Microsoft Azure Sentinel – ServiceNow app installation guide

# Blog

Many companies currently rely on ServiceNow to manage their security incidents. Reasons for using ServiceNow instead of the Azure Sentinel portal can be incident assignment workflows, task assignment outside of the SOC, custom reporting and more.

As we are continuously working on improving the analysts experience by seamlessly integrating with the non-Microsoft solutions used by the SOC team, we are glad to announce our new integration between Azure Sentinel and ServiceNow, which provides bi-directional sync between both platforms.  
The solution is running on the Now platform as an app, and only requires access to the Azure Sentinel Management API to synchronize incidents.

In this blog post, we’ll guide you through the key features, the app installation and its configuration.  
For those who prefer videos, you can use this link and watch a full deployment walkthrough.



## Key features

The application provides the following capabilities:

* Incident creation (Azure Sentinel to ServiceNow only)
* Incident alerts synchronization
* Incident entities synchronization
* Incident comments synchronization
* Incident status synchronization
* Incident severity synchronization
* Incident owner assignment synchronization
* Multi-workspaces support
* Custom ServiceNow incident table support

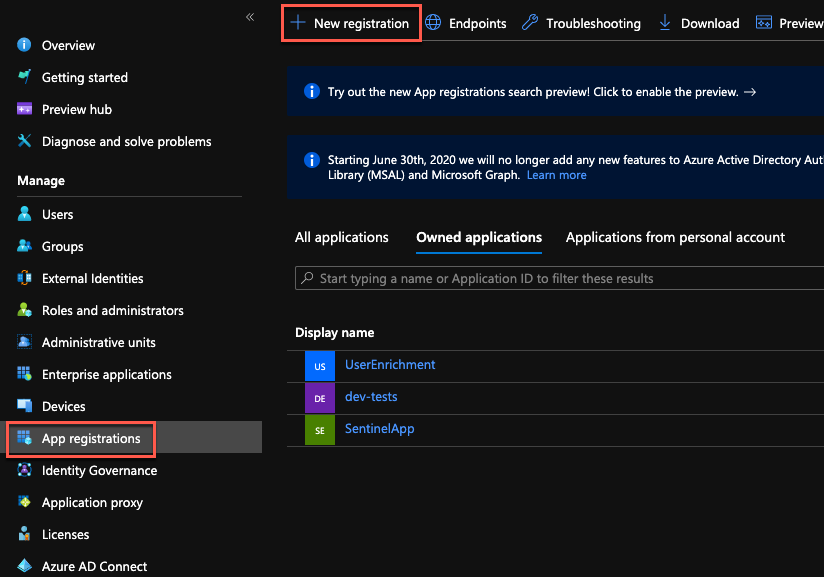
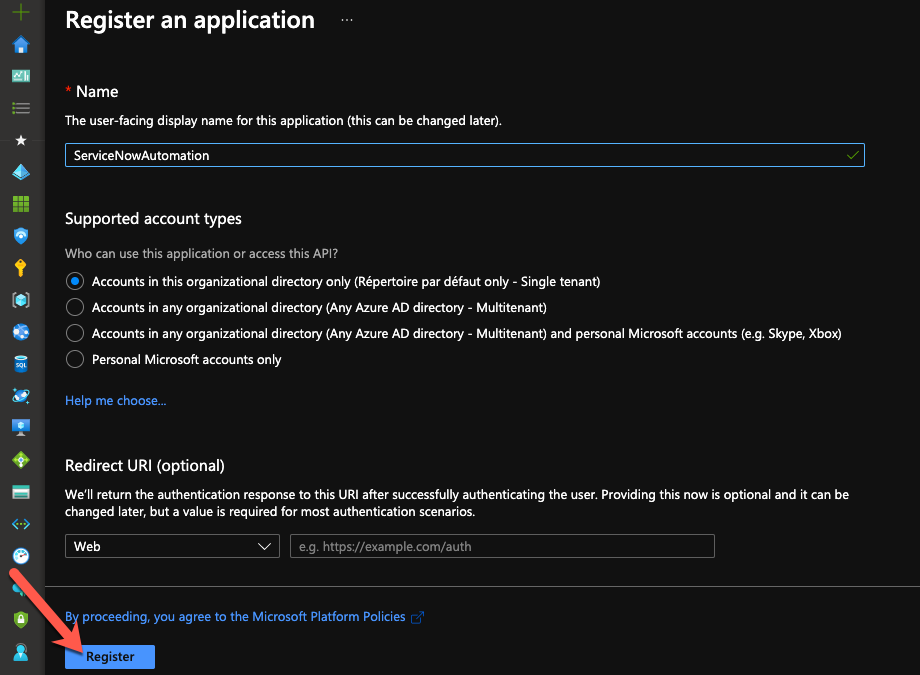
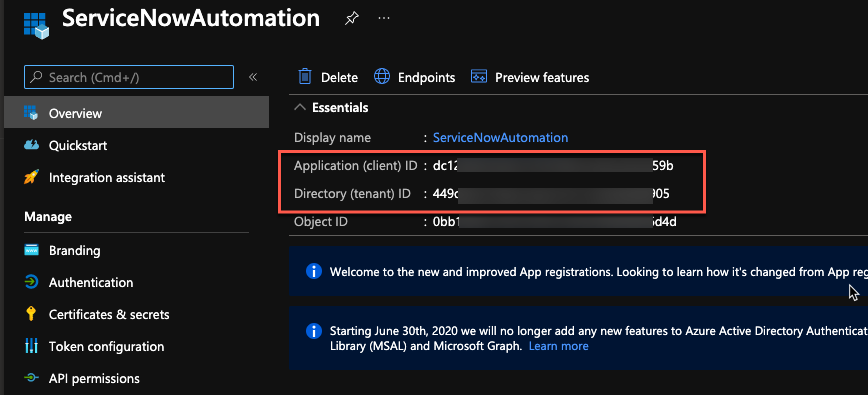
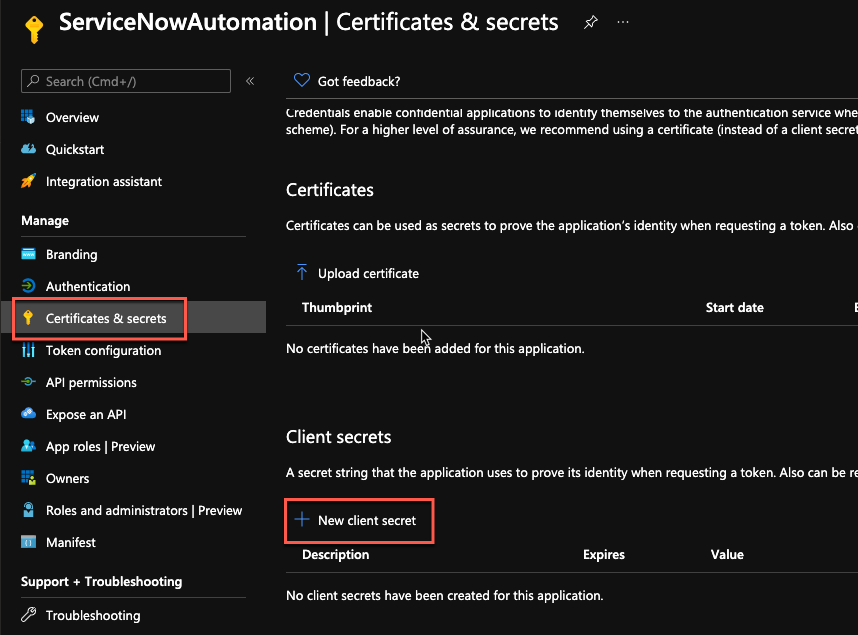
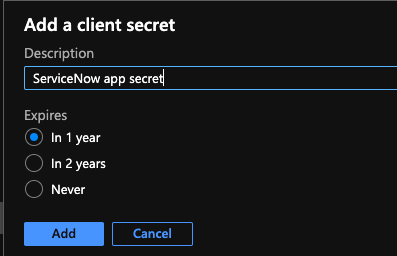
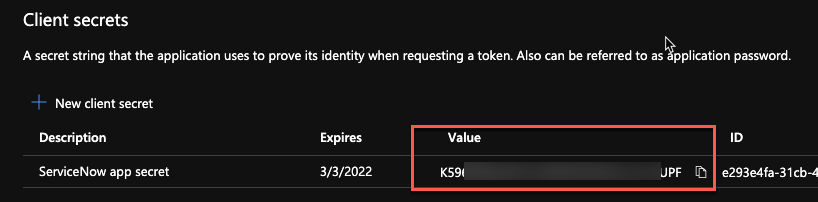
## Prerequisites

