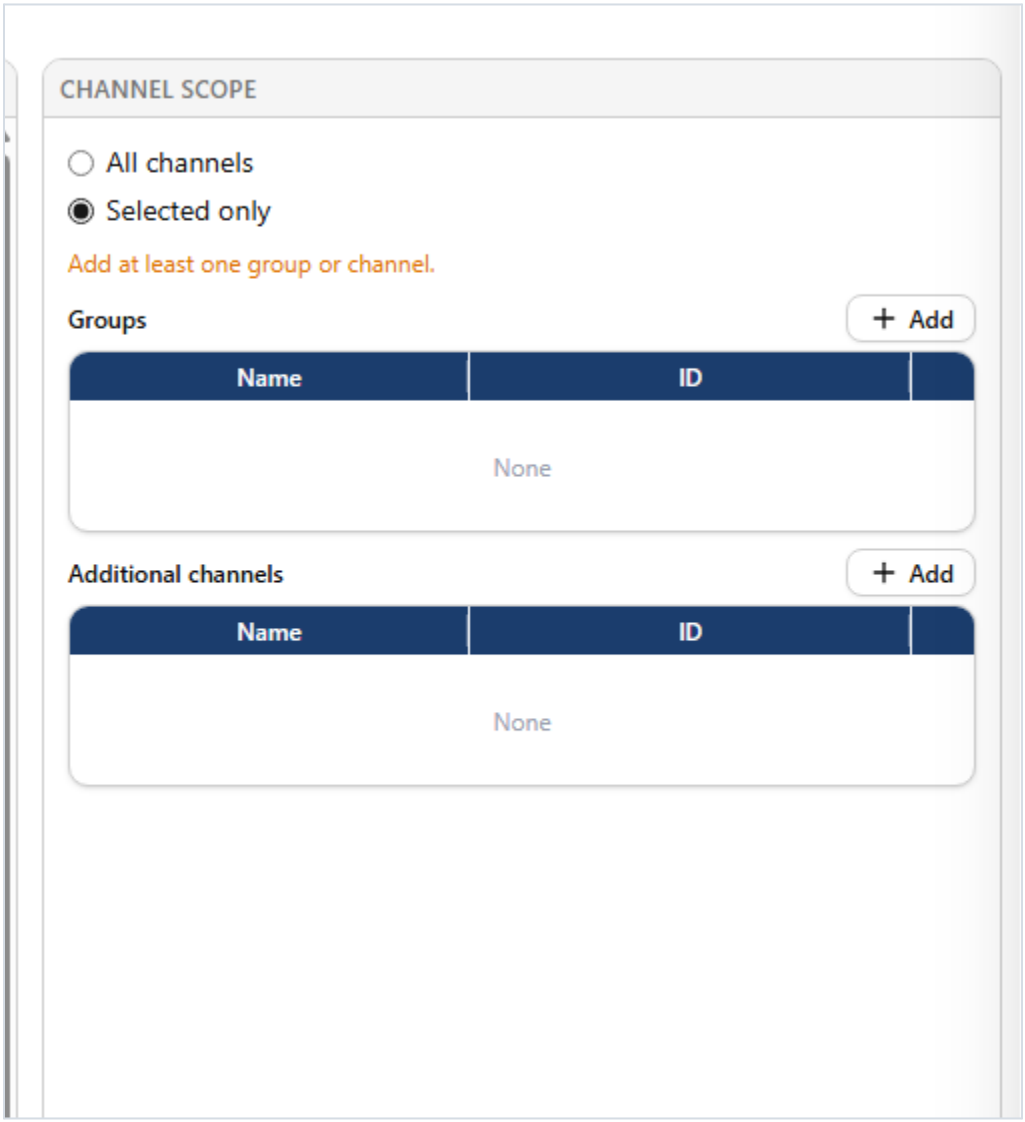

Figure 12: The Channel Scope panel with Selected only chosen and no groups or channels added yet.

3. Under **Groups**, click **Add** to open the **Add Channel Groups** dialog.
4. Check each channel group to include, or use **Search...** to find one.
5. Click **Add**.

