BeyondTrust

Privilege Management
ServiceNow Scripting Guide

Powered By Defendpoint

TC:6/11/2019

Table of Contents

ServiceNow and Endpoint Privilege Management Integration

The Privilege Management for Windows ServiceNow integration can be used with Privilege Management for Windows version 5.3 and later. You can download the integration from the BeyondTrust Support Portal.

- The ServiceNow integration is comprised of two files:
  - **Log-ServiceNowIncident.ps1**
  - **ServiceNowSettings.json**
- The URL of your ServiceNow instance. For example, **instancename.service-now.com**
- The username and password of a user that has the ServiceNow **itil** role. Users with the **util** role can open, update, and close incidents as required.
- A Challenge / Response message

All end-users need to have a corresponding account in ServiceNow for Privilege Management for Windows to raise the incident successfully.

In the default configuration, when a user runs an application you are targeting with the ServiceNow Rule Script, they are presented with the option to raise an incident in ServiceNow or cancel the request. The ticket in ServiceNow includes:

- Caller
- Short Description
- Description including the business justification, the program name, program publisher, program path, Challenge Response Code, and the business justification the end-user provided.

You can then action the incident in ServiceNow and supply the end-user with a Challenge Response Code. The end-user can then start the application and enter the Challenge Response Code to run the application.

In your Privilege Management for Windows policy, you need to set up the following:

- A Workstyle that targets the ServiceNow Rule Script
- An Application Group that contains the applications you want to target
- A Message configured for Challenge / Response

For more information, please see "Use the ServiceNow Integration" on page 4.

Use the ServiceNow Integration

The following steps configure Privilege Managementfor Windows to use our supported ServiceNow integration script.

In your Privilege Management Policy Editor, you need to set up:

- A Workstyle that will target the ServiceNow Rule Script
- An Application Group that contains the applications you want to target
- A Message configured for Challenge / Response.

For more information, please see "Use the ServiceNow Integration" on page 4.

For more information, please see the Administration Guide for your policy editor for details on any of these steps if required. This summary is intended for those who are familiar with editing policy in Privilege Management Policy Editor.

In your policy editor:

1. Create a **Message** and configure it for Challenge / Response. Call this message **Allow Message (with Challenge)**. If you do not have an existing Shared Key, ensure you configure one before you continue.
2. Create an **Application Group** called **ServiceNow Applications** and populate it with application definitions you want your end-users to raise a ServiceNow ticket for.
3. Create a Workstyle called **ServiceNow** and add an Application Rule.

In the Application Rule:

1. Set the **Target Application Group** to **ServiceNow Applications**.
2. From the **Run a Rule Script** list, select **Manage Scripts**.
3. From the **Rule Scripts** node, click **Import Script**.
4. Navigate to the ServiceNow integration script **Log-ServiceNowIncident.ps1** you downloaded previously and click **Open**.
5. Click **Settings**, and then **Import Settings**. Navigate to the **ServiceNowSettings.json** file you downloaded previously.
6. At the top of the **ServiceNowSettings.json** file, navigate to the **Authentication** section and make the following changes:
   - Replace the **URL** with your ServiceNow URL in the form **yourinstance.service-now.com**, ensuring you remove the asterisks. Do not use *HTTPS*. This is a restriction of the ServiceNow API. The secure connection is managed by the client.
   - Replace the **Username** and **Password** with your ServiceNow user credentials with the **util** permission, ensuring you remove the asterisks.
7. Click **Save** and then **Close** on the **Script Manager**. The **ServiceNowSettings.json** file is now associated with your ServiceNow Rule Script **Log-ServiceNowIncident.ps1**. Any time you use the ServiceNow Rule Script, the same Settings file will be automatically assigned to it. Any edits to the settings file will need to be made in one place, and they will be used in all instances of that Rule Script.
8. Set the **Default Action** to **Allow Execution**.
9. Set the **Default End User Message** to **Allow Message (with Challenge)**.
10. Set the **Default Access Token** to **Add Admin Rights**.
11. Set **Raise an Event** to **On**, and click **OK** to finish configuring the Application Rule.

