Microsoft Azure Sentinel – ServiceNow app installation guide

# Prerequisites

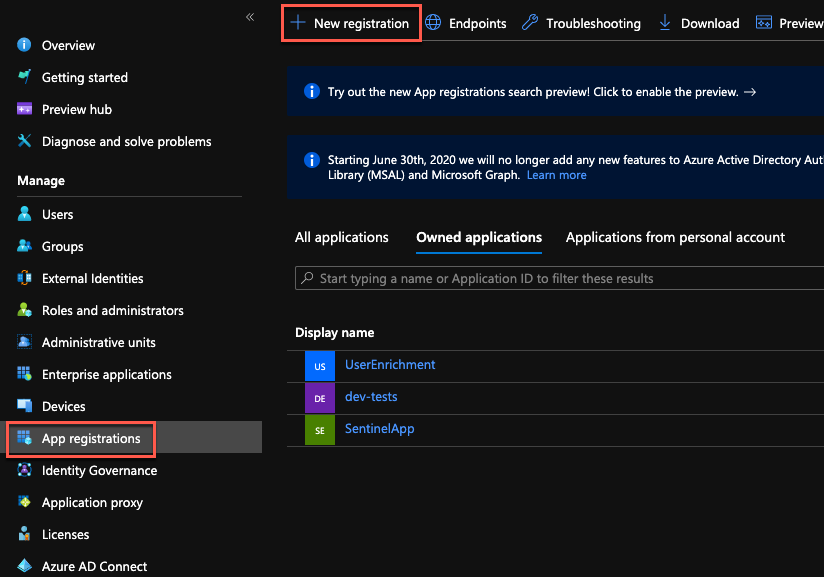
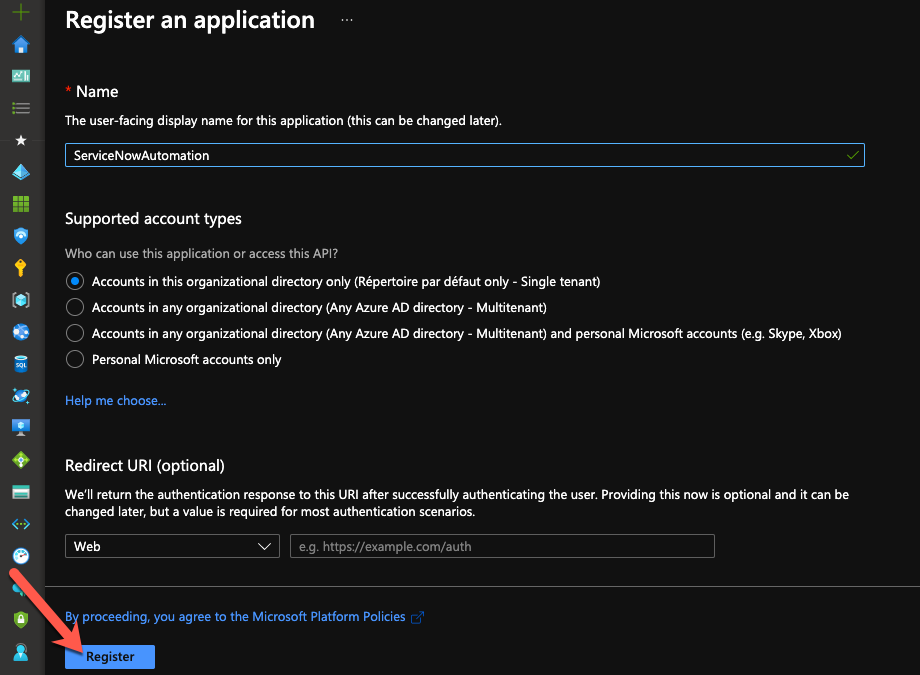
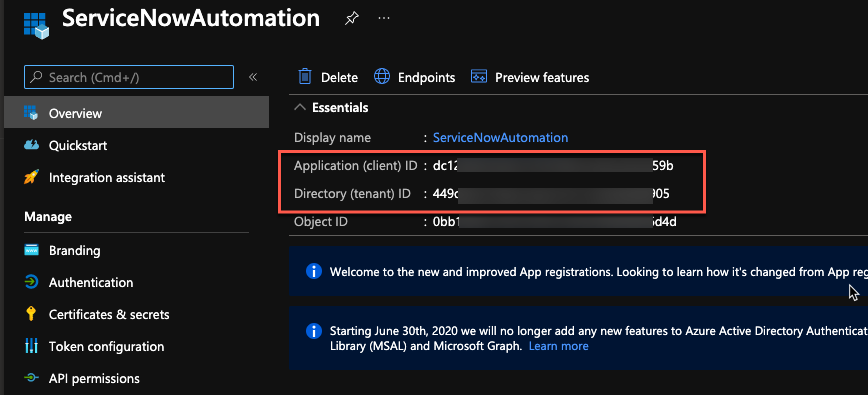
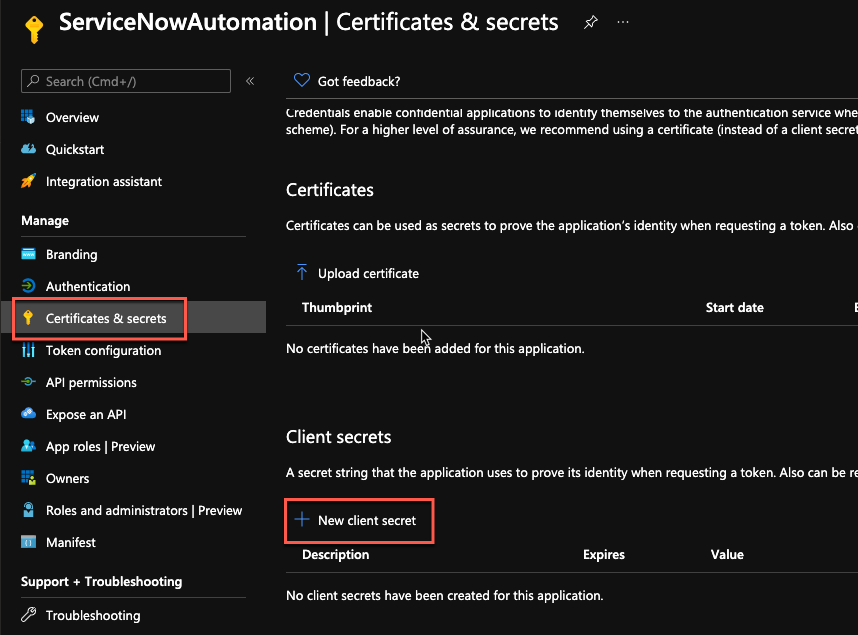
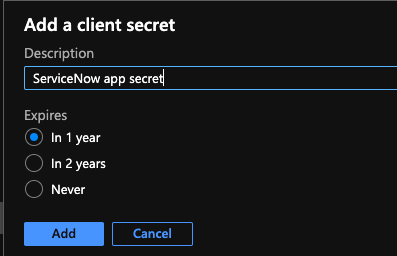
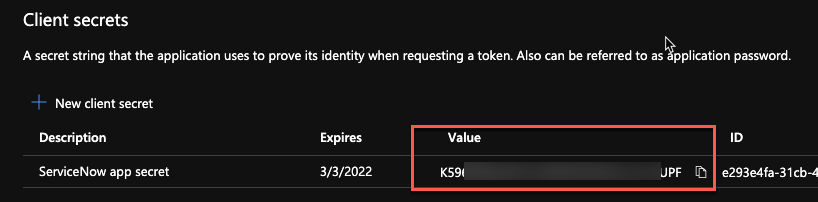
This ServiceNow application fully rely on the Azure Sentinel **Management API** to provide bi-directional sync between both platforms.

