Recast

Microsoft Azure Virtual Desktop Connector

Last Modified on 2026-09-24

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.

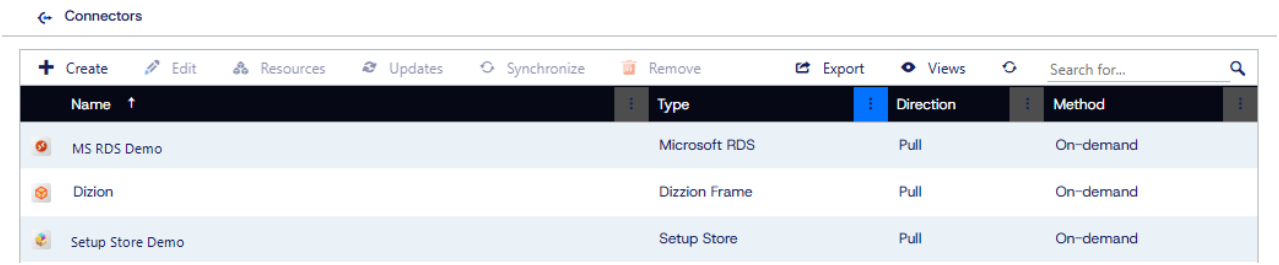
Prerequisites

- An EntraID 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.

Create an Azure Virtual Desktop Connector

To create a new Microsoft Azure Virtual Desktop connector:

1. On the **Connectors** page, click the **Create** button.



2. As the Connector **Type**, select 'Microsoft Azure Virtual Desktop'.

3. Accept the Terms and conditions.

4. Configure settings on the **Overview** and **On-demand** tabs. See Create a Connector for descriptions of options common to multiple connector types.

5. On the **Settings** tab, choose connector-specific options:

   General settings:
   - **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** for 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 settings:
   - **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** – When enabled, the RDP file is downloaded or the web client is opened in a web browser when no Agent is present.

6. Configure appropriate settings on the **Entitlements** and **Releases** tabs. See Create a Connector for descriptions of options common to multiple connector types.

Add API Permissions for Azure Virtual Desktop

Before AVD ARM resources can be synchronized, you'll need to register the desired applications within Entra ID and grant the '**User.Access**' API permission for Azure Virtual Desktop. A registered application can be, for example, the Application Workspace application, which is also used for a Microsoft Entra ID (Azure AD) identity source.

To add API permissions for Azure Virtual Desktop:

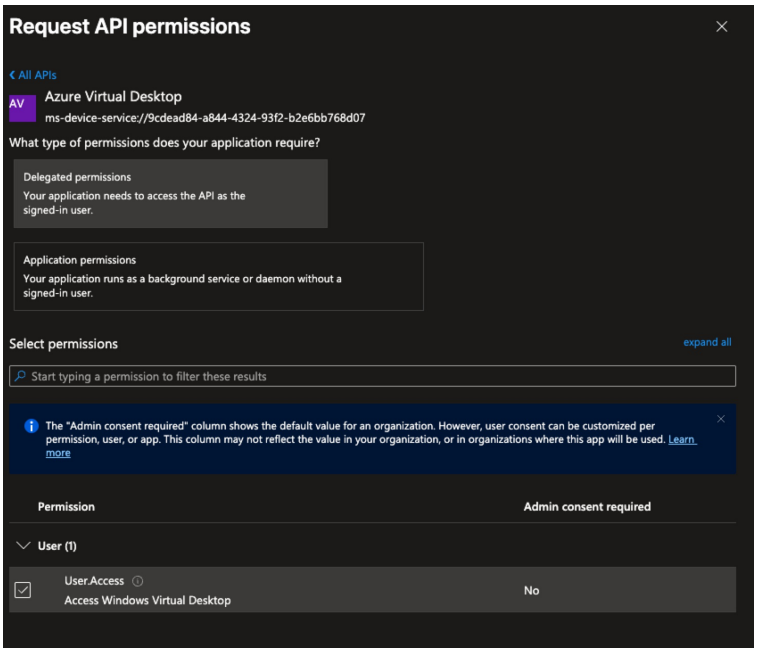
1. Navigate to the desired registered application within the Azure Portal.

2. On the **App registrations** page, under **Manage**, click **API Permissions**.

3. Select **Add a permission**.

4. On the **APIs my organization uses** tab, choose **Azure Virtual Desktop** with the Application ID "9cdead84-a844-4324-93f2-b2e6bb768d07".

5. On the **Delegated permissions** tab, select the 'User.Access' permission.



6. Click **Grant admin consent for [Tenant Name]**.

> It can take up to an hour before these settings take effect in Microsoft Entra ID (Azure AD).

Further reading

Web API app registration and API permissions – Microsoft identity platform | Microsoft Learn

Recast Blog: Building a Golden Image for AVD with Packer and Application Workspace

Recast Blog: Optimize New MS Teams for AVD with Application Workspace

Recast