Cloudbrink How-To Guide: Configure an Identity Provider (IDP)

Introduction 1

Prerequisites 1

Instructions 1

- Login 1
- Authentication Configuration 3
- Authentication Validation 4

Introduction

Configuring an identity provider (IDP) with Cloudbrink enables enterprises to use existing single sign-on (SSO) and active directory user groups. Once the IDP is configured, user credentials will be utilized by Cloudbrink administrators to log in to the Cloudbrink portal, and by end users to authenticate via the Cloudbrink App.

Prerequisites

In order to successfully follow this documentation, please ensure the following prerequisites are met:

1.1. The primary contact email address and temporary Cloudbrink password
1.2. A SAML 2.0 based corporate identity provider, with necessary privileges to create application policies

Instructions

Login

2.1. Navigate to https://admin.cloudbrink.com, enter your **username** and **password** that were provided during onboarding, and click **login**.

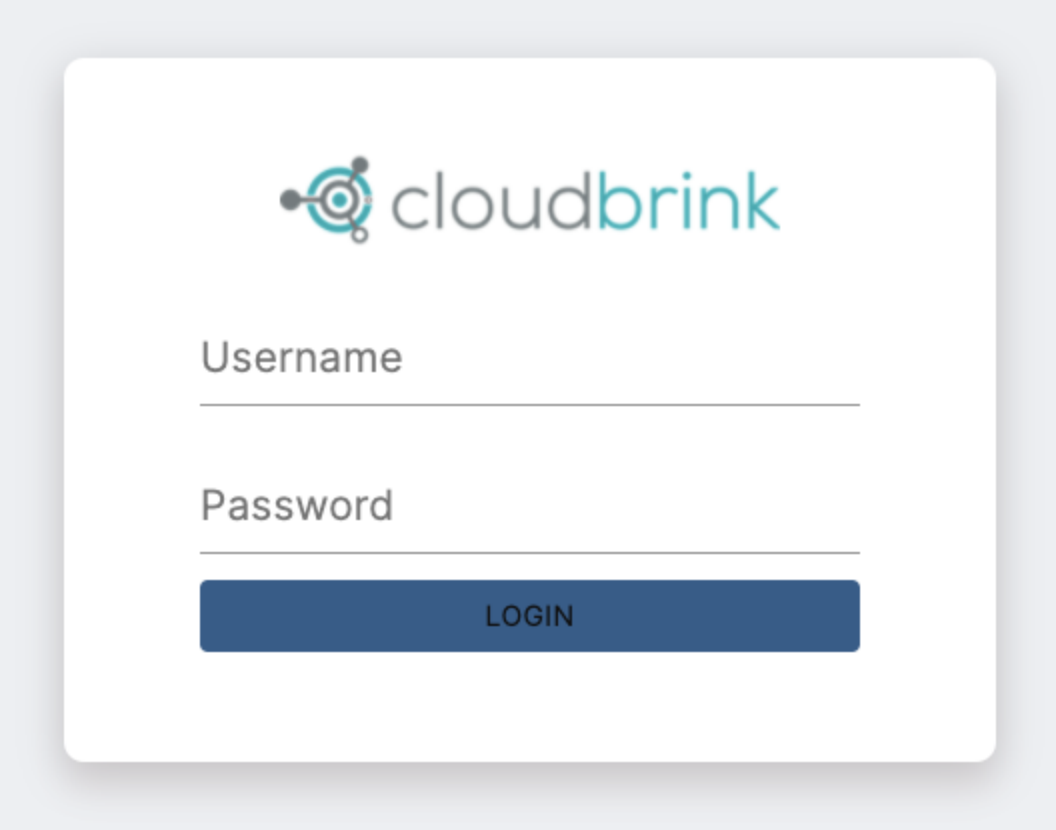

Figure 1: Cloudbrink Portal Login

2.2. After a successful login you'll be redirected to the Cloudbrink Dashboard.

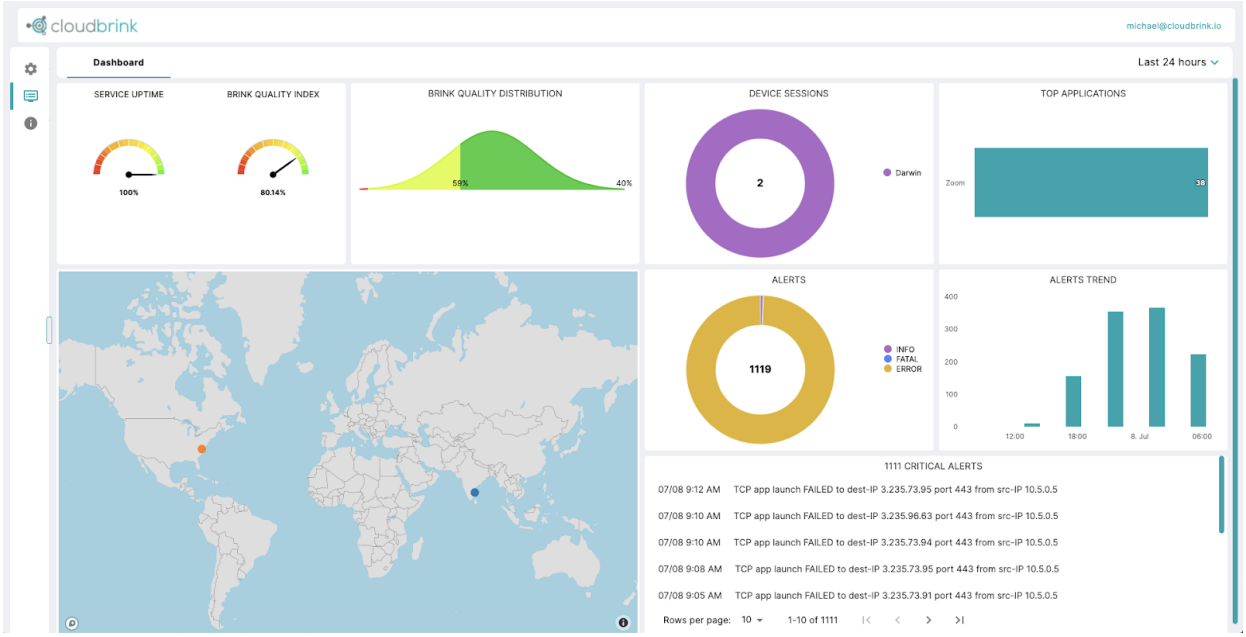

Figure 2: Cloudbrink Portal Dashboard

Authentication Configuration

3.1. In the upper left corner of the Cloudbrink Portal, click either the **Gear Icon** or the **Configure** button (depending on whether the left menu is collapsed or expanded, respectively)

