HYCU for Microsoft Entra ID

R-Cloud Module Guide

Table of Contents

About the module 3

Prerequisites 3

Limitations 4

Protecting data 7

Backing up data 8

Restoring data 8

Copyright notice

About the module

The R-Cloud module for Microsoft Entra ID enables you to protect the contents of your Microsoft Entra ID.

Prerequisites

Before you can add the Microsoft Entra ID module to R-Cloud as a source, your authentication service account must be granted the minimum permissions set. This can be created under App registrations on the Microsoft Entra ID tenant itself. The following permissions must be included and given consent:

- `AccessReview.ReadWrite.All`
- `AccessReview.ReadWrite.Membership`
- `AdministrativeUnit.ReadWrite.All`
- `Application.ReadWrite.All`
- `Application.ReadWrite.OwnedBy`
- `AppRoleAssignment.ReadWrite.All`
- `CrossTenantInformation.ReadBasic.All`
- `CustomSecAttributeDefinition.ReadWrite.All`
- `CustomSecAttributeAssignment.ReadWrite.All`
- `Directory.ReadWrite.All`
- `Directory.Write.Restricted`
- `Domain.ReadWrite.All`
- `Group.Create`
- `Group.ReadWrite.All`
- `IdentityRiskyUser.ReadWrite.All`
- `Policy.Read.All`
- `Policy.ReadWrite.AccessReview`
- `Policy.ReadWrite.ApplicationConfiguration`
- `Policy.ReadWrite.AuthenticationFlows`
- `Policy.ReadWrite.AuthenticationMethod`

- `Policy.ReadWrite.Authorization`
- `Policy.ReadWrite.ConditionalAccess`
- `Policy.ReadWrite.ConsentRequest`
- `Policy.ReadWrite.CrossTenantAccess`
- `Policy.ReadWrite.ExternalIdentities`
- `Policy.ReadWrite.FeatureRollout`
- `Policy.ReadWrite.FedTokenValidation`
- `Policy.ReadWrite.IdentityProtection`
- `Policy.ReadWrite.PermissionGrant`
- `Policy.ReadWrite.SecurityDefaults`
- `Policy.ReadWrite.TrustFramework`
- `PrivilegedAccess.ReadWrite.AzureAD`
- `PrivilegedAccess.ReadWrite.AzureADGroup`
- `PrivilegedAccess.ReadWrite.AzureResources`
- `PrivilegedAssignmentSchedule.ReadWrite.AzureADGroup`
- `PrivilegedEligibilitySchedule.ReadWrite.AzureADGroup`
- `RoleManagement.ReadWrite.Directory`
- `ServicePrincipalEndpoint.ReadWrite.All`
- `User.EnableDisableAccount.All`
- `User.ManageIdentities.All`
- `User.ReadWrite.All`
- `UserAuthenticationMethod.ReadWrite.All`

Limitations

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

- Only Microsoft 365 and security groups can be backed up and restored. Mail-enabled and distribution groups can only be backed up.

- *For the Microsoft 365 type of groups:* If the Group has no owners, the service principal that handles requests is added automatically.
- If the naming prefixes are specified after the backup, it is not possible to restore the groups that do not match the specification.
- The domains have defined MX or TXT records that need to be verified manually by the customers.
- For the custom security attributes to be restored, the SaaS application that is related to the module that you add as a source to R-Cloud must be assigned at least the Attribute Assignment Reader role.
- Restoring the Publisher domain property of the Application registration is not possible.
- Updates to unverified domains are not allowed.
- Default named locations created by Microsoft Entra ID, such as “All Compliant Network Access”, take priority when restoring and may cause some custom named locations not to be restored.
- The named location Multifactor authentication trusted IPs is only available to be selected if the policy is configured so that it requires Multifactor authentication in the grant options. It is not possible to restore it and a related warning to add it manually will be shown if it was present.
- Compliant Network Locations can only be added if that option is enabled by the user.
- It is not possible to update the PIM status of the Groups.
- MFA must be reenabled after the User granular restore if the User was deleted.
- The restore of an existing user will overwrite current settings.
- When restoring a group that was referenced as a member in another group, the association between the groups is not possible if both groups were deleted.
- User’s photo size is limited to 4 MiB.
- Duplicates can appear for the assignments in the Role itself if the start date is different, because the start time is reset. On the level of the specific objects, the assignments are not duplicated.
- Deleting an Enterprise App that has provisioning enabled and then restoring it, requires the Secret Token to be updated manually on provisioning (when it was defined).

