Recast

Microsoft Azure Virtual Desktop

Last Modified on 04.16.26

This connector type allows you to set up a connection to Microsoft Azure Virtual Desktop (ARM or legacy) to import the applications defined there as ready-to-use applications within Application Workspace for distribution.

Prerequisites

- A Microsoft Entra ID (Azure AD) username and password to connect to Microsoft AVD.
- A template type credential within the Recast Credential Store that can provide the username for the Remote Desktop application. A common format for the username is "${Identity.UserName}".
- If your service account is MFA-enabled, you need to use either the Conditional Access or Trusted IP feature in Microsoft 365 to bypass MFA. Once you have configured one of these features, proceed to configure the service account on the connector.

For more information about the **Overview**, **Entitlements**, **Synchronization Profile**, **Releases** and **Managed packages** screens, see Connectors.

Settings screen

Scope – The type of resources that will be synchronized.
Username – The username which will be used to import the applications; it should be a Microsoft Entra ID (Azure AD) UPN. The identity needs to have permission to read all the desired applications and desktops.
Password – The password of the username.
Application ID – The Azure application ID that should be used for authentication (applies only to ARM resources).
Client secret – The Azure application client secret that should be used for authentication (applies only to ARM resources).

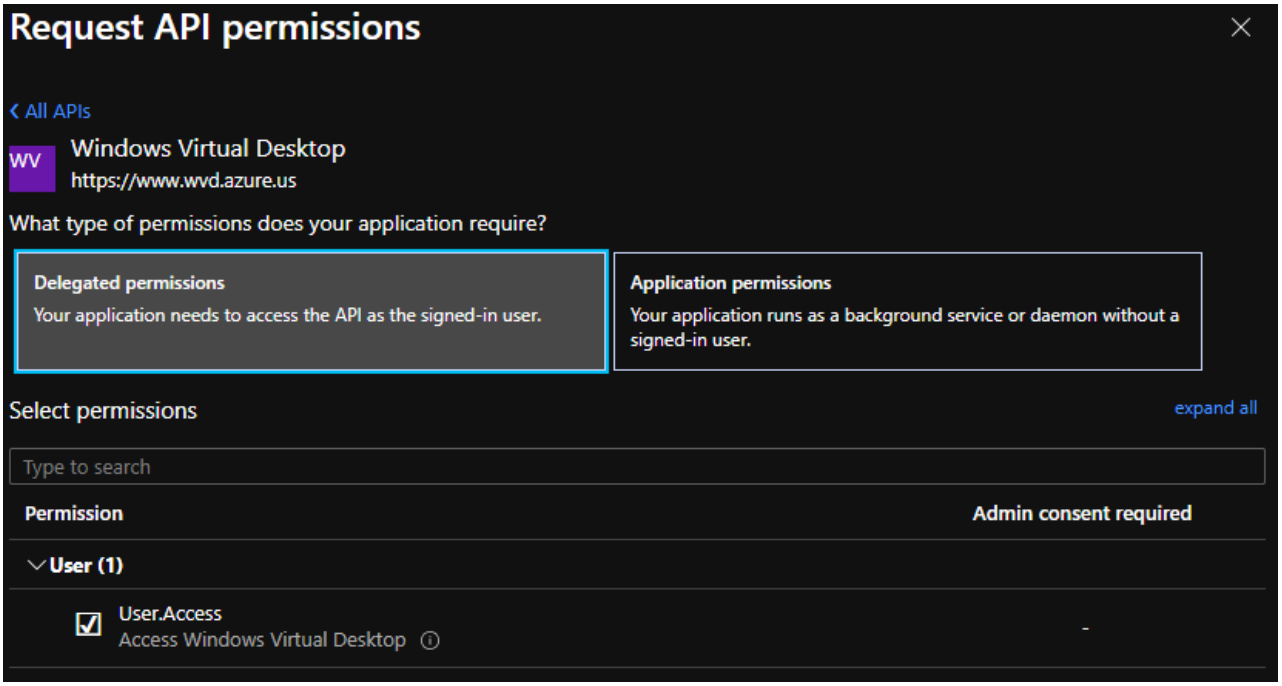
Package
Network Credentials – The template type credential within the Credential Store that will be used to start up the Remote Desktop application.
Install dependency – Adds an install dependency to the managed packages.
Use web client when no agent is present – If selected, the RDP file is downloaded or the web client is opened in a web browser when no Agent is present.

Azure Resource Manager

Before AVD ARM resources can be synchronized, make sure the desired applications are registered within the Microsoft Entra ID (Azure AD) and have the "Windows Virtual Desktop" – "User.Access" API permissions. A registered application can be for example the Application Workspace application, which is also used for a Microsoft Entra ID (Azure AD) identity source.

Adding permissions

1. Navigate to the desired registered application within the Azure Portal.
2. In the left pane, navigate to **Manage** > **API permission**.
3. Click **Add Permission** and then go to the **APIs my organization uses** tab.
4. Choose **Windows Virtual Desktop** with the Application ID "9cdead84-a844-4324-93f2-b2e6bb768d07".
5. Go to the **Delegated permissions** tab and select the *User.Access*.



6. Click on the **Grant admin consent for {your tenant}**. It can take up to an hour before these settings take effect in Microsoft Entra ID (Azure AD).

Further reading

Granting API permissions in Azure Portal (Microsoft documentation)

Azure Virtual Desktop technical (ARM-based model) deployment walkthrough

Building a Golden Image for AVD with Packer and Application Workspace

Optimize New MS Teams for AVD with Application Workspace