

# Acronis Cyber Cloud

Integration with Microsoft Entra ID

# Table of contents

- Solution overview ..... 3**
  - Features and capabilities ..... 3
  - Scope and limitations ..... 3
  - Prerequisites ..... 3
  - Adding Acronis Cyber Protect Cloud from the Entra Gallery ..... 4
  - Configuring Single Sign-On ..... 4
    - Advanced configuration ..... 5
  - Activating the Microsoft Entra ID Integration ..... 7
    - Post-activation actions .....11
  - Deactivating the Microsoft Entra ID integration .....13
- Single Sign-On and Single Logout .....16**
  - Single Sign-On .....16
  - Single Logout .....16
    - Enabling Single Logout .....16
    - Disabling Single Logout .....16

# Solution overview

Microsoft Entra ID, formerly known as Microsoft Azure AD, is a cloud-based service for identity and access management. It enables employees within an organization to access external resources utilizing their universal company credentials.

The integration of Acronis Cyber Protect Cloud with Microsoft Entra ID eliminates a need for separate credentials to access Acronis Cyber Protect Cloud. This enhancement not only simplifies the authentication process for users, but also enhances security by mitigating password-related risks.

## Features and capabilities

- **Single Sign-On (SSO) and Single Logout (SLO):** The integration enables users to access Acronis Cyber Protect Cloud using their universal company credentials, removing the necessity for a separate credentials. Additionally, it allows for centralized logout when the session terminates.
- **Multi-factor authentication support:** The integration seamlessly works with the multi-factor authentication status in Microsoft Entra ID, automatically suppressing the second-factor challenge by Acronis Cyber Protect Cloud if Microsoft Entra ID multi-factor authentication has been successfully completed.

## Scope and limitations

- The integration can be enabled at the level of a partner tenant in Acronis Cyber Protect Cloud.
- Identifier of the Acronis Cyber Protect Cloud application in the Microsoft Entra admin center is a fixed string value, unique per an Acronis datacenter. This practically means that only one instance of the application can be configured in one Entra tenant per one Acronis datacenter.
- The functionality to provision users from Microsoft Entra to Acronis Cyber Protect Cloud awaits review and publication by Microsoft. Once approved, it will be made available for immediate use.

## Prerequisites

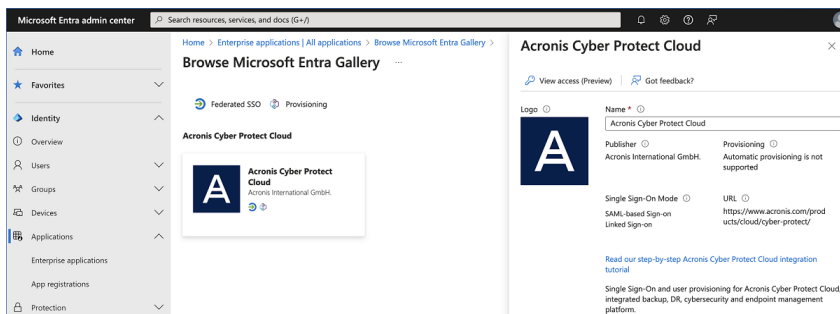
To integrate Microsoft Entra ID with Acronis Cyber Protect Cloud, you need to have:

- A Microsoft Entra subscription.
- A Microsoft Entra user account with one of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.
- An Acronis Cyber Protect Cloud subscription. You can subscribe for a [free 30-day trial](#).
- An Acronis Cyber Protect Cloud partner tenant.
- An Acronis Cyber Protect Cloud user account with the Company Administrator role.

# Adding Acronis Cyber Protect Cloud from the Entra Gallery

To configure the integration of Acronis Cyber Protect Cloud into Microsoft Entra ID, you need to add the Acronis Cyber Protect Cloud application from the gallery to your list of managed SaaS apps.

