

Identity Aware Platform

Operation Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

Application Management

SSO Configuration

Operation Guide

Application Management

Last updated : 2024-11-06 18:07:13

Prerequisites

CLB instances have been created and displayed in the IAP application management list. If you need to create a CLB instance, see [Creating CLB Instances](#).

OIDC SSO has been configured in the IAP console. If you need to configure it, see [SSO Configuration](#).

Enabling IAP

1. Log in to the [IAP console](#).
2. In the left sidebar, select **Application Management**.
3. On the **Application Management** page, select the CLB resource name or ID for which you want to enable IAP, and then click **Show**.
4. After selecting a listener, click the **IAP enabling button** for the corresponding URL resource.
5. In the IAP **pop-up window**, select a base policy.

Allow by Default: When an IAP exception occurs, resource access requests initiated by this URL will be allowed.

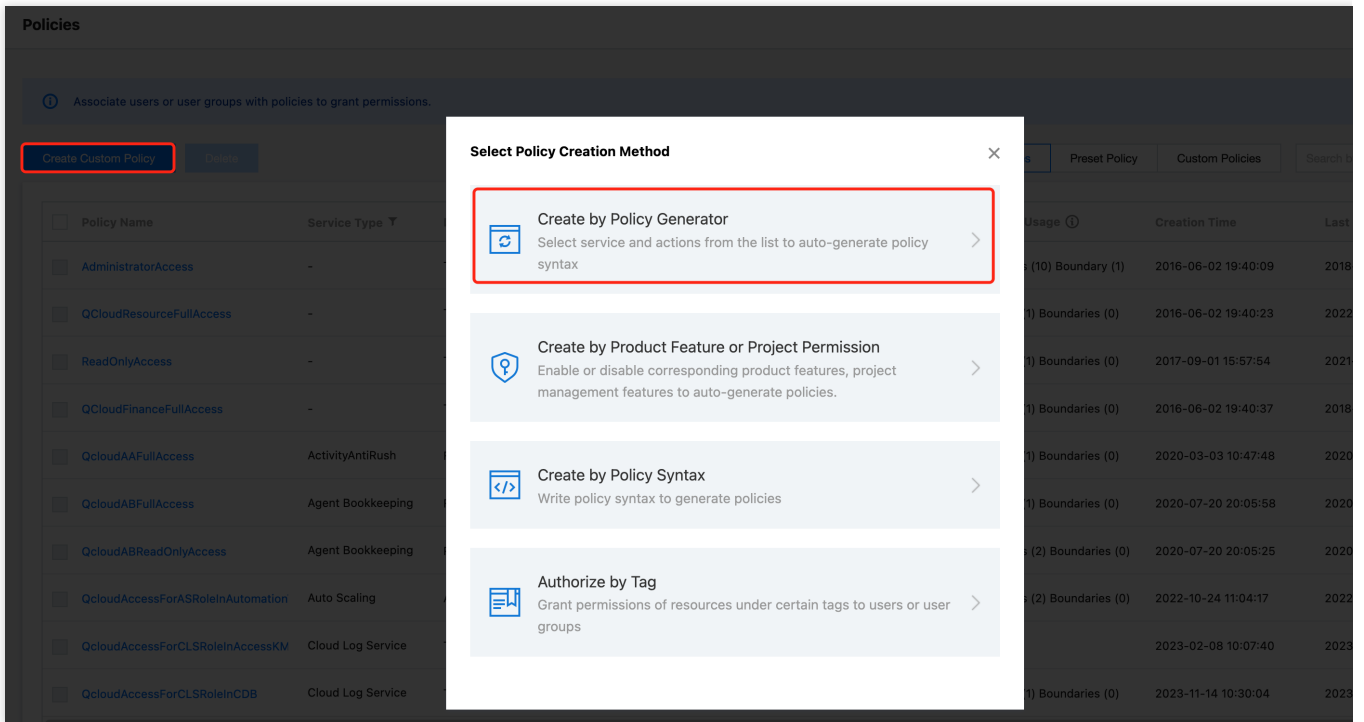
Reject by Default: When an IAP exception occurs, resource access requests initiated by this URL will be rejected.

6. Click **OK** to enable the IAP feature.

After IAP is enabled, it will request login credentials from connection requests of the CLB. Only accounts with permissions can access the resources.

Configuring Permissions

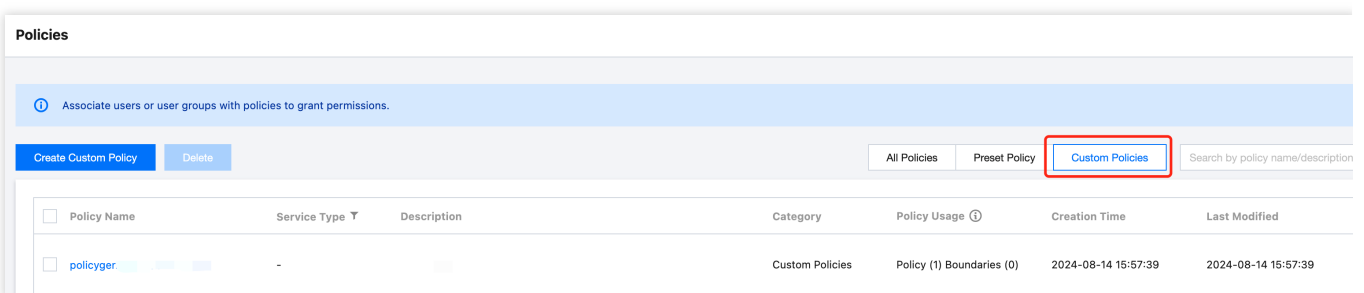
1. In the IAP console, click **Configure Permissions** to enter the **Policies** menu of the CAM console. In the **Create by Policy Generator** section, create a custom policy.



2. For detailed configuration methods of custom policies, see [Creating Custom Policies by Policy Generator](#).

Viewing Permissions

1. In the IAP console, click **View Permissions** to enter the **Policies** menu of the CAM console.
2. On the **Policies** page, click **Custom Policies** to view the configured custom policies.



SSO Configuration

Last updated : 2024-11-06 18:01:38

IAP establishes an association relationship with enterprise IdP users through OIDC SSO. If you need to control the resource access permissions with IAP, you should configure OIDC SSO first. This document introduces the SSO configuration and login status management configuration.

SSO Configuration

1. Log in to the IAP console > [SSO Configuration](#) page.
2. In the **SSO Configuration** section, click **Edit**.

SSO Configuration

SSO Status Not enabled

3. On the **SSO Configuration** page, enter the following information as needed and click **Save**.

SSO Configuration

SSO Configuration

SSO Protocol **OIDC**

IdP URL *

Client ID *

User Mapping Field *

Authorization Request Endpoint *

Authorization Request Scope *

Authorization Request Response Type *

Authorization Request Response Mode *

Signature Public Key *

4. The configuration is completed.

SSO Settings

User-Based SSO ⓘ **Enable**

SSO Protocol * **OIDC**

IdP URL * **https://accounts.google.com**

Client ID * **1**

Redirect URL **https://cloud.tencent.com/sso/oidc/post?uin=100034279333** [Copy](#)

Login Status Management

1. In the **Login Status Management** section, click **Modify**.

Login Status ManagementMax Login Time Not set. [Modify](#)

2. In the pop-up window, modify the maximum login retention period. The modification range is 1 to 72 hours.

Modify Max Login Time ×Max Login Time Hour

The adjustment range is greater than or equal to 1 hour, and less than or equal to 48 hours. When the value is beyond this time range, the system will log out.

OK

Cancel

3. Click **OK** to complete the modification.