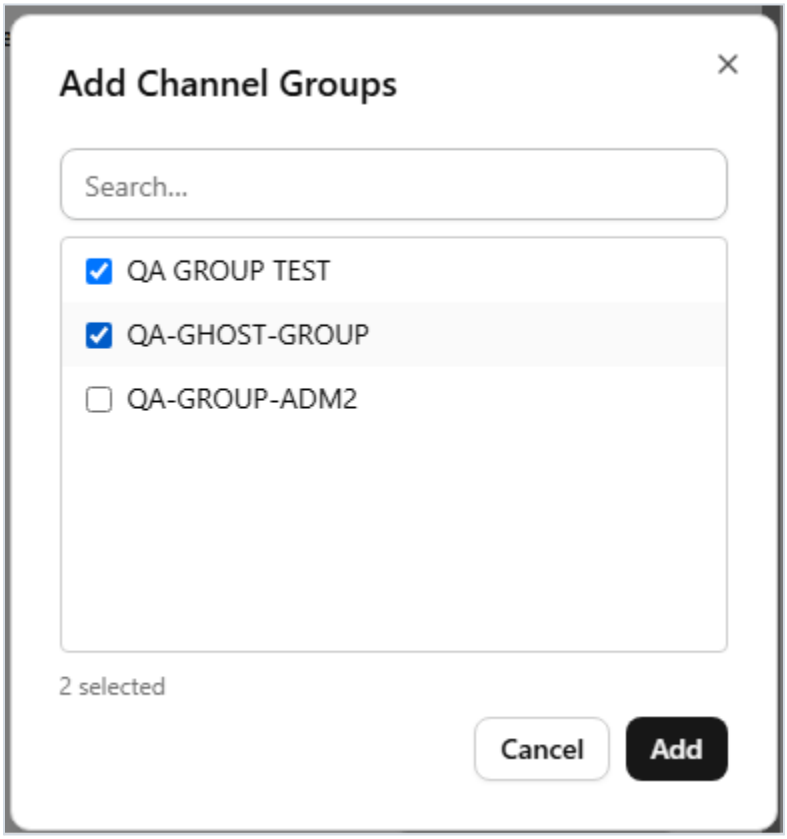

Figure 13: The Add Channel Groups dialog with two channel groups checked.

6. Under **Additional channels**, click **Add** to open the **Add Channels** dialog and add individual channels on top of (or instead of) whole groups.
7. Expand a channel group to see its channels (ungrouped channels are listed under **Default Group**), and check each channel to include.
8. Click **Add**.

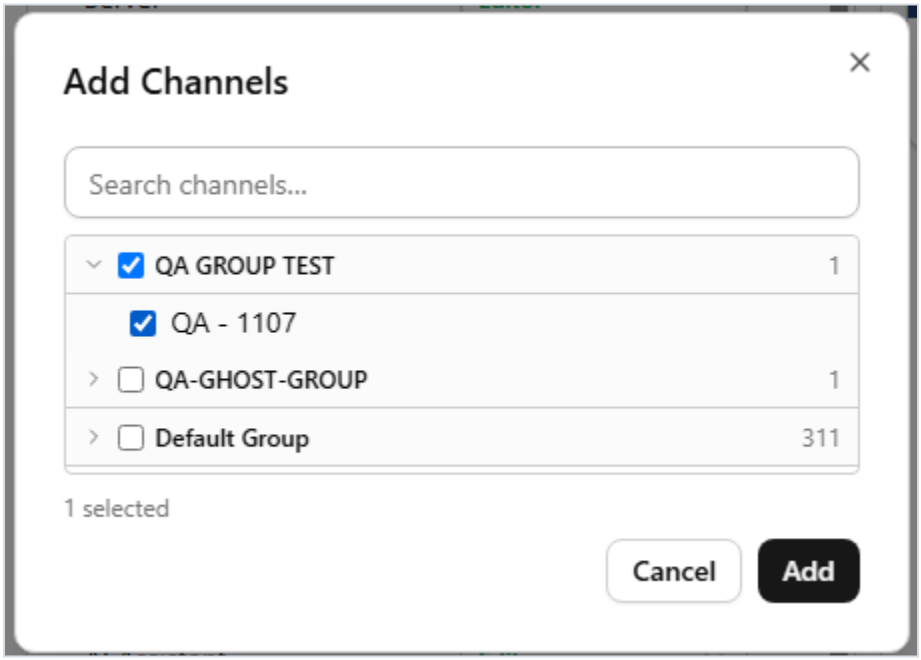

Figure 14: The Add Channels dialog, showing channel groups expanded into their individual channels.