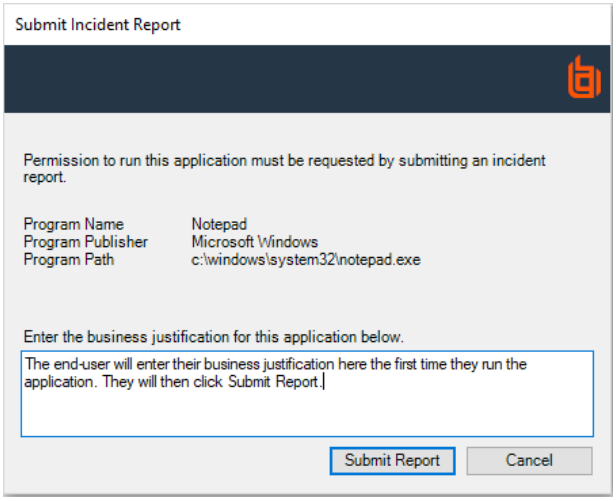
Verify the Workstyle is enabled, so you can test the ServiceNow integration.

You can confirm the ServiceNow integration is working by running an application that will match on the **ServiceNow Applications** Application Group. When the ServiceNow script runs successfully, a dialog box like the one below is displayed. A Settings error message might be displayed.

For more information, please see "ServiceNow Error Codes" on page 19.

The first time the end-user sees this message they will enter their business justification, and click **Submit Report**.

Once they receive the Challenge Response Code, they can run the application. Then they can click **Enter Response Code** to enter the Challenge Response Code and run the application.



ServiceNow Workflows

There are three workflows you can use with Privilege Management for Windows and ServiceNow integration:

- **Challenge Response**: This is the default, out-of-the-box configuration discussed earlier in this guide. The button on the lower-left of the dialog box reads *Enter Response Code* or your chosen wording so users can enter their Challenge Response Code when it is provided to them. Or, they can enter their business justification to raise an incident in ServiceNow if they do not have a Challenge Response Code.
- **Run as Designated User**: The button on the lower-left of the dialog box reads *Login as Other User*, so you can provide your end-user with administrator credentials or type them in. Alternatively, they can enter their business justification to raise an incident in ServiceNow if they don't have the required credentials.
- **No option**: The button on the lower-left is removed so your end-users can only enter their business justification and raise an incident in ServiceNow.

For each of these options, you need to configure an appropriate message to make sure your users have the correct experience if the Default Rule is run.

To change the behavior of the integration for each of these workflows, you need to edit the **ServiceNowSettings.json** file.

For more information, please see "Edit the Settings File " on page 6.

Note: *Settings files are encrypted at the endpoint and must be encoded in UTF-8.*

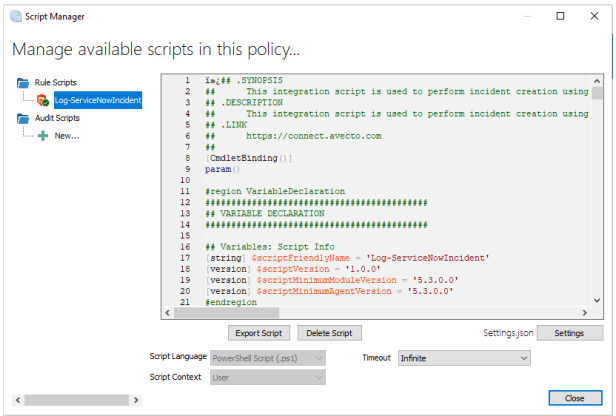
Edit the Settings File

You need to edit the **ServiceNowSettings.json** file to change the workflow you want to use.

Note: *All associated rules with the same Power Rules script will inherit the changes you make. You do not need to edit the settings file multiple times.*

To edit the **ServiceNowSettings.json** file:

1. In the **Edit Application Rule** dialog box, select **Manage Scripts** from the **Run a Rule Script** drop-down list.
2. Click **Settings** on the bottom-right of the dialog box.



