



HYCU for Okta Workforce Identity Cloud

R-Cloud Module Guide

Table of Contents

About the module.....	3
Prerequisites.....	3
Limitations	3
Consideration	6
Recommendations	7
Protecting data.....	7
Backing up data	8
Restoring data	8

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 Workforce Identity Cloud, you can back up your Workforce data securely and efficiently.

Prerequisites

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

- Okta user or service account must be granted admin privileges.
- The API token for the Okta account is required.
- The organization URL of your Okta tenant is required.

Example

Organization URLs:

```
https://companyname.okta.com  
https://companyname.oktapreview.com  
https://companyname.okta-emea.com
```

Limitations

When adding the module to R-Cloud and protecting the related SaaS application, the following limitations apply:

- The created or modified timestamps are not preserved during the restore. The timestamps are recreated.
- The object IDs are changed during the restore since they are recreated.
- Setting up automatic policy assignment with labels or tags is not supported.
- *For the Okta Classic engine subscription:* The Okta application sign-on policy rules are not preserved during the restore.
- The application visibility options are not restored if the OIDC is used as the Single Sign-On and Authentication (SSO) option.
- You can restore Okta WIC data to a different source only at the Organization level.

- For the OIDC applications, the following cannot be restored:
 - The customized Application Rate Limits value
 - The Groups claim type and Groups claim filter fields
 - The Callback URI field
- The Provisioning checkbox and Assertion Encryption fields of the SAML_2.0 type applications cannot be restored.
- Okta allows deleting a group even if the group is linked to the global session policy. If the global session policy is not linked to any of the backed-up groups, the restore of such global session policy will fail.
- Due to the Okta API limitation, if the SAML 2.0 Identity Provider (IdP) settings have the IdP Usage parameter set as Factor only, the parameter will be restored as SSO Only. The SSO Only value must be updated to Factor only after the restore. All the other SAML 2.0 IdP parameters will be restored as they are.
- *For the application restore (due to the Okta API limitations and/or design):*
 - The Okta admin console session values cannot be protected.
 - The SAML signing certificates cannot be restored. Okta generates these certificates by default when an application is created.
 - While creating and updating an application with a shared username and password, the password will be updated to default tPassword.
 - The application settings cannot be restored if an application is inactive.
 - The custom admin roles will not be restored during the Application Granular restore. They will be restored only if you perform the Organization or Resource Set/Role Granular restore.
 - *For the SAML 2.0 applications created via the Create App Integration:*
 - The applications that have the signature certificate uploaded, but do not have the SP Issuer property set, will be restored with the default value for the SP Issuer property (R-Cl oud).
 - To enable the restore, at least one of the SAML assertions or responses must be signed.
 - While backing up certain OIN applications that are created by using the browse app catalog, Okta does not provide the parameters that are required for a successful restore. These applications cannot be restored.
 - Okta does not provide certain required properties when responding to the GET calls for the OIN applications. To ensure a successful restore, the following is done by the module during the restore procedure:
 - *For the SGNL applications:* The cl i entName property is set to R-Cl oud.

- *For the Axiad applications:* The tenantName, tenantPlatform, acsUrl, and audienceUri properties are set to R-Cloud.
- *For the role restore:*
 - Due to the Okta API limitation, the standard admin roles including their assignments cannot be protected.
 - The permissions for the roles will only be added and not replaced during the update.
- *For the policy and the policy rule restore (due to the Okta API limitations and/or design):*
 - If the authenticators are not configured, the restore of the policy and the policy rule will be completed with the following error:

This rule uses authenticators that have not been set up for your org. Please add at least one of the following authenticators in order to activate this rule: Custom App Authenticator, Email, Google Authenticator, IdP Authenticator, Okta Verify, On-Prem MFA, Phone, RSA SecurID, Security Key or Biometric, Symantec VIP, Yubi Key Authenticator.
 - The policies and the policy rules that were deleted after the backup will not be inserted according to their backup priority but will be created towards the end of the priority list—just before the default policy or the default policy rule.
 - During the restore, the authenticators for the MFA_ENROLL policies that were not configured in the restore account will be skipped. If these authenticators are not skipped, Okta will report the following error: Not one of the allowed values.
 - If the policy or the policy rule is deleted after the backup and recreated with same name, it will not be updated during the restore.
 - For applications like Microsoft 365, for which application-specific authentication policies get added with the same name during application integration, the following error can be expected during the Organization/Policy restore:

Policy name already in use.
- *For the group restore:*
 - The inactive applications cannot be assigned to the groups. As a result, the restore will be completed as DONE_WITH_WARNINGS due to the Okta design.

