SMA TECHNOLOGIES

OPCON

# ServiceNow Connector

***User Guide***

***19.0***

For further information about SMA's documentation, please contact:

SMA Technologies
15333 JFK Blvd
Suite #300
Houston, TX 77032
Phone (281) 446-5000
Fax (281) 446-7492
Toll-free 877-363-2305
E-mail*: contact@smatechnologies.com*
*www.smatechnologies.com*

| Version | Date | Description |
|---|---|---|
| 17.1-01 | 12 February 2018 | Initial User Guide |
| 17.1-02 | 14 February 2018 | changes<br>• Enhanced Connector to support PROXY settings.<br>• When job fails, first check if ticket already assigned for job and if it is re-open the existing ticket. |
| 17.1-03 | 30 March 2018 | Changes<br>• Added TAG ROUTING section |
| 18.3.1.01 | 11 December 2018 | Changes<br>• Ticket information now written to the new Incident Ticket ID field in the Job Information section. |
| 19.0.3.03 | 30 December 2019 | Changes<br>• Added correlation_display and correlation_id fields when creating ticket.<br>• Added ServiceNow SMA OpCon Application.<br>• Added check to see if Incident ticket is closed or cancelled when creating ticket.<br>• Added existing ticket number to task documentation and incident ticket description if task errors and existing ticket is closed or has been cancelled.<br>• Changed installer to NSIS |

*Table of Contents*

# General Information

The ServiceNow Connector can be used to submit incident tickets automatically to ServiceNow from OpCon when a task has an error condition. When the incident ticket is accepted in ServiceNow (State moved to In Progress) the task state in OpCon can automatically be changed to Under Review indicating that the error is being worked on. When the error is corrected and the ticket in ServiceNow state changes to Resolved, the task state in OpCon can be changed to either Fixed or Restart. If the ticket in ServiceNow is cancelled, the OpCon task can be automatically cancelled.

## Components

The OpCon ServiceNow implementation includes components that detect when a task errors, create the ServiceNow Incident record (includes adding task job log) and automatically update the OpCon task status when the Incident record Status changes.