As the application relies on the Azure Sentinel Management API for the bi-directional sync between both platforms, we must create a Service Principal in Azure Active Directory with the required permissions.  
This service principal will then be used by the app to perform the API calls.

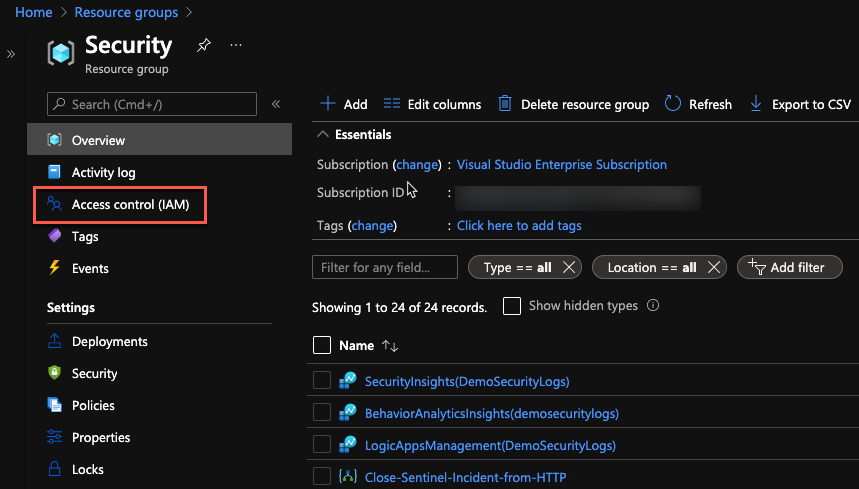
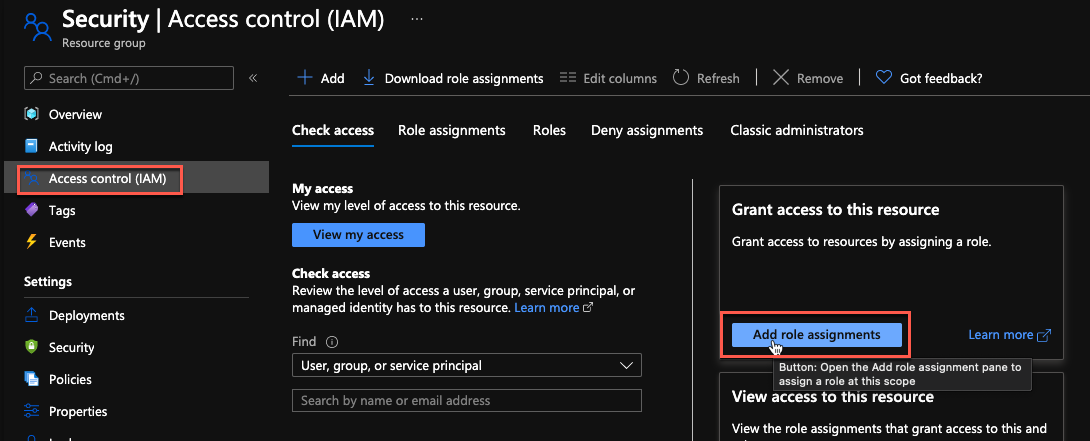
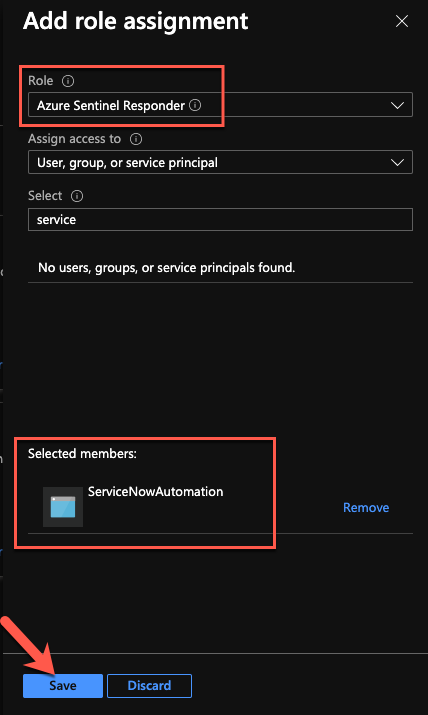
thumbnail image 1 of blog post titled 
 
