

# 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 and billing data.

If you using reservations, the application must also be assigned the role of "Reader" for each reservation order. See [Working with Reservations](#) for details on additional configuration.

## 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 and billing 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.

## Collecting Billing Data

When collecting billing data, no additional configuration is required within your Azure subscription. You need to create a cloud connection using the same information used for collection of utilization data, as listed above.

Densify collects and analyzes the data and then generates various cost optimization reports. You can review these reports through the Cloud Cost Intelligence console. See [Viewing Your Public Cloud Billing Reports on page 1](#).

If you are using Azure reservations, see [Working with Reservations](#) for details of additional configuration.

## Limitation on the Types of Subscriptions

Due to limitations when using the Microsoft Azure APIs, only the following types of subscriptions are collected:

- Enterprise Enrollments;
- Web Direct Subscriptions.

Currently the following subscriptions are not supported for billing optimization:

- MS-AZR-0145P (CSP)
- MS-AZR-0036P (sponsored)
- MS-AZR-0144P (DreamSpark)
- MS-AZR-0146P (CSP)
- MS-AZR-0143P (sponsored)
- MS-AZR-159P (CSP)
- MS-AZR-0015P (internal)

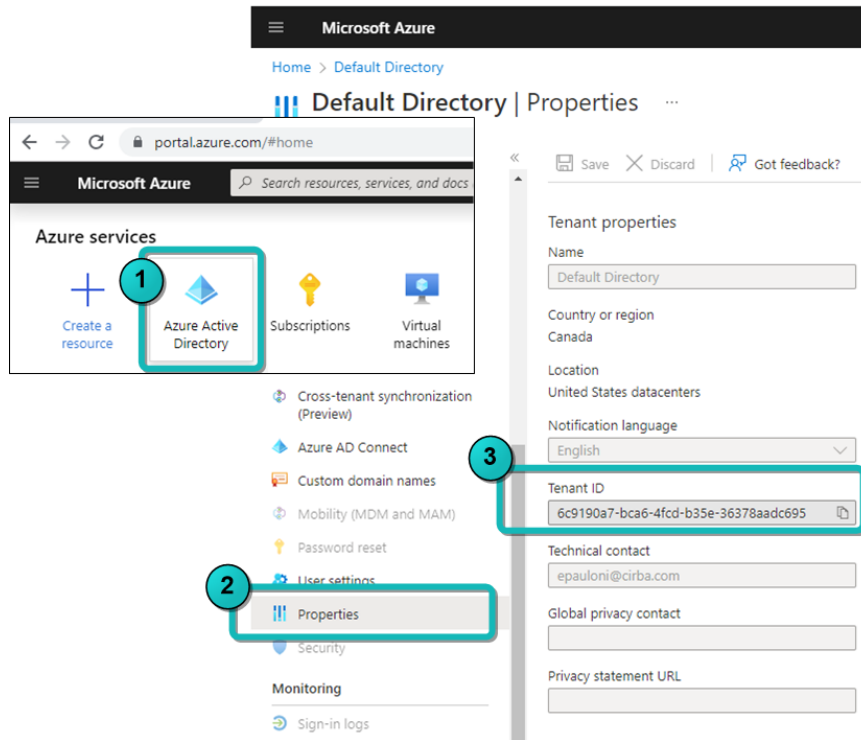
The APIs are continually updated to support other types of Azure subscriptions. See Microsoft's [Consumption API Overview](#) for details.