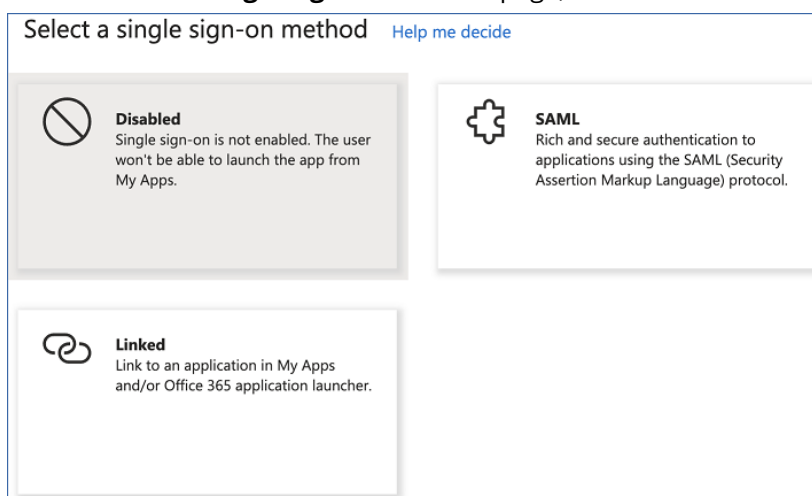
1. Sign in to the [Microsoft Entra admin center](#) as at least a [Cloud Application Administrator](#).
2. Browse to **Identity** → **Applications** → **Enterprise applications** → **New application**.
3. Type Acronis Cyber Protect Cloud in the search box.
4. Select Acronis Cyber Protect Cloud from results panel and then add the app.



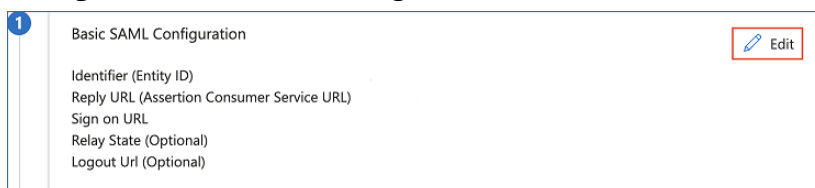
## Configuring Single Sign-On

Follow these steps to enable and configure the Microsoft Entra single sign-on for the Acronis Cyber Protect Cloud application within the Microsoft Entra admin center:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Cloud Application Administrator](#).
2. Browse to **Identity** → **Applications** → **Enterprise applications** → **Acronis Cyber Protect Cloud** → **Single sign-on**.
3. On the **Select a single sign-on method** page, select **SAML**.



4. On the **Set up single sign-on with SAML** page, click the **Edit** button for **Basic SAML Configuration** to edit the settings.



1 Basic SAML Configuration Edit

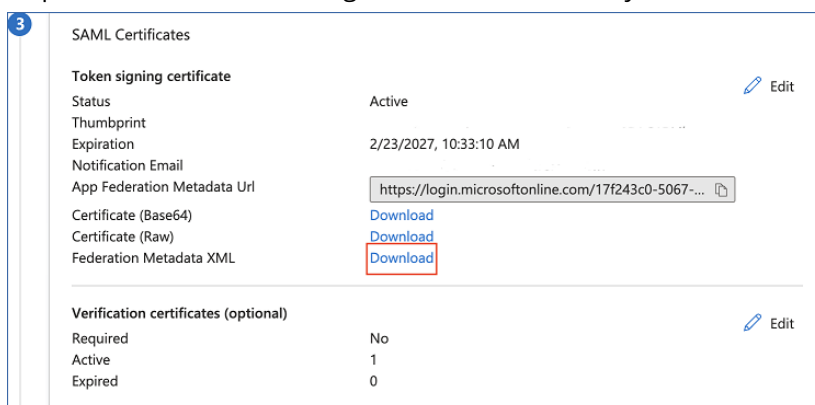
Identifier (Entity ID)  
Reply URL (Assertion Consumer Service URL)  
Sign on URL  
Relay State (Optional)  
Logout Url (Optional)

5. Copy the values for the following mandatory fields from the Microsoft Entra ID integration wizard in Acronis Cyber Protect Cloud console and paste them accordingly:

- **Identifier (Entity ID)**
- **Reply URL (Assertion Consumer Service URL)**

Optionally, copy the value of the Logout URL from the Microsoft Entra ID integration wizard in Acronis Cyber Protect Cloud console and paste it in the Logout Url field. This setting is required to enable the Single Logout function for the Acronis Cyber Protect Cloud application, namely the application will be able to receive a logout request from Microsoft Entra ID and end the session accordingly.

