

Acronis Cyber Cloud

1.0.1

Integration with Microsoft Intune

Table of contents

Introduction	3
Integration permissions	3
Prerequisites	5
Acronis URL branding limitation	6
Activating the integration	8
Opening the integration	9
Managing tenants	10
Mapping a tenant	10
Granting admin consent permissions	11
Viewing tenant mapping info	14
Deleting a mapping	15
Performing actions	17
Installing the Acronis agent	17
Applying a protection plan	23
Uninstalling Acronis agent	27
Checking the last action	31
Created objects	33
Objects created in Acronis	33
Objects created in customer Microsoft Entra ID	34
Objects created in customer Microsoft Endpoint Manager	35
Deactivating the integration	37
Troubleshooting Intune PowerShell scripts	38

Introduction

Microsoft Intune is a cloud-based endpoint management solution that allows organizations to manage and secure apps and devices from a single console. It helps protect company data on company-owned devices, offering features like app management, device enrollment, compliance policies, and reporting.

This guide describes how to activate and configure the integration of Acronis Cyber Cloud with Intune so you can:

- Establish mapping between Acronis customer tenant and Microsoft Entra ID tenant.

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

- Perform activities on mapped tenant devices which are enrolled in customer Intune:
 - Deploy Acronis agent.
 - Apply protection plan.
 - Uninstall Acronis agent.

Note

These operations are performed by PowerShell scripts, created by the integration in the customers' Intune space. This is achieved using Microsoft Graph API.

Integration permissions

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

The integration can perform these operations:

- Deploy Acronis agent.
- Apply protection plan.
- Uninstall Acronis agent.

In order to do this, the integration needs permissions to access API objects and execute API calls:

- Access basic tenant information.
- Read the devices list.
- Read the list of Microsoft Entra ID groups.

- Create Microsoft Entra ID groups.
- Create Intune PowerShell scripts.

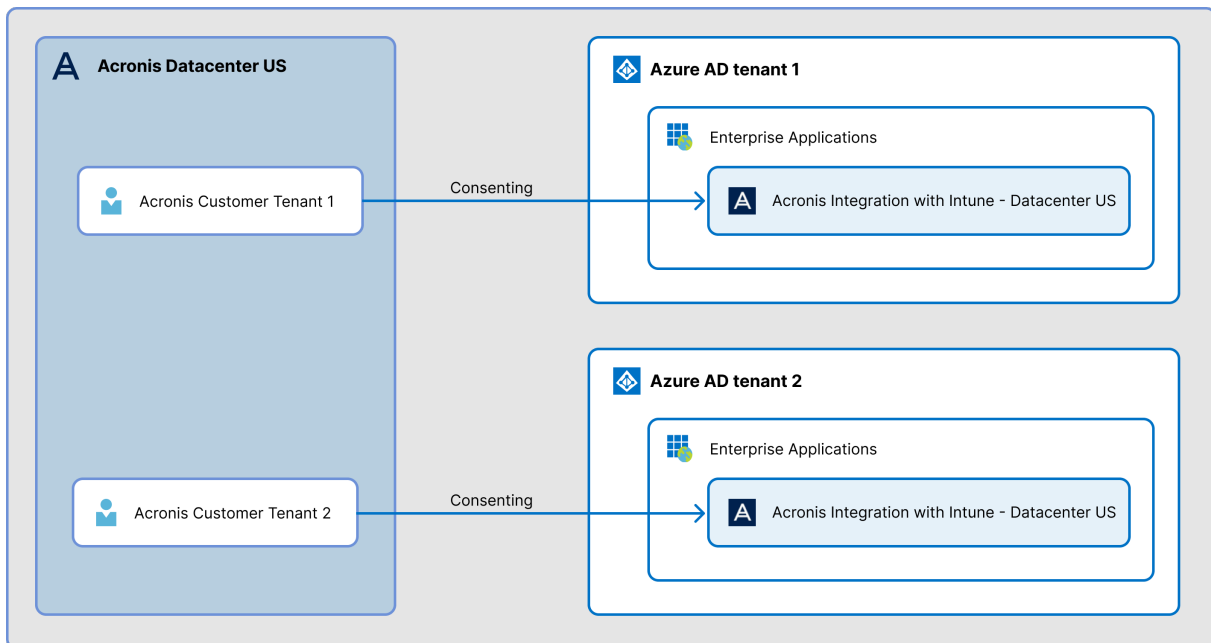
These permissions must be granted for every Microsoft Entra ID tenant you want to manage through the integration.

Note

The process of granting permissions is referred to as 'admin consent'. It is part of the integration tenant mapping wizard.

For more information, see [Managing Tenants](#).

The admin consent process will result in the creation of an enterprise application object (or service principal) in the customer tenant's Microsoft Entra ID directory. The name of this object is **Integration with Intune - (Datacenter)**. It can be found under the Enterprise applications blade in the Microsoft Entra ID portal of the customer tenant.



For more information, see <https://learn.microsoft.com/entra/identity-platform/app-objects-and-service-principals?tabs=browser>

Prerequisites

Note

Due to a Microsoft limitation, the integration must use the standard Acronis data center URL.

This means that, for this integration to function correctly, you cannot configure the Acronis branded **URL for Acronis Cyber Cloud services** feature. For more information, see [Acronis URL branding limitation](#).

- You must have a fully configured Acronis Cyber Cloud partner tenant account.
- The user account that you use to activate and configure the integration must be a Company Administrator.
- You must not have disabled support access.

Note

For more information, see [the Management Portal Partner Administrator guide](#).

- [Optional] One or more customer tenants.

Note

Only customer tenants that are provisioned as **Managed by service provider** will appear as active for mapping.

Management mode ⓘ

<input checked="" type="radio"/> Managed by service provider <ul style="list-style-type: none">✓ Manage protection for the customer✓ Access backups and other resources	<input type="radio"/> Managed by customer <ul style="list-style-type: none">✗ Manage protection for the customer✗ Access backups and other resources
---	--

-
- [Optional] One or more protection plans.