 
  
 
 
 
    
  
   
    
      
       Azure Sentinel API 101
       
      
     
   
  
 
   
 
 
 
 
 


Azure Sentinel APIs reference

### In Azure: Create the application 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. Copy the secret and keep it in a safe location for later use.  
   

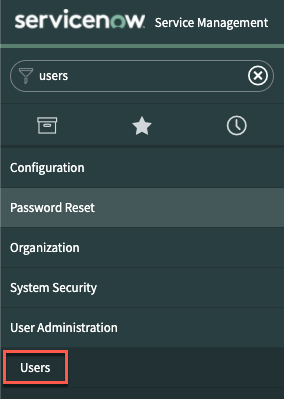
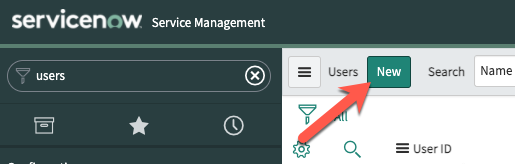
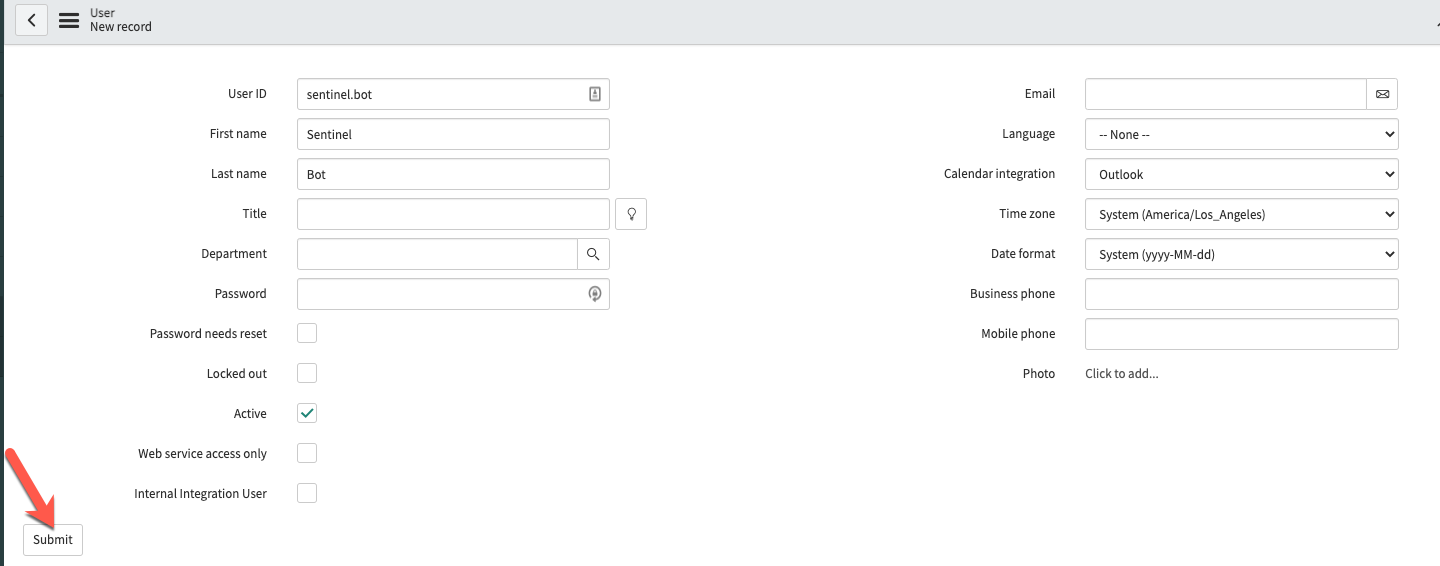
### Delegate permissions to the Service Principal

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.