thumbnail image 1 of blog post titled 
 
 
  
 
 
 
    
  
   
    
      
       Azure Sentinel API 101
       
      
     
   
  
 
   
 
 
 
 
 

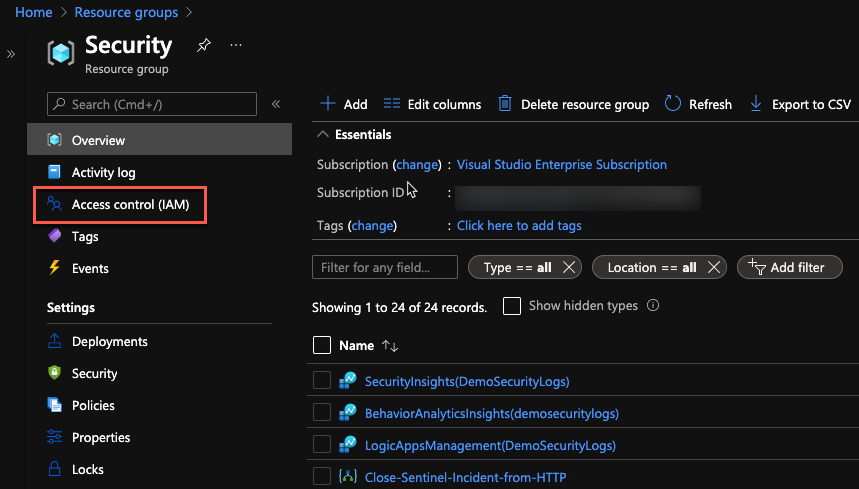
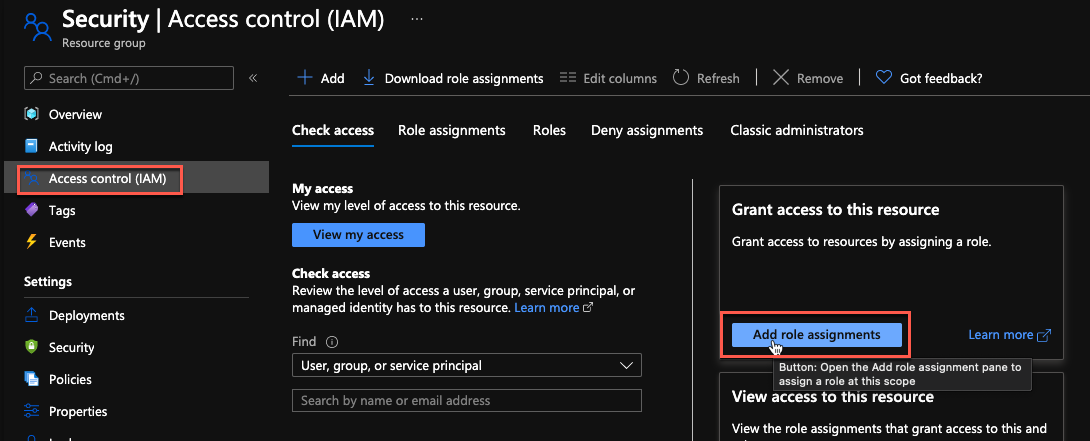
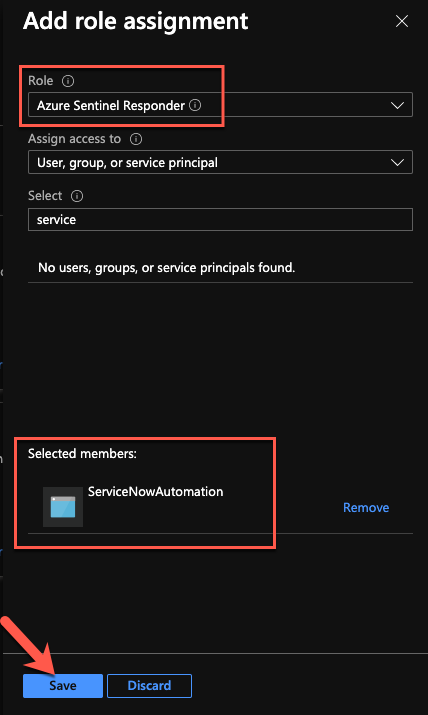

Azure Sentinel APIs reference

To provide access to our application, we have to create a Service Principal in Azure Active Directory, and assign to it the required permissions.

## Azure: Create the Service Principal

1. Go to the Azure portal, in Azure AD service, App Registrations:  
   <https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps>
2. Click on “New registration”.  
   
3. Provide a name for the app and click “Register”.  
   
4. Take note of the Application (client) ID and Directory (tenant) ID. We’ll need them during the ServiceNow configuration.
5. Go to “Certificates & secrets” and click on “New client secret”.  
   