Acronis customer tenants can be mapped to Microsoft Entra ID tenants that comply with the following requirements:

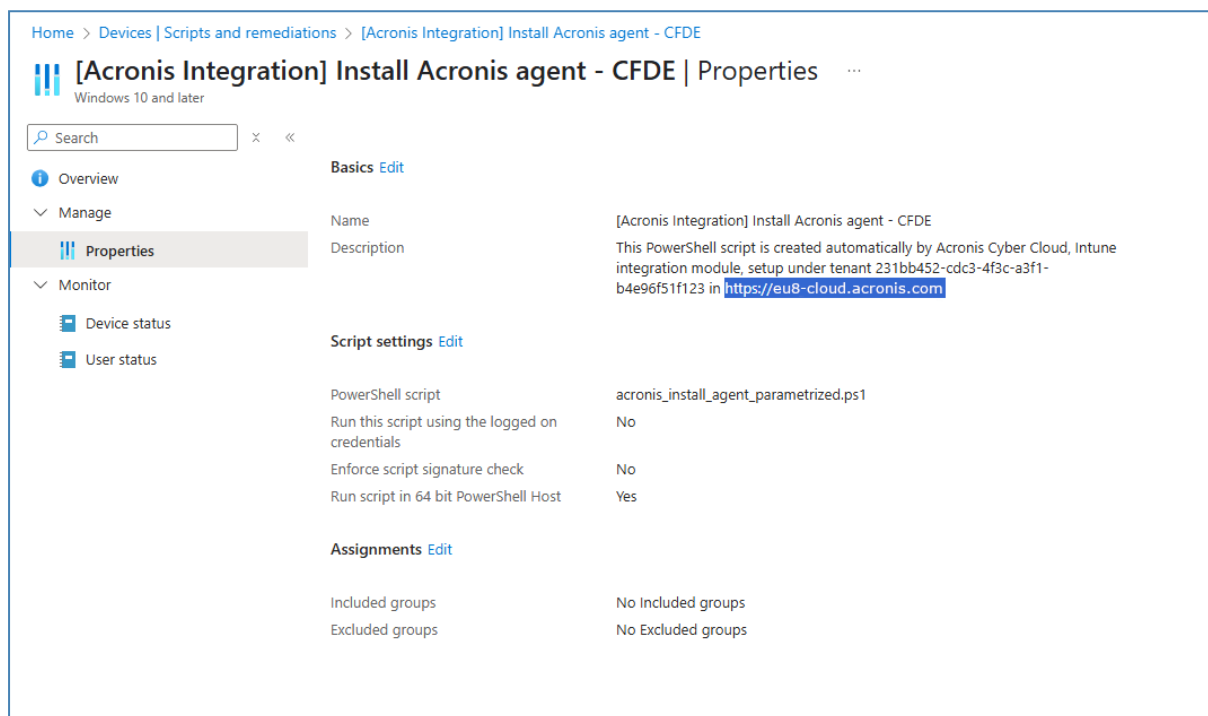
- Microsoft Entra ID tenants must have an active subscription with a license including Intune. For more information, see <https://docs.microsoft.com/mem/intune/fundamentals/licenses>.
- Microsoft Entra ID tenants must have a user with the following permissions (also referred to as an admin user in this document):
 - Global Administrator
 - Intune Service Administrator (also known as Intune Administrator)
- The admin user must have an Intune license assigned. For more information, see <https://docs.microsoft.com/mem/intune/fundamentals/licenses-assign>.
- One or more devices should be enrolled in the Microsoft Entra ID tenant endpoint manager. For more information, see <https://docs.microsoft.com/mem/intune/enrollment/>.

Important

The integration currently supports Windows 32-bit and 64-bit devices. Support for macOS devices will be added in future versions.

Acronis URL branding limitation

When the integration creates PowerShell scripts in Intune, it uses the Acronis Cyber Cloud services URL.



Due to a Microsoft limitation, this integration must use the standard Acronis data center URL. This means that, for this integration to function correctly, you cannot configure the Acronis branded **URL for Acronis Cyber Cloud services** feature.

Note

There is no need to disable other custom branding settings.

For more information on Acronis branding features, see [the Management Portal Partner Administrator guide](#).

DemoPartner

+ New

CLIENTS

MONITORING

REPORTS

MY COMPANY

INTEGRATIONS

SETTINGS

Locations

Branding

API clients

Acronis
Cyber Protect Cloud

Powered by Acronis Cyber Platform

Documentation and support

Home URL	https://www.demo-msp.com	
Support URL	https://www.demo-msp.com/support/	
Support phone	0800-999-9999	
Knowledge base URL	https://care.demo-msp.com/s/submit-ticket-for...	
Management Portal administrator's guide	https://ww.demo-msp.com/adminguide.pdf	
Management Portal administrator's help	https://www.demo-msp.com/adminguide-online	

URL for Acronis Cyber Protect Cloud services

You can make Acronis Cyber Protect Cloud services accessible at a URL of your choice, such as cloud.example.com.

Configure

Activating the integration

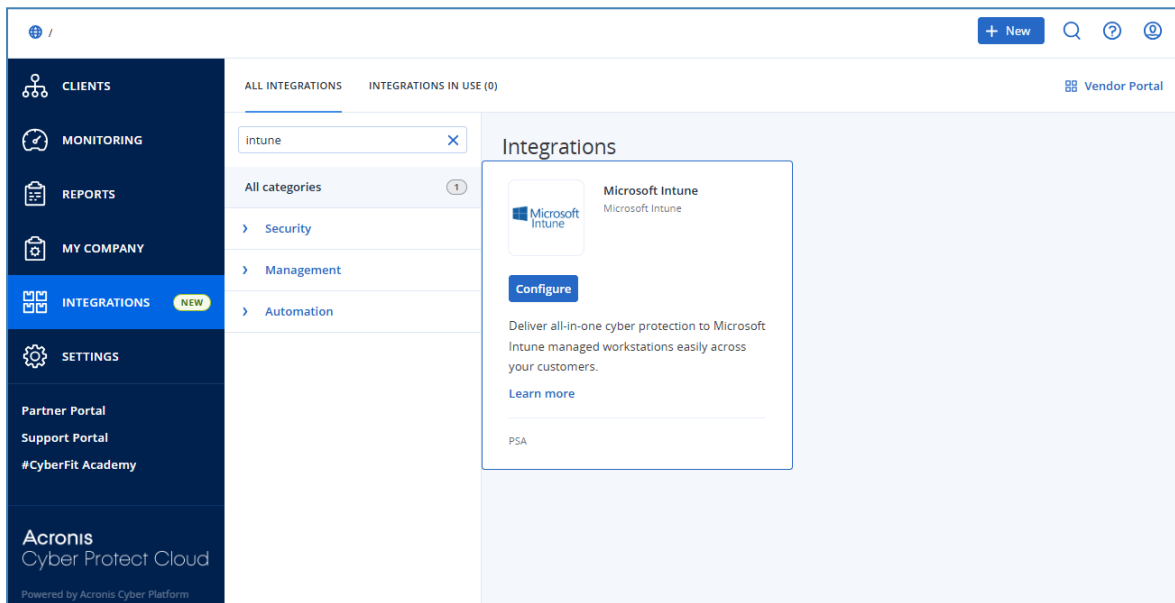
To activate the integration

1. Log in to Acronis Management Portal.
2. Click **INTEGRATIONS**.
3. Search for the Microsoft Intune catalog card.

Note

For more information, see [the Management Portal partner administrator guide](#).