6. On the **Set up Single Sign-On with SAML** page, in the **SAML Signing Certificate** section, click **Download** to download the **Federation Metadata XML** and save it to be used later. This file is required to activate the integration in the Acronis Cyber Protect Cloud console.



3 SAML Certificates Edit

Token signing certificate

Status Active

Thumbprint

Expiration 2/23/2027, 10:33:10 AM

Notification Email

App Federation Metadata Url <https://login.microsoftonline.com/17f243c0-5067-...>

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional) Edit

Required No

Active 1

Expired 0

7. Finalize the integration activation in the Acronis Cyber Protect Cloud console following the instructions in section [Activating the Microsoft Entra ID integration](#).

## Advanced configuration

### Enforcing signed SAML authentication

Microsoft Entra ID can be configured to validate requests against the public key provided in Acronis Cyber Protect Cloud application settings in Microsoft Entra admin center.

---

## Important

When enabled, this functionality works for SP-initiated authentication requests only, causing IDP-initiated authentication requests (like SSO testing feature, the MyApps portal or the Microsoft 365 app launcher) to fail.

---

### *To enforce signed requests*

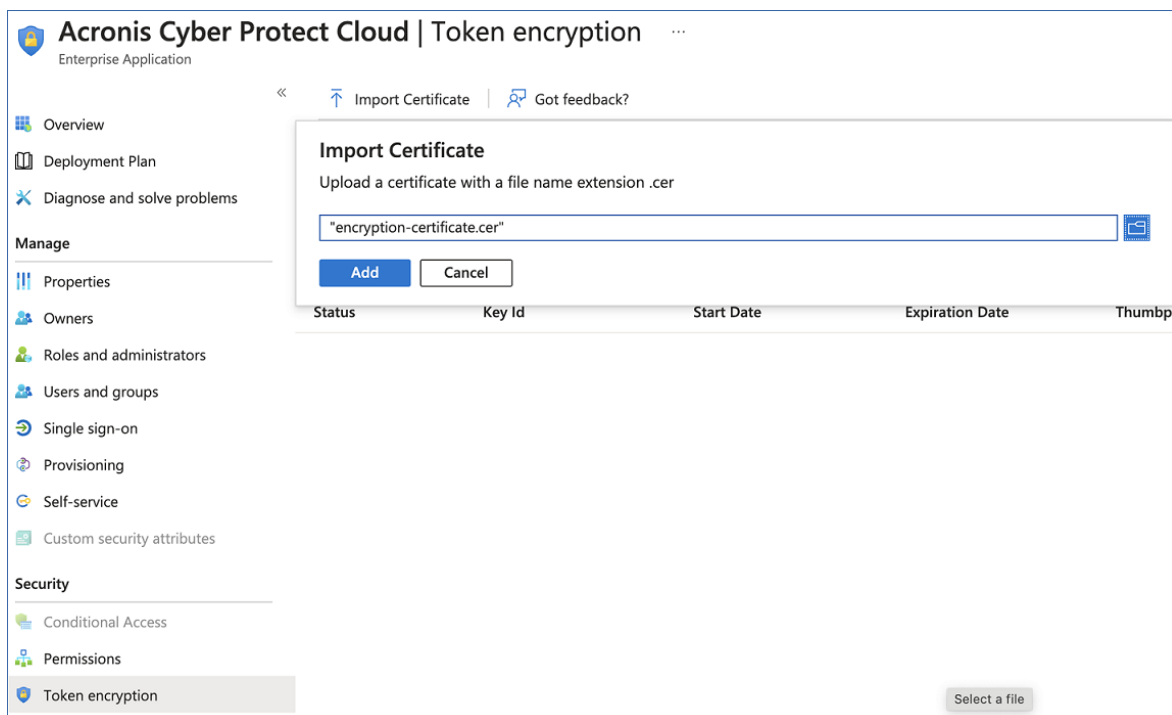
1. Download the verification certificate from the integration settings page in Acronis Cyber Protect Cloud following the instructions in section [Activating the Microsoft Entra ID integration](#).
2. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator.
3. Browse to **Identity → Applications → Enterprise applications → All applications**.
4. Type Acronis Cyber Protect Cloud in the search box, and then select the application from the search results.
5. Navigate to **Single sign-on** and scroll down to the subsection called Verification certificates under SAML Certificates.
6. Click **Edit** to open the **Verification certificates**.
7. Select the **Require verification certificates** checkbox and upload the downloaded verification certificate.
8. Click **Save** to apply the changes.