### In 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 incidents.

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

**NOTE**: Currently, we provide this integration on our Azure Sentinel GitHub as an xml file, with community support, but we are working with ServiceNow to have it directly in the ServiceNow store, with Microsoft support.  
We will announce official support once available.

The file is available at **this address**.

1. In the menu, 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.

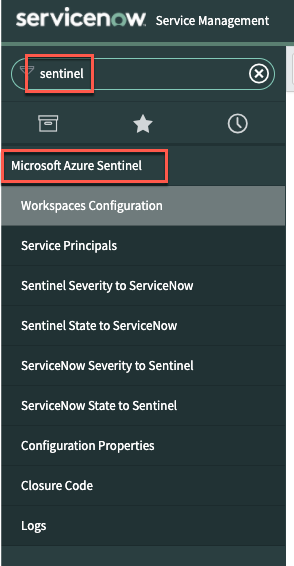
Graphical user interface, application

Description automatically generated

Rectangle

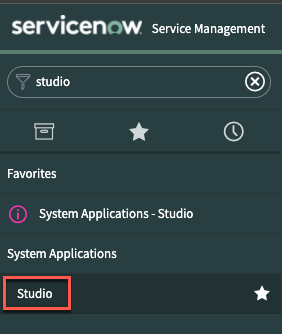
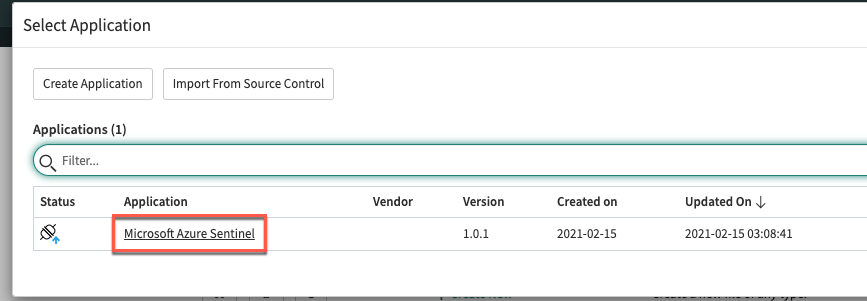
Description automatically generated

The application is now imported and available in ServiceNow!



## Configuration

Now that we have imported the application, we must configure it.  
We’ll start by running a script that will prepare the application:

1. Search for “Studio” and open it. Then, select the newly imported application.  
     
   

Scroll to the “FixScript” section and run the “**tablesInit**” script.  
This script will populate the tables used by the application.  
Graphical user interface, text, application

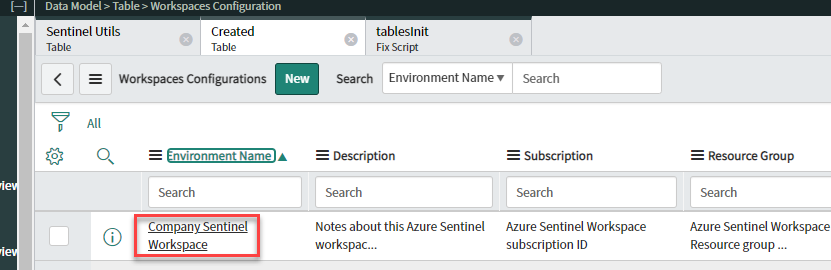
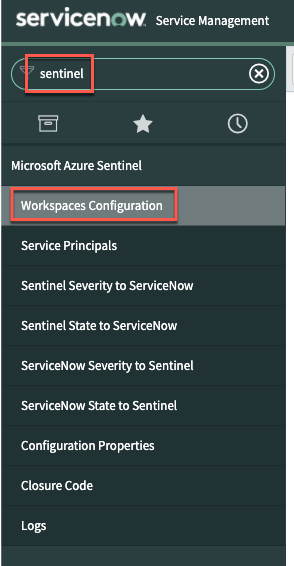
Description automatically generated  
  
