Microsoft Azure Data Collection Prerequisites for a Service Principal

Overview

A Service Principal is an identity created within your on-premises Active Directory (AD) and that is allowed to access one or more resources within your AD. You can delegate the minimum required permissions to the service principal so that it can be used to create a connection to Densify to collect data.

To learn more about the Azure prerequisites for a service principal, watch the video: Data Collection Prerequisites for Azure Using a Service Principal

> ***Note:*** *Azure Stack is not supported. This data collection method currently only supports Azure Cloud.*

If you are using a standalone Azure Active Directory account (i.e. an Azure AD), then see *Microsoft Azure Data Collection Prerequisites* (Help Topic ID 410110).

The Service Principal possesses the following characteristics:

- An application that is created within your Active Directory. This application will be associated with the user that creates it.
- A service principal is then created for that application;
- The service principal is granted access to the Azure subscription.

The following procedure allows you to use a federated Azure Active Directory (AD) account to create a cloud connection. In this case a Service Principal is required to connect Densify to your Azure subscriptions.

> ***Note:*** *In this case "federated" indicates that your on-premise Active Directory is linked with your Azure Cloud's Active Directory so you can use your existing on-premise AD credentials to access your Azure portal.*

Requirements to Create a Cloud Connection

To connect Densify to your Azure subscriptions, you need the following items to complete the audit setup:

- Tenant ID/Directory ID
- Service Principal/Application ID
- Secret Key
- Subscription ID—Only required when using the Densify API.

Additionally, the application must be assigned the role of "Reader" for each of the subscriptions from which data will be collected. The Reader role is sufficient for resource utilization data.

Required Account Permissions

In order to create the account required for Densify, you must have admin/owner privileges for your Azure portal. Typically, your on-premise Active Directory is federated with the Azure AD. In this case, the admin access is likely provided from an on-premise Active Directory account (via federation) and will possess the required Azure admin privileges.

The user account/Service Principal to be used for data collection only requires the "Reader" role privileges to collect resource utilization data.

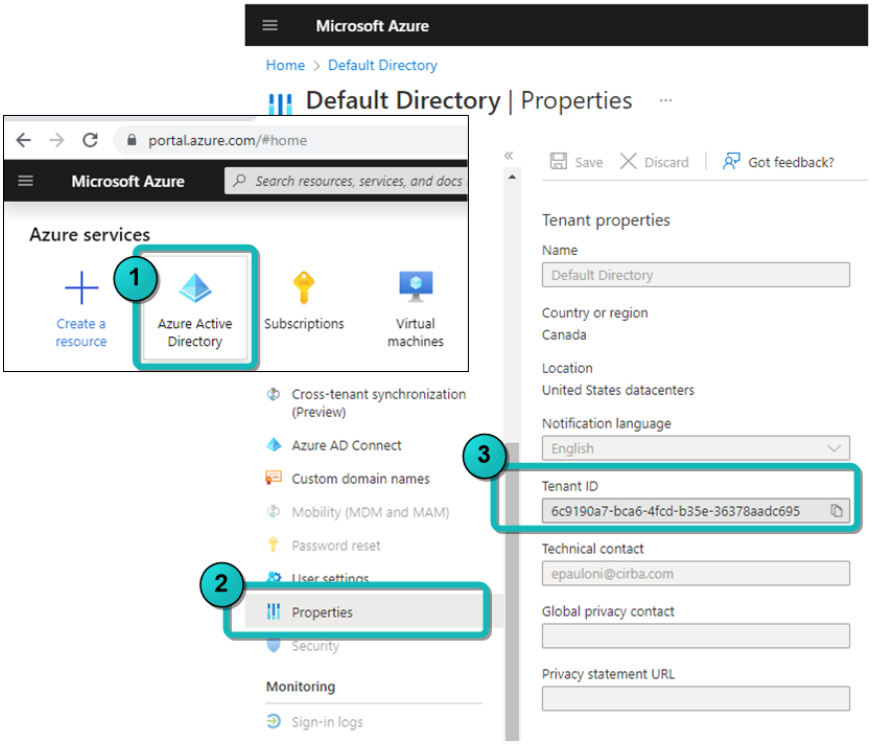
If necessary you can configure a custom role that is more restrictive than the "Reader" role privileges. See Configuring a Role with Minimum Permissions for Data Collection for details.

Obtaining the Tenant ID/Directory ID

The tenant ID corresponds to the Azure Active Directory (AD).