4. Hover over the Microsoft Intune catalog card and click **Configure**.



The welcome screen appears.

5. Click **Continue**.
6. Click **Map** to start mapping Acronis customer tenants to Microsoft Entra ID tenants.

Opening the integration

To open the integration

1. Log in to Acronis Management Portal as administrator.
2. Select **INTEGRATIONS** on the main menu.
3. Select the **INTEGRATIONS IN USE** tab.
4. Locate the Microsoft Intune integration catalog card.

Note

For more information, see [the Management Portal partner administrator guide](#).

5. Click **Manage**.

Managing tenants

Mapping a tenant

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

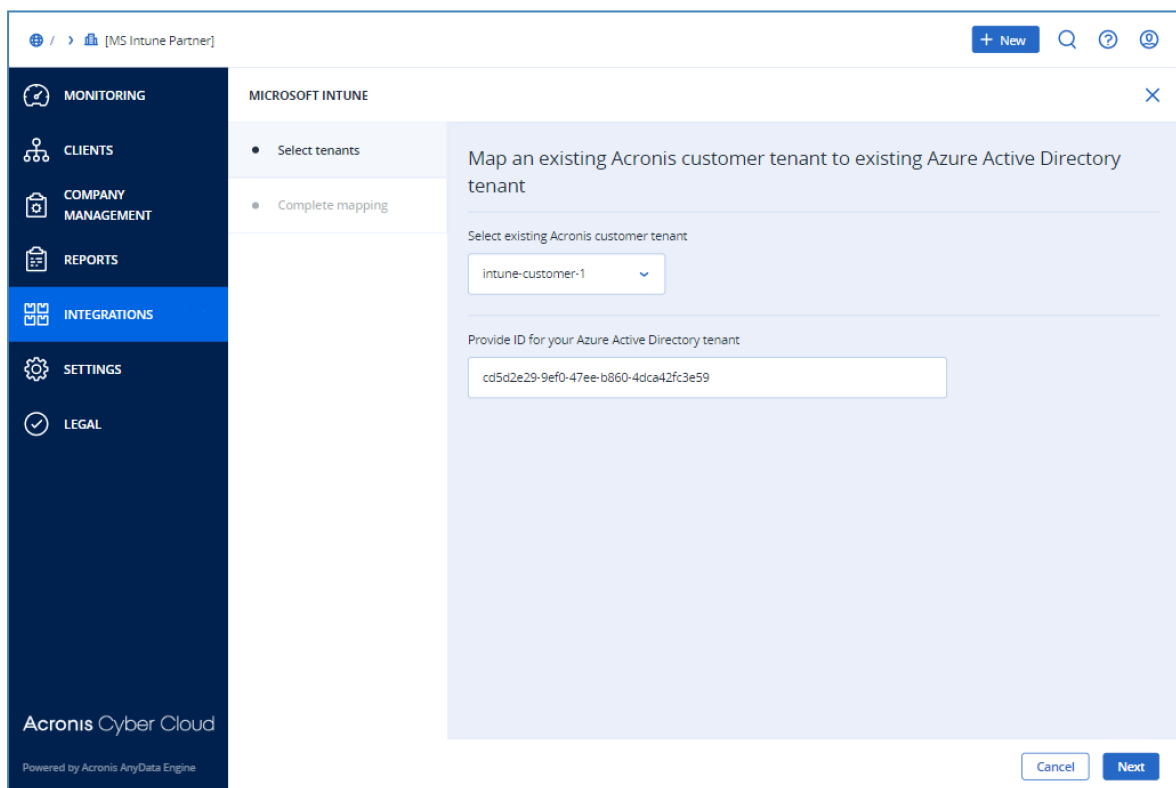
To map a tenant

1. [Open the integration](#).
2. Click the **Add Azure AD tenant** button.
3. Choose the existing Acronis customer tenant you want to map.

Note

Make sure the tenant has at least one active user with a **Company administrator** role.

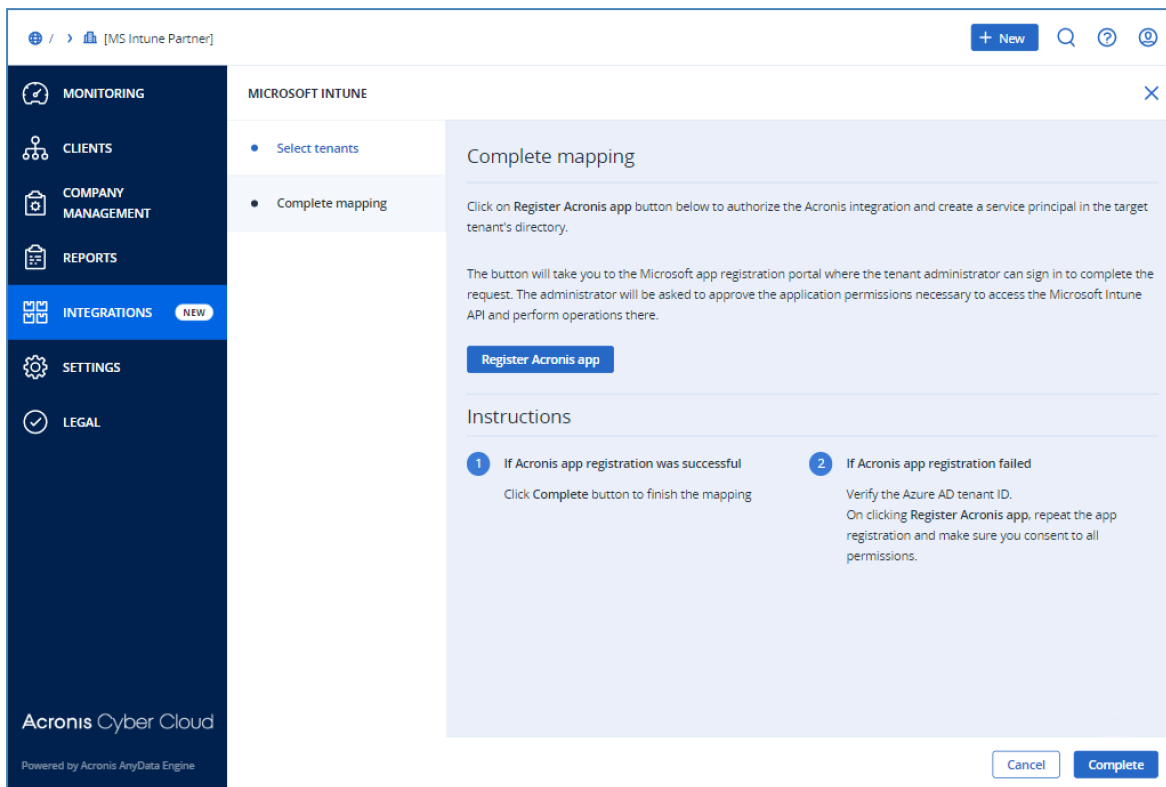
4. Enter the Microsoft Entra ID tenant ID of the customer you want to map.
5. Click **Next**.