9. Click **Save** in the task panel.

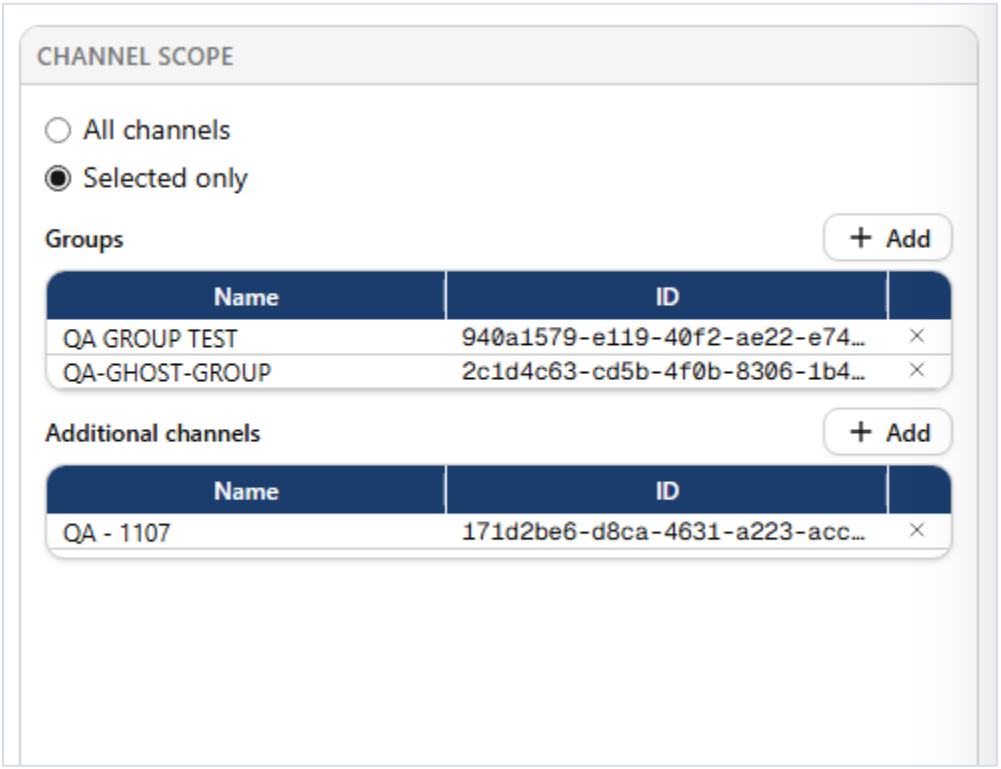

Figure 15: The Channel Scope panel with two channel groups under Groups and one channel under Additional channels.

The role's users can now only see and act on channels in the selected groups plus any individually added channels. Click the **x** next to a group or channel to remove it from the

scope. If a role's Channel Scope is **Selected only** with no groups or channels added, clicking **Save** shows an error naming that role, and none of your changes are saved until you fix it.