## 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

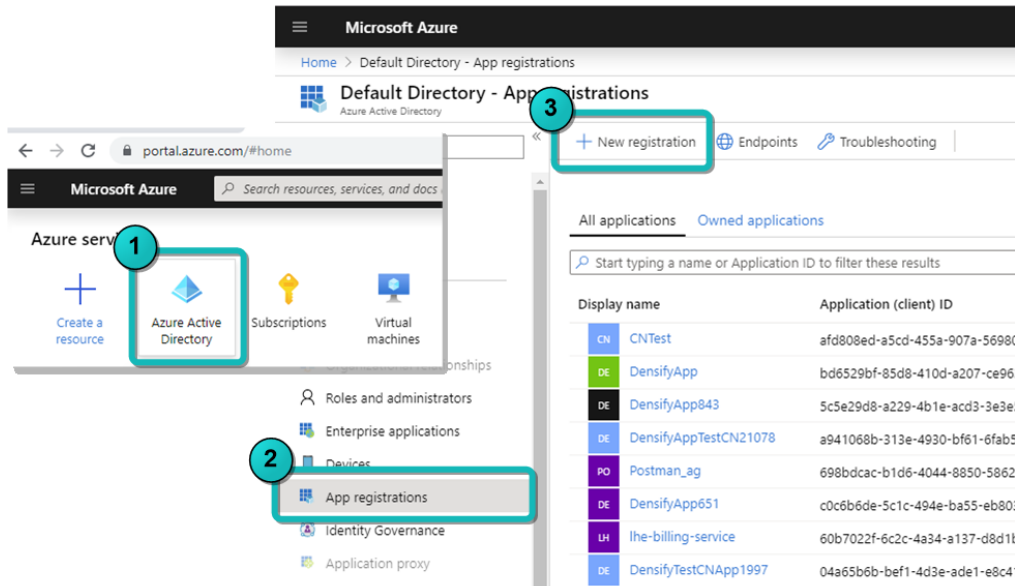


## Obtaining the Application ID and Client Secret

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

Microsoft Azure

Home > Default Directory > App registrations > Register an application

### Register an application

**\* Name**  
The user-facing display name for this application (this can be changed later).

Densify\_Connection ✓

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web  
https://Densify.com ✓

By proceeding, you agree to the [Microsoft Platform Policies](#)

**4** Register

- 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

Microsoft Azure

Search resources, services, and docs (G+/I)

Home >

### DensifyAppRegistration

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Essentials

Display name : DensifyAppRegistration

**5** Application (client) ID : 01da2890-c867-4bb4-8cce-a80a5e4b672b

Object ID : 785e9a00-b583-4832-8e08-a5613f24fd89

Directory (tenant) ID : 6c9190a7-bca6-4fcd-b35e-36378aad695

Supported account types : [My organization only](#)

**6** Client credentials : [Add a certificate or secret](#)

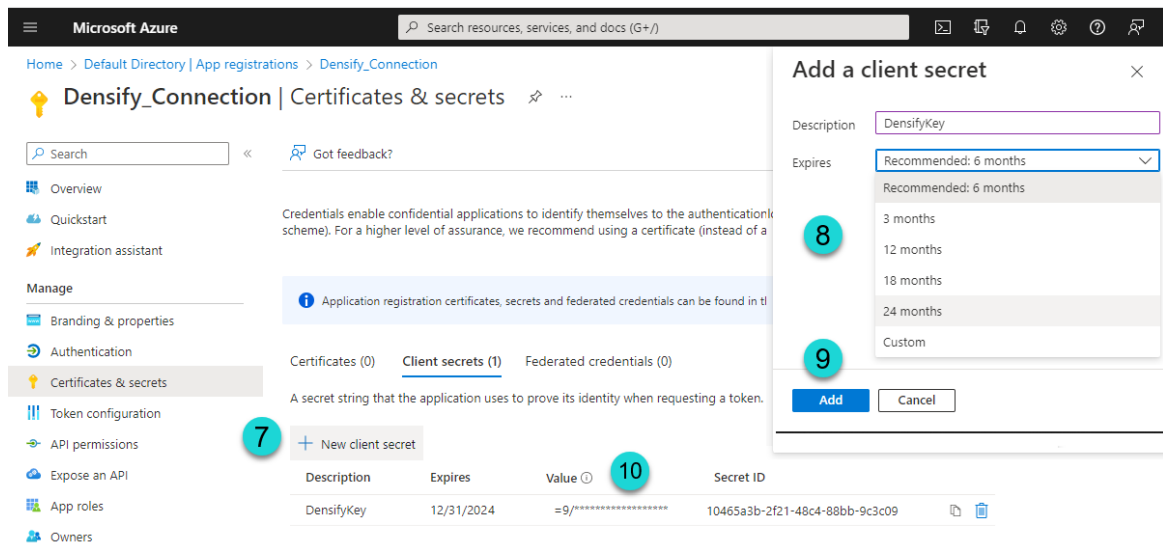
Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : [DensifyAppRegistration](#)