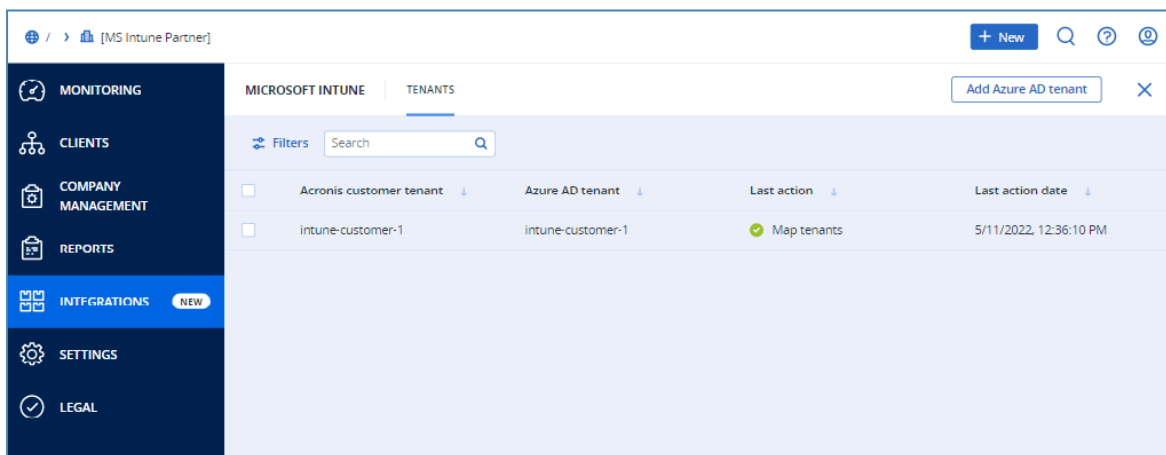
The screenshot shows the Acronis Cyber Cloud interface. On the left is a dark blue sidebar with navigation links: MONITORING, CLIENTS, COMPANY MANAGEMENT, REPORTS, INTEGRATIONS (highlighted), SETTINGS, and LEGAL. The main content area is titled 'MICROSOFT INTUNE' and has a close button (X) in the top right. Below the title are two steps: 'Select tenants' (active) and 'Complete mapping'. The 'Select tenants' step contains a dropdown menu labeled 'Select existing Acronis customer tenant' with 'intune-customer-1' selected. The 'Complete mapping' step contains a text input field labeled 'Provide ID for your Azure Active Directory tenant' with the value 'cd5d2e29-9ef0-47ee-b860-4dca42fc3e59'. At the bottom right are 'Cancel' and 'Next' buttons. The footer of the sidebar reads 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'.

6. Click **Register Acronis app**.
A new browser tab opens and triggers the Microsoft Entra ID admin consent process.
For more information, see [Granting admin consent permissions](#).

7. When the Microsoft Entra ID admin consent process has finished, click **Complete**.
The wizard closes.



The new mapping is in the tenants list. The **Last action** status is **Map tenants**.



Granting admin consent permissions

In order for the Acronis integration to access Microsoft Entra ID and Intune resources of customer tenants through API, it needs permission. Permissions are granted through the admin consent process.

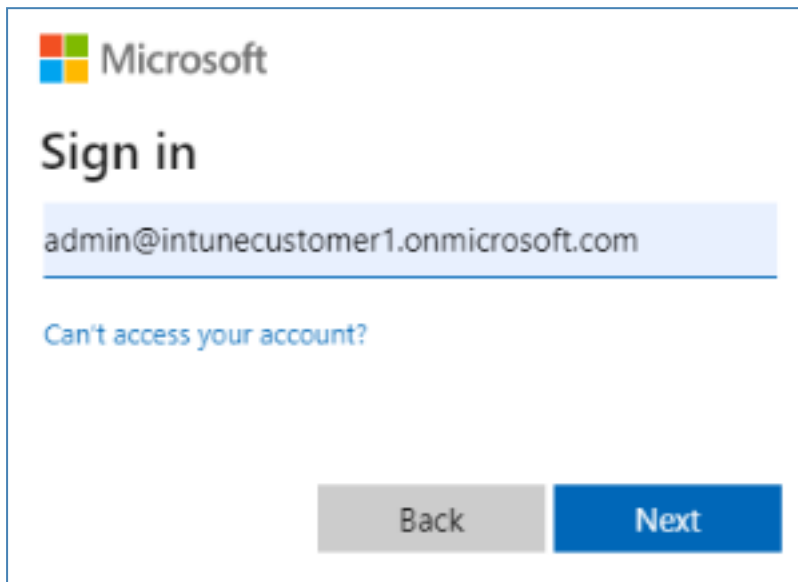
To grant admin consent permissions

1. [Open the integration.](#)
2. Click either:

- **Register Acronis app** in the tenant mapping wizard.
- **Re-authorize Acronis app** in the mapping info dialog.

A new browser tab opens.

3. Sign in as a Microsoft Entra ID admin user.



Information about the permissions requested by Acronis is displayed.



admin@intunecustomer11.onmicrosoft.com

Permissions requested Review for your organization

Acronis Integration with Intune - C16

unverified

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read Microsoft Intune devices
- ✓ Read and write directory data
- ✓ Read and write Microsoft Intune apps
- ✓ Read and write Microsoft Intune device configuration and policies
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

4. Click **Accept**.

In the browser, switch back to the **Integration** tab and continue your operations.

Note

If the process fails, repeat the admin consent process by switching back to the **Integration** tab in your browser and clicking the app registration button again.

Viewing tenant mapping info

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

The mapping info window displays the Acronis customer tenant name, and the Microsoft Entra ID tenant ID and name.

To view tenant mapping info

1. [Open the integration.](#)
2. Select the mapping row.

MICROSOFT INTUNE

TENANTS

▶ Perform action

📄 Last action summary

ℹ Mapping info

🗑 Remove mapping

<div>−</div>	Acronis customer tenant	↓	Azure AD tenant	↓
<div>✓</div>	intune-customer-1		intune-customer-1	
<div>□</div>	intune-customer-2		intune-customer-2	

3. Click **Mapping info** in the toolbar.

←
intune-customer-1
Add Azure AD tenant

Mapping information

Existing Acronis customer tenant

intune-customer-1

Azure Active Directory tenant ID

cd5d2e29-9ef0-47ee-b860-4dca42fc3e59

Azure Active Directory tenant name

intune-customer-1

Troubleshooting

Use the link below to troubleshoot problems caused by faulty service principal in the target tenant's directory. It will take you to the Microsoft app registration portal where the tenant administrator can sign in to complete the request.