1. Login into your Azure account and click on **Azure Active Directory** > **Properties** .
2. In the **Properties** pane, copy the **Tenant ID** (e.g. 6c9190a7-bca6-4fcd-b35e-36378aadc).

Figure: Azure Active Directory Properties

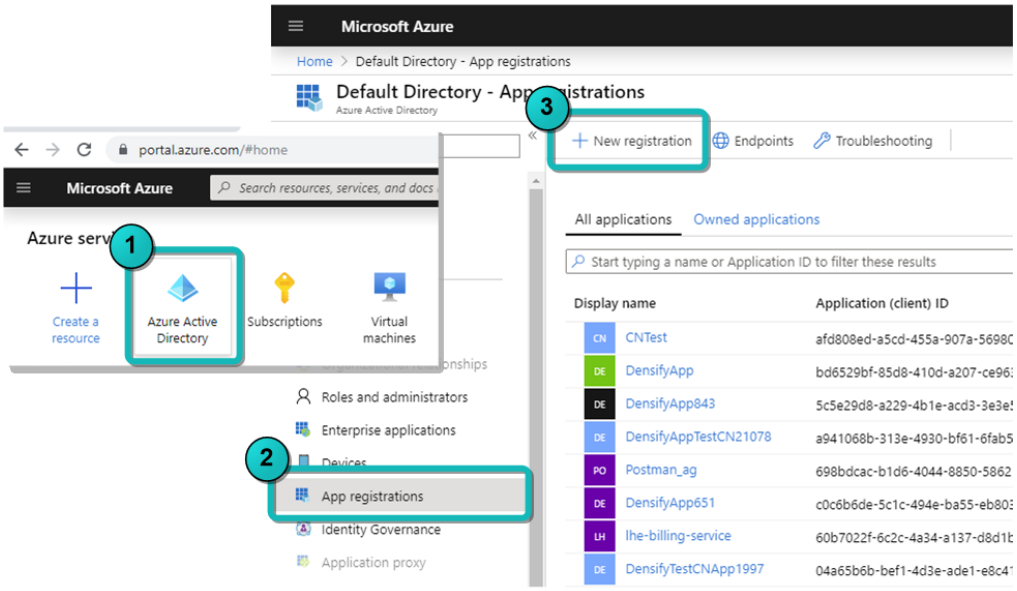


Obtaining the Application ID and Client Secret

You now need to create a new application registration. This will be the service principal for Densify. You will need the Application ID and corresponding client secret (key), to complete the Densify connection.

1. Click **Azure Active Directory** > **App Registration**.
2. In the App Registration pane, click **New registration**.

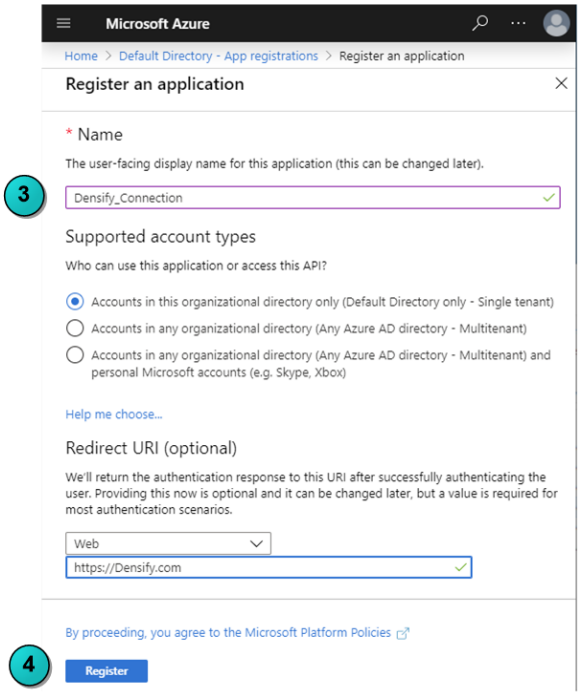
Figure: Create New Registration



3. In the **Create** pane enter the following information:
   - The **Name** of the application (e.g. Densify_Connection).
   - Select who can access the application. Leave the default of "Single Tenant".
   - Select the **Redirect URI (optional)** as “Web” and specify a **Sign-on URI** (e.g. https://Densify.com).