3. Locate the **Misc** section. Within **Misc**, locate the **DefaultRule** setting. For the recommended ServiceNow workflow, this is set to **ChallengeResponse**. However, you can change it here:
    - "ServiceNow and Challenge / Response (Default Workflow)" on page 7: Provides the user with an option to enter a Privilege Management Response Code.
    - "ServiceNow and Designated User Must Authorize" on page 8: Provides the user with an option to enter designated user credentials.
    - "ServiceNow Only" on page 9: User can only submit an incident to ServiceNow or cancel their request.
4. Click **Save**.

ServiceNow and Challenge / Response (Default Workflow)

This is the default and recommended configuration for the ServiceNow integration.

ServiceNowSettings.json Configuration

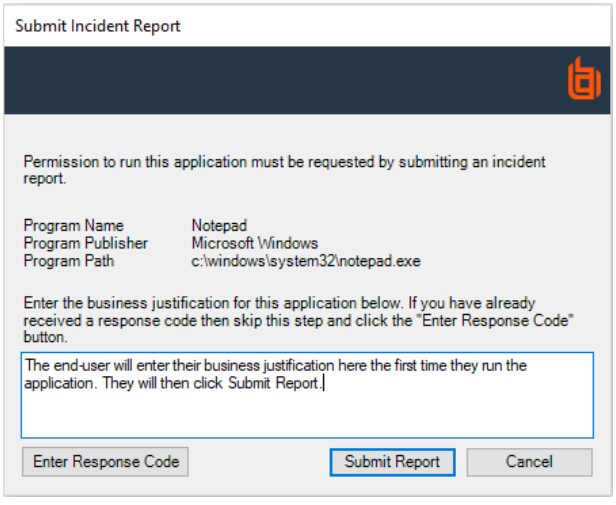
For more information, please see "Edit the Settings File " on page 6.

```
"Misc": {
    "_comment": "DefaultRule - Should be DesignatedUserMustAuthorize, ChallengeResponse, or empty.",
    "DefaultRule": "ChallengeResponse"
},
```

User Experience

The **Submit Incident Report** dialog box looks similar to the one shown here depending on other settings:

- **Enter Response Code**: The user clicks the button and enters a Privilege Management code to run the application.
- **Submit Report**: The user clicks the button to submit an incident to ServiceNow.



Message

Configure a message for **Challenge / Response** to ensure the end-user can enter their challenge code to run the application.

ServiceNow and Designated User Must Authorize

This is an alternative configuration that allows your users to enter Designated User Credentials instead of a Challenge Response Code.

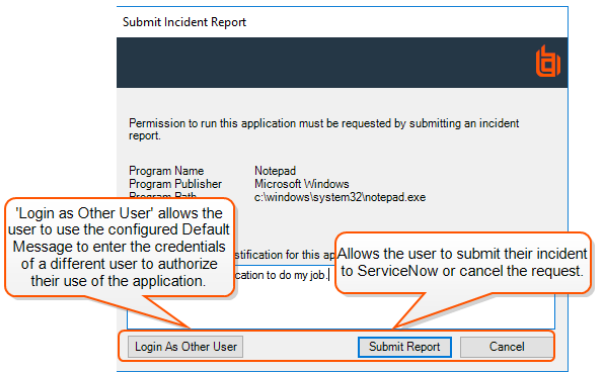
ServiceNowSettings.json Configuration

For more information, please see "Edit the Settings File " on page 6.

```
"Misc": {
    "_comment": "DefaultRule - Should be DesignatedUserMustAuthorize, ChallengeResponse, or empty.",
    "DefaultRule": "DesignatedUserMustAuthorize"
},
```

User Experience

The **Submit Incident Report** dialog box looks similar to the one shown here depending on other configuration.



Message

Configure a message for **Designated User Must Authorize** to ensure the end-user can enter the designated user credentials and run the application.

ServiceNow Only

This is an alternative configuration that means the user can only submit an incident to ServiceNow or cancel their request.