Assigning Roles to Users

1. Click the **User Configuration** tab.

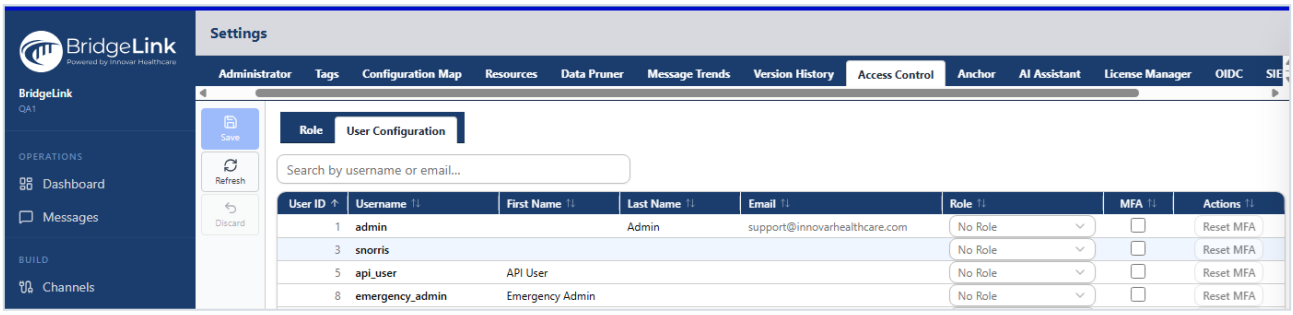

Figure 7: The User Configuration tab, listing users with their Role and MFA columns.

2. Use **Search by username or email...** to find a user, or scroll the list.
3. Click the **Role** dropdown next to a user and select the desired role, or **No Role**.
4. Click **Save** in the task panel.

The user's WebAdmin session reflects the new role's permissions the next time they log in or refresh their session. The table also includes **User ID**, **Username**, **First Name**, **Last Name**, and **Email** columns, and an **Actions** column with a **Reset MFA** button per user (see Resetting a User's MFA in Multi-Factor Authentication (MFA)). Rows for users with MFA enabled are highlighted.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication is part of the same plugin as Advanced Access Control. When MFA is enabled for a user, they must enter a one-time code from an authenticator app in addition to their username and password at login.

Enabling MFA for a User

1. Click **Settings**, click the **Access Control** tab, then click the **User Configuration** tab.
2. Locate the user and check the box in the **MFA** column for that user's row.

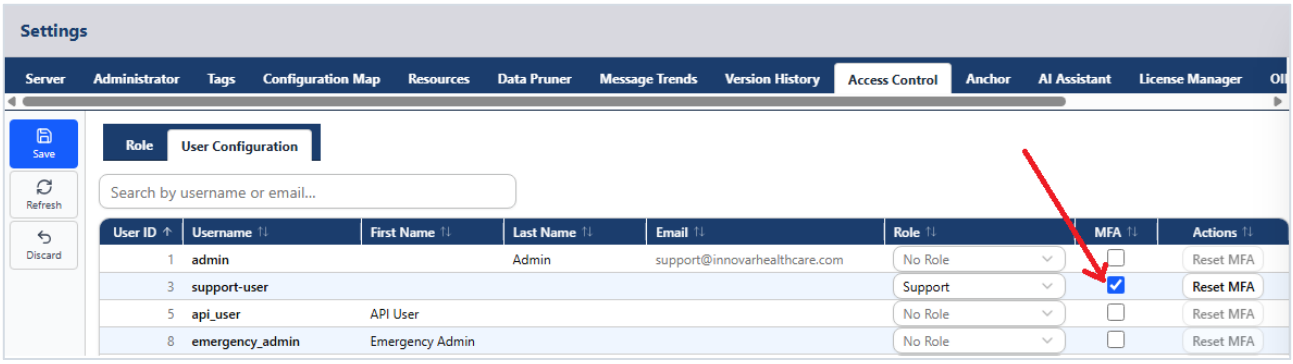

Figure 8: The MFA column checkbox checked for a user, with a Reset MFA button in the Actions column.

3. Click **Save** in the task panel.

The next time this user logs in, WebAdmin walks them through First-Time MFA Setup.

> **Enabling MFA affects REST API access for that account.** Enabling MFA enforces a second factor on interactive sign-ins. A script or integration that authenticates to the REST API with a single HTTP Basic Auth request (a username and password only) is rejected with `401 Unauthorized` once MFA is enabled, because Basic authentication has no way to supply the verification code. REST access remains possible when the calling code performs the full session-based login (submit credentials, receive the MFA challenge, submit the verification code) and then reuses the resulting session cookie. There is no API key or token that bypasses MFA, so do not enable MFA on an account used only for machine-to-machine Basic Auth calls.

First-Time MFA Setup

The first time a user with MFA enabled logs in, WebAdmin generates a new authenticator secret and shows it immediately, with no separate generate step.