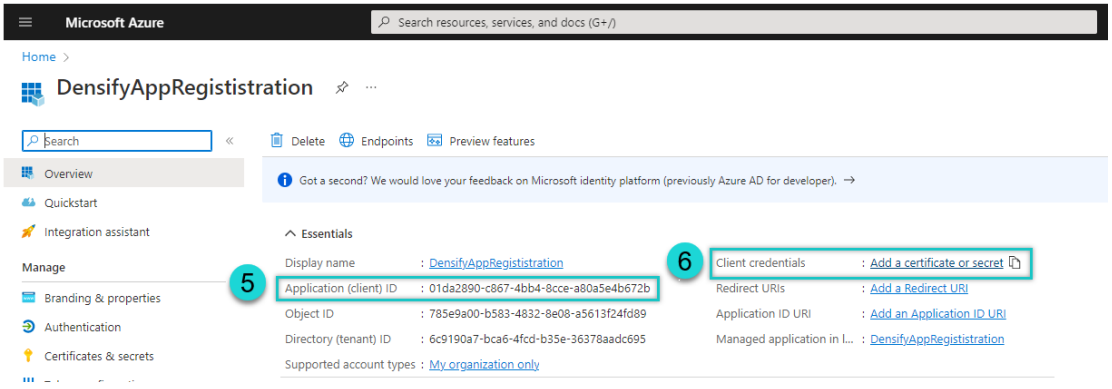
   The **Register** button becomes available once you enter valid data.
4. Click **Register** to create and register the application. This is the service principal that Densify will use to collect data.

Figure: Configure the Registration



5. Copy the Application ID (e.g. 7d16fbf8-1fc3-4e08-b48a-626). You need to copy this ID and save it to a location from which you can easily retrieve it. You will need the Application ID to create the Densify connection.

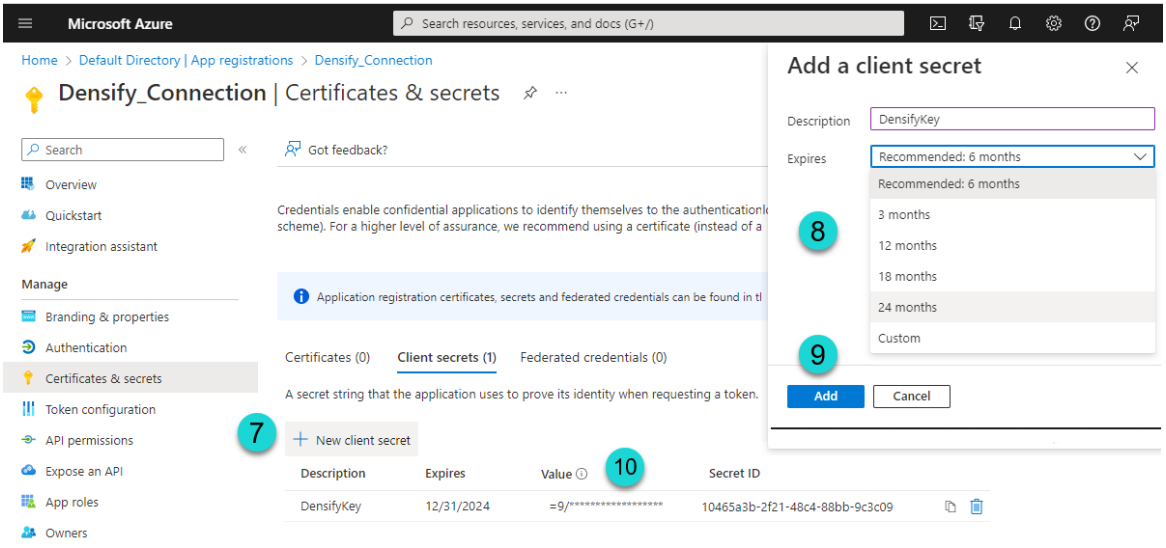
   Figure: Obtain the Application ID



6. Click **Client credentials** to see the page.
7. Click on **New client secret** to create a new key.
8. In the **Add a new client secret** pane, enter a **Description** (e.g. DensifyKey) and an expiration period (e.g. 1 year, 2 years or never expires).
9. Click **Add** to create the key.

10. Copy the secret key **Value** to a location from which you can easily retrieve it. You will need this key to create the Densify connection.

Figure: Generate the Secret Key



Obtaining the Subscription ID

If you are using the API, data collection and analysis are created and then refreshed daily on a per subscription basis (1-to-1). You can associate many subscriptions with a service principle, but when using the API to initiate data collection, you must specify a subscription ID and the audit and analysis are created for each subscription, separately.