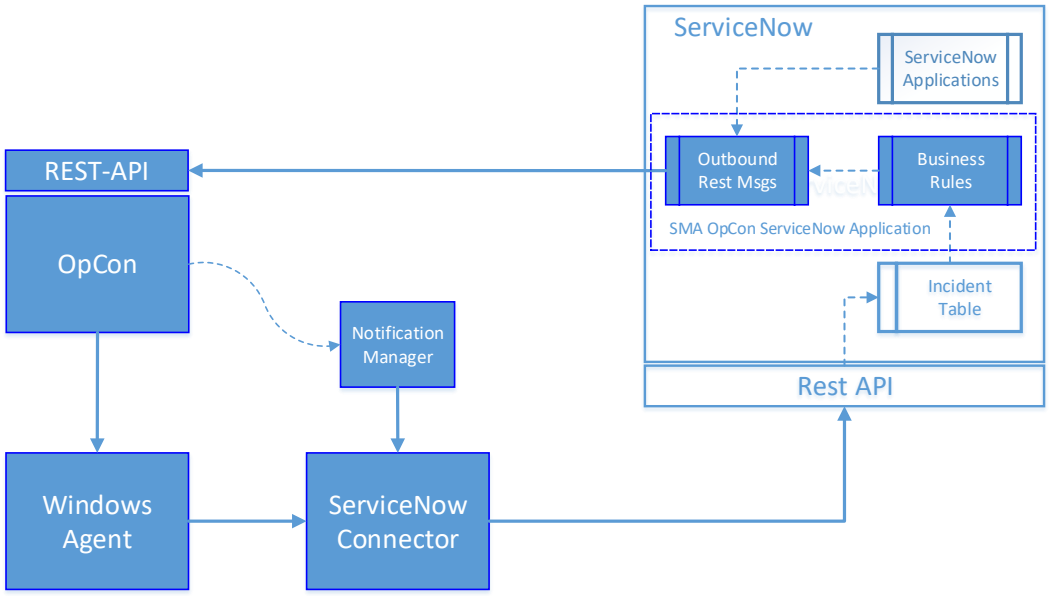



*Figure 1 : OpCon ServiceNow Connector Components*

- Notification Manager — An OpCon feature that initiates the ServiceNow Connector when a task encounters an error condition.
- Windows Agent — An OpCon Windows Agent that is used to execute the ServiceNow connector.
- ServiceNow Connector — An OpCon connector that communicates with ServiceNow through the ServiceNow Rest-API to create an incident.
- Business Rules — Part of a ServiceNow OpCon application that contains business Rules that are triggered when the Status of the incident ticket is updated.
  - *OpConTicketAccepted*
  - *OpConTicketResolved*
  - *OpConTicketRelease*
  - *OpConTicketCanceled*
- Outbound Rest Messages — Part of a ServiceNow OpCon application that contains Outbound Rest Messages to communicate with OpCon Through the OpCon Rest-API. This includes messages to update the task status as well as additional messages that can

be used by other ServiceNow applications to issue instructions to OpCon.

- *updateJobStatusById*
- *buildSchedule*
- *getDailyScheduleByNameAndDate*
- *addJobToScheduleInDaily*
- *getApiVersion*

## Process

The ticket creation process consists of the following steps.

1. The ServiceNow Connector is executed by the Notification Manager when a failed task is detected. The Notification Manager uses the following standard OpCon properties to pass information to the ServiceNow Connector.
   - $MACHINE NAME The name of the Agent on which the task was executing.
   - $JOB TERMINATION The termination code of the task.
   - $SCHEDULE DATE-SNOW A special version of the Schedule Date format created to support ServiceNow Connector.
   - $SCHEDULE ID The schedule ID of the workflow in the OpCon System.
   - $SCHEDULE INST The schedule instance of the workflow in the Daily OpCon table.
   - $SCHEDULE NAME The name of the workflow.
   - $JOB NAME The name of the task.
2. Before creating a new incident ticket, the ServiceNow Connector checks to see if an incident ticket has already been created for the task. The task information is extracted from the OpCon Daily Job table.

