Advanced Access Control Plugin

User Manual

Table of Contents

1 Overview

The Advanced Access Control plugin (also known as the Role-Based Access Control or RBAC plugin) lets BridgeLink administrators define roles with granular, per-feature permissions and assign those roles to users. Instead of managing permissions individually for each user, you create reusable roles that control what each user can see and do across the BridgeLink interface.

The plugin is part of the BridgeLink commercial security suite (bundled with Multi-Factor Authentication). It requires a valid license to activate.

2 Key Concepts

2.1 Roles

Roles are named permission profiles that you create and manage. Each role specifies a permission level for every feature area in BridgeLink. You can create as many roles as your organization needs, such as Administrator, Support, Interface Engineer, or Vendor.

2.2 Permission Levels

Permission levels are assigned per feature within each role. There are three levels:

- **Editor**: Full access. The user can view the feature and make changes (create, edit, delete).
- **View**: Read-only access. The user can see the feature and its data but cannot make changes.
- **No Permission**: The feature is completely hidden from the user. It will not appear in the sidebar navigation or the Settings tabs.

2.3 User Assignment

User assignment links a role to a specific BridgeLink user. Each user can be assigned one role. Users with no role assigned retain full access to all features (backward compatible behavior).

3 Accessing the Plugin

Navigate to **Settings → Access Control** in the BridgeLink Administrator. The plugin has two tabs: **Role** and **User Configuration**. Only users whose role grants Editor permission on the "Access Control" feature can access this screen. Typically, this should be restricted to full administrators.