6. Provide a name for the secret and a validity period.  
   Important: when the secret will expire, you’ll have to create a new one and update the ServiceNow configuration.  
   
7. Note the secret and keep it in a safe location for later use.  
   

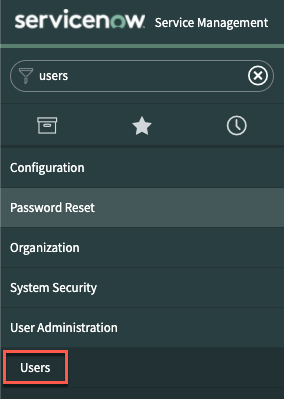
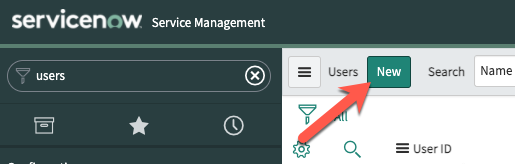
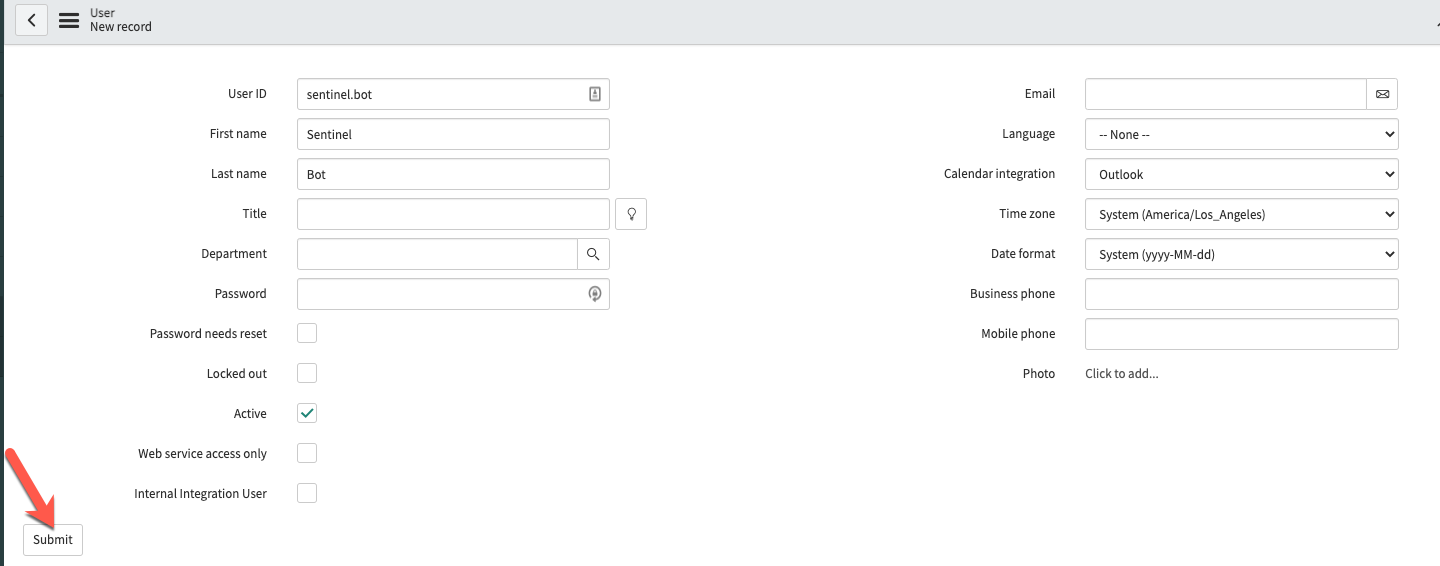
## Delegate permissions to the Service Principal

1. In the Azure portal, go to the Resource Group containing your Azure Sentinel workspace and click on “Access control (IAM)”.  
   
2. Click on “Add role assignments”.  
   
3. In the new blade, select the “Azure Sentinel Responder” role, then select the Service Principal we created before, and click on the “Save” button.  
   

We are now done with the Azure configuration part.