- Click **Client credentials** to see the page.
- Click on **New client secret** to create a new key.
- 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).
- Click **Add** to create the key.
- 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.

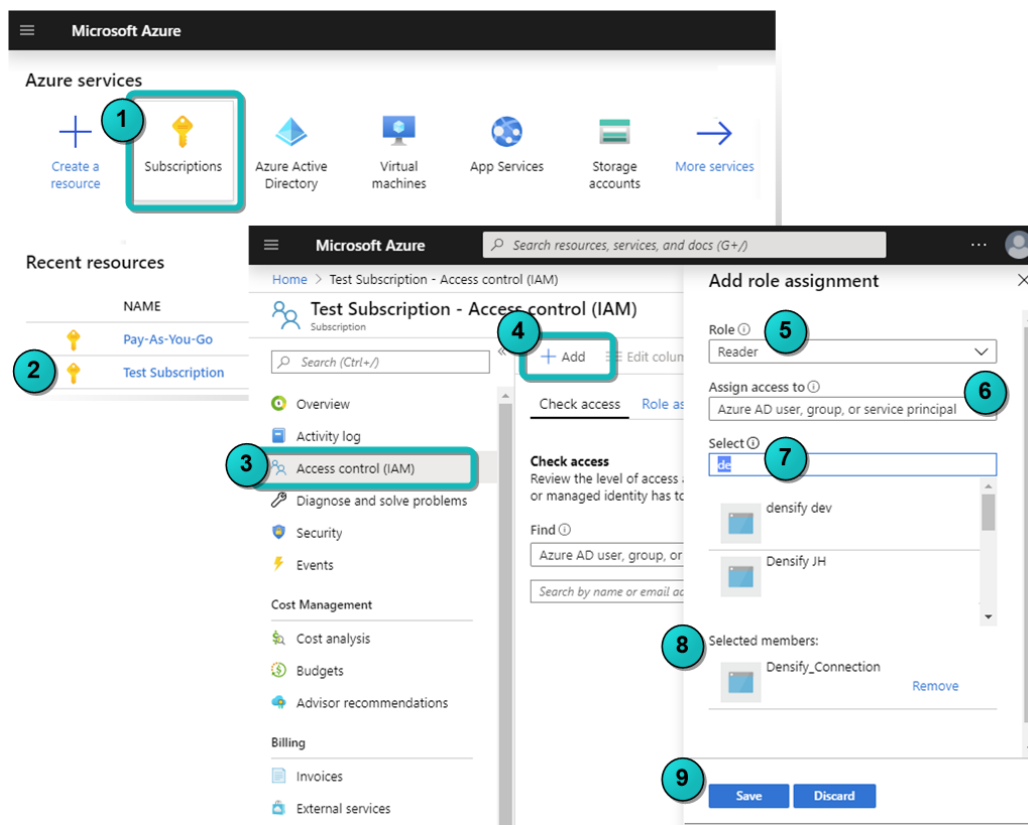
1. Navigate to **Subscriptions** in the main menu. You may need to click on **More services** to see **Subscriptions**.
2. Click on a subscription to open the configuration page.
3. Copy the Subscription ID. You need to copy this ID and save it to a location from which you can easily retrieve it. You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

**Note:** If you are using reservations, the application must also be assigned the role of "Reader" for each reservation order. See [Working with Reservations](#) for details on additional configuration.