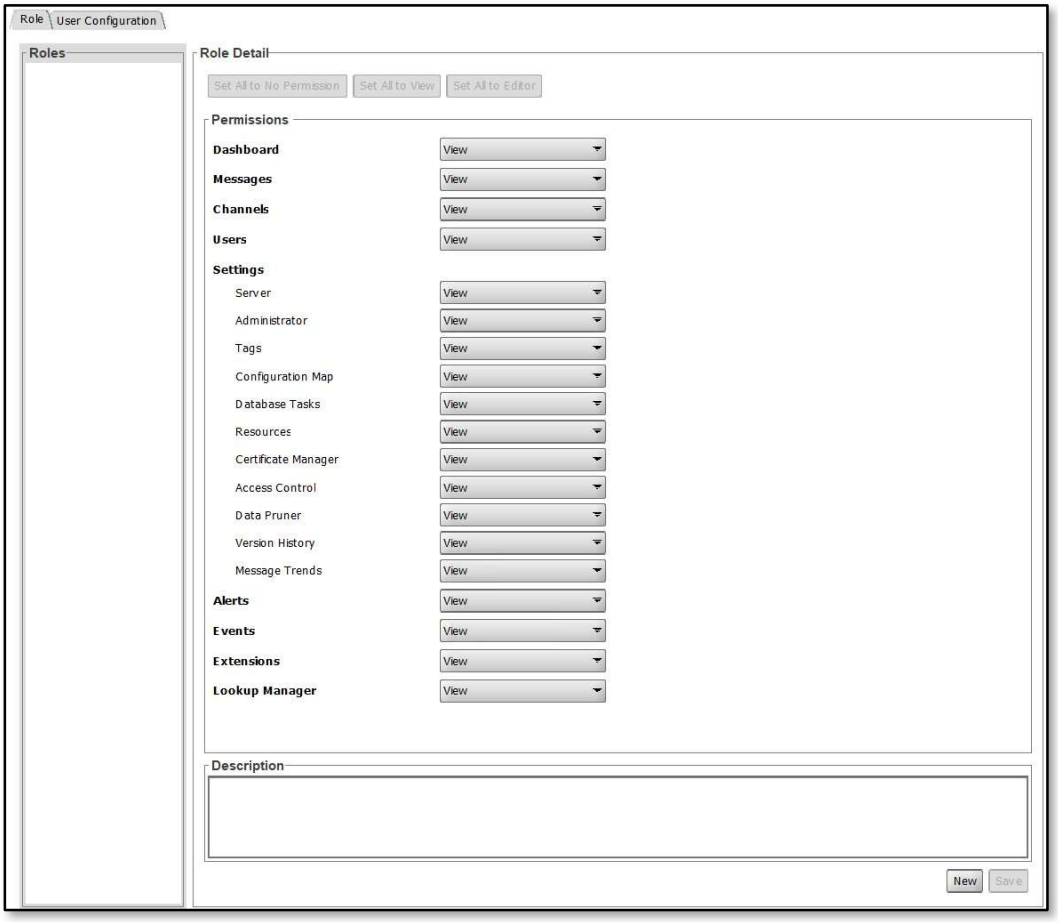

Figure 1: *The Role tab showing the Roles list, permission grid with dropdowns, bulk-set buttons, Description field, and New/Save buttons.*

4 Managing Roles

4.1 Creating a Role

1. Open the Access Control settings panel and select the **Role** tab.
2. Click **New** at the bottom right of the panel.

3. In the dialog that appears, enter a descriptive name for the role (e.g., “Support” or “Read-Only Viewer”) and click OK.

Figure 2: *The Enter Role Name dialog.*

4. The new role appears in the **Roles** list on the left. The Role Detail panel on the right defaults all permissions to **No Permission**.
5. For each feature area, use the dropdown to select the desired permission level: Editor, View, or No Permission.
6. Optionally, use the bulk-set buttons at the top of the panel (**Set All to No Permission**, **Set All to View**, or **Set All to Editor**) to quickly configure a baseline, then adjust individual features as needed.
7. Use the **Description** field at the bottom to add notes about the role’s intended purpose.