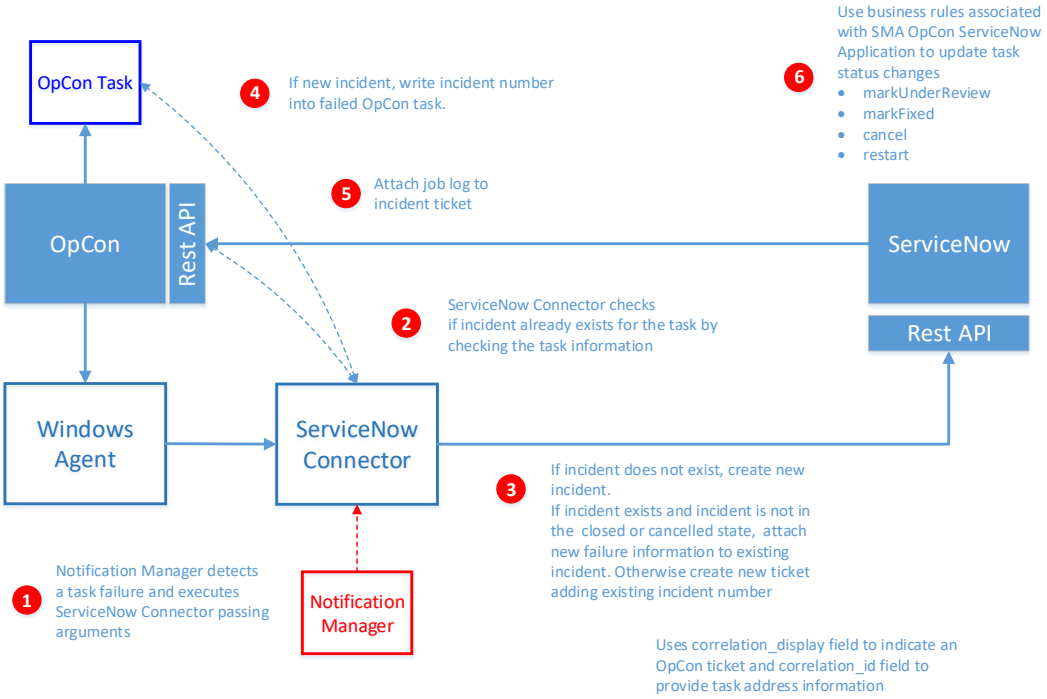



*Figure 2 : ServiceNow Connector Overview*

3. If an incident ticket exists, the existing incident ticket is retrieved from ServiceNow and a check is made to see if the incident ticket state is *closed* or *canceled*. If the incident ticket is either *closed* or *canceled*, a new ticket is created. The previous ticket number is attached to the task

documentation and the incident ticket description. Otherwise the ticket is updated reflecting the new task error information and the is re-opened (state set to *New*).

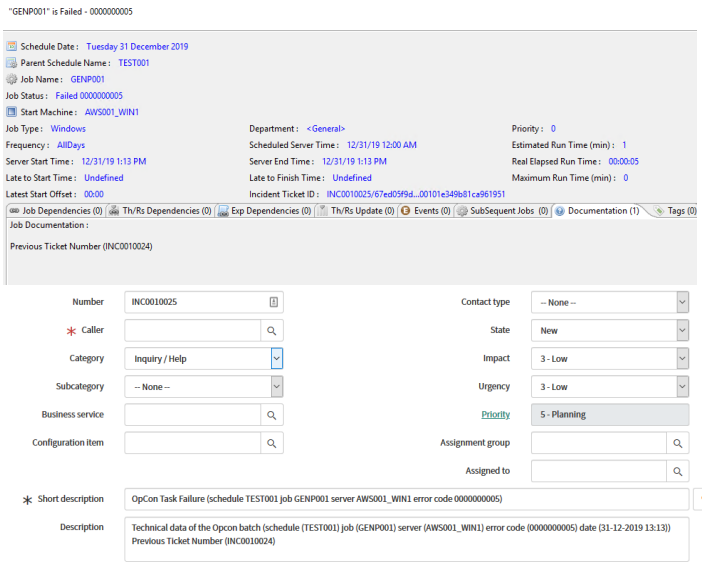



*Figure 3 : Previous ticket number added to restart failures*

When creating an incident ticket, the workflow name, the task name, the agent the task was executing on and the termination code are included in the incident description. The correlation_display field is used to indicate that the request is from OpCon (sets the value to SMA_OPCON) and the correlation_id field is used to provide the identifier of the task that errored (includes the OpCon Rest-API address and the unique job id) allowing the business rules in the SMA OpCon ServiceNow Application to complete task status changes.

4. The returned incident number and sys_id fields are written into the OpCon task in the task Incident Ticket ID field. If there was an existing ticket and a new ticket was created, the previous ticket number is written into the task documentation field.

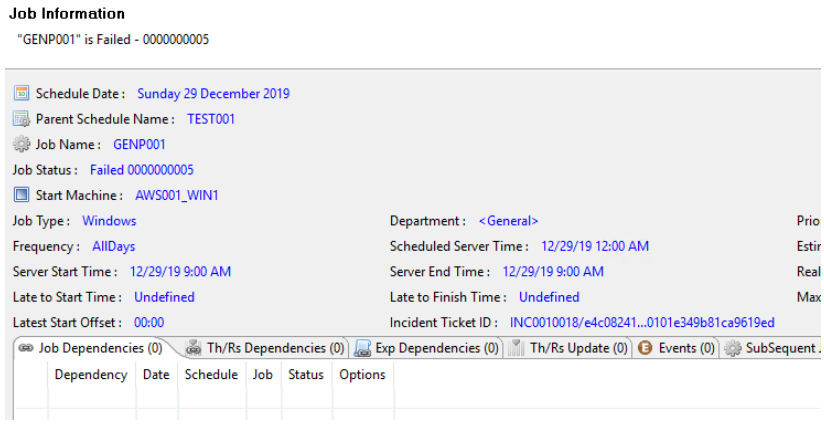
5. 