The administrator will be asked to re-authorize the application permissions necessary to access the Microsoft Intune API and perform operations there.

[Re-authorize Acronis app](#)

- Click the **Re-authorize Acronis app** link at the bottom of the screen to repeat the admin consent process for the current mapping. You must do this if the permissions granted during the first admin consent have been changed by an Microsoft Entra ID tenant admin at some point. This will take you through the [admin consent process](#) again.
- Click the back arrow to return to the main view.

Deleting a mapping

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

Note

When you delete a mapping, any objects created in Microsoft Entra ID and Intune of the target Microsoft Entra ID tenant are not deleted. These include:

- The enterprise application object, created during the admin consent process.
- Any Microsoft Entra ID group created as part of the Perform Action wizard.
- PowerShell script objects created as a result of the Perform Action wizard.

Only the Microsoft Entra ID tenant admin can manually clear these from the Microsoft Entra ID and Microsoft Endpoint Manager portals.

To delete a mapping

1. Open the integration.
2. Select the mapping row.
3. Click **Remove mapping** in the toolbar.

MICROSOFT INTUNE		TENANTS
▶ Perform action 📄 Last action summary ℹ Mapping info 🗑 Remove mapping		
<input type="checkbox"/>	Acronis customer tenant ↓	Azure AD tenant ↓
<input checked="" type="checkbox"/>	intune-customer-1	intune-customer-1
<input type="checkbox"/>	intune-customer-2	intune-customer-2

Performing actions

Future versions will have more options and flexibility, as well as support for macOS devices.

Installing the Acronis agent

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

To install the Acronis agent

1. [Open the integration.](#)
2. Select the target tenant.
3. Click **Perform action** in the toolbar.

The perform action wizard starts.

MICROSOFT INTUNE		TENANTS	
▶ Perform action ☰ Last action summary ℹ Mapping info 🗑 Remove mapping			
<input type="checkbox"/>	Acronis customer tenant ↓		Azure AD tenant ↓
<input checked="" type="checkbox"/>	intune-customer-1		intune-customer-1
<input type="checkbox"/>	intune-customer-2		intune-customer-2

4. Select the **Install Acronis agent** option and click **Next**.

Select the operation to perform through Microsoft Intune.

☒ **Install Acronis agent**

This option creates an Intune PowerShell object necessary to install the Acronis agent on the assigned devices. Once deployed on the target device, the PowerShell script will download the latest version of the installer and perform the installation silently.

☐ **Apply protection plan**

This option creates an Intune PowerShell object necessary to apply a protection plan on devices that already have Acronis agent installed and registered under the current Acronis partner account.

☐ **Uninstall Acronis agent**

This option creates an Intune PowerShell object required to remove the Acronis agent from the devices that already have this installation.

5. Configure the agent installation parameters.

These parameters are used for generating a token for the agent installation background. For more information about the generated tokens, see "Created objects" (p. 33).

- Select the Acronis customer tenant user
- [Optional] Select **Set protection plan** option.
This applies a protection plan to the device immediately after installing the Acronis agent.
- Select the protection plan you want to apply.

Note

If no protection plans are defined, you will get a warning message.

Configure

Select Acronis user

intune-customer-1

☒ Set protection plan (Optional)

Select protection plan

Cloud Backup of %ALLUSERSPROFILE%

Cloud Backup of %ALLUSERSPROFILE%

Local Backup of %ALLUSERSPROFILE%

6. Click **Next**.

7. Select the target.

The target defines the devices on which the operation is applied. The selected target determines the assignment property of the Intune PowerShell script object that is created.

Note

The Intune admin can manually change the assignment property later, through the Microsoft Endpoint Manager portal.

On all devices

The operation will target all current and future devices enrolled in Intune.

This is the default option for operations. If selected, the virtual Intune **All devices** group is assigned as an Included group on the created Intune PowerShell object.

Note

"**All devices**" is a pre-created group. It is considered 'virtual', because you do not create or view it in Microsoft Entra ID.

In selected Azure Active Directory group

The operation will target devices that are members of an existing Microsoft Entra ID group that you must select.

The PowerShell script will be applied only on devices which are listed as members of the selected Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices which are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Select target

Select the target for your operation

In selected Azure Active Directory group

Select Azure Active Directory group

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 0317baed-7d9a-4437-8e3a-74ebf4a1b215

Group 03a5502e-f4ce-4403-bd3a-0c27f41088f6

Group 0a2a7909-0328-47c1-8b0e-15fcccfd99a2

Group 0af5a8e5-952b-4bde-83c4-344ee10980ee

Group 0e320798-7f78-42da-a089-15c3611fa928

Group 0e7c32e4-0bf8-41af-8cd9-0da72c099e10

Group 12312040-1122-424c-b2f4-4ac9e0bb9ec7

Create a group and select devices

Create an Microsoft Entra ID group in the customer's Microsoft Entra ID tenant and assign devices to it. The operation will target devices in this new group.

The PowerShell script is applied only to the devices listed as members of the new Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices that are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Create a group and select devices

Add a name for the group

Group name
New Group

Select devices that will be included in the group

Filters

Search

3 items selected

	Device name	Acronis agent
<input type="checkbox"/>	IM-Win10	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-056286	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-477795	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-687318	⚠ Not installed
<input type="checkbox"/>	XYZ-902405	⚠ Not installed

Do not assign any devices

Does not target any devices. Only creates the Intune PowerShell script object that will execute the operation, without assignment.

You can subsequently provide an assignment manually, through the Microsoft Endpoint Manager portal.

Select target

Select the target for your operation

On all devices ^

On all devices
This is every device, enrolled in Intune, including those enrolled after creating the Intune script object.

In selected Azure Active Directory group
Intune-enrolled devices that are also members of the selected Azure Active Directory group.

Create a group and select devices
A new Azure Active Directory security group will be created and a selection of enrolled devices - assigned to it.

Do not assign any devices
Only create the script object in Microsoft Intune

8. Click **Next**.
9. The **Summary** page opens.

MICROSOFT INTUNE

1. Select operation
2. Configure
3. Target
4. Summary

Summary

PowerShell object will be created to install the Acronis agent on the assigned devices. Once deployed on the target device, the PowerShell script will download the latest version of the installer and perform the installation silently. It is recommended to delete the token from Acronis once the script has been applied to all devices in Intune.

Selected operation	Install Acronis agent
Target	On all devices
Acronis user	acronisintegrations-customer

Cancel
Complete

10. Review the information and click **Complete**.

The integration creates a PowerShell script object in Intune and the information about the last action of the target tenant is updated. Information about the new PowerShell script object can be obtained by clicking **Last action summary** in the toolbar.