When using the Connection Wizard in the Densify UI, you do not need the subscription ID, as all subscriptions that are associated with the service principle are collected and listed once the connection has been verified. You can then select one or more of the subscriptions that you want to analyze (1-to-Many). When using the Connection Wizard, data collection and analysis are created and then refreshed daily for all of the subscriptions that you selected when you created the connection.

Use the following instructions to get the Subscription ID.

1. Navigate to **Subscriptions** in the main menu. You may need to click on **More services** to see **Subscriptions**.
2. Click on a subscription to open the configuration page.
3. Copy the Subscription ID. You need to copy this ID and save it to a location from which you can easily retrieve it. You will need the Subscription ID to initiate data collection, when using the Densify API.

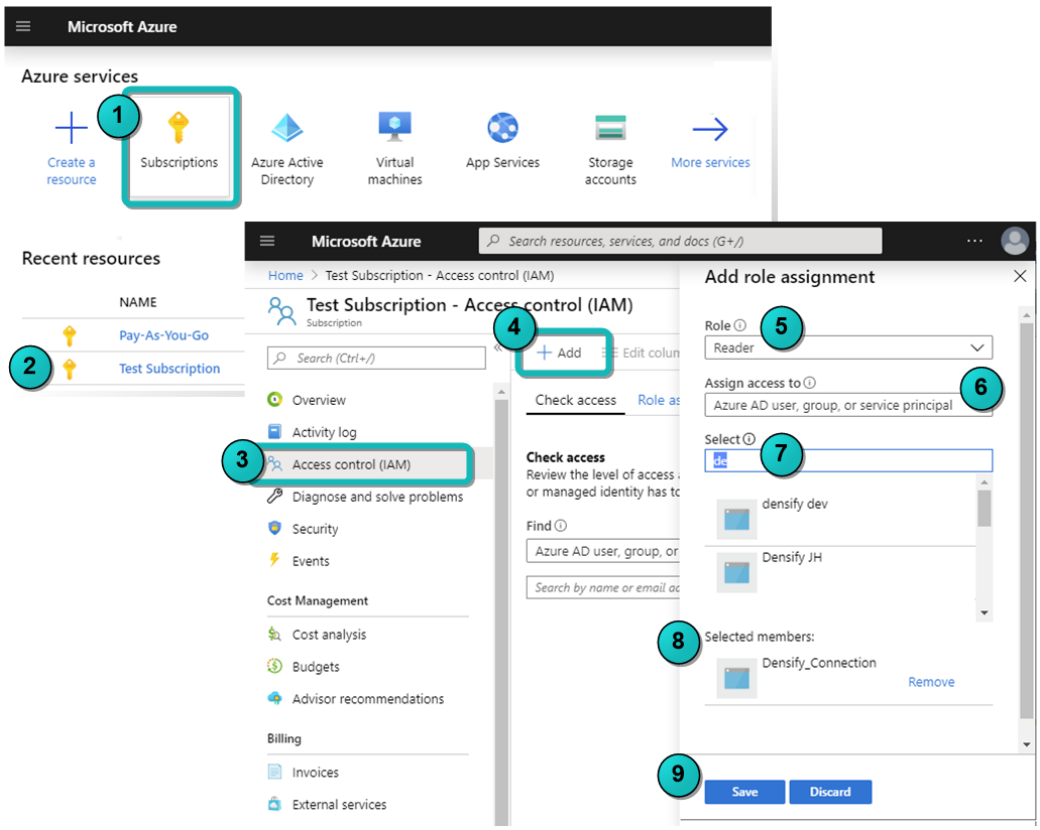
Assigning Access to Subscriptions

The application registered above, now needs access to each of your subscriptions. You need to assign the "Reader" role to the Application for each subscription being audited. Use the following

process:

1. Navigate to **Subscriptions** in the main menu. You may need to click on **All services** to see **Subscriptions**.
2. Click on a subscription to select and open the configuration pane.
3. Click **Access Control (IAM)**.
4. Click **Add > Add role assignment**.
5. In the **Add role assignment** pane select the **Role** of "Reader".
6. Ensure **Assign Access to** is set to "Azure AD user, group or service principal".
7. Search for or scroll to locate the service principle (Densify_Connection), created above.
8. Select your application. It will appear under **Selected members**.
9. Click **Save** to save these changes.
10. Repeat this process for each subscription to be included in data collection.