## 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](#)
- [Working with Reservations](#)

## 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 and billing 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 and billing 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

```
1  {
2      "properties": {
3          "roleName": "DensifyResourceUtilizationMetricsReaderCustomRole",
4          "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",
5          "assignableScopes": [
6              ],
7          "permissions": [
8              {
9                  "actions": [
10
11                      "Microsoft.Capacity/appliedreservations/read",
12                      "Microsoft.ClassicCompute/virtualMachines/read",
13                      "Microsoft.Compute/virtualMachines/read",
14                      "Microsoft.Compute/virtualMachines/instanceView/read",
15                      "Microsoft.Compute/virtualMachineScaleSets/read",
```

**Custom Role: Densify Resource Utilization Metrics Reader**

```

16 |         "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
17 |         "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read",
18 |         "Microsoft.Insights/AutoscaleSettings/Read",
19 |         "Microsoft.Insights/Metrics/read",
20 |         "Microsoft.Insights/MetricDefinitions/read",
21 |         "Microsoft.Network/networkInterfaces/read",
22 |         "Microsoft.Network/networkSecurityGroups/read",
23 |         "Microsoft.Network/virtualNetworks/read",
24 |         "Microsoft.Resources/subscriptions/read",
25 |         "Microsoft.Resources/subscriptions/resourceGroups/read",
26 |         "Microsoft.Sql/servers/databases/read",
27 |         "Microsoft.Sql/servers/elasticPools/read",
28 |         "Microsoft.Sql/servers/read"
29 |     ],
30 |     "notActions": [],
31 |     "dataActions": [],
32 |     "notDataActions": []
33 | }
34 | }
35 | ]
36 | }
37 | }

```

The “Densify Billing Reader” custom role grants read-only permissions for collecting billing and reservation data associated with the subscriptions, specified in the assigned scope.

**Custom Role: Densify Billing Reader**

```

1 | {
2 |   "properties": {
3 |     "roleName": "DensifyBillingReaderCustomRole",
4 |     "description": "This custom role defines the minimum read-only
permissions required by Densify for collecting billing and reservation data
associated with the subscriptions specified in the assigned scope",
5 |     "assignableScopes": [
6 |     ],
7 |     "permissions": [
8 |       {
9 |         "actions": [
10 |           "Microsoft.Resources/subscriptions/read",
11 |           "Microsoft.Capacity/reservationorders/read",
12 |           "Microsoft.Capacity/reservationorders/reservations/read",
13 |           "Microsoft.Consumption/reservationRecommendations/read",
14 |           "Microsoft.Consumption/reservationSummaries/read",
15 |           "Microsoft.Consumption/usageDetails/read"
16 |         ],
17 |         "notActions": [],
18 |         "dataActions": [],
19 |         "notDataActions": []
20 |       }
21 |     ]
22 |   }

```

```
Custom Role: Densify Billing Reader
```

```
23 | }
```

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. Repeat steps 3 to 8 to create the other custom role.
11. Assign the custom roles 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 Azure website for details: [Create an Azure service principal with the Azure CLI](#).

## Working with Reservations

When you buy an Azure reservation, access is restricted to the user who bought it (e.g. user-adm@IT.on.microsoft.com) and the account administrator (e.g. IT@Densify.com). There are two ways to allow the Densify service principal to access and collect data related to these reservations:

- Assign the Reservations Reader role at the tenant level—Assigning the reservation reader role at the tenant level automatically grants read access to all reservations in the Azure AD tenant (directory). When you grant access at the tenant level, you do not need to grant access to new reservations as they are acquired, nor do you need to provide access to each subscription individually.
- Assign the Reader role to each reservation order—Assigning the reader role at the reservation order level requires you to grant access to each existing order and to new reservations as they are

acquired. However, this method allows you to grant access to a sub-set of reservation orders, if appropriate.

Use this method if only a subset of your subscriptions are being analyzed by Densify. Collecting reservation data at the tenant level is not applicable for this use case.

## Assigning the Reservation Reader Role at the Tenant Level

You must elevate your access privileges to perform the required configuration, to enable "Access management for Azure resources".