Graphical user interface, application

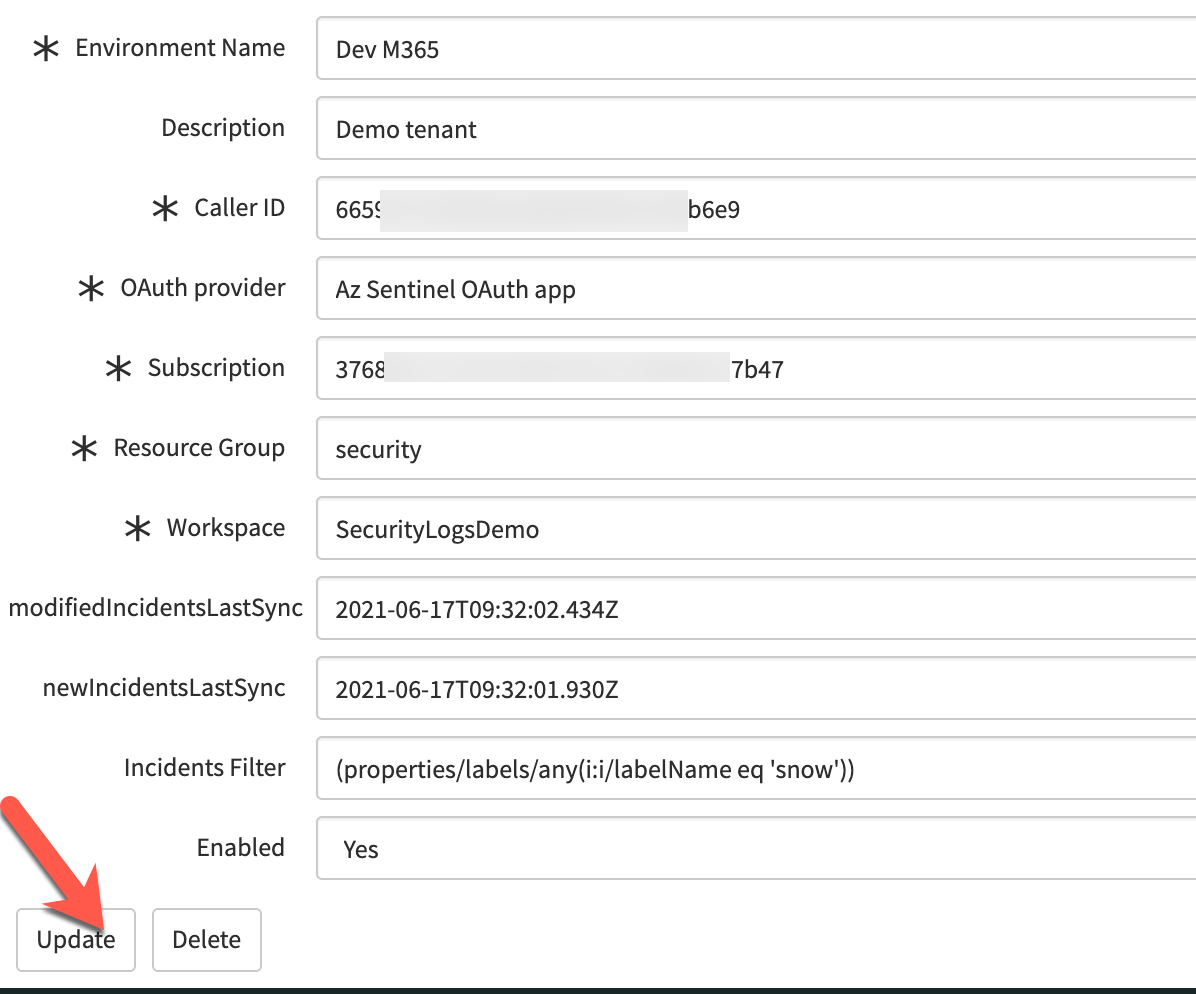
Description automatically generated  
  
Graphical user interface, text, application

Description automatically generated

You can now close “Studio”.

Azure Sentinel workspace(s) configuration  
In the Azure Sentinel module, the “Workspaces Configuration” section contains the Azure Sentinel workspaces configuration.  
Click on this section and edit the current row (you can create multiple configurations):



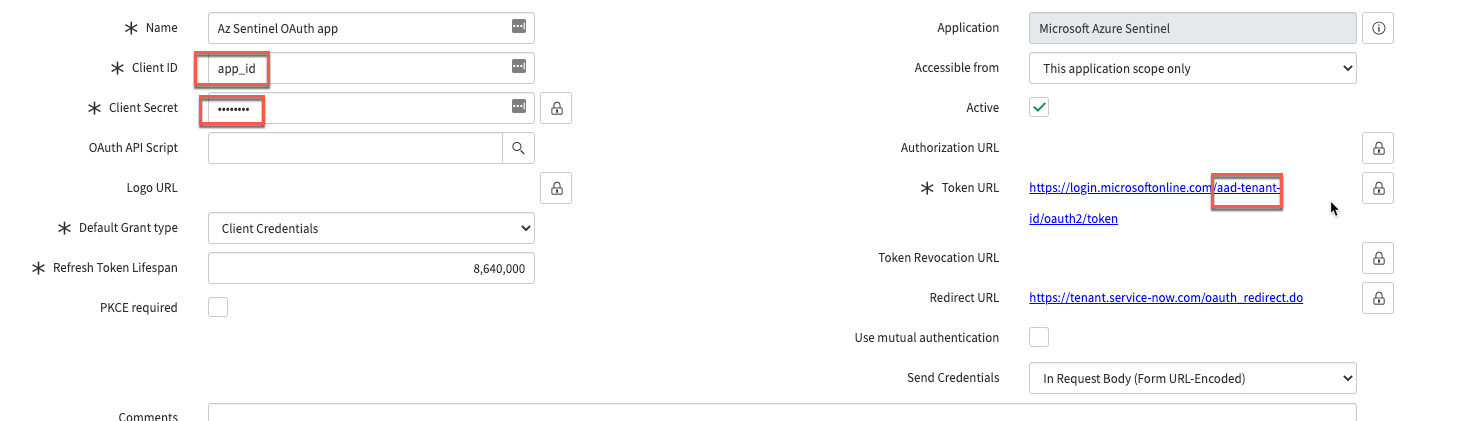
Provide the required values (available in Azure Sentinel) and click on the **Update** button:  


**Note**: In addition to the workspace configuration, you have the following properties:

* **Caller ID**: this is the ServiceNow user we created in the prerequisites section
* **OAuth provider**: this is the service principal object used to call the Azure Sentinel API. By default, the application uses “Az Sentinel OAuth App”, but you can create another credentials set if needed.
* **newIncidentsLastSync**: timestamp automatically updated once the app successfully contacts the Sentinel API to retrieve the new incidents since last update. If needed, you can manually change the value to query incidents newer than your specified date.
* **modifiedIncidentsLastSync**: timestamp automatically updated once the app successfully contacts the Sentinel API to retrieve the updated incidents since last update
* **Incidents filter**: filter used to retrieve only the matching incidents from Sentinel API. By default, it filters the incidents with a tag “snow”. To get all incidents, just delete the content of this field.
* **Enabled**: boolean value to specify if the workspace is enabled or not. When disabled, the incidents are not retrieved and the timestamps are not updated.