- The users assigned by using the group rules will not get mapped at the group level restore. These users will be mapped during the Group Rule restore.
- If the associated groups that are linked to the policies are deleted after the backup, the policies remain valid. However, without the association with the groups, the module will not be able to update or create such policies.
- *For the group rule restore:* Okta does not support updating the `assignUserToGroups.groupIds` section of the actions object in a group rule.
- *For the resource set restore:*
 - The module does not support protecting the auth-server. As a result, only the existing auth-servers will be added as a resource during the restore.
 - The users, the apps, the groups or the auth-servers for a given resource set during the restore will be added. They will not be replaced.
- *For the network zone restore:* The Legacy IP Zone is the default zone. If the gateways and the proxies are blank (default) during the backup, the restore will be completed as `DONE_WITH_WARNINGS` because of the Okta API limitation.
- *For the UI schema restore:* The user attributes that are present in an Okta source during the UI schema restore will only be created or updated. The attributes that are present in backup but missing in Okta Source during the restore will be skipped.
- *For the user restore:*
 - If the custom attributes are not present in the destination account, they will not be updated or created during the restore.
 - When a user is assigned several applications individually, and is then later assigned to a group which includes the same applications, the Okta user interface displays these application assignments as individual assignments. However, if the user is deleted and then restored, the applications will appear as group-assigned (and not individually assigned) because the restore process uses the following order: user, group, applications.

Consideration

Before you add the module as a source, consider the following:

- The R-Cloud module for Okta WIC supports restoring SaaS application data to a different source (that is, a different SaaS module of the same type). For instructions on how to do this, see *HYCU R-Cloud Help*.
- The following actions must be performed after restoring the IdP to the same source:
 - *For the SAML 2.0 IdP:* The Audience URI and ACS URL parameters must be updated at the IdP side.
 - *For the OAuth2.0 and OpenID Connect IdPs:* The ClientId (Okta App ID) parameter must be updated in the Authorize URL.
- *The following actions must be performed after restoring the IdP to a different source:*
 - *For the SAML 2.0 IdP:* The Audience URI and ACS URL parameters must be updated at the IdP side.
 - *For the OAuth2.0 and OpenID Connect IdPs:*
 - The Redirect URI parameter must be updated at the IdP and at the Okta App (client) side.
 - The ClientId (Okta App ID) parameter must be updated in the Authorize URL.

Recommendations


To avoid throttling issues, make sure to assign 95–100 percent of the API limits to the token created for R-Cloud. This can be configured by editing the token:

1. Sign in your Okta Admin dashboard. Go to Security, then API, and then to Tokens. Click the **Edit** button for the token you're using.
2. Click the **Edit** button of the **Token rate limits** section.
3. Slide the pointer to 95 percent.

Protecting data

R-Cloud starts protecting your Okta WIC 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 to R-Cloud, see *HYCU R-Cloud Help*.

 **Note** The R-Cloud module for Okta WIC backs up data using a staging target. Select the preferred staging target when adding the module as a source in R-Cloud.

Backing up data

For details on how to back up the SaaS application data, see *HYCU R-Cloud Help*.

Restoring data

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

- Administrator Role
- Application
- Behavior Detection Rule
- Brand Customizations
- Custom Domain
- Group
- Group Role
- Identity Provider
- Network Zone
- Organization
- Policy and Policy rules
- Resource Set
- Role
- SMS Template
- Trusted Origin
- UI Schema
- User

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

For details on how to restore the SaaS application 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!