*Figure 4 : Job Information example showing ServiceNow Incident number*

6. The ServiceNow Connector calls the OpCon Rest-API to retrieve the task's job log and attaches this to the created or existing ServiceNow Incident ticket.
7. The SMA OpCon ServiceNow Application, provides Business Rules that are triggered when the state of the Incident ticket is changed. These business rules then submit outbound Rest message calls to the OpCon Rest-API to change the task status. The correlation_display value is used to determine if the updated incident ticket is an OpCon ticket and the correlation_id

values are inserted into the outbound Rest message to route the message to the correct OpCon system and task.

The following Business rules are provided:

a. OpConTicketAccepted — triggered when the OpCon incident is updated and the state changes from ‘New’ to ‘In Progress’. The OpCon task is set to the markUnderReview status indicating that the problem is being worked on.

b. OpConTicketResolved — triggered when the OpCon incident is updated and the state changes from ‘In Progress’ to ‘Resolved’. The OpCon task is set to the markFixed status indicating that the problem has been fixed. The task can then be restarted.

c. OpConTicketRelease — an alternate rule that is triggered when the OpCon incident is updated and the state changes from ‘In Progress’ to ‘Resolved’. The OpCon task is restarted.

d. OpConTicketCanceled — triggered when the OpCon incident is updated and the state changes to ‘Canceled’. The OpCon task is canceled.

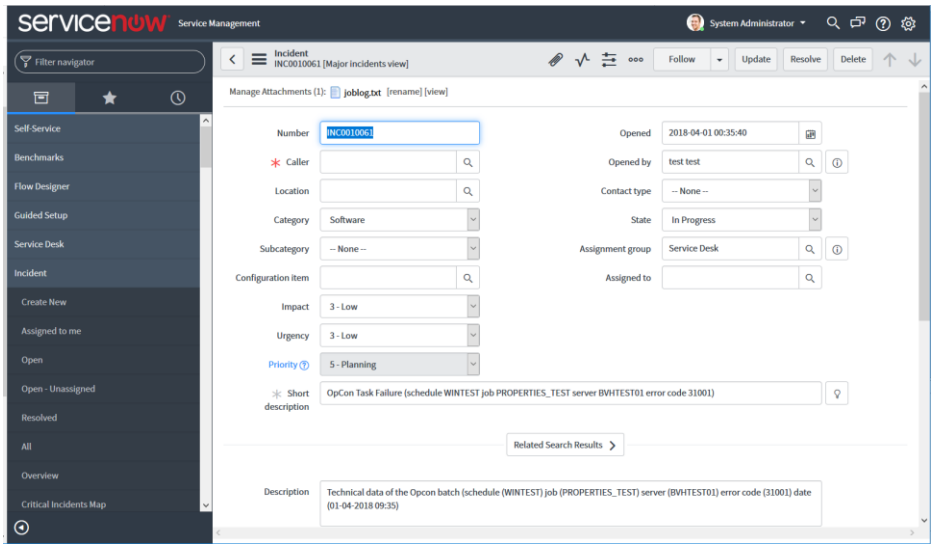



*Figure 5 : ServiceNow example created Incident*

Figure 4 shows an example of a created incident ticket. The short description and the description fields contain the workflow name, the task name, the agent name that was executing the task, the termination code and the date / time when the execution failed. The job log of the failed task can be accessed by double-clicking on the Manage Attachments in the upper left-hand corner.