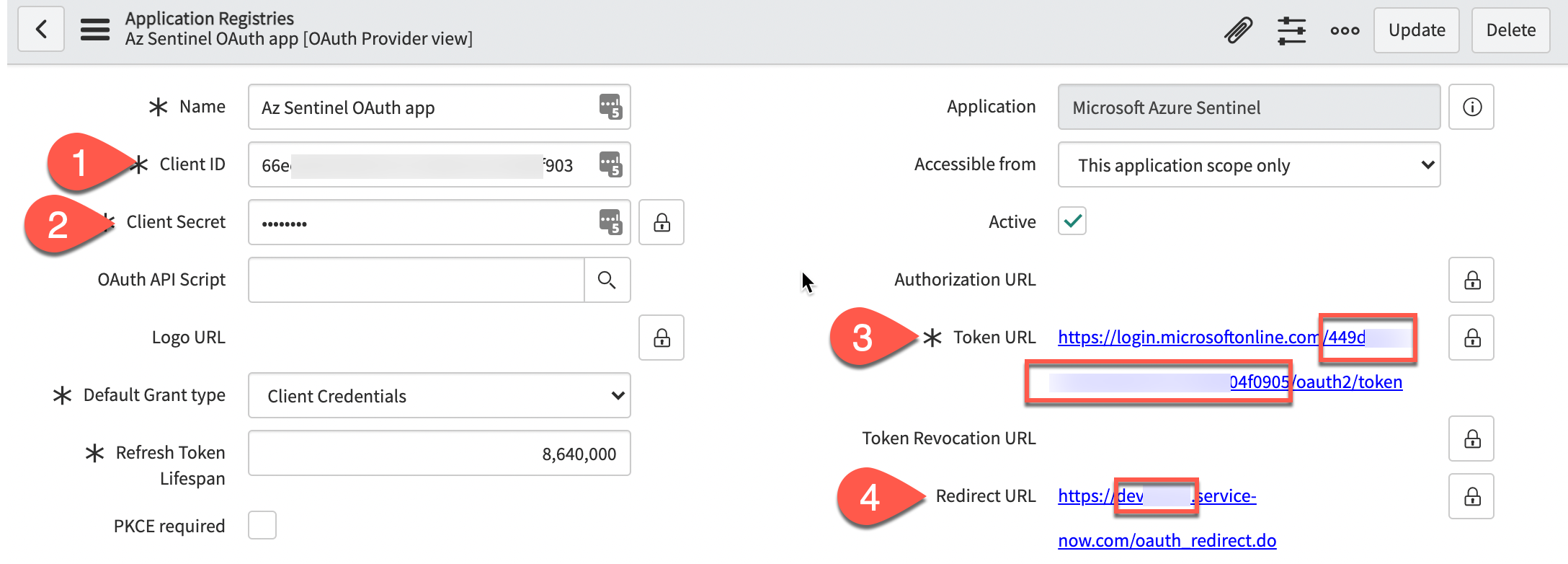
### Service Principal configuration

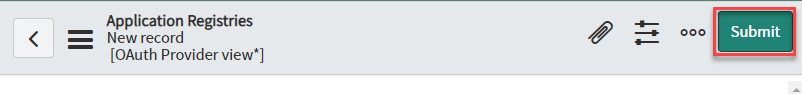
To be able use the Azure Sentinel Management API from ServiceNow, we must configure the credentials we created previously in Azure AD. This is done using an “Application Registry”.

1. In the “Service Principals” section, open the “Az Sentinel OAuth app” application registry.
2. Update the client id, client secret and Azure AD tenant ID values, using the values you saved during the service principal creation:  
   
3. Optional: Create a new set of credentials.   
   Click “New”.  
   Graphical user interface, text, application

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

   Description automatically generated
5. On the credentials configuration page, you must provide the information we collected during the Service Principal creation:
   * Name: This name has to be the same as the one used by the workspace configuration
   * 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.  
   

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. You should verify that the values used by your ServiceNow instance are the same as the ones provided.   
Note that because Sentinel has four different severities values, while we have only three in ServiceNow, both “Informational” and “Low” have been assigned the value **3**:



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.  
Review the values to validate that they match your environment configuration.



Verify the “ServiceNow Severity to Sentinel” table mapping  
This table is used to map the ServiceNow severity to the Sentinel value, when updating Sentinel incidents, based on ServiceNow updates  
Review the values to validate that they match your environment configuration.