1. On the WebAdmin login screen, enter your **Username** and **Password** and click **Login**.
2. On the **Set Up Two-Factor Authentication** screen, open your authenticator app and scan the QR code, or enter the key shown under **Or enter this key manually** into the app by hand.
3. In your authenticator app, note the current 6-digit code.

4. Enter that code in **Verification Code**.

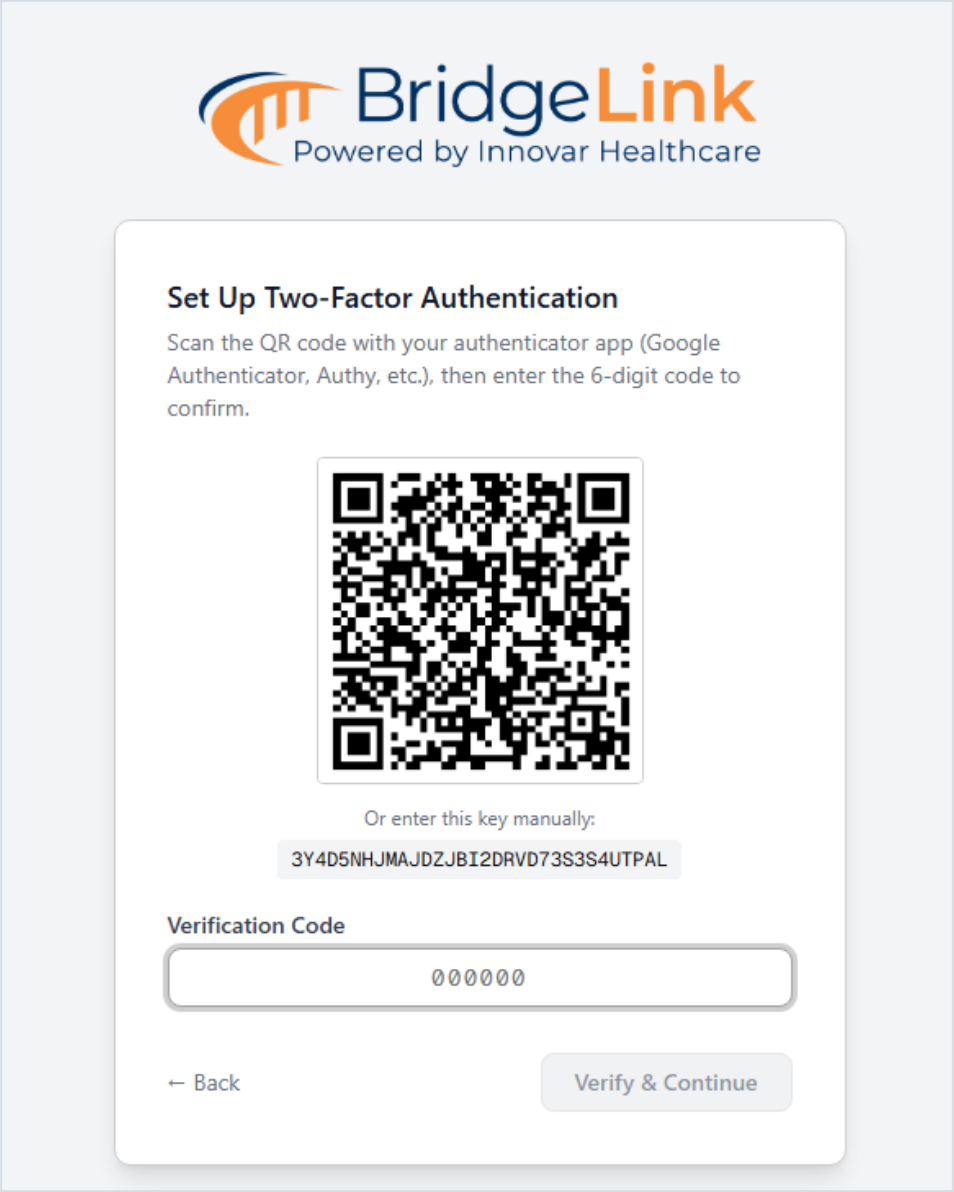

Figure 11: The Set Up Two-Factor Authentication screen, showing the QR code, manual key, and Verification Code field.