## Enabling token encryption

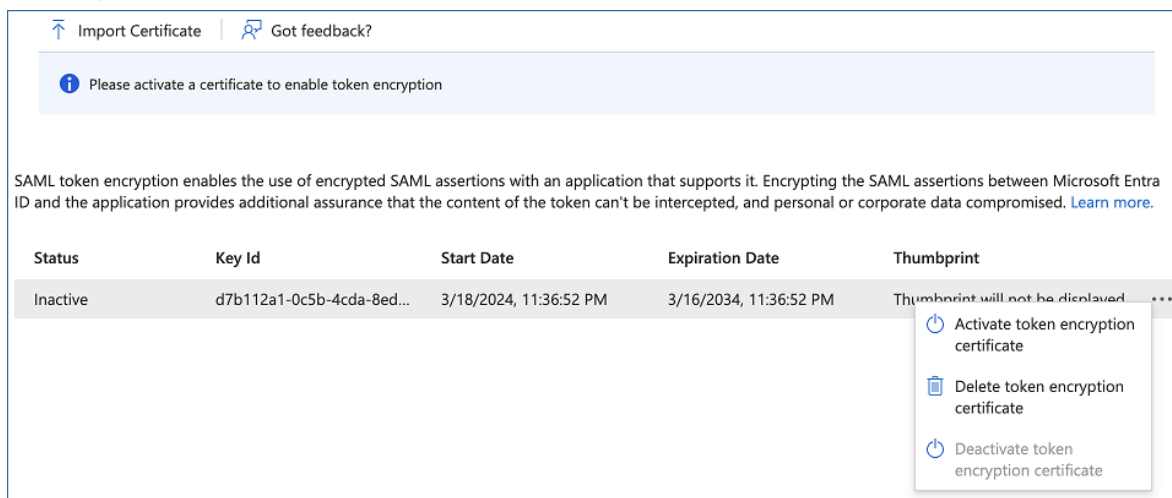
SAML token encryption is a security feature that allows encrypted SAML assertions to be used between Microsoft Entra ID and Acronis Cyber Protect Cloud. This provides an extra layer of security to ensure that the contents of the token cannot be intercepted by unauthorized parties. To enable token encryption, you will need to upload an X.509 certificate file containing the public key to the Acronis Cyber Protect Cloud application within the Microsoft Entra admin center. You can download this certificate by visiting the Microsoft Entra ID integration settings page in Acronis Cyber Protect Cloud

### *To add the public certificate to the Acronis Cyber Protect Cloud application within the Microsoft Entra admin center*

1. Download the encryption certificate from the integration settings page in Acronis Cyber Protect Cloud following the instructions in section [Activating the Microsoft Entra ID integration](#).
2. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator.
3. Browse to **Identity → Applications → Enterprise applications → All applications**.
4. Type Acronis Cyber Protect Cloud in the search box, and then select the application from the search results.
5. On the application's page, select **Token encryption**.
6. On the **Token encryption** page, select Import Certificate to import the downloaded .cer file that contains a public X.509 certificate.



- Once the certificate is imported, activate the encryption by selecting the ... option, next to the thumbprint status, and then select **Activate token encryption certificate** from the options in the drop-down menu.



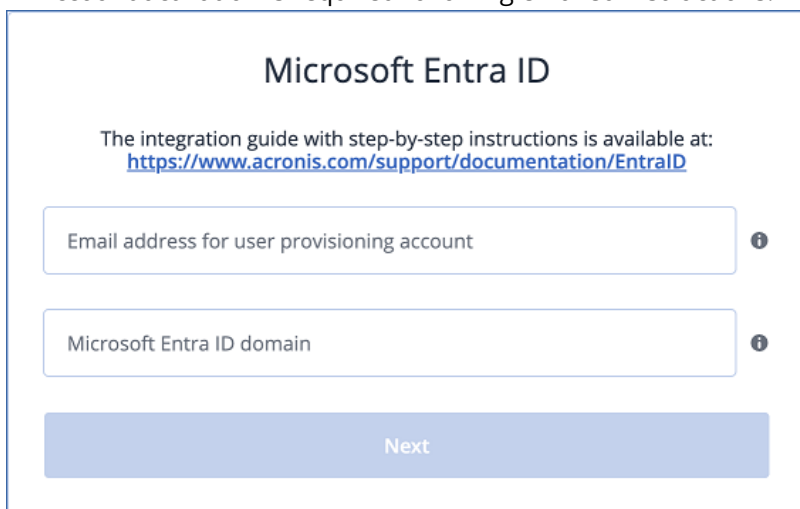
- Select **Yes** to confirm activation of the certificate.