1. Login to your Azure portal as a Global Administrator.
2. Navigate **Azure Active Directory** > under **Manage** > **Properties**.
3. Enable "Access management for Azure resources" for your role. This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. Refer to the Azure documentation for details: <https://docs.microsoft.com/en-us/azure/role-based-access-control>.

You can now assign the "Reservations Reader" role to the Densify Service Principal at the tenant level:

1. Obtain your Tenant ID/Directory ID corresponding to your Azure Active Directory. See [Obtaining the Tenant ID/Directory ID](#).
2. Obtain your Densify Service Principal name. See [Obtaining the Application ID and Client Secret](#).
3. Launch Azure Power Shell in your Azure portal and execute the following commands, substituting your tenant ID and the Densify service principal name as highlighted below.

Example: Assigning the "Reservations Reader" role to the Densify Service Principal

```
#Import required resources
Import-Module Az.Accounts
Import-Module Az.Resources

# Connect to Active Directory
Connect-AzAccount -Tenant <Tenant ID> -UseDeviceAuthentication

# Get the Densify Service Principal ID
$ServicePrincipalId = (Get-AzADServicePrincipal -DisplayName
<Densify Service Principal name> -First 1).Id

# Assign the Reservation Reader role to the Densify Service
Principal
New-AzRoleAssignment -Scope "/providers/Microsoft.Capacity" -
PrincipalId $ServicePrincipalId -RoleDefinitionName "Reservations
Reader"
```

Refer to the Azure documentation for details: <https://docs.microsoft.com/en-us/azure/cost-management-billing/reservations/view-reservations>

## Assigning the Reader Role to Each Reservation Order

If Densify is not analyzing all subscription in the Azure tenancy you can use this method to add Reader access to the reservation order to collect data for each associated reservation.

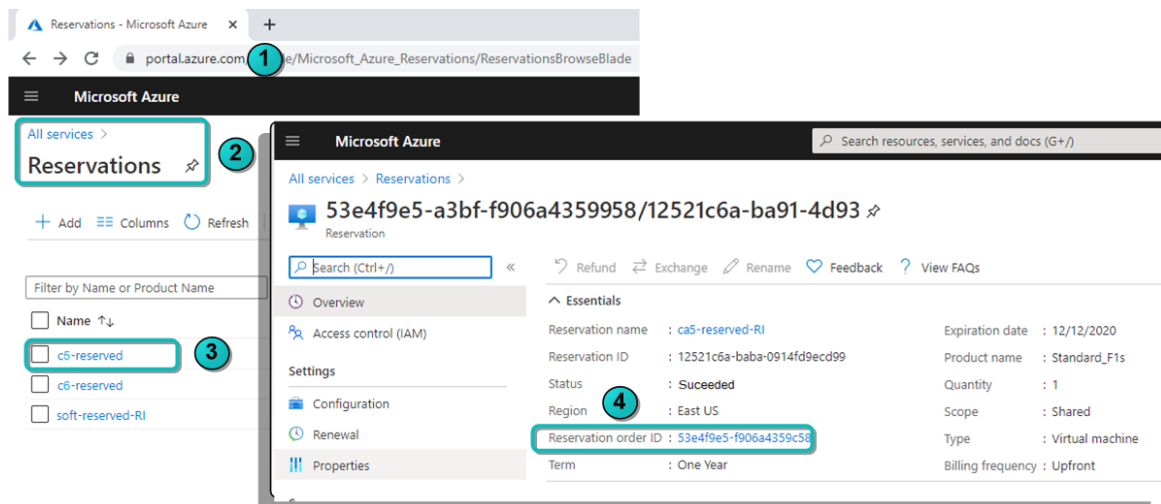
**Note:** Granting access to the Reservation only, is insufficient. Reader access must be granted to the reservation order.

When you give a user permission to manage a reservation, that does not give that user rights to manage the subscription. Allowing Densify to access the subscription does not also allow it to the reservation automatically.