Note

Intune is now responsible for notifying the target devices about the new PowerShell script object, so that they can download and execute it. The notification time range varies between immediate and a few hours. For more information, see [the Microsoft Intune help system](#).

Applying a protection plan

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

To apply a protection plan

1. [Open the integration](#).
2. Select the target tenant.
3. Click **Perform action** in the toolbar.
4. Select the **Apply protection plan** option.
5. Click **Next**.
6. On the **Protection plan configuration** step:
 - a. Choose the Acronis customer tenant user.
 - b. Choose the protection plan that you want to apply.

Note

If no protection plans are defined, you will get a warning message, and cannot continue.

These parameters are used for generating a token for the agent installation background. For more information about the generated tokens, see "Created objects" (p. 33).

7. Click **Next**.
8. Select the target.

The target defines the devices on which the operation is applied. The selected target determines the assignment property of the Intune PowerShell script object that is created.

Note

The Intune admin can manually change the assignment property later, through the Microsoft Endpoint Manager portal.

On all devices

The operation will target all current and future devices enrolled in Intune.

This is the default option for operations. If selected, the virtual Intune **All devices** group is assigned as an Included group on the created Intune PowerShell object.

Note

"**All devices**" is a pre-created group. It is considered 'virtual', because you do not create or view it in Microsoft Entra ID.

In selected Azure Active Directory group

The operation will target devices that are members of an existing Microsoft Entra ID group that you must select.

The PowerShell script will be applied only on devices which are listed as members of the selected Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices which are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Select target

Select the target for your operation

In selected Azure Active Directory group

Select Azure Active Directory group

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 0317baed-7d9a-4437-8e3a-74ebf4a1b215

Group 03a5502e-f4ce-4403-bd3a-0c27f41088f6

Group 0a2a7909-0328-47c1-8b0e-15fcccfd99a2

Group 0af5a8e5-952b-4bde-83c4-344ee10980ee

Group 0e320798-7f78-42da-a089-15c3611fa928

Group 0e7c32e4-0bf8-41af-8cd9-0da72c099e10

Group 12312040-1122-424c-b2f4-4ac9e0bb9ec7

Create a group and select devices

Create an Microsoft Entra ID group in the customer's Microsoft Entra ID tenant and assign devices to it. The operation will target devices in this new group.

The PowerShell script is applied only to the devices listed as members of the new Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices that are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Create a group and select devices

Add a name for the group

Group name
New Group

Select devices that will be included in the group

Filters

Search

3 items selected

	Device name	Acronis agent
<input type="checkbox"/>	IM-Win10	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-056286	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-477795	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-687318	⚠ Not installed
<input type="checkbox"/>	XYZ-902405	⚠ Not installed

Do not assign any devices

Does not target any devices. Only creates the Intune PowerShell script object that will execute the operation, without assignment.

You can subsequently provide an assignment manually, through the Microsoft Endpoint Manager portal.

Select target

Select the target for your operation

On all devices

On all devices
This is every device, enrolled in Intune, including those enrolled after creating the Intune script object.

In selected Azure Active Directory group
Intune-enrolled devices that are also members of the selected Azure Active Directory group.

Create a group and select devices
A new Azure Active Directory security group will be created and a selection of enrolled devices - assigned to it.

Do not assign any devices
Only create the script object in Microsoft Intune

9. Click **Next**.
10. On the **Summary** page, review the information.
11. Click **Complete**.

The integration creates a PowerShell script object in Intune and the information about the last action of the target tenant is updated. Information about the new PowerShell script object can be obtained by clicking **Last action summary** in the toolbar.

Note

Intune is now responsible for notifying the target devices about the new PowerShell script object, so that they can download and execute it. The notification time range varies between immediate and a few hours. For more information, see [the Microsoft Intune help system](#).

Uninstalling Acronis agent

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

To uninstall the Acronis agent

Note

If **Self-protection** and **Agent Uninstallation Protection** are enabled in the protection plan, you must first perform some steps in Acronis Protection Console.

1. Navigate to the customer tenant > **Settings** > **Agents**.
 2. Find the Acronis Cyber Protection agent in the list, and click on the row.
 3. In the **Actions** panel that appears on the right, go to **Agent Update Settings**.
 4. Under **Set the permitted duration for the agent to be uninstalled or updated**, select the duration of the maintenance window needed to uninstall the agent.
-

1. [Open the integration](#).
2. Select the target tenant.
3. Click **Perform action** in the toolbar.
4. Select **Uninstall Acronis agent**.
5. Click **Next**.
6. Select the target.

The target defines the devices on which the operation is applied. The selected target determines the assignment property of the Intune PowerShell script object that is created.

Note

The Intune admin can manually change the assignment property later, through the Microsoft Endpoint Manager portal.

On all devices

The operation will target all current and future devices enrolled in Intune.

This is the default option for operations. If selected, the virtual Intune **All devices** group is assigned as an Included group on the created Intune PowerShell object.

Note

"**All devices**" is a pre-created group. It is considered 'virtual', because you do not create or view it in Microsoft Entra ID.

In selected Azure Active Directory group

The operation will target devices that are members of an existing Microsoft Entra ID group that you must select.

The PowerShell script will be applied only on devices which are listed as members of the selected Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices which are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Select target

Select the target for your operation

In selected Azure Active Directory group

Select Azure Active Directory group

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 01407e3b-dfad-40db-b548-01083a5a43cd

Group 0317baed-7d9a-4437-8e3a-74ebf4a1b215

Group 03a5502e-f4ce-4403-bd3a-0c27f41088f6

Group 0a2a7909-0328-47c1-8b0e-15fcccfd99a2

Group 0af5a8e5-952b-4bde-83c4-344ee10980ee

Group 0e320798-7f78-42da-a089-15c3611fa928

Group 0e7c32e4-0bf8-41af-8cd9-0da72c099e10

Group 12312040-1122-424c-b2f4-4ac9e0bb9ec7

Create a group and select devices

Create an Microsoft Entra ID group in the customer's Microsoft Entra ID tenant and assign devices to it. The operation will target devices in this new group.

The PowerShell script is applied only to the devices listed as members of the new Microsoft Entra ID group and enrolled in Intune.

Important

The Microsoft Entra ID groups may contain devices that are not enrolled in Intune. You are responsible to verify that the device members list of the target Microsoft Entra ID group is correct.

Create a group and select devices

Add a name for the group

Group name
New Group

Select devices that will be included in the group

Filters

Search

3 items selected

	Device name	Acronis agent
<input type="checkbox"/>	IM-Win10	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-056286	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-477795	⚠ Not installed
<input checked="" type="checkbox"/>	XYZ-687318	⚠ Not installed
<input type="checkbox"/>	XYZ-902405	⚠ Not installed

Do not assign any devices

Does not target any devices. Only creates the Intune PowerShell script object that will execute the operation, without assignment.