# Installation

The ServiceNow Connector installation consists of multiple steps that are required to complete the installation successfully.

The connector requires a SMA OpCon Windows Agent to provide the connection between Notification Manager in the OpCon System and the ServiceNow Connector software.
It requires the OpCon Rest-API to extract the unique id of the task in the daily tables, the retrieval of the job log and the updating of the task status by the outbound Rest messages of the SMA OpCon ServiceNow Application.

## Supported Software Levels and Requirements

The following software levels are required to implement the ServiceNow Connector.

- OpCon Release 19.0 or higher.
- OpCon RESTFul API Configured to not use TLS if self-signed certificates are being used.
- OpCon Windows Agent to provide link to ServiceNow Connector.
- OpCon Notification Manager.
- A ServiceNow implementation that supports the Rest API.

## Installation

The installation process consists of the following steps:

- OpCon Windows Agent Installation.
- OpCon ServiceNow Connector Installation.
- OpCon ServiceNow Connector Configuration.
- OpCon Notification Manager Definition.
- ServiceNow SMA OpCon ServiceNow Application Installation.

## OpCon Windows Agent Installation

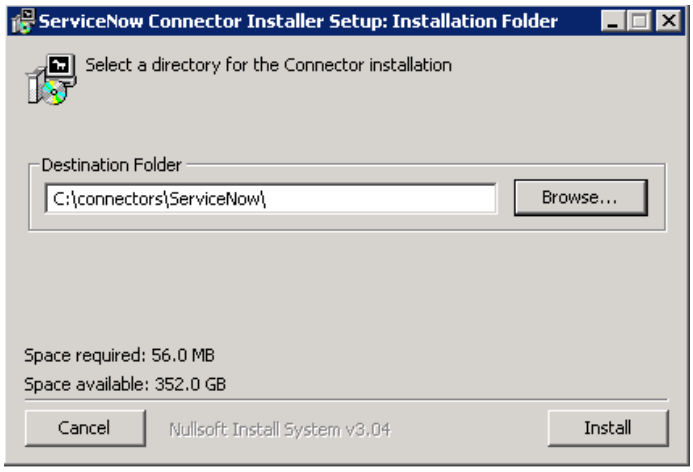
The ServiceNow Connector requires the installation of a Windows Agent on the same system as the ServiceNow Connector.

Either use an existing Windows Agent or complete the installation of the Windows Agent.

## OpCon ServiceNow Connector Installation

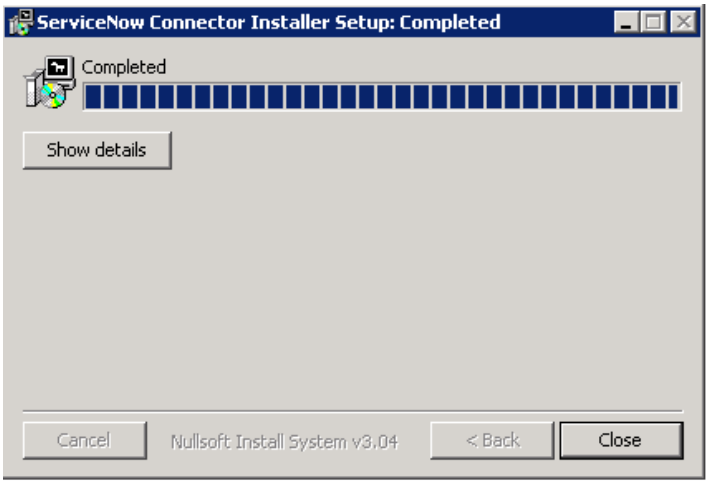
Copy the supplied install file ServiceNow.zip and extract it into a temp directory (c:\temp). Execute the ServiceNow_installer_windows.exe from the temp directory as the 7z.exe and 7z.dll files are needed to extract the OpenJavaSDK 1.8 software into the /java directory.

Execute the ServiceNow_installer_windows.exe.