## Activating the Microsoft Entra ID Integration

To activate and configure the integration of Microsoft Entra ID within Acronis Cyber Protect Cloud, you need to enable the Microsoft Entra ID integration in the INTEGRATIONS section of the management console, and then follow the configuration wizard:

- Sign in to Acronis Cyber Protect Cloud Management Console as a Company Administrator.
- Navigate to the **INTEGRATIONS** section.

3. Type **Microsoft Entra ID** in the Search box.
4. Locate **Microsoft Entra ID** in the search results, and then click **Configure** on the corresponding tile.
5. The integration configuration wizard opens. Enter the following values and click **Next** to proceed to the next step.
  - **Microsoft Entra ID domain** - The unique Microsoft Entra ID domain name for your organization within the Microsoft Entra admin center.
  - **Email address for the user provisioning account** - An email associated with a service user account that will be automatically created upon integration activation. The account will be used exclusively to provision users from the Microsoft Entra to Acronis Cyber Protect Cloud. Account activation is required following emailed instructions.



**Microsoft Entra ID**

The integration guide with step-by-step instructions is available at:  
<https://www.acronis.com/support/documentation/EntraID>

Email address for user provisioning account ⓘ

Microsoft Entra ID domain ⓘ

Next

6. Copy the values of the following fields, because these will be required in the next steps of the integration configuration:
  - **Identifier (Entity ID)**
  - **Reply URL (Assertion Consumer Service URL)**
  - **Logout URL**



## Microsoft Entra ID

Set up an Acronis application in the Microsoft Entra ID portal using the information below.

Identifier (Entity ID):  
**urn:cyber:protect:saml:ci-gdt2**

Reply URL (Assertion Consumer Service URL):  
**https://mc-ci-gdt2.public.acronis.dev/api/2/saml/callback**

Logout URL:  
**https://mc-ci-gdt2.public.acronis.dev/api/2/saml/logout**

Encryption certificate:[Click here to download](#)

Verification certificate:[Click here to download](#)

Enter the **App Federation Metadata** and the **Logout redirect URL** (optionally) to complete the setup process.

App Federation Metadata  
app\_metadata.xml

X

Browse files...

i

Logout redirect URL (optional)

i

Activate

- Open a new browser tab or windows, and sign in to the [Microsoft Entra admin center](#) as at least a [Cloud Application Administrator](#) and paste the values copied in the previous step in the corresponding fields in the **Basic SAML Configuration** section of the Acronis Cyber Protect Cloud application. Then download the **Federation Metadata XML** file.

1

### Basic SAML Configuration

Edit

Identifier (Entity ID)	urn:cyber:protect:saml:ci-gdt2
Reply URL (Assertion Consumer Service URL)	https://mc-ci-gdt2.public.acronis.dev/api/2/saml/callback
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://mc-ci-gdt2.public.acronis.dev/api/2/saml/logout

2

### Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

### SAML Certificates

Token signing certificate	
Status	Active
Thumbprint	EBD5EB2022417ED47E8E005919128B49BD7C1DA7
Expiration	2/23/2027, 10:33:10 AM
Notification Email	vstestuser1@3drnbt.onmicrosoft.com
App Federation Metadata Url	<div>https://login.microsoftonline.com/17f243c0-5067-... </div>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

Please refer to [Configuring Microsoft Entra Single Sign-On](#) for further instructions.

- Return to the integration configuration wizard and upload the downloaded App Federation Metadata file.

## Microsoft Entra ID

Set up an Acronis application in the Microsoft Entra ID portal using the information below.