Figure: Allow Application to access a Subscription



Once the account has been configured you can use the tenant ID, application ID and secret key to create the cloud connection as outlined in *Using the Public Cloud Connection Wizard* (Help Topic ID 380290) .

Advanced Topics

The following sections contain detailed instructions for more advanced configuration. Some sections are referenced in the procedures above. Other advanced topics cover optional configuration.

- Configuring a Role with Minimum Permissions for Data Collection
- Create the Service Principal Through the Azure CLI

Configuring a Role with Minimum Permissions for Data Collection

To simplify setup and maintenance of the role used for performing data collection, Densify recommends using the "Reader" role. This role provides read-only access to your Azure services and resources and supports the requirements for resource utilization data collection. As the Densify continues to evolve and expand, you do not need to update permission policy to include newly added services and features, when using the "Reader" role.

Alternatively, if you must restrict the role with the minimum permissions you can create a custom role with only the required permissions. These custom roles provide an alternative method for granting permissions that are more restrictive than the built-in “Reader” role. These custom roles (JSON) define the minimum permissions required by Densify to collect resource utilization metrics data, respectively.

The “Densify Resource Utilization Metrics Reader” custom role grants read-only permissions for collecting data related to VMs, SQL servers and reservations in the subscriptions specified in the assigned scope.

Custom Role: Densify Resource Utilization Metrics Reader

```
{
    "properties": {
        "roleName": "DensifyResourceUtilizationMetricsReaderCustomRole",
        "description": "This custom role defines the minimum read-only permissions required by Densify for collecting data related to VMs, SQL servers and reservations associated in the subscriptions specified in the assigned scope",
        "assignableScopes": [
        ],
        "permissions": [
            {
                "actions": [

                    "Microsoft.Capacity/appliedreservations/read",
                    "Microsoft.ClassicCompute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachineScaleSets/read",
                    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
                    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read",
```

Custom Role: Densify Resource Utilization Metrics Reader

```
                    "Microsoft.Insights/AutoscaleSettings/Read",
                    "Microsoft.Insights/Metrics/read",
                    "Microsoft.Insights/MetricDefinitions/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/virtualNetworks/read"
                    "Microsoft.Resources/subscriptions/read",
                    "Microsoft.Resources/subscriptions/resourceGroups/read",
                    "Microsoft.Sql/servers/databases/read",
                    "Microsoft.Sql/servers/elasticPools/read",
                    "Microsoft.Sql/servers/read"

                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

Use the following instructions to create the custom roles:

1. Copy the above sample and save it as JSON files.
2. Login into your Azure account. You must have admin or owner privileges for your Azure portal. See Required Account Permissions.
3. Navigate to **Subscriptions** in the main menu. You may need to click on **All services** to see **Subscriptions**. Select a subscription.
4. Click **Access Control (IAM)**.
5. Click **Add** > **Add custom role**.
6. In **Create a custom role**, select **Start from JSON** and then select one of the custom role JSON files, that you saved above. The role name and description fields are populated with details from the JSON file. The file will also be validated.
7. Click Next and review the list of permissions.
8. Click the **Assignable scope** tab and select subscription as the **Type**. Select the subscriptions to which the custom role will be assigned.
9. Click the JSON tab to review your settings and then create the custom role and click Save.
10. Assign the custom role to the Densify service principal. See Assigning Access to Subscriptions.

Create the Service Principal Through the Azure CLI

If you are comfortable working with the command line, you can create the service principle through the Azure CLI. You can then use the resulting .JSON file when working with the Densify API. Refer to the Azure website for details: Create an Azure service principal with the Azure CLI.

Creating the Cloud Connection in Densify

Once all of the prerequisites are complete, you can create the cloud connection through the Cloud Connection wizard. See *Using the Public Cloud Connection Wizard* (Help Topic ID 380290).

Modifying Your Azure Cloud Connection

When you create the Azure cloud connection for the first time, Densify discovers all of the subscriptions, associated with the user or service principal. Upon saving the connection it will schedule data collection from each of the discovered and selected subscriptions.

If subsequently, subscriptions are added, they will not be included in data collection. Additionally, subscriptions that are removed will continue to be included, resulting in wasted time and resources. To add new subscriptions or remove old ones, edit the cloud connection. See *Editing a Connection*, in the topic *Using the Public Cloud Connection Wizard* (Help Topic ID 380290).