8. Click **Save**.

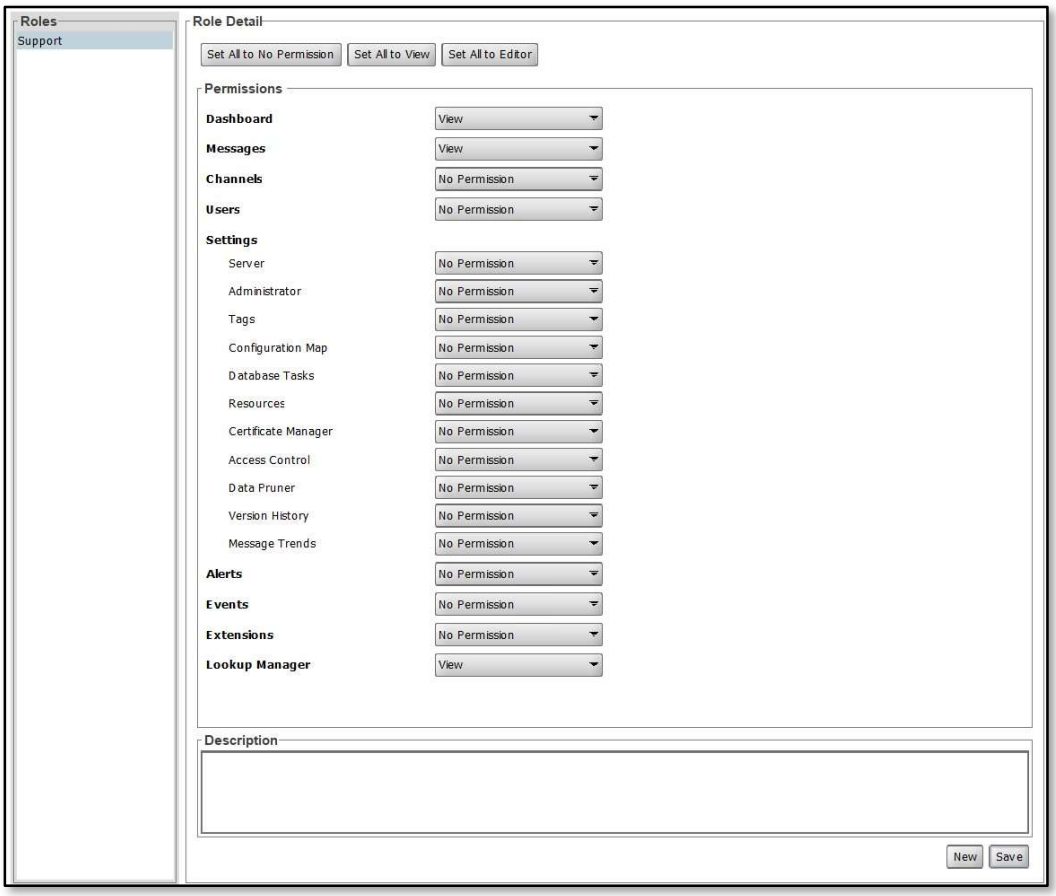

Figure 3: *A configured "Support" role with Dashboard and Messages set to View, and most other features set to No Permission.*

4.2 Editing, Duplicating, and Deleting Roles

Right-click on any role in the **Roles** list to open a context menu with three options:

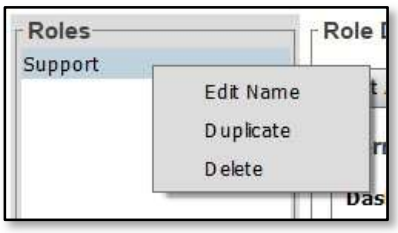

Figure 4: *The right-click context menu on a role.*

- **Edit Name**: Opens a dialog where you can rename the role. The role's permissions and user assignments are unchanged.

- **Duplicate**: Creates a copy of the selected role with all of its permissions. The new role will appear in the Roles list and can be renamed and customized, saving time when building roles with overlapping permissions.
- **Delete**: Removes the role. Users who were assigned to the deleted role will revert to "No Role," which grants full access to all features. Reassign those users to another role promptly.

After making any changes, click **Save** to persist them.

Figure 5: *The Access Control task panel with Refresh and Save buttons.*

You can find the Save button in the Access Control task panel on the left side of the screen. If you navigate away from the Access Control settings without saving, a prompt will appear asking whether you want to save your changes.

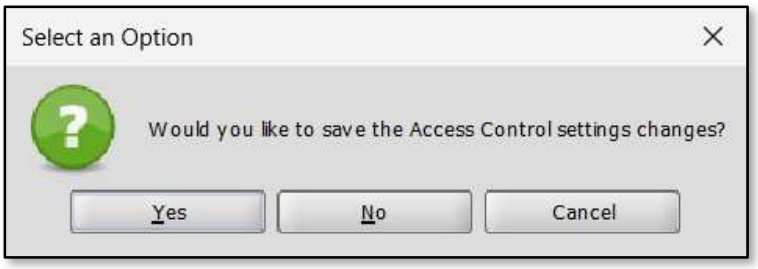

Figure 6: *The save confirmation prompt that appears when navigating away with unsaved changes. Click Yes to save, No to discard, or Cancel to stay on the current screen.*

5 Feature Areas and Permission Mapping

The following features can be individually controlled for each role. Setting a feature to "No Permission" hides it from both the sidebar navigation and any associated settings tab.

5.1 Core Features

Dashboard, Messages, Channels, Users, Alerts, Events, Extensions, Lookup Manager

5.2 Settings Sub-Permissions

The Settings section contains granular sub-permissions for individual settings tabs: Server, Administrator, Tags, Configuration Map, Database Tasks, Resources, Certificate Manager, Access Control, Data Pruner, Version History, and Message Trends.

If all sub-items within Settings are set to “No Permission,” the Settings link itself is hidden from the sidebar.

6 Assigning Roles to Users

1. Open the Access Control settings panel and select the **User Configuration** tab.
2. A table lists all BridgeLink users with columns for User ID, Username, First Name, Last Name, Email, Role, and MFA Enabled.
3. Click the **Role** dropdown next to a user and select the desired role. The dropdown shows all defined roles plus “No Role.”
4. Save your changes. The user’s interface will reflect their role’s permissions on their next login or session refresh.