You can subsequently provide an assignment manually, through the Microsoft Endpoint Manager portal.

Select target

Select the target for your operation

On all devices

On all devices
This is every device, enrolled in Intune, including those enrolled after creating the Intune script object.

In selected Azure Active Directory group
Intune-enrolled devices that are also members of the selected Azure Active Directory group.

Create a group and select devices
A new Azure Active Directory security group will be created and a selection of enrolled devices - assigned to it.

Do not assign any devices
Only create the script object in Microsoft Intune

7. Click **Next**.
8. On the **Summary** page, review the information.
9. Click **Complete**.

The integration creates a PowerShell script object in Intune and the information about the last action of the target tenant is updated. Information about the new PowerShell script object can be obtained by clicking **Last action summary** in the toolbar.

Note

Intune is now responsible for notifying the target devices about the new PowerShell script object, so that they can download and execute it. The notification time range varies between immediate and a few hours. For more information, see [the Microsoft Intune help system](#).

Checking the last action

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

To check the last action performed on a customer tenant

1. [Open the integration.](#)
2. Select the tenant.
3. In the toolbar, locate and click **Last action summary**.
4. The summary view opens with the following information:

SECTION	FIELD	NOTES
SUMMARY	Acronis customer tenant	The target Acronis customer tenant
	Azure AD tenant	The target Microsoft Entra ID tenant
	Action	Can be one of the following, depending on the type of operation: <ul style="list-style-type: none"> • [Windows PowerShell] Deploy Acronis agent • [Windows PowerShell] Apply protection plan • [Windows PowerShell] Uninstall Acronis agent
	Target devices	Can be one of the following, depending on the type of operation: <ul style="list-style-type: none"> • Perform the operation on all devices • Perform the operation on all devices in group "XYZ" • Create group "XYZ" and perform the operation on its associated devices • Target devices not assigned
	Acronis user	The Acronis user that participated in the operation. Not applicable in case of agent uninstallation.
	Protection plan	The Acronis protection plan used for the operation. Not applicable in case of agent uninstallation.
	Started	Date/time when the operation to create an Intune object started
	Completed	Date/time when the operation to create an Intune object finished
RESULT	PowerShell script ID	The internal ID of the created Intune PowerShell script
	PowerShell script name	The name of the Intune PowerShell script created. Script naming rules are explained in the the reference chapter .
	Azure AD group ID	The object ID of the selected/created Microsoft Entra ID group
	Azure AD group name	The name of the selected/created Microsoft Entra ID group

Use the information from the **Result** section to locate objects, created in Microsoft Entra ID and the Microsoft Endpoint Manager.

The screenshot displays two interfaces side-by-side. On the left is the Microsoft Endpoint Manager admin center for tenant 'intune-customer-1'. It shows a 'Last action summary' for a PowerShell script deployment and a 'Result' section with the following details:

PowerShell script ID	83d3ac59-f493-4b62-8a3e-b79c95b0e0d2
PowerShell script name	[Acronis Integration] Install Acronis agent - SECE
Azure AD group ID	7d87b75c-0339-4ae2-be83-0f1a26dcf4ab
Azure AD group name	A new group

On the right is the Microsoft Azure portal for the same tenant. It shows a list of PowerShell scripts under 'Windows | PowerShell scripts'. The script '[Acronis Integration] Install Acronis agent - SECE' is highlighted with a green box. A green arrow points from this script to the 'A new group' entry in the 'Groups | All groups' list, which is also highlighted with a red box. A red arrow points from the 'A new group' entry in the Azure AD groups list to the 'A new group' entry in the PowerShell script result table.

Created objects

Objects created in Acronis

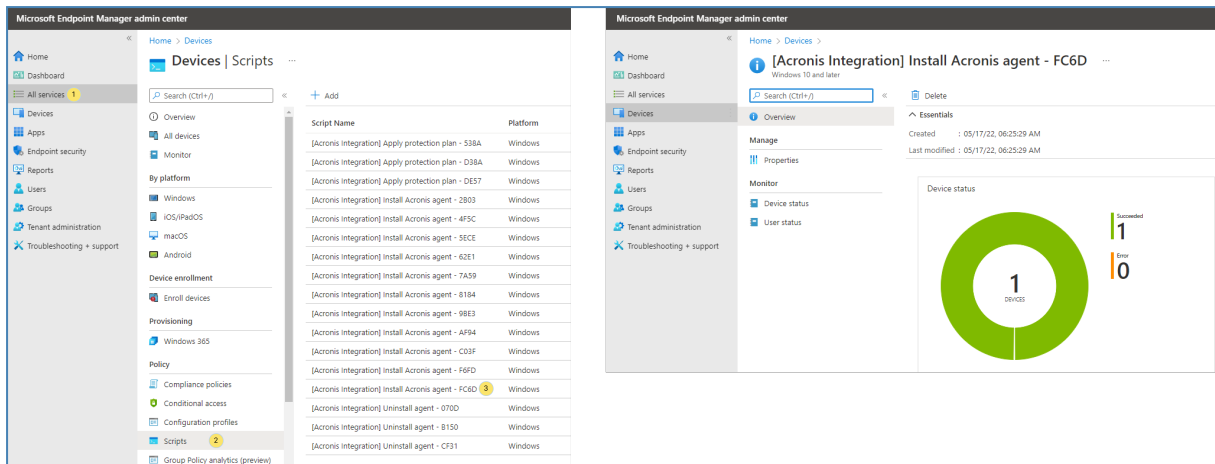
In order to deploy an Acronis agent and apply a protection plan, the integration generates a token per customer/operation pair.

Each token is valid for one year and is embedded into the Intune PowerShell script.