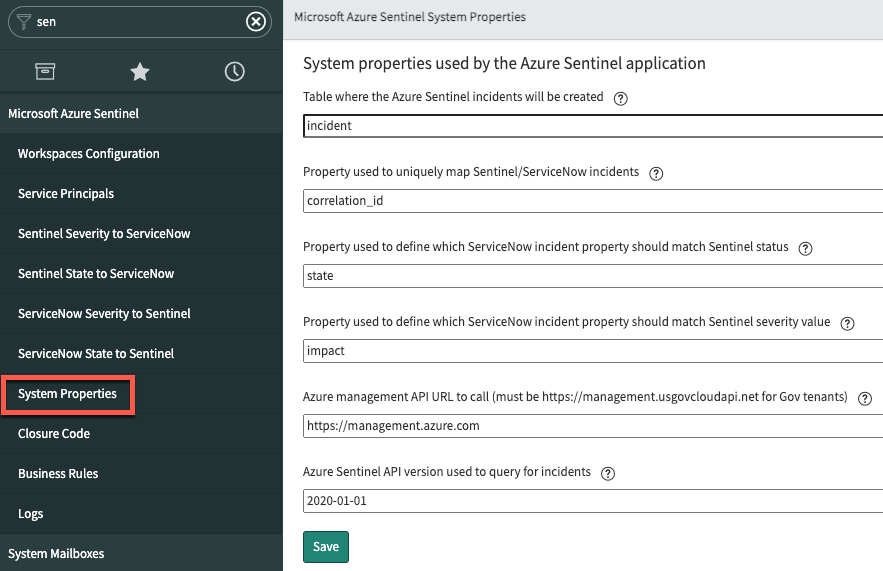


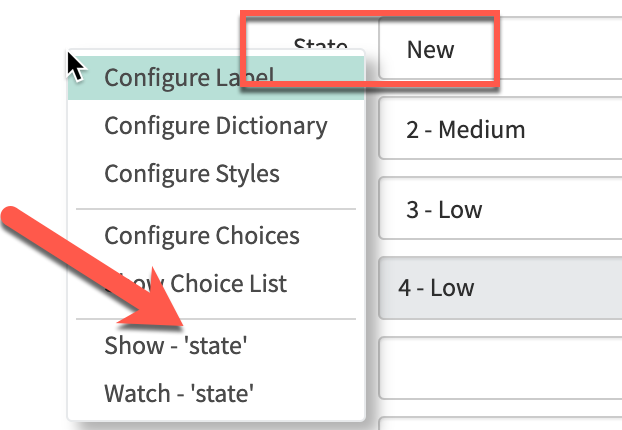
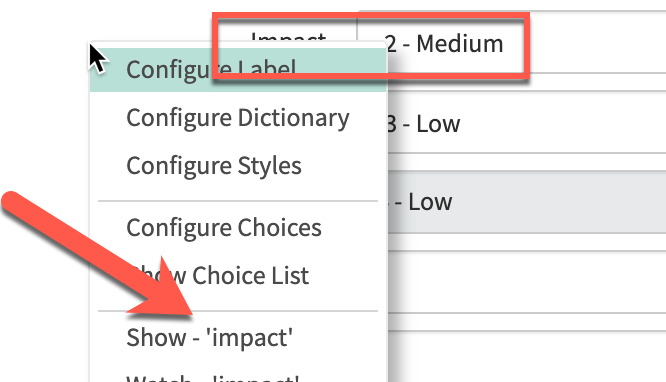
Verify the “ServiceNow State to Sentinel” table mapping  
This table is used to map the ServiceNow severity to the Sentinel value, when updating Sentinel incidents, based on ServiceNow changes.  
Review the values to validate that they match your environment configuration.



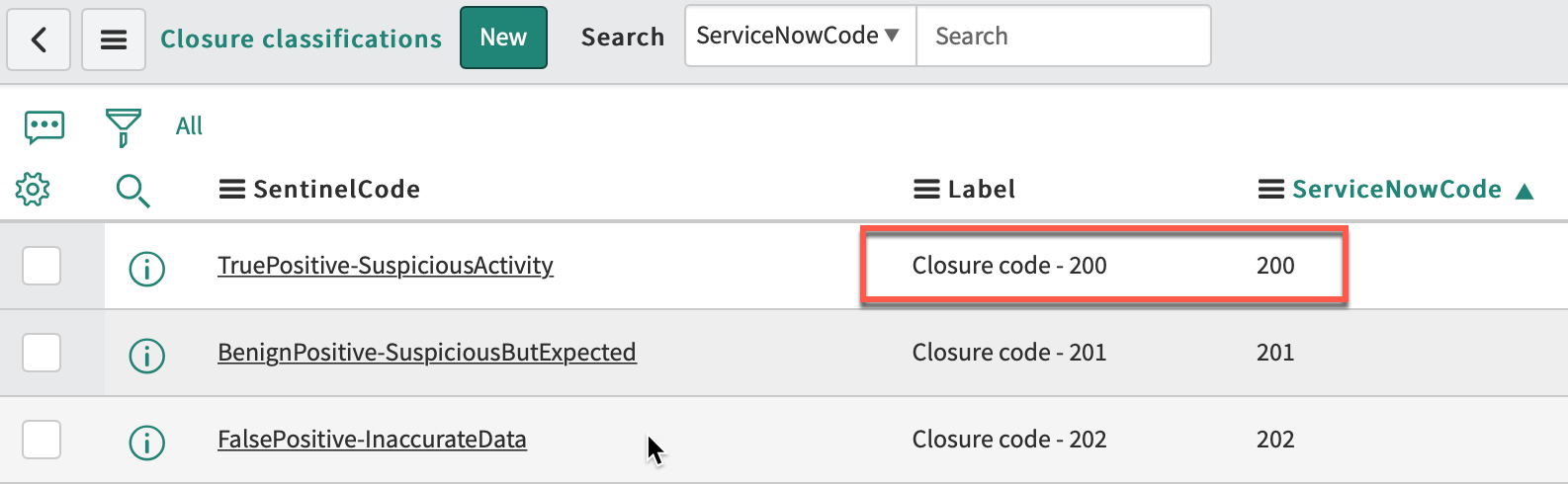
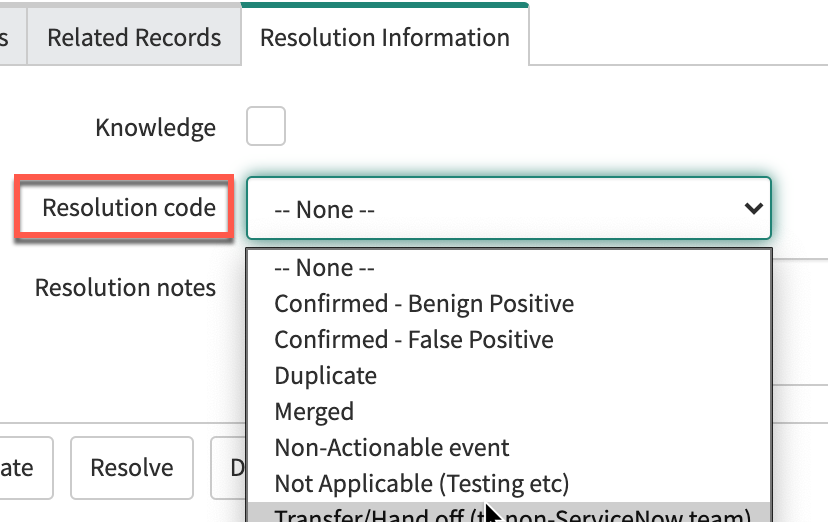
### Review and validate the system properties