## ServiceNow: create a user for Azure Sentinel

To identify the incidents created from Azure Sentinel incidents, we will create a user. This user will be used as the “caller\_id” property, when creating new records.

1. In ServiceNow, under “User Administration”, click on “Users”.  
   
2. Click on the ”New” button.  
   
3. Provide the required details and click on “Submit”.  
   

# Installation

## Import the application in ServiceNow

1. Search for “update set” and select the “Retrieved Update Sets” module. Then, click on the “**Import Update Set from XML**” link.

Graphical user interface, text, application

Description automatically generated

1. Click on the “Choose File” button and select the application XML file.  
   Then, click on the “Upload” button.

Graphical user interface

Description automatically generated

1. Once uploaded, you will see the new imported update set. Click on it to open it.

Graphical user interface, application

Description automatically generated

1. Click on the “Preview Update Set” button.

Graphical user interface

Description automatically generated

Shape, rectangle

Description automatically generated

1. Click on the “Commit Update Set” button.

Graphical user interface, application

Description automatically generated

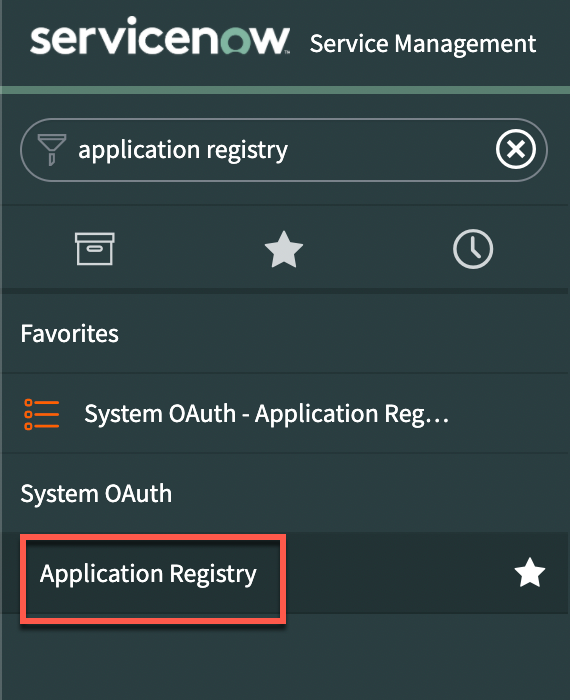
Rectangle

Description automatically generated

The application is now imported and is available in “Studio”.