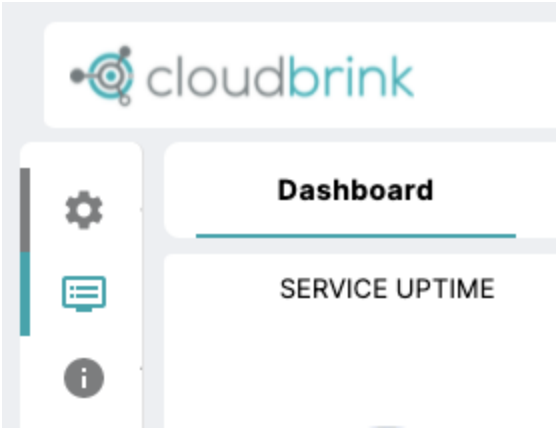

Figure 3: Gear Icon

3.2. On the page that appears, click the **Policies** tab

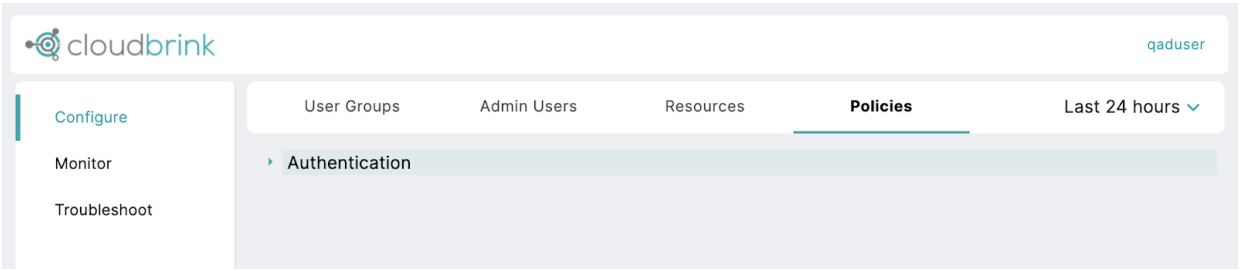

Figure 4: Configure: Policies

3.3. Expand the **Authentication** section, and click the **teal +** button

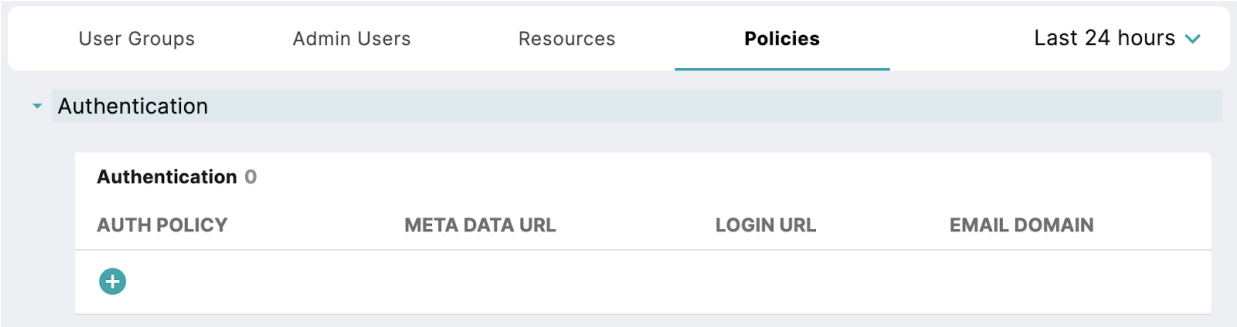

Figure 5: Policies: Authentication

3.4. In the configuration pane that appears, fill in the following information and then click the ✔ **icon**:

3.4.1. **Auth Policy**: a friendly name for this identity provider

3.4.2. **Metadata URL**: the URL of the identity provider's metadata page, which contains the IDP certificate, entity ID, and redirect URL
3.4.3. **Login URL**: the single sign on URL of the identity provider
3.4.4. **Email Domain**: one or more email domains to associate with this authentication configuration

Figure 6: Authentication Configuration

Authentication Validation

4.1. Follow the steps outlined in the **How To: Publish an App to a User Group** document to publish an app to a user group
4.2. Install and start the **Brink Agent** on an end-user device

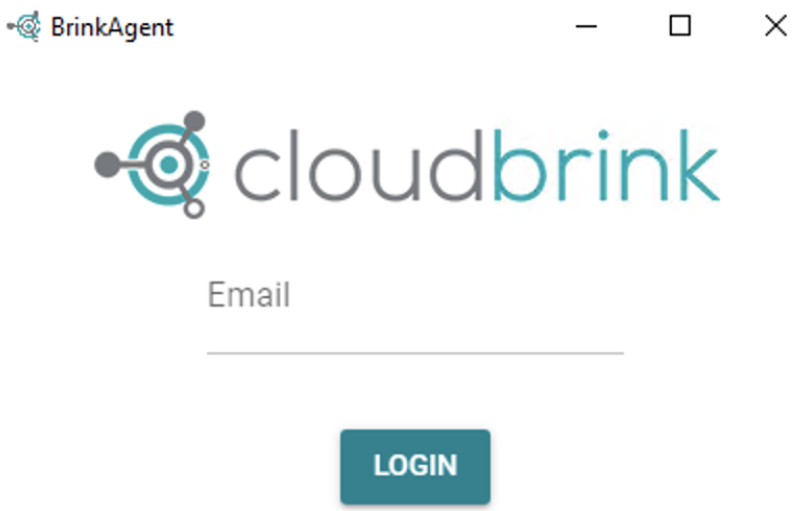

Figure 7: Brink Agent Login

4.3. Enter your **email address** (with a matching domain from step 3.4.4), and click **Login**
4.4. Verify that you're redirected to the appropriate Identity Provider your organization utilizes. Follow the IDP specific prompts, and ensure the Brink Agent starts up as expected.