Identifier (Entity ID):  
**urn:cyber:protect:saml:ci-gdt2**

Reply URL (Assertion Consumer Service URL):  
**https://mc-ci-gdt2.public.acronis.dev/api/2/saml/callback**

Logout URL:  
**https://mc-ci-gdt2.public.acronis.dev/api/2/saml/logout**

Encryption certificate: [Click here to download](#)

Verification certificate: [Click here to download](#)

Enter the **App Federation Metadata** and the **Logout redirect URL** (optionally) to complete the setup process.

App Federation Metadata
×
Browse files...
?

app\_metadata.xml

Logout redirect URL (optional)
?

**Activate**

9. As an optional step, specify the URL to redirect users after successfully logging out of Acronis Cyber Protect Cloud. This value is required only if you need to disable the single logout functionality for your Acronis Cyber Protect Cloud application. If left empty, the application will broadcast a LogoutRequest to all applications in the same Microsoft Entra ID session to initiate a single logout. If you are unsure, leave the field empty. You will be able to specify the redirect URL anytime in the future.
10. Click **Activate** to enable Microsoft Entra ID as the default identity provider for the tenant and activate Entra SSO to access Acronis Cyber Protect Cloud.

## Post-activation actions

After successful activation and configuration of the integration, you can take the following post-activation actions:


- Review and modify the integration settings.
- Switch existing user accounts to sign in through Microsoft Entra ID.

## Reviewing and modifying the integration settings

**To review and modify integration settings, follow these steps**

1. Sign in to Acronis Cyber Protect Cloud Management Console as a Company Administrator.
2. Navigate to the **INTEGRATIONS** section and type **Microsoft Entra ID** in the search box.

3. Locate **Microsoft Entra ID** in the search results and then click **Configure** on the corresponding tile.
4. Navigate to the **INTEGRATION SETTINGS** page, to see the configuration options.

Connection details 	
App Federation Metadata ⓘ	<a href="#">Click here to download</a>
Logout redirect URL ⓘ	
Static connection details	
Email address of user provisioning account	[redacted]
Microsoft Entra ID domain	[redacted].ccsctp.net
Identifier (Entity ID)	urn:cyber:protect:saml:ci-gdt2
Encryption certificate:	<a href="#">Click here to download</a>
Verification certificate:	<a href="#">Click here to download</a>

5. On the **INTEGRATION SETTINGS** page, you can do the following:

- Download the encryption certificate
- Download the verification certificate
- Download the saved App Federation Metadata file
- Upload a new App Federation Metadata XML file

## Switching existing users

To ensure better predictability, when you enable the integration, user accounts that are already registered within the tenant will not be automatically switched to using Microsoft Entra ID. This is done to preserve their direct access to Acronis Cyber Protect Cloud. If the administrator chooses to do so, existing user accounts with direct access can be switched to using Microsoft Entra ID after the integration is enabled and configured.

### Important

Switching the sign-on method of existing user accounts to Microsoft Entra ID will temporarily suspend their access to Acronis Cyber Protect Cloud. This is because the corresponding user accounts will need to be provisioned to the connected Acronis Cyber Protect Cloud application within the [Microsoft Entra admin center](#).

### ***To switch existing user accounts with direct access to Acronis Cyber Protect Cloud to using Microsoft Entra ID***

1. Sign in to Acronis Cyber Protect Cloud Management Console as a Company Administrator.
2. Navigate to the **INTEGRATIONS** section and type **Microsoft Entra ID** in the search box.

3. Locate **Microsoft Entra ID** in the search results and then click **Configure** on the corresponding tile.
4. Navigate to the **INTEGRATION SETTINGS** page, to see the configuration options. If you have the user accounts permitted to sign in to Acronis Cyber Protect Cloud without using Microsoft Entra ID, you will have displayed the **Switch existing users to Microsoft Entra ID** button on this page.

Connection details	
App Federation Metadata ⓘ	<a href="#">Click here to download</a>
Logout redirect URL ⓘ	
The tenant has users with direct access to Acronis Cyber Protect Cloud.	<b>Switch existing users to Microsoft Entra ID</b>

Static connection details	
Email address of user provisioning account	<a href="#">Click here to download</a>
Microsoft Entra ID domain	aad168.ccsctp.net
Identifier (Entity ID)	urn:cyber:protect:saml:ci-gdt2
Encryption certificate:	<a href="#">Click here to download</a>
Verification certificate:	<a href="#">Click here to download</a>

5. Click the **Switch existing users to Microsoft Entra ID** button.
6. Click **Confirm**.

## Deactivating the Microsoft Entra ID integration

If you deactivate the Microsoft Entra ID integration, user accounts registered in your tenant will continue to exist in Acronis Cyber Protect Cloud. Although they will no longer be able to sign in with their Microsoft Entra ID credentials, they will still be able to gain access to Acronis Cyber Protect Cloud credentials by using the password reset functionality for the account.