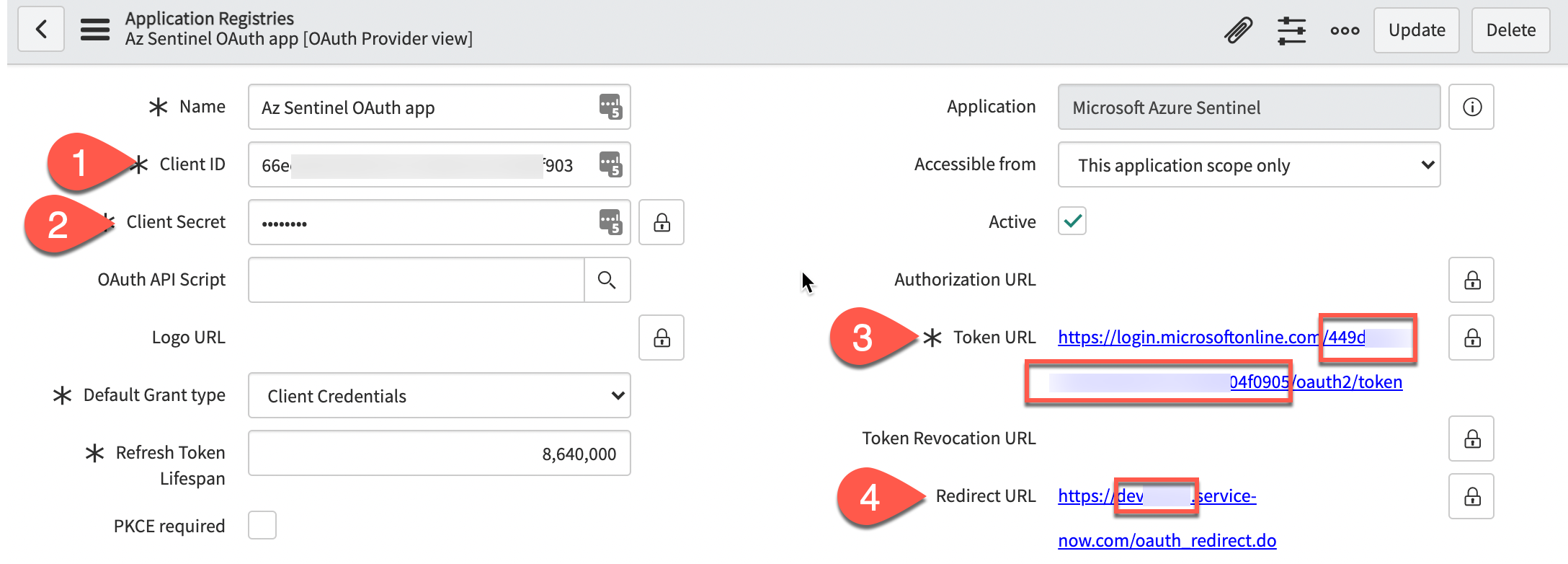
## Configure the OAuth credentials

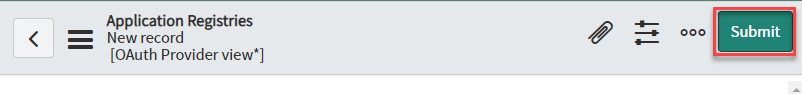
To be able use the Azure Sentinel Management API from ServiceNow, we must configure the credentials we created previously in Azure AD. This is done using an “Application Registry”.

1. Search for “Application Registry” and click on the link.  
   
2. Create a new set of credentials. We’ll use “Az Sentinel OAuth app” but you can use any name you want.  
   Graphical user interface, text, application

   Description automatically generated.
3. Select “Connect to a third party OAuth Provider”.  
   Graphical user interface, text, application

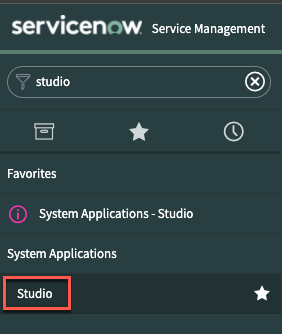
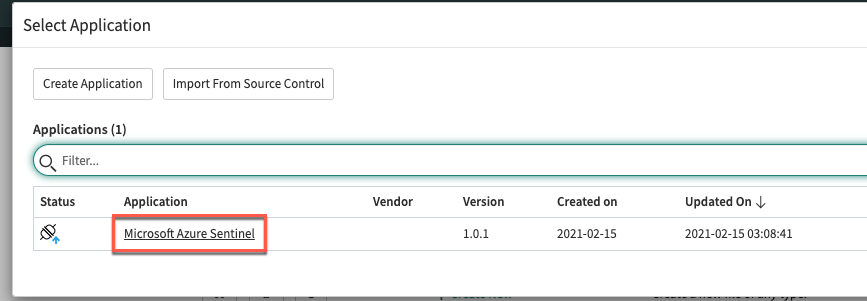
   Description automatically generated
4. On the credentials configuration page, we must provide the information we collected during the Service Principal creation:
   * Client ID (1): Azure AD application/client ID
   * Client secret (2): Azure AD client secret
   * Default Grant type: Client Credentials
   * Token URL (3): add your Azure AD tenant ID in the URL:  
     [https://login.microsoftonline.com/{AAD\_tenant\_id}/oauth2/token](https://login.microsoftonline.com/%7bAAD_tenant_id%7d/oauth2/token)
   * Token Revocation URL (4): add your ServiceNow instance name in the URL:  
     https://{instance\_name}.service-now.com/oauth\_redirect.do



1. Click on the “Submit” button to save your changes.  
   

## Configure the application

Now that we have imported the application, we must configure the details to connect to the Azure Sentinel Management API.