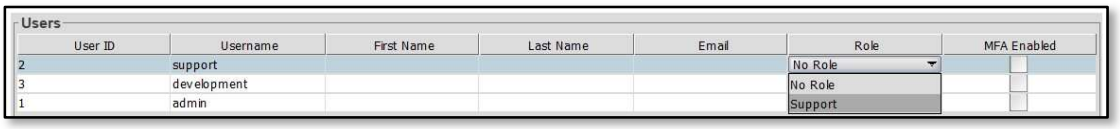

Figure 7: *The User Configuration tab showing the user list with Role dropdowns.*

7 Setting Up Multi-Factor Authentication (MFA)

The User Configuration tab also allows administrators to enable Multi-Factor Authentication for individual users. When MFA is enabled, users must provide a one-time password (OTP) from an authenticator app each time they log in, adding an extra layer of security beyond their username and password.

MFA is compatible with any TOTP-based authenticator app, including Google Authenticator, Microsoft Authenticator, Authy, 1Password, and similar applications.

7.1 Enabling MFA for a User

1. Open the Access Control settings panel and select the **User Configuration** tab.
2. Locate the user in the Users table and check the **MFA Enabled** checkbox in the rightmost column.

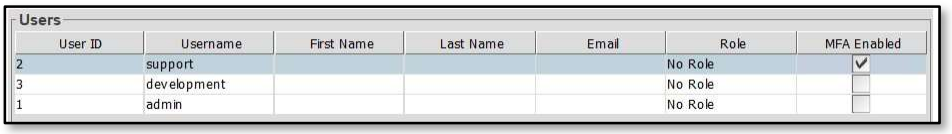

Figure 8: *The User Configuration tab with MFA Enabled checkbox checked for the support user.*

3. Click **Save** to persist the change. The next time this user logs in, they will be prompted to set up MFA.

Warning: Enabling MFA for a user will disable API access for that account. Users with MFA enabled will not be able to authenticate against the BridgeLink REST API. If the user requires both MFA and API access, a separate service account without MFA should be used for API integrations.

7.2 First-Time MFA Setup

When a user with MFA enabled logs in for the first time after activation, a Setup MFA dialog will appear:

4. The dialog displays the **Issuer** (your organization name) and **Account Name** (the username) pre-filled.

5. Click **Generate** to create a secret key.

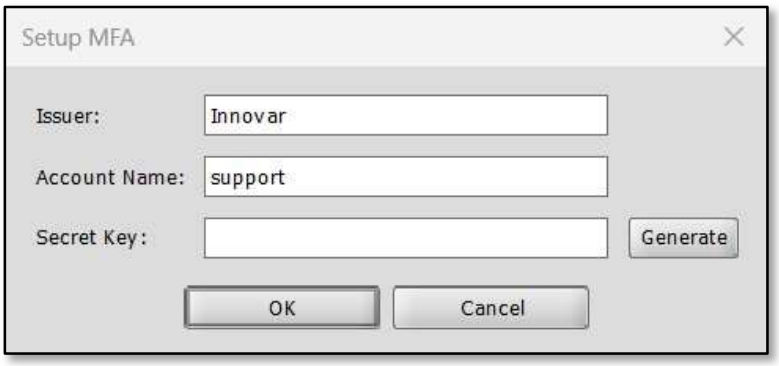

Figure 9: *The Setup MFA dialog before generating a secret key.*

6. A secret key will be generated and displayed in the Secret Key field.

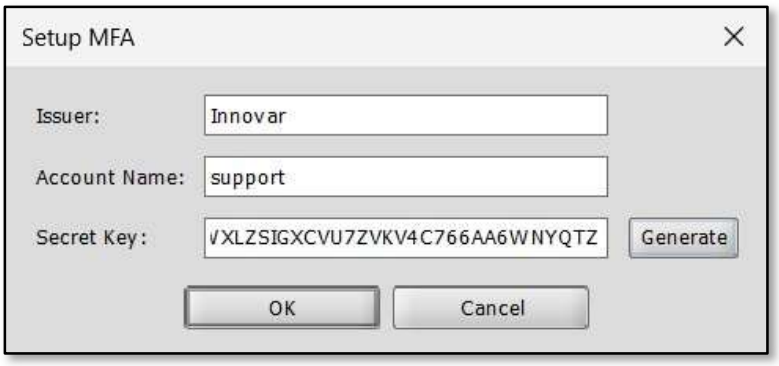

Figure 10: *The Setup MFA dialog after clicking Generate, showing the secret key.*