- When restoring the Conditional Access Policy, the relation to apps cannot be restored.
- Sensitive data, such as passwords and certificate data, cannot be backed up.
- All Built-in information, such as the Authentication strength policy and the Default access roles, cannot be restored.
- *For custom security attributes:*
  - After the option “Allow predefined values to be assigned“ is changed from `true` to `false`, it is no longer possible to restore the custom security attribute's values. For example, if during the backup the value is set to `true`, and after the backup the value is manually set to `false`, it cannot be set back to `true` during the restore.
  - Updating active role assignment for the attribute set and expired assignments are not supported.
- During the restore of the Tenant settings for Users, it is not possible to restore the following settings:
  - Administration center
  - LinkedIn account connections
  - Show keep user signed in
  - User features (Users can use preview features for My Apps, Administrators can access My Staff)
  - Collaboration restrictions
- During the restore of the Tenant settings for Groups, it is not possible to restore the Self Service Groups Management settings (Owners can manage group membership requests in My Groups, Restrict user ability to access group features in My Groups)
- If another authentication strength is selected in a conditional access policy, granular restore of the strength policy does not restore the original.
- Eligible assignments are not supported.
- Active role assignments are restored without the schedule information.
- The restore of the user does not add it to application owners, the restore of the application is needed instead.
- If a naming policy is enabled, you cannot restore the groups that do not follow the naming policy.
- Under App registration, the Mobile and desktop applications Redirect URIs toggle value cannot be restored.

- When restoring the Enterprise applications, the SAML SSO optional Verification certificates, the Signing Option, and the Signing Algorithm settings cannot be restored.
- The named locations, the users, and the groups must be granularly restored before the Conditional Access Policies if the policy assignments must be retained after the restore.
- The Conditional Access Policy requires at least one defined named location to enable a successful restore of the Network settings. If not, the Network settings will be restored with a disabled configuration.
- In the Authentication strengths, the present external certificates (Other Certificate Issuers by SubjectKeyIdentifier) cannot be verified. A warning will be reported after restoring the authentication strength.
- The correct order for restoring the Conditional Access settings is to restore the Authentication Strength first, and then to continue with the Policies. This approach prevents the policies from appearing without an Authentication Strength assignment.
- Rate limitations apply. For details about Microsoft Entra ID throttling and rate limits, see Microsoft documentation.
- The following are known limitations by Microsoft:
  - If you delete an application that was mapped to the role with a user, Microsoft retains the mapping relation. To avoid the restore warnings, delete the mapping relations manually before restoring.
  - After the restore, unusual data may appear in the Entra ID dashboard. Most often if stale (deleted, but not refreshed) IDs are involved. The "Refresh" link does not resolve this issue. It is recommended to refresh the browser page instead.

Protecting data

R-Cloud starts protecting your Microsoft Entra ID 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, see *HYCU R-Cloud Help*.

Backing up data

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

Restoring data

R-Cloud allows you to restore your protected Microsoft Entra ID data at the following levels:

- User
- Group
- Application (App registration)
- Custom domain names
- Administrative unit
- Role
- Conditional access policy
- Authentication strengths
- Custom security attributes
- Service principal (Enterprise app)
- Named location
- Tenant
- User settings
- Group settings

For details on how to restore your 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!

www.hycu.com

HYCU®