ServiceNowSettings.json Configuration

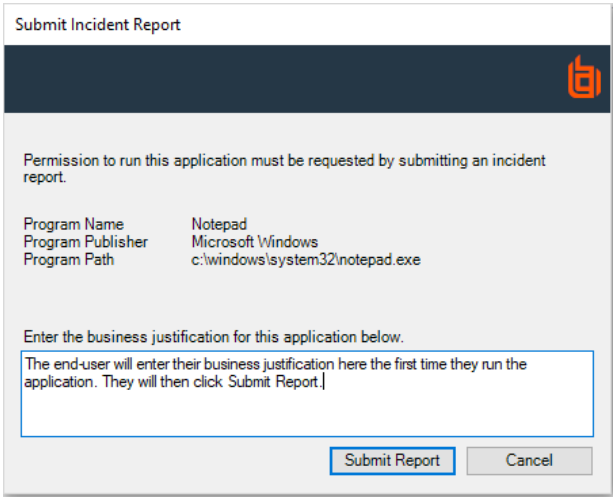
For more information, please see "Edit the Settings File " on page 6.

```
"Misc": {
    "_comment": "DefaultRule - Should be DesignatedUserMustAuthorize, ChallengeResponse, or empty.",
    "DefaultRule": ""
},
```

User Experience

The **Submit Incident Report** dialog box looks similar to the one shown here depending on other configuration.

The user can enter a business justification and click **Submit Report** to send an incident to ServiceNow.



Message

The end-user is presented with a text box to enter their business justification for the task they are trying to perform. There is no option to run the Default Rule for the end-user.

ServiceNowSettings.json File Configuration

The **ServiceNowSettings.json** file contains some settings you must change and some settings you can optionally configure.

Mandatory Configuration

The mandatory configuration of the ServiceNow integration is discussed earlier but shown here for completeness. For more information, please see "Use the ServiceNow Integration" on page 4.

You must edit the following lines in the **ServiceNowSettings.json** file before you associate it with the ServiceNow Rule Script. You can change the file before or after you import it.

This script must be a valid *.json file when you are finished editing it.

Authentication

Note: *Remove the asterisks but leave the quotes in place.*

Field	Description
"URL": "*REQUIRED*",	The URL in the form **instance-name.service-now.com**. Do not use **HTTPS** as the secure connection is managed by Privilege Management for Windows client.
"Username": "*REQUIRED*",	The ServiceNow user name the client will use.
"Password": "*REQUIRED*"	The ServiceNow password the client will use.

Example

```
"Authentication":
{
    "URL": "instance-name.service-now.com",
    "Username": "adminuser",
    "Password": "Js£DhijZE85pw"
}
```

Optional Configuration

You can optionally edit the following lines in the **ServiceNowSettings.json** file. You may want to edit these to change the information shown to the user, modify button names, or configure logging.

> ***Note:** In the **ServiceNowSettings.json** file, **&** represents a keyboard shortcut.*

ServiceNowIncident

These fields are present in ServiceNow and populated by Privilege Management for Windows client.

Field	Description
ShortDescription	This maps to the ServiceNow Short Description.
FullDescription	This maps to the ServiceNow Description.
AssignmentGroup	This maps to the ServiceNow Assignment Group.
Category	This maps to the ServiceNow Category.
Subcategory	This maps to the ServiceNow Subcategory.
Comment	This maps to the ServiceNow Comments.

Example

```
"ServiceNowIncident":
{
    "ShortDescription": "Avecto Defendpoint application execution request for $($dpProgramName)",
    "FullDescription": "The customer has requested the following application be allowed to execute
on their computer:\n\nProgram Name: $($dpProgramName)\nProgram Publisher:
$($dpProgramPublisher)\nProgram Path: $($dpProgramPath)\n\nChallenge Code:
$($dpChallengeCode)\n\nBusiness Justification: $($dpBusinessJustification)",
    "AssignmentGroup": "UK-Support",
    "Category": "Endpoint-Agents",
    "Subcategory": "Avecto",\
    "Comment": "Created by Avecto Defendpoint $($scriptFriendlyName) integration script."\
}
```

Logging

These are the logging options you can configure for the ServiceNow integration.