5. Click **Verify & Continue**.

After setup, WebAdmin prompts for a fresh 6-digit code from the authenticator app on every subsequent login (the **Two-Factor Authentication** screen, with an **Authentication Code** field and a **Verify** button).

Resetting a User's MFA

Use **Reset MFA** when a user loses their authenticator device, rather than unchecking and re-checking the **MFA** column.

1. Click **Settings**, click the **Access Control** tab, then click the **User Configuration** tab.

2. In the user's row, click **Reset MFA** in the **Actions** column. This button is only available for users with MFA enabled.
3. In the **Reset MFA?** dialog, click **Reset MFA** to confirm.

Resetting takes effect immediately; it does not require clicking **Save** in the task panel. The user's stored secret is cleared, MFA stays required for them, and they go through First-Time MFA Setup again with a new secret the next time they log in.

To turn MFA off for a user entirely, uncheck the **MFA** column instead and click **Save**.

How Permissions Are Enforced

Permissions are enforced at two levels:

- **UI level**: features set to **No Permission** are removed entirely from the sidebar and Settings tabs, not just hidden with styling
- **Server level**: the BridgeLink server also checks every API call against the role's permissions. Calling a REST API endpoint directly does not bypass a feature set to **No Permission** or **View**.

Channel Scope is enforced the same way: when a role's Channel Scope is **Selected only**, the server limits that user to the channels in the selected groups plus any individually added channels for channel-scoped operations. A role with **All channels** (the default) is unrestricted regardless of its **Channels** permission level.

Important Behaviors

Plugin Not Installed or Disabled

If Role-Based Access Control is not installed or is disabled, every feature remains fully visible and accessible to all users.

No Role Assigned

A user with **No Role** retains full access to every feature. The plugin does not restrict unassigned users.

Administrator Best Practice

Keep at least one user on a role with **Editor** on every feature, including the **Access Control** Settings sub-permission, so no one can lock everyone else out of this configuration screen by accident.

Bulk-Set Then Customize

When building a restrictive role, click **No Permission** under **Set all to:** first, then raise individual rows to **View** or **Editor** as needed.

Example Role Configuration

A `Support` role that can only view the Dashboard, Messages, and Lookup Manager, with access to every channel:

Feature	Permission Level
Dashboard	View
Messages	View
Channels	No Permission
Users	No Permission
All Settings sub-permissions	No Permission
Alerts	No Permission
Events	No Permission
Extensions	No Permission
Lookup Manager	View
Channel Scope	All channels

For a full Administrator role, set every feature to **Editor**. To also limit a role like `Support` to specific channels, set Channel Scope to **Selected only** and add the relevant channel groups or channels.

Troubleshooting

Symptom	Likely cause	What to do
A user can't see a feature they should have access to	The user's role grants less than **View** on that feature, or a role change has not taken effect yet	Confirm the user's role on the **User Configuration** tab and that it grants at least **View**. Have the user log out and back in.
A deleted role left users with full access	Expected behavior: deleting a role reverts its users to **No Role**	Reassign those users to an appropriate role as soon as possible.
The **Access Control** tab is not visible	The current user's role grants **No Permission** on the **Access Control** Settings sub-permission	Have an administrator with **Editor** on **Access Control** grant at least **View**.
All features are visible even though roles are configured	The plugin is not installed or is disabled	Confirm **Role-Based Access Control** is installed and enabled in **Extensions**.
A role with **Selected only** Channel Scope will not save	No groups or channels have been added to that role's scope	Add at least one group or channel under **Groups** or **Additional channels**, then click **Save**.
A user is locked out of MFA (lost device)	The user's authenticator app no longer matches the stored secret	Click **Reset MFA** for that user on the **User Configuration** tab; they will set up MFA again at their next login.

Support

Contact Innovar Healthcare support at `support@innovarhealthcare.com` for help beyond this guide. Include your BridgeLink version, the Role-Based Access Control plugin version, and any relevant Server Log or SIEM entries when you reach out.