Table of Contents

Britive Profile Management

Managing Britive Profiles

Application administrators can configure a Britive profile to associate the permissions of an onboarded application, and setup policies so that certain members can have access to the profile with or without approval.

Application administrators can create and manage Britive profiles using the following steps.

Creating a Britive Profile

1. Login to Britive with administrator privileges.
2. Click on **Admin -> Application and Access Profile Management**.
3. Click on the application and select **Profiles** from the navigation menu.
4. You have two options for profile creation:
    1. **Clone a profile:** Clone an existing profile using the **Clone profile icon** in front of the profile. A cloned profile is in an active state after creation.
        1. Select the profile sections you want to clone for the new profile.

            Notes:

            - Only the selected sections are cloned.
            - If you select **Permissions,** the **Associations** section is automatically selected.
            - Only the **Associations** section can be selected.

        2. Edit the profile as per your requirements.
    2. **Create a profile:** Click on **CREATE PROFILE** to create a new profile.
        1. Enter the following on the **Create Profile** page:
            1. Enter the following in the **General** section of the page:
                1. Enter **Name**.
                2. Enter **Description** (Optional).
                3. Check **Use Default App Console URL** to use the default application console URL or

enter the **Console URL**. The user is directed to a specified console URL instead of the default landing page of an onboarded application.

2. Enter the following in the **Expiration** section of the page:
    1. Enter the **Expiration Timeout** in minutes.
3. Click **Done**.

5. After the profile is created, enter the details in the following tabs to complete a profile:
    - Associations
    - Permissions
    - Policies
    - Identities
    - Tags
    - Session Attributes (For AWS and AWS-standalone applications only)

Associations

The **Associations** tab displays the scope of the permissions applied in a particular application. An administrator can select the environment(s)/resource(s) to be associated with this profile. This tab varies as per the application.

Permissions

The **Permissions** tab displays the list of permissions granted for the profile. The applicable permissions are displayed for selection and are specific to each application.

To add the existing permissions:

1. Click on the **SELECT PERMISSION** button.
2. In the **Add Permissions** page, select the required permission, click **+** icon to add this permission.
3. The list of permissions depends on the onboarded application. For example: For AWS, the user can add only one role per profile, or for OCI, the user can add only groups.
4. [For AWS applications only] Britive-managed roles:

Administrators or users can create their own roles with the required AWS-managed policies or inline policies so that Britive profiles can be built using those permissions. These roles get provisioned in AWS after they are checked out from Britive.

1. Click **CREATE PERMISSION.**
2. Enter the following in the **Create Role** page:
    1. Name
    2. Description
    3. Permissions:
        1. **Select Existing Policy**: Select from the listed policies. Click on the information icon to view the policy details.
        2. **Create Inline Policy**: Enter the **Name** and the **Policy code** in JSON format in the **Create Policy** page. Click **Validate** to validate the policy details.
    4. **Add New Tag** (Optional): Enter the **Key** and **Value** pair and click **Add**.
    5. Click **Save**.
3. Britive-managed permissions are displayed with icon **b,** indicating that a role is Britive-managed.

Policies

The **Policies** tab displays the list of policies created for a profile. An application administrator can create a policy to select which users can use the profile and whether the profile needs approval or not before checking out a profile.

1. Click on the **ADD POLICY** button to add a new policy and enter the following:
    - **General**
        - Enter the **Policy Name**.
        - Enter the **Description** (Optional)
    - **Members:**
        - **Users**: Add selected users for this policy by clicking on **Add Users**.
        - **Tags**: Add selected tags for this policy by clicking on **Add Tags**.
        - **Service identities**: Add selected service identities for this

policy by clicking **Add Service Identities**.

- **Generic Conditions**:
  - IP based: Select if you want access based on the IP addresses. Enter an IP address or a list of comma-separated IP addresses in the text box.
  - Time based: Select the **Start and End Date/TimeDate-time range** or **Set Time Schedule** for applying the policy.
- **Step-up Verification:** Select **Yes** to enable step-up verification for this profile. Once enabled, you can select if the previous successful verification can be used for subsequent profile checkouts. The step-up verification validity is configured in the step-up verification validity settings in the **Security** tab. For more information, see Configuring Step-up Verification Validity.
- **Approvals**: Select whether the user needs approval to access a profile. Enter the following details if you select **Approval Required** as **Yes**:
  - **Notifications:** Select notification medium(s) using the **Add Notification** button. Before use, notification mediums can be created in the **Admin->Global Settings** section. For more details, see Creating and Managing Notification Mediums.

    Note:

    You can add only one Slack notification medium per policy.

  - **Users**: Select the users from the user list. A notification is sent to these users for approval.
  - **Tags**: Select the tags from the list.
  - **Maximum time to Approve:** Enter the time in Hours:Minutes format. The approval request expires if it is not approved in this specified time.
  - **Access Validity after Approval**: Enter the number of days or hours for access validity after the request is approved.

2. Click **Save and Enable** after all the configuration is done.

Users can Edit/Clone/Enable/Disable/Delete a policy by clicking **Manage** for a particular policy.

Session Attributes

> Note: This tab is specific to AWS and AWS-standalone applications only.

The **Session Attributes** tab displays the session attributes added to the profile.

There are two types of attributes:

- Identity: The selected value for the attribute is collected from the user's profile when they checkout the AWS profile from the **My Access** tab.
- Static: The user has to specify a value that remains the same for all users in the **Attribute Value** field.

To add a session attribute:

1. Click on the **ADD SESSION ATTRIBUTE** button.
2. Enter the following on the **Session Attribute** page:
    1. Select the **Attribute Type**, either Identity or Static.
    2. Select the **Attribute**.
    3. Enter the name of the attribute as defined in the role configured in AWS in the **Mapping Name** field.
    4. Select **Transitive** to pass the session attributes when assuming other roles and those roles have the same attributes defined.
    5. Click **ADD SESSION ATTRIBUTE**.