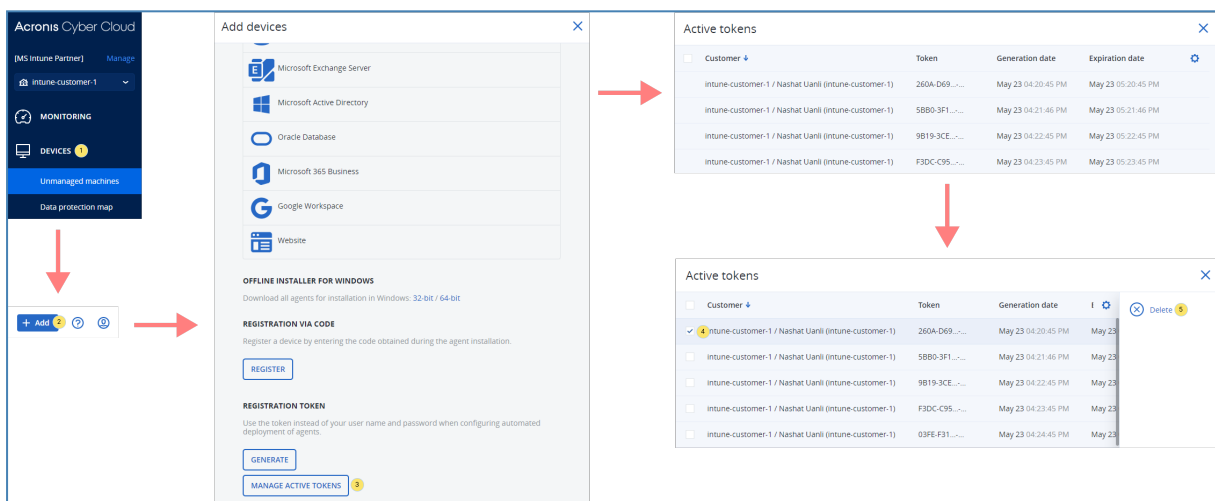
Important

It is recommended to delete the generated tokens once you verify that the Intune PowerShell script has been downloaded and executed on all assigned devices.

You can check the script execution status in the Microsoft Endpoint Manager portal:



Find the generated tokens in Acronis Management Portal of the customer tenant:



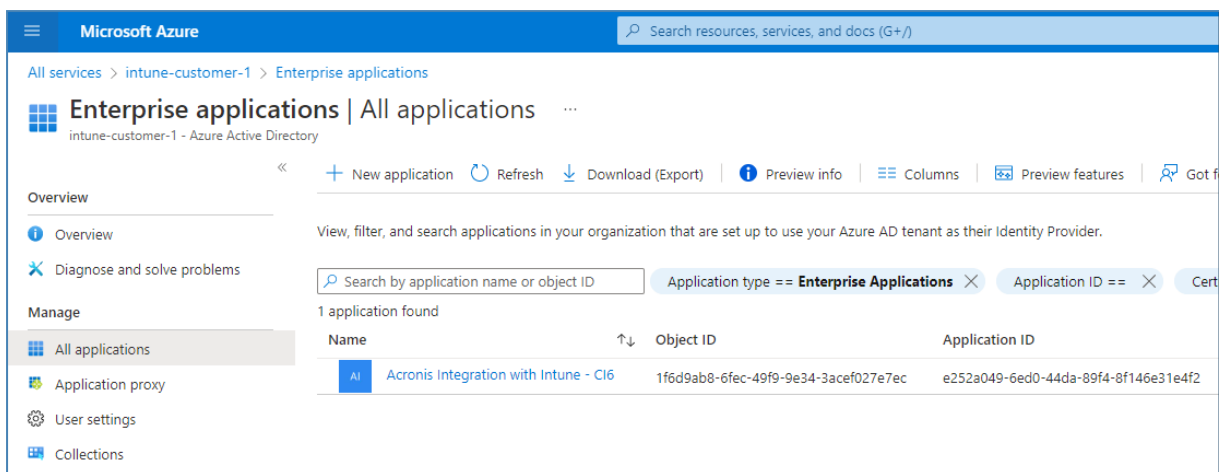
Objects created in customer Microsoft Entra ID

Note

The Acronis integration with Microsoft Intune predates the Microsoft product name change from Azure Active Directory to Microsoft Entra ID. Therefore, the integration UI still refers to Azure AD. This will be updated in a future release of the integration.

Enterprise applications

The admin consent process results in the creation of enterprise applications in the Microsoft Entra ID of the customer tenants. The enterprise application object is located under the **Enterprise applications** blade in the Microsoft Entra ID portal of the customer tenant.



The enterprise application is listed as **Acronis Integration with Intune - XYZ**, where **XYZ** is the name of the data center from where the consent process was triggered.

Note

You may have more than one Acronis enterprise application. This is possible by mapping the same Microsoft Entra ID tenant to two or more different customer tenants, residing on different data centers.

Microsoft Entra ID groups

If you choose the option to create a Microsoft Entra ID group and assign devices to it when [performing an action](#), then you can find the created group or groups under the **Groups** blade in the Microsoft Entra ID portal of the customer tenant.

Objects created in customer Microsoft Endpoint Manager

The integration can create three types of Intune PowerShell objects, with the following attributes:

To install the Acronis agent

PROPERTY	VALUE
Name	[Acronis Integration] Install Acronis agent - XXXX (XXXX is a random 4-digit hexadecimal number)
Description	This PowerShell script is created automatically by Acronis Cyber Cloud > Intune integration module > setup under tenant (tenant ID) in (Cloud URL)
PowerShell script	Acronis_install_agent_parametrized.ps1
Run this script using the logging credentials	No
Enforce script signature check	No
Run script in 64-bit PowerShell host	Yes

PROPERTY	VALUE
Included groups	"All devices" or the name of the group, if such is configured in the wizard
Excluded groups	--

To apply a protection plan

PROPERTY	VALUE
Name	[Acronis Integration] Apply protection plan - XXXX (XXXX is a random 4-digit hexadecimal number)
Description	This PowerShell script is created automatically by AcronisCyber Cloud > Intune integration module > setup under tenant (tenant ID) in (Cloud URL)
PowerShell script	Acronis_manage_protection_plan.ps1
Run this script using the logging credentials	No
Enforce script signature check	No
Run script in 64-bit PowerShell host	Yes
Included groups	"All devices" or the name of the group, if such is configured in the wizard
Excluded groups	--

To uninstall the Acronis agent

PROPERTY	VALUE
Name	[Acronis Integration] Uninstall agent - XXXX (XXXX is a random 4-digit hexadecimal number)
Description	This PowerShell script is created automatically by AcronisCyber Cloud > Intune integration module > setup under tenant (tenant ID) in (Cloud URL)
PowerShell script	acronis_uninstall_agent.ps1
Run this script using the logging credentials	No
Enforce script signature check	No
Run script in 64-bit PowerShell host	Yes
Included groups	"All devices" or the name of the group, if such is configured in the wizard
Excluded groups	--

Deactivating the integration

To deactivate the integration

1. Log in to Acronis Management Portal as administrator.
2. Select **INTEGRATIONS** on the main menu.
3. Select the **INTEGRATION IN USE** tab.
4. Locate the Microsoft Intune integration catalog card.

Note

For more information, see [the Management Portal partner administrator guide](#).

5. Click **Deactivate**.
6. Click **Delete**.

Troubleshooting Intune PowerShell scripts

For articles and resources about how to debug and troubleshoot Intune PowerShell scripts, see [the official Microsoft Intune page](#).

You can find Acronis logs generated by PowerShell script execution at %systemdrive%\Windows\Temp.