In addition to the configuration stored in tables, the app keeps some information in system properties.  
Review the default values and change it to match your environment, if required.

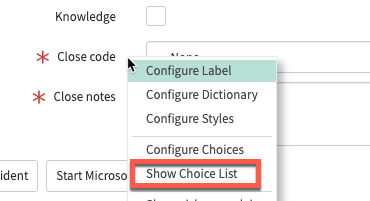


* **Incident Table Name**: table where the incidents are created (by default, incidents will be created in the “***incident***” table).
* **Incident Unique Key**: ServiceNow incident property used to uniquely map incidents between Sentinel and ServiceNow. By default, the app uses “*correlation\_id*”. If you are already using this property, you should specify or create another one
* **Status Field**: incident property to store the incident state. By default, the app uses “***state***”.  
  
* **Severity Field**: incident property to store the incident severity. By default, the app uses “***impact***”.  
  
* **Api Url**: URL to the Azure Sentinel API. If your workspace is in Gov Cloud, you must change it to [*https://management.usgovcloudapi.net*](https://management.usgovcloudapi.net)
* **Api Version**: Azure Sentinel API version (should not be changed)

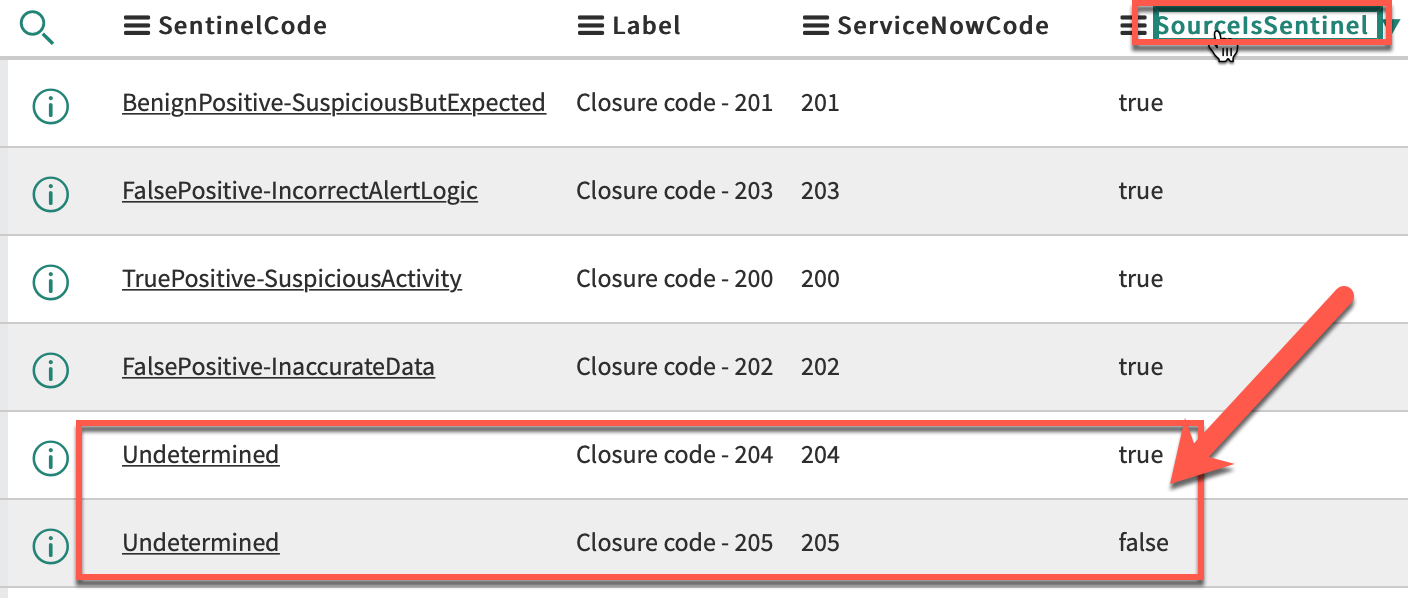
Verify the “Closure classification” table entries  
This table should match the closure codes you are using when closing your incidents in ServiceNow.  
You should update the provided values with your environment ones. Usually, ServiceNow UI shows you the **label**, but you will also need the code **value** (integer) and configure those in the table:

To get the actual values, you have to go to “Show Choice List”:



**IMPORTANT**: in this table, the last column, “SourceIsSentinel” contains Boolean values to define which values should be used in ServiceNow when a close status has been set in Sentinel incidents.  
You should have only one “true” row per Sentinel possible status:



Business Rules  
If you changed the default incident table, status or state property, you must update the Business Rule used by the application to match them.  
The application uses two business rules: one for the work notes (comments), the other for the owner, status and severity updates.