Select a directory to install the connector into. The installer builds up the data directory in ProgramData using the selected installation directory. Therefore do not install the connector in Program Files, but rather create a Connectors directory and install the connectors in this as can be seen from the above example.

Select Install




Select Close

Installation complete.

After the installation is complete, the root installation directory (c:\Connectors\ServiceNow) contains the connector executable (ServiceNow.exe) and two directories java and application. The java directory contains the java software required to execute the connector (OpenJDK 1.8) and the application directory contains the ServiceNow SMA OpCon Application file that can be used to import the business rules and Rest messages into ServiceNow.

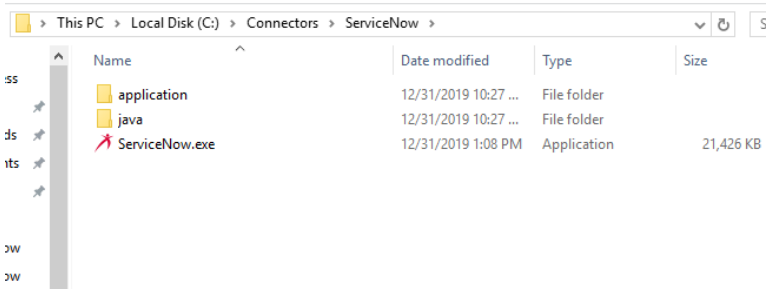



*Figure 6 : ServiceNow Connector root installation directory*

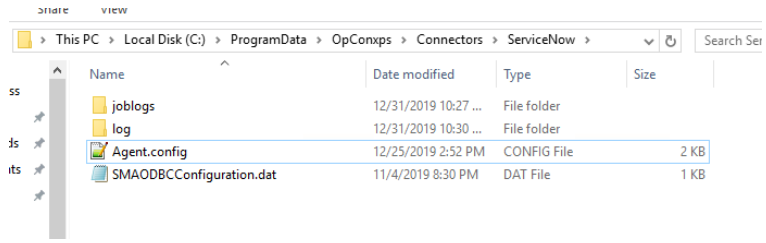



*Figure 7 : ServiceNow Connector data directory*

The data directory is created in ProgramData/OpConxps using the root installation directory name (C:\ProgramData\OpConxps\Connectors\ServiceNow) and contains the Agent.config file and the directories for the connector log and joblogs.

### *Create $SCHEDULE DATE-SNOW Global Property*

Create the special $SCHEDULE DATE-SNOW property that contains the schedule date in the yyyy-MM-dd format.

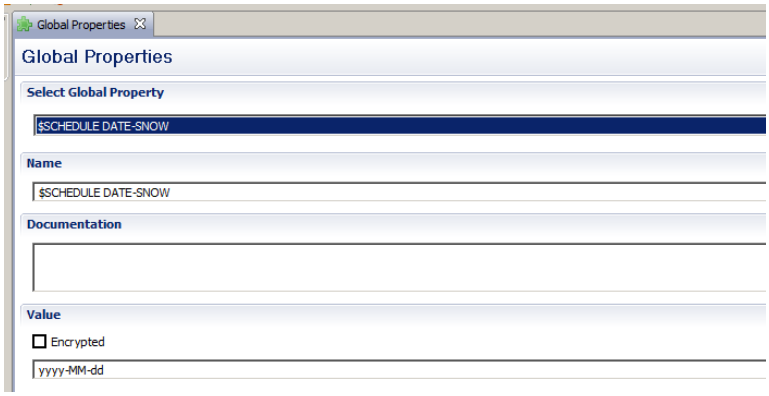



*Figure 8 : $SCHEDULE DATE-SNOW Global Property Example*

## OpCon ServiceNow Connector Configuration

The configuration of the ServiceNow Connector requires setting the connection information for the various systems, the definition of working hours and the values to set when creating an incident ticket. All encrypted values must be encrypted using the Password Encryption Tool available in Enterprise Manager.