Field	Description
LogToConsole	Whether or not to log to the console where present. Options are **true** or **false**.
LogToFile	Whether or not to log to a file. Options are **true** or **false**.
LogFilePath	The absolute file path of the file you want to log to.

Example

```
"Logging":
{
    "LogToConsole": true,
    "LogToFile":true,
    "LogFilePath": "C:\Users\MyUser\Desktop"
```

Misc

Note: *Remove the asterisks but leave the quotation marks in place.*

"DefaultRule": "*REQUIRED*"	This must be set to either **DesignatedUserMustAuthorize**, **ChallegeResponse**, or empty. **ChallengeResponse** is the default configuration. This setting determines the button on the bottom left of the **Submit Incident Report** dialog box. If the field is empty, no button is displayed.  For more information, please see "ServiceNow Workflows" on page 6.

Example

```
"Misc":
{
    "_comment": "DefaultRule - Should be DesignatedUserMustAuthorize, ChallengeResponse, or empty.",
    "DefaultRule": "ChallengeResponse"
}
```

Dialog Boxes

The integration displays various dialog boxes according to the workflow you define:

CommonSettings

The following settings apply to all dialog boxes.

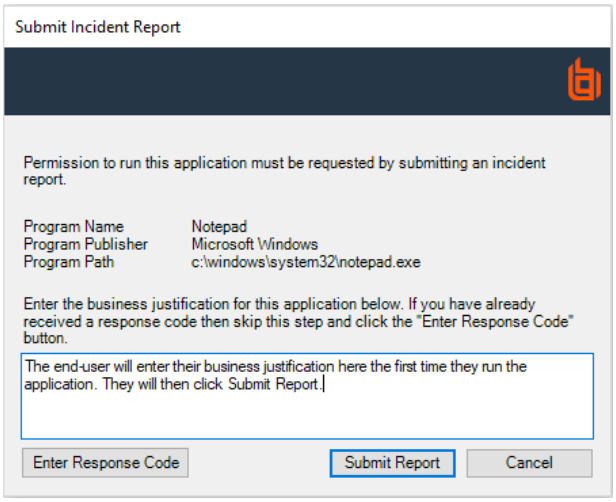
Field	Description
BannerImageFile	The absolute file path to the banner image you want to use for all dialog boxes. The recommended size for this is 450 x 50px. You must use the following format: `C:\\Users\\StandardUser\\Desktop\\my_image.jpg` This file must be accessible on the endpoint. Ensure you use two backward slashes as the file is a JSON format and the character must be escaped.

You can localize the following dialog boxes by creating a new section with the appropriate localization abbreviation. For example, **"Language_FR"**. This section is used if the operating system was originally installed with French as the language.

BusinessJustificationDialog

The dialog box varies based on the workflow you are using.

The dialog box and associated variables are shown here:

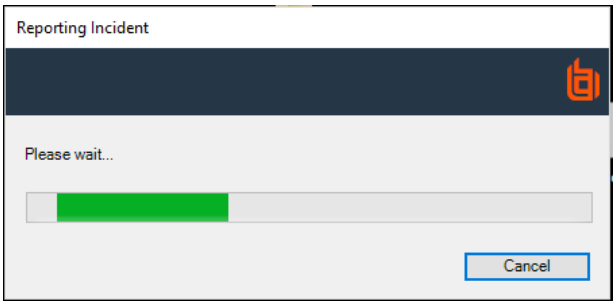


Field	Description
Title	The title of the business justification dialog box. **Default**: *Submit Incident Report*
LabelHeader	The first piece of text on the business justification dialog box. **Default**: *Permission to run this application must be requested by submitting an incident report.*
LabelInputBoxDefault	The text that tells the user what to do in this dialog when the **DefaultRule** in the **ServiceNowSettings.json** file is set to **empty** or **DesignatedUserMustAuthorize**. **Default**: *Enter the business justification for this application below.*