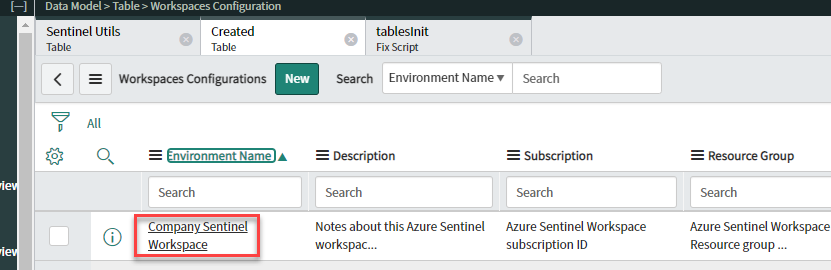
1. Search for “Studio” and open it. Then, select the newly imported application.  
     
   
2. Scroll to the “FixScript” section and run the “tablesInit” script.  
   This script will populate the tables  
   Graphical user interface, text, application

   Description automatically generated  
     
   Graphical user interface, application

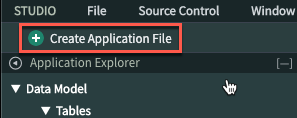
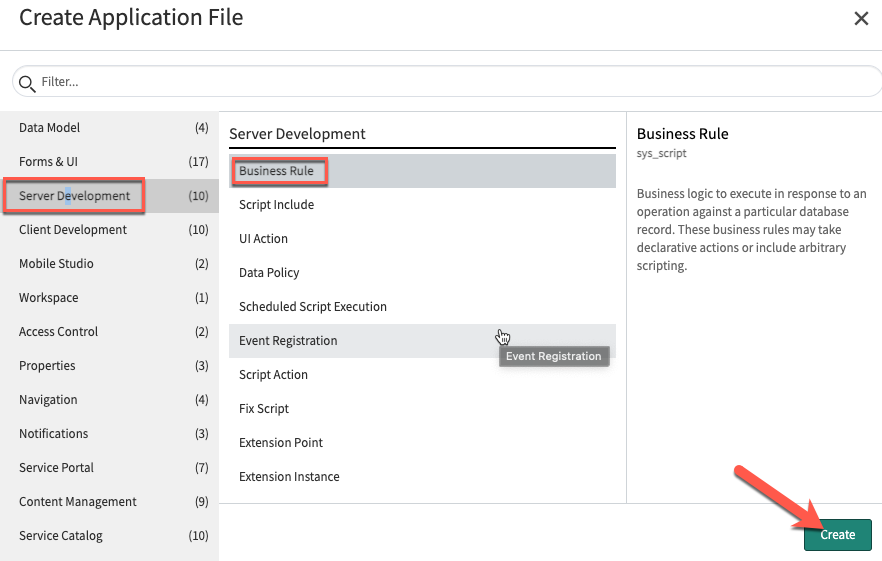
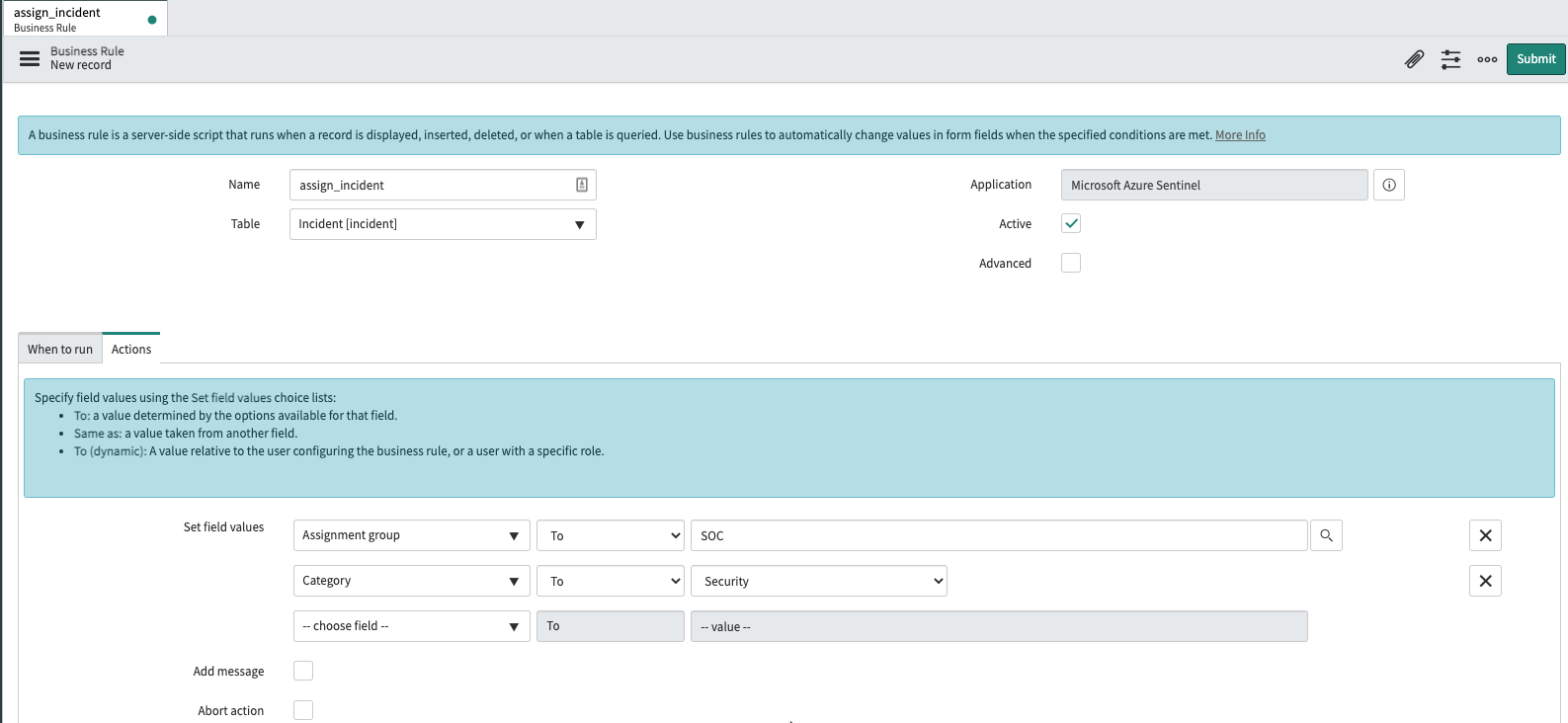
   Description automatically generated  
     