If your objective is to revoke access to Acronis Cyber Protect Cloud for users in your organization, it is recommended to manage user access directly in the Microsoft Entra admin center. You can either remove users from the application or delete the application altogether.

---

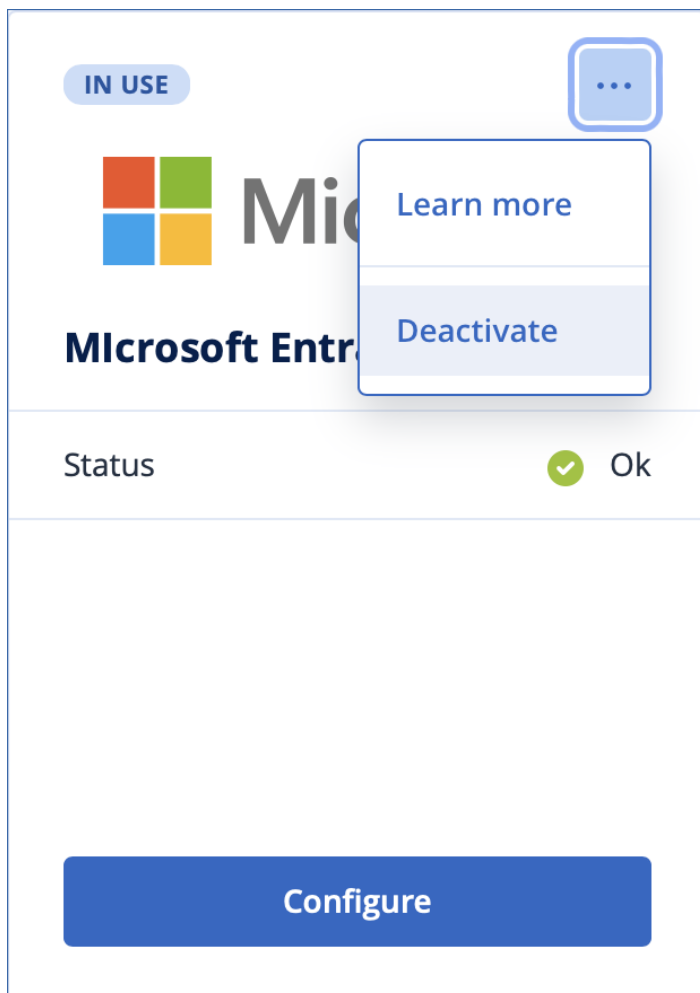
### Note

After deactivating the integration, administrators still have the option to reactivate it using the standard flow. This can be done without the need to recreate the Acronis Cyber Protect Cloud application in the Microsoft Entra admin center.