Field	Description
LabelInputBoxChallengeResponse	The text that tells the user what to do when the **DefaultRule** in the **ServiceNowSettings.json** file is set to **ChallengeResponse**. Default: *Enter the business justification for this application below. If you have already received a response code, you can skip this step and click the "Enter Response Code" button.*
CustomButtonTextChallengeResponse	The text on the button that is displayed on the bottom left when the **DefaultRule** in the **ServiceNowSettings.json** file is set to **ChallengeResponse**. **Default**: *&Enter Response Code*
CustomButtonTextDesignatedUserMustAuthorize	The text on the button that is displayed on the bottom left when the **DefaultRule** in the **ServiceNowSettings.json** file is set to **DesignatedUserMustAuthorize**. **Default**: *&Login As Other User*
LabelProgramName	The program name description. **Default**: *Program Name*
LabelProgramPublisher	The program description. **Default**: *Program Publisher*
LabelProgramPath	The program path. **Default**: *Program Path*
ButtonCancel	The text on the button that is displayed on the bottom right to cancel the request. **Default**: *&Cancel*
ButtonOK	The text on the button that is displayed on the bottom right to submit an incident to ServiceNow. **Default**: *&Submit Report*

ProgressDialog

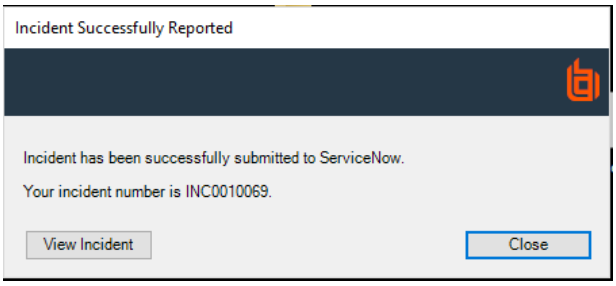
This dialog box is displayed when Privilege Management for Windows client is communicating with ServiceNow.



Field	Description
Title	The title of the reporting incident dialog box. **Default**: *Reporting Incident*
LabelHeader	The text on the dialog box while the Power Rule is processing. **Default**: *Please wait...*

MessageSuccessDialog

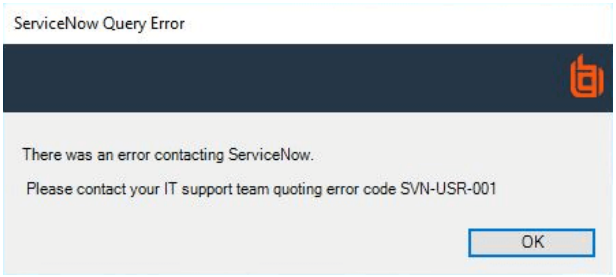
This dialog box is displayed when Privilege Management for Windows has raised an incident in ServiceNow.



Field	Description
Title	The title of the incident successfully reported dialog box. **Default**: *Incident Successfully Reported*
LabelHeader	The text on the dialog box that tells the user what has happened and what their incident number is in ServiceNow. **Default**: *Incident has been successfully submitted to ServiceNow.\n\nYour incident number is INC_NUM.*
ButtonLinkVisible	Toggles the availability of the button that is displayed on the bottom left of the dialog box. **Default**: *Whether or not a button allowing the user to view their incident is visible. Options are true or false.*
ButtonLinkText	The text on the button that is displayed on the bottom left of the dialog box if it is displayed. **Default**: *View Incident*
ButtonOK	The text on the button that is displayed on the bottom right to close the dialog box. **Default**: *&Close*

ErrorDialogs: ServiceNowQueryError

This dialog box is displayed if Privilege Management for Windows client was unable to raise an incident in ServiceNow.



