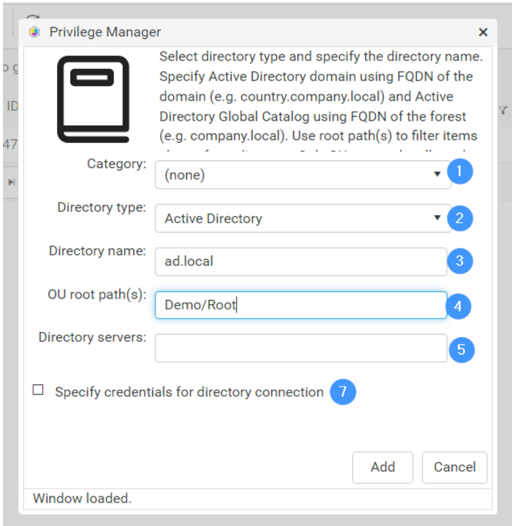
Add Or Modify Directory

Active Directories can be on-premises AD directories or cloud-based Azure AD directories. For some products you can add the same domain multiple times when using different categories.

On-premises Active Directories



Privilege Manager

Select directory type and specify the directory name. Specify Active Directory domain using FQDN of the domain (e.g. country.company.local) and Active Directory Global Catalog using FQDN of the forest (e.g. company.local). Use root path(s) to filter items

Category: (none)

Directory type: Active Directory

Directory name: ad.local

OU root path(s): Demo/Root

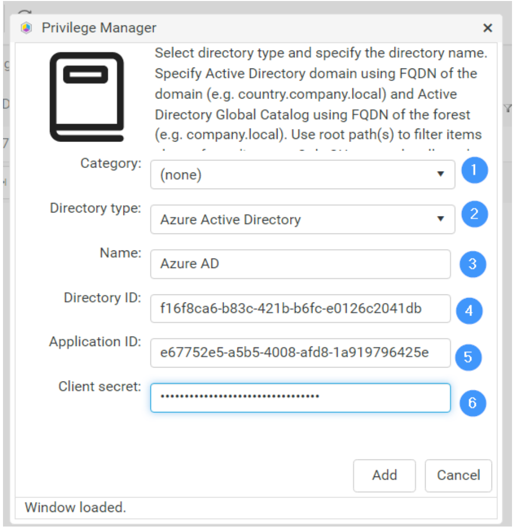
Directory servers:

□ Specify credentials for directory connection

Window loaded.

1. Select the **Category** for an Active Directory connection. Only for Pandeiro product, for Privilege Manager, always use the default (none). For Pandeiro each category that need to support group requests must also have Active Directory connection specified
2. As a **Directory type**, select **Active Directory** type for connection. Use **Active Directory** if single domain type is required and use **Active Directory (Global Catalog)** if forest type is required. All domains in forest can also be added as single domains. If you use **Global Catalog** type (forest) for your AD, then only subset of attributes are available.
3. Specify an Active **Directory name** using the forest or domain DNS name.
4. If this Active Directory connection should show only part of the Active Directory information, specify the OU root paths to show as a comma-separated canonical name list. Do not specify domain name in the canonical name. For example OU with OU=Root,OU=Demo,DC=ad,DC=local distinguished name would be specified as Demo/Root
5. If Active Directory domain controllers cannot be found using DNS and the specified directory name, specify the location of the **Directory servers** using the FQDN name or IP addresses. You can specify several domain controllers by separating values with commas.
6. If the identity used to run Recast Privilege Manager and the Recast Agent Gateway web sites (default is Network Service that will use servers computer object as identity) does not have permissions to connect to Active Directory, enable **Specify credentials for directory connection** and specify credentials to be used in connecting Active Directory service. The user account name format can be pre-Windows 2000 account format (DOMAIN\account) or user account format (email)

Azure AD



Select directory type and specify the directory name. Specify Active Directory domain using FQDN of the domain (e.g. country.company.local) and Active Directory Global Catalog using FQDN of the forest (e.g. company.local). Use root path(s) to filter items

Category: (none) 1

Directory type: Azure Active Directory 2

Name: Azure AD 3

Directory ID: f16f8ca6-b83c-421b-b6fc-e0126c2041db 4

Application ID: e67752e5-a5b5-4008-afd8-1a919796425e 5

Client secret: •••••••••••••••••••••••••••••••••• 6

Window loaded.

1. Select the **Category** for Active Directory connection. Only for Pandeiro product, for Privilege Manager always use the default (none). For Pandeiro each category that need to support group requests must also have Active Directory connection specified.
2. As a **Directory type**, select **Azure Active Directory**.
3. Enter a display **Name** that will be shown in the Privilege Manager Portal for your Azure AD directory.
4. Enter your Azure AD **Directory** (tenant) **ID**. You get this value when creating Azure AD App Registration.
5. Enter your Azure AD **Application** (client) **ID**. You get this value when creating Azure AD App Registration.
6. Enter your Azure AD App registration **Client secret**. You get this value when creating Azure AD App Registration.
7. Click **Add**.