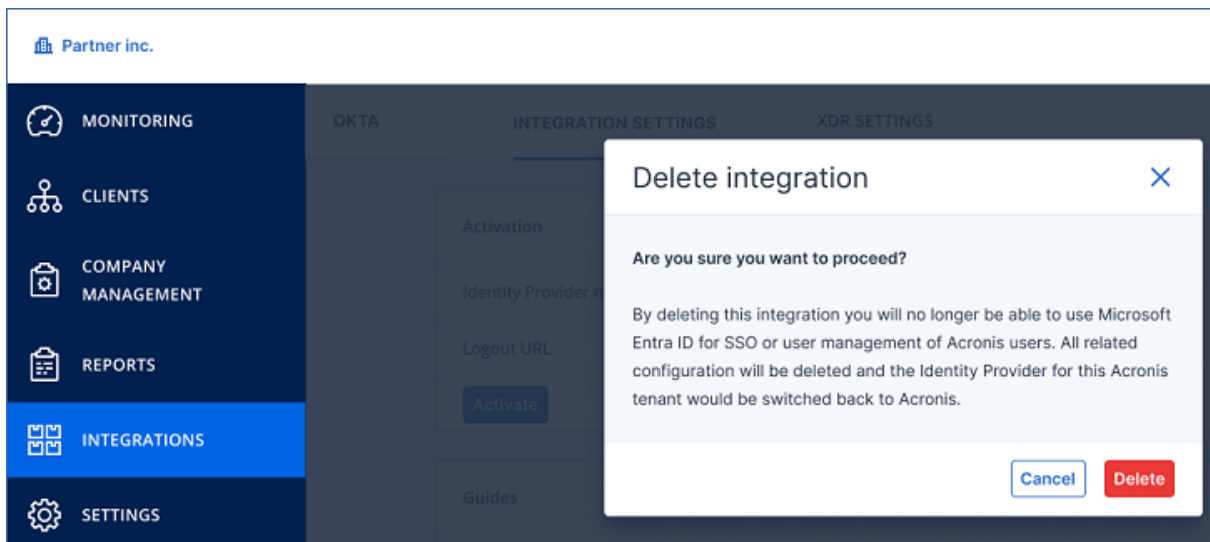
---

### ***To deactivate the Microsoft Entra ID integration***

1. Sign in to Acronis Cyber Protect Cloud Management Console as a Company Administrator.
2. Navigate to **INTEGRATIONS** section.
3. Type **Microsoft Entra ID** in the search box.
4. Locate **Microsoft Entra ID** in the search results and then find and click the **Deactivate** button on the corresponding tile to initiate the integration deactivation process.



5. The **Delete integration** pop up window opens. Click **Delete** to confirm that you want to proceed with the integration deactivation.



After you confirm the deactivation process for the integration, the system will take the following actions:

- It will disable the Microsoft Entra ID identity provider for the respective tenant.
- It will switch the default sign-on method for the tenant and all user accounts registered within the tenant back to Acronis credentials.
- It will delete the user provisioning account linked to the integration.

# Single Sign-On and Single Logout

## Single Sign-On

By authenticating with Microsoft Entra ID using their universal corporate credentials, users seamlessly gain access to Acronis Cyber Protect Cloud without entering any platform-specific credentials.

The integration supports two single sign-on (SSO) options:

- **SP-initiated SSO:** Users initiate the sign-on process through one of the available Acronis Cyber Protect Cloud login pages: [cloud.acronis.com](https://cloud.acronis.com) or [<dc-name>.acronis.com](https://<dc-name>.acronis.com).
- **IDP-initiated SSO:** Users initiate the sign-on process through various Microsoft resources, such as the [MyApps Portal](#) and the [Microsoft 365 app launcher](#).

---

### Important

IDP-initiated SSO is not compatible with [signed SAML authentication](#).

---

## Single Logout

The Acronis Cyber Protect Cloud integration with Microsoft Entra ID ensures seamless Single Logout (SLO) functionality, supporting both SP-initiated and IDP-initiated SAML SLO processes. This feature guarantees that logging out of the Acronis Cyber Protect Cloud triggers a corresponding logout from Microsoft Entra ID and any other connected applications, and vice versa.

- In **SP-initiated SLO**, when a user logs out of the Acronis Cyber Protect Cloud console, the Acronis application notifies Microsoft Entra ID and any other connected applications about the session termination.
- Conversely, in **IDP-initiated SLO**, when a user logs out of Microsoft Entra ID or any connected application supporting SLO, the Acronis application receives a logout request from Microsoft Entra ID, leading to the termination of the corresponding Acronis Cyber Protect Cloud session.

## Enabling Single Logout

To enable both SP-initiated and IDP-initiated SLO, it is essential to specify the Logout URL in the Acronis Cyber Protect Cloud application's single sign-on settings in the Microsoft Entra admin center (see instructions in section "Configuring Single Sign-On" (p. 4) for details). If this URL is missing or incorrect, communication failures will occur, resulting in users remaining logged into the Acronis Cyber Protect Cloud even after logging out of Microsoft Entra ID.

## Disabling Single Logout

Disabling IDP-initiated SLO for the Acronis Cyber Protect Cloud, it is enough to leave the Reply URL value empty. Disable SP-initiated SLO involves specifying a Logout redirect URL in the integration configuration settings (see "Post-activation actions" (p. 11) for details).