Field	Description
Title	The title of the unable to raise a ticket in ServiceNow dialog box. **Default**: *ServiceNow Query Error*
LabelHeader	The text that tells the user what happened including any error codes. **Default**: *There was an error contacting ServiceNow.\n\n Please contact your IT support team quoting error code.*
ButtonOK	The text on the button that is displayed on the bottom right of the dialog box. **Default**: *&OK*

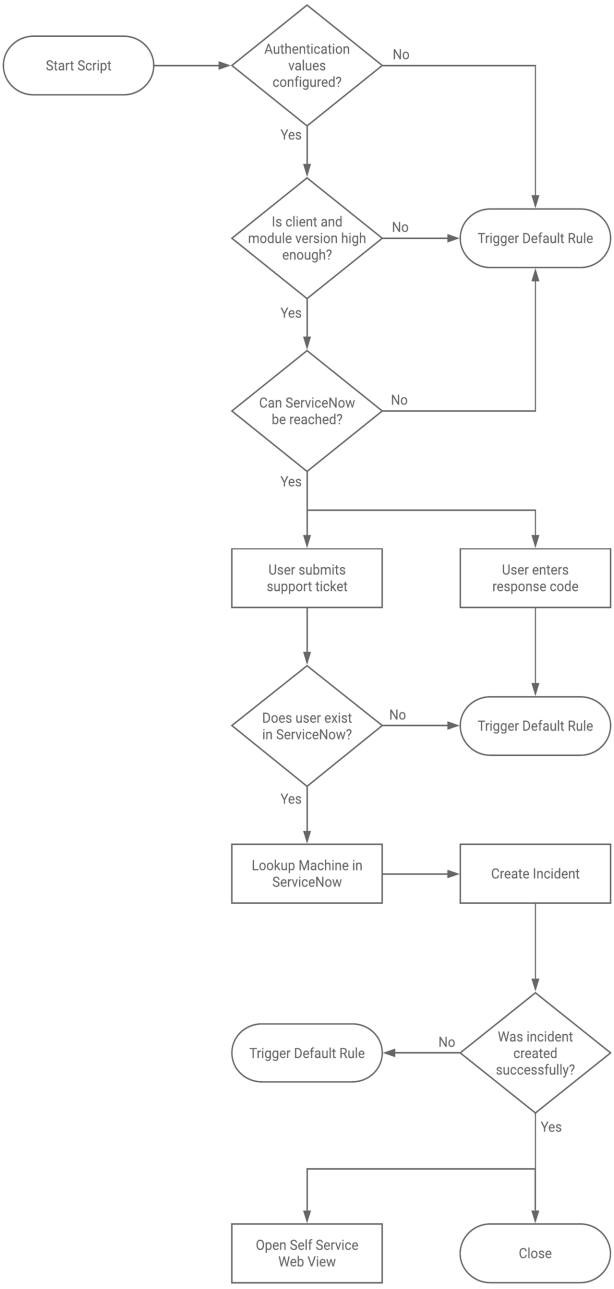
ErrorDialogs: ServiceNowReportIncidentError

The dialog box is only displayed if there is an error contacting ServiceNow after all the validation has passed, but before the incident is created.

Field	Description
Title	The title of the ServiceNow error dialog box. **Default**: *Unable to Report Incident*
LabelHeader	The text that tells the user what happened including error codes. **Default**: *There was an error contacting ServiceNow and we were unable to report this incident.\n\n Please contact your IT support team quoting error code*
ButtonOK	The text on the button that is displayed on the bottom right of the dialog box. **Default**: *&OK*

ServiceNow Architecture Diagram

The diagram shows the ServiceNow integration workflow for the recommended configuration in detail, including the workflows that trigger the Default Rule.



ServiceNow Error Codes

These codes may be shown in dialogs that are displayed at various points in the ServiceNow integration.

Error Code	Symptom
SVN-STG-001	Authentication values are not configured in the **ServiceNowSettings.json** file.
SVN-VSN-001 SVN-VSN-002	Either the Privilege Management for Windows or the Privilege Management Policy Editor versions are not high enough to support Power Rules.
SVN-URL-001	The instance of ServiceNow in the **ServiceNowSettings.json** file cannot be reached.
SVN-USR-001	The end-user trying to create the incident in ServiceNow does not have an account in ServiceNow.
SVN-INC-001	The incident was not created successfully.