To delegate Reader access for a reservation order:

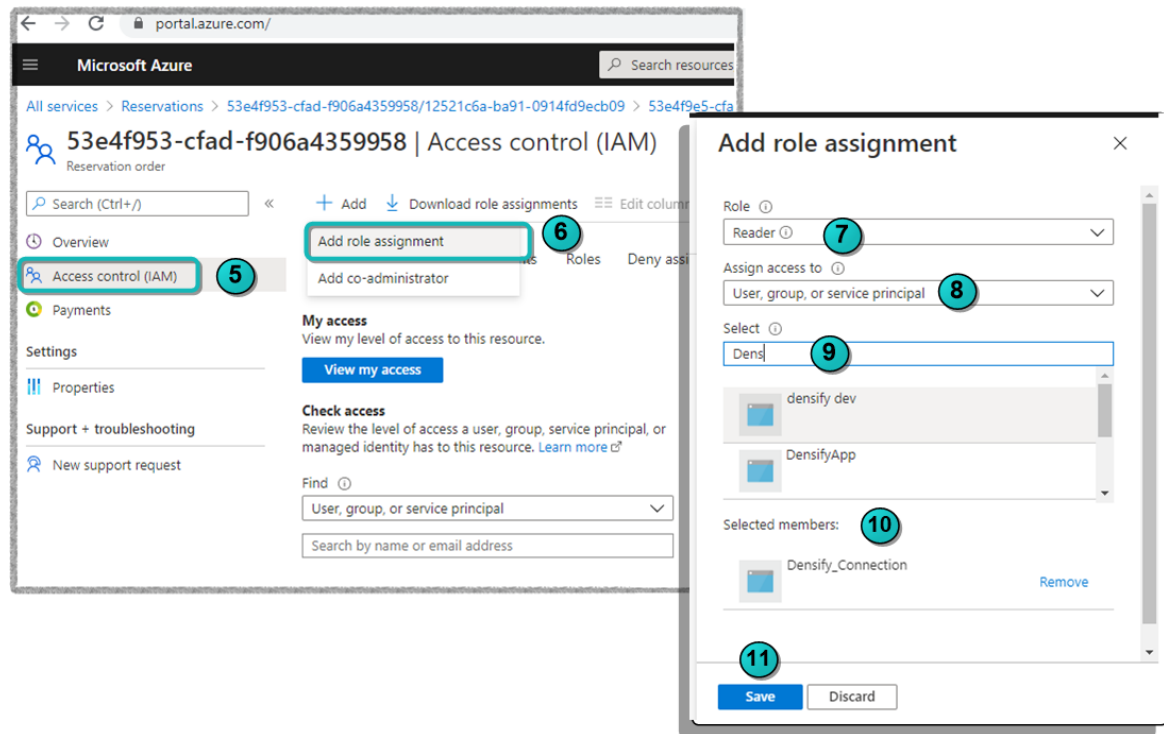
1. Login into your Azure portal
2. Click **All services** and navigate to **Reservations**.
3. In the Reservation pane you will see a list showing all the reservations for which you have the Owner or Reader role. Click a reservation link to open the configuration pane.
4. Click **Reservation order ID** to select and open the Reservation order pane.

Figure: Adding Reader Access to the Reservation Order



5. Click **Access Control (IAM)** in the left side-menu.
6. Select **Add > Add role assignment**
7. In the **Add role assignment** pane select **Reader**. Reader provides the minimum required permissions.
8. Ensure **Assign Access to** is set to "User, group, or service principal"
9. Search or scroll to locate the application (Densify\_Connection), that you created previously.
10. Locate and select your application. It will appear under **Selected members**.

Figure: Adding Reader Access to the Reservation Order



11. Click **Save** to save your changes.
12. Repeat this process for each reservation order to be included in Densify's data collection.

If the role assignment is done through the reservation order, then Densify can collect data for all reservations in the selected order. At the time of purchase, a reservation order has one Reservation; however, actions such as splitting, merging, obtaining a partial refund, or exchanging create new reservations under the reservation order.

## 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).