



HYCU for Okta Customer Identity Cloud

R-Cloud Module Guide

Table of Contents

About the module.....	3
Prerequisites.....	3
Getting the client ID and the client secret.....	3
Limitations	5
Considerations related to the module design	7
Protecting data.....	7
Backing up data	7
Restoring data	9

Copyright notice

© 2024 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

About the module

With the R-Cloud (formerly HYCU Protégé) module for Okta Customer Identity Cloud, you can back up your Auth0 tenant data securely and efficiently.

Prerequisites

Before you add the R-Cloud module for Okta Customer Identity Cloud (CIC) as a source, the following prerequisites must be met:

- The domain of the tenant must be available.
- The client ID and the client secret of the Machine-to-Machine application must be available. For details, see [Getting the client ID and the client secret](#).

Getting the client ID and the client secret

To get the client ID and the client secret, follow these steps:

1. Sign on to your Auth0 dashboard with a user that is granted the admin privileges to create an application.
2. On the dashboard, go to Applications, click **Create Application**, and then select **Machine-to-Machine Applications**.
3. Click **Create**.
4. From the drop-down menu, select **Auth0 Management API**. Add the following permissions to the API:

read: users	create: roles
update: users	update: roles
create: users	read: prompts
read: users_app_metadata	update: prompts
create: users_app_metadata	update: branding
read: clients	create: role_members

update: clients	read: role_members
create: clients	read: attack_protection
read: connections	update: attack_protection
update: connections	read: organizations_summary
create: connections	read: organizations
read: resource_servers	update: organizations
update: resource_servers	create: organizations
create: resource_servers	create: organization_members
read: rules	read: organization_members
update: rules	create: organization_connections
create: rules	read: organization_connections
read: hooks	update: organization_connections
update: hooks	create: organization_member_roles
create: hooks	read: organization_member_roles
read: actions	create: organization_invitations
update: actions	read: organization_invitations
create: actions	create: phone_providers
read: tenant_settings	read: phone_providers
update: tenant_settings	update: phone_providers
update: triggers	create: phone_templates
read: triggers	read: phone_templates
read: grants	update: phone_templates
read: guardian_factors	read: client_credentials
update: guardian_factors	create: client_credentials

read: email_templates	update: client_credentials
update: email_templates	read: client_grants
read: mfa_policies	create: client_grants
update: mfa_policies	read: stats
read: roles	read: custom_domains
read: branding	create: custom_domains

5. Click **Authorize**.

After the application is created, go to its Settings tab and copy the domain, client ID, and client secret values. Use these values when adding the module as a source to R-Cloud.

Limitations

When adding the module and protecting the related SaaS applications, the following limitations apply:

- The created or modified time stamps are not preserved during the restore. The timestamps are recreated.
- The object IDs are changed during the restore because they are recreated.
- Only the database (including a custom database) and passwordless (SMS and email) connection users can be restored.

Note During a tenant-level or a database-connection (if using a custom database) restore, an admin must provide the right values of the database settings keys in the restore prompt to restore the users of that connection successfully.

- The rules configuration key-value settings are not preserved as part of rules backup because the Auth0 API doesn't expose the values of the configuration keys.
- Secret values of the Hook and Action cannot be preserved as the Auth0 API doesn't expose the secret values.
- Due to the Auth0 API limitations, the following cannot be backed up:
 - Tenant members
 - Customized login page of the Universal Login customizations

- WebAuthn with FIDO Security Keys (Enterprise MFA), WebAuthn with FIDO Device Biometrics (Enterprise MFA), and Duo Security (Pro MFA) MFA factor settings.

Note Only their enabled or disabled status will be preserved.

- The AWS Secret Access Key, the Google Play Store URL, and the Apple App Store URL related to the Amazon SNS push notification service settings present under MFA Security Settings
- The Google Play Store URL, the FCM Server Key, the Apple App Store URL, and the APNs Certificate related to the platform-specific push notification service configuration present under MFA Security Settings
- Due to the Auth0 API limitations, the following cannot be restored:
 - Enterprise and social connection users
 - The application credentials of the Private Key JWT authentication method
 - The bot detection attack protection security settings
 - The pre-built or installed actions
 - Secret values of the Hook and Action

Note Only the secret keys will be restored. The secret values should be updated with the right values to make sure that the Hook or Action are operational after the restore, because the module will assign a fixed unknown value to each key.

- Enable Adaptive MFA Risk Assessment toggle value present under Define policies > MFA Risk Assessors section
- Created At and Expires At timestamps of the organization invitations
- The order of the rules
- The flows are restored with the Done with errors status if there are no actions configured before the backup. The following error is reported during the restore:
[Error message: Tenant does not exist].
- Due to the Okta CIC SDK limitation, the Universal Login customizations are restored with the Done with warnings status if the branding information is not configured for a new tenant during the backup. The following error is reported during the restore:
[Error while restoring branding settings of universal login customizations. Error message: Payload validation error: 'Too few properties defined (0), minimum 1'.]

Considerations related to the module design

- The Authentication Profile configurations available under Authentication will be restored as a part of the Universal Login Customizations restore.
- If you rename a hook after the backup, the backed-up hook with the original name will be restored even if the renamed hook exists in the tenant.
- During the action restore, an action will not be added to its respective flow. You must restore the respective flow separately after that action is restored to add the restored action to the flow.
- For Identity and Access Management systems, the configurations or settings of any object are critical. So, during a tenant-level restore if an object already exists, the module skips that object and does not update its existing configurations or settings. Its associations will be restored as they were in the backup.
- After the database-connection user is restored, the admin/user should reset their password, as the module is using a random password to restore a user because the Auth0 API doesn't provide user passwords.

Protecting data

R-Cloud starts protecting your Okta CIC data after you add the module as a source to R-Cloud and assign a policy to the related SaaS application.

For details on how to add the module as a source and how to assign the policies, see *HYCU R-Cloud Help*.

Backing up data

After adding Okta CIC as a source in R-Cloud, all the Okta CIC supported objects are automatically discovered.

The supported objects are:

- Tenant
- Tenant settings (general and advanced)

- Applications
 - Settings
 - Credentials
 - Connections
 - Organizations
 - APIs
- APIs
 - Settings
 - Permissions
- Authentication connections
 - Database connection (config and applications)
 - Social connection (config and applications)
 - Enterprise connection (config and applications)
 - Passwordless connection (config and applications)
- Organizations
 - Branding
 - Members
 - Invitations
 - Connections
- Users
 - Permissions and roles
- Roles
 - Permissions and users
- Branding
 - Universal login customizations
 - Custom email templates
- Security
 - Attack protection security settings
 - Suspicious IP throttling
 - Brute-force protection
 - Breached password detection
 - MFA security settings
 - Status of all the factors
 - Settings of phone message and push notification factor

- Actions (only custom)
- Flows
- Rules
- Hooks
- Custom domain


For details on how to back up Okta CIC data, see *HYCU R-Cloud Help*.

Restoring data

R-Cloud allows you to restore the protected Okta CIC data at the following levels:

- Tenant
- Tenant settings
- API
- Application
- Database connection
- Social connection
- Enterprise connection
- Passwordless connection
- Organization
- User
- Role
- Action
- Flow
- Rule
- Hook
- Universal login customizations
- Custom email template
- MFA security settings
- Attack protection security settings

- Custom domain

 **Note** When restoring your Okta CIC data, all hierarchical relations between the content items are preserved at all levels.

For details on how to restore the Okta CIC data, see *HYCU R-Cloud Help*.

Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

info@hycu.com

We will be glad to hear from you!