   Graphical user interface, text, application

   Description automatically generated
3. Verify the “Sentinel Severity to ServiceNow” table mapping.  
   This table is used to map the Sentinel severity to the ServiceNow value, when creating or updating Azure Sentinel incidents.  
   Open the table => Show list, and review the values.
4. Verify the “Sentinel State to ServiceNow” table mapping.  
   This table is used to map the Sentinel state to the ServiceNow value, when creating or updating Azure Sentinel incidents.  
   Open the table => Show list, and review the values.
5. Verify the “ServiceNow Severity to Sentinel” table mapping.  
   This table is used to map the ServiceNow severity to the Sentinel value, when updating ServiceNow incidents.  
   Open the table => Show list, and review the values.
6. Verify the “ServiceNow State to Sentinel” table mapping.  
   This table is used to map the ServiceNow severity to the Sentinel value, when updating ServiceNow incidents.  
   Open the table => Show list, and review the values.
7. Configure the workspace(s) details. Open the “Workspaces Configuration” table and click on **Show List**.  
   Graphical user interface, text

   Description automatically generated
8. Open to edit the current row.



1. Provide the required values (available in Azure Sentinel) and click on the **Update** button.  
   Graphical user interface, text, application

   Description automatically generated
2. If needed, create a new Business Rule to assign specific properties, like the “Assignment Group” or the “Category”.  
   This can be achieved by clicking on “Create Application File”, selecting “Server Development”, “Business Rule”.  
     
     
     
   

## 

Table of Contents

[Prerequisites 1](#_Toc66278655)

[Azure: Create the Service Principal 1](#_Toc66278656)

[Delegate permissions to the Service Principal 4](#_Toc66278657)

[ServiceNow: create a user for Azure Sentinel 5](#_Toc66278658)

[Installation 7](#_Toc66278659)

[Import the application in ServiceNow 7](#_Toc66278660)

[Configure the OAuth credentials 7](#_Toc66278661)

[Configure the application 8](#_Toc66278662)