7. Click **OK** to proceed. A QR code dialog will appear.

7.3 Scanning the QR Code

The MFA QR Code dialog provides everything needed to link the account to an authenticator app:

8. Open your authenticator app (Google Authenticator, Microsoft Authenticator, Authy, or any TOTP-compatible app) on your mobile device.
9. Scan the QR code displayed in the dialog. Alternatively, you can manually enter the secret key shown below the QR code.
10. The authenticator app will begin generating six-digit one-time passwords that refresh every 30 seconds.

11. Enter the current OTP from your authenticator app into the **Enter OTP** field at the bottom of the dialog.
12. Click **OK** to complete the setup.

Figure 11: *The MFA QR Code dialog showing the QR code, secret key, and OTP entry field.*

After successful setup, the user will be required to enter an OTP from their authenticator app on every subsequent login.

7.4 Resetting a User's MFA

If a user loses access to their authenticator app or device, an administrator can reset their MFA by unchecking the MFA Enabled checkbox on the User Configuration tab and saving. The next time MFA is re-enabled and the user logs in, they will go through the setup process again with a new secret key.

8 How Permissions Are Enforced

Permissions are enforced at two levels:

- **UI Level**: Features set to “No Permission” are hidden entirely from the sidebar and settings tabs. The navigation items are fully removed from the rendered interface so users cannot stumble onto restricted areas.
- **Server Level**: All API calls are also gated by the RBAC permissions. Even if a user were to call an API endpoint directly (e.g., via the REST API), the server rejects or returns empty responses when the request is for features the user’s role does not permit.

9 Important Behaviors

9.1 Plugin Not Installed or Disabled

If the RBAC plugin is not installed or is disabled, all features remain fully visible and accessible to all users. This ensures backward compatibility.

9.2 No Role Assigned

If a user has “No Role” assigned, they retain full access to all features. The plugin does not restrict unassigned users.

9.3 Administrator Best Practice

Always ensure at least one user retains a role with full Editor permissions on all features, including the “Access Control” settings sub-permission. This prevents accidental lockout from the RBAC configuration.

9.4 Bulk-Set Then Customize

When creating restrictive roles, it’s fastest to click **Set All to No Permission** first, then selectively grant View or Editor on the specific features that role needs.

10 Example Role Configuration

Below is a sample “Support” role configuration where the user can only view the Dashboard, Messages, and Lookup Manager. Everything else is hidden:

Feature	Permission Level
Dashboard	View
Messages	View
Channels	No Permission
Users	No Permission
All Settings sub-items	No Permission
Alerts	No Permission
Events	No Permission
Extensions	No Permission
Lookup Manager	View

For a full Administrator role, set all features to Editor. For a Business Analyst role, you might grant View on most features and Editor on Channels and Messages.

11 Troubleshooting

11.1 A user can’t see a feature they should have access to

Check that the user is assigned to the correct role on the User Configuration tab, and confirm that role grants at least “View” on the relevant feature. If the plugin was recently enabled, the user may need to log out and back in.

11.2 A deleted role left users with full access

This is expected behavior. Users revert to “No Role” which grants full access. Reassign those users to an appropriate role as soon as possible.

11.3 The Access Control settings tab is not visible

Ensure the current user’s role includes Editor access on the “Access Control” settings sub-permission. Only users with that permission can manage roles and user assignments.

11.4 All features visible even though RBAC is configured

Verify the plugin is both installed and enabled in the Extensions panel. If it’s disabled, the system defaults to full access for everyone.