### *Agent.config File*

Now configure the Agent.config file in the main directory setting the required information.

The Agent.config contains the following definitions.

| Property Name | Value |
|---|---|
| **[GENERAL]** | Header |

| | |
|---|---|
| LOG_FILES_DIRECTORY | The name of the directory where the retrieved log files are stored. After successful attachment to the ServiceNow Incident, the log file is deleted.<br><br>The name is a sub directory of the installation directory. |
| DEBUG | The Connector supports a debug mode, it can be turned on to add additional information in logs.<br>Value either ON or OFF (default OFF). |
| **[SERVICE NOW CONNECTION]** | Header<br>Used to define the connection to the ServiceNow Rest-API |
| USE_PROXY | If a proxy server is required when connecting to ServiceNow, set the value to True.<br>Value either True or False (default False). |
| PROXY_ADDRESS | The address of the proxy server. |
| PROXY_PORT | The port of the proxy server. |
| ADDRESS | The address of the ServiceNow instance where the Incident ticket is created. |
| INCIDENT_URL | Defines the incident URL to be used when submitting a ticket creation. |
| ATTACHMENT_URL | Defines the attachment URL to be used when attaching a job log to the incident. |
| USER | The user which has the required ServiceNow privileges to submit incident and attachment requests via the web services interface.<br><br>The name must be encrypted using the password encryption tool available in Enterprise Manager. |
| PASSWORD | The password of the user which has the required ServiceNow privileges to submit incident and attachment requests via the web services interface.<br><br>The password must be encrypted using the password encryption tool available in Enterprise Manager. |
| **[OPCON API CONNECTION]** | Header<br>Used to define the connection to the OpCon API |
| SERVER | The address of the OpCon API. |
| PORT | The port number used by the OpCon Rest-API. |
| USES_TLS | Indicates if the OpCon Rest-API uses a TLS connection. Values are True or False.<br><br>Please note that only if a certificate purchased from a certified certificate provider is used is a TLS connection supported as ServiceNow does not support connections to web servers using self-signed certificates. |
| TOKEN | An application token used to communicate with the OpCon-API. |
| **[OPCON CONNECTION]** | Header<br>Used to define the connection to the OpCon System. |
| PROFILE_NAME | The profile name to use when connecting to the OpCon database.<br><br>Please note that only SQL Connections are supported. |
| DAT_FILE_NAME | The name of the dat file that contains the database connection information. The file is usually a copy of the dat file in the SAM folder.<br><br>Please note that only SQL Connections are supported and that a server value must be present and not localhost. |

| | |
|---|---|
| USER | The user which has the required privileges to connect to the OpCon System to update jobs in the daily table.<br><br>The name must be encrypted using the password encryption tool available in Enterprise Manager. |
| PASSWORD | The password of the user which has the required privileges to connect to the OpCon System to update jobs in the daily table.<br><br>The password must be encrypted using the password encryption tool available in Enterprise Manager. |
| **[RULES]** | Header<br>General rules used to define if features are enabled. |
| INCLUDE_JOBLOG_AS_ATTACHMENT | Indicates if the job log should be attached to the incident ticket.<br><br>Value either True or False (default True). |
| **[TAG ROUTING]** | Header<br>Optional capability that allows values of user defined tags to define fields passed when creating the Incident ticket. |
| TAG_END | If a tag value ends in this definition include the field and value when creating the Incident ticket.<br><br>When using TAG_ROUTING a special definition DEFAULT should be defined as this indicates to the Connector what value to use if tags are defined for the task and there is no match.<br><br>Value<br>TAG_END=<value to check>=<incident field name>=<value to submit><br>value to check: is the end part of the tag name to match<br>incident field name: is the name of the field in the incident ticket to set<br>value to submit: is the value to submit when creating the incident ticket. |
| **[WORKING HOURS]** | Header<br>Defines the working hours of the day. |
| MONDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| TUESDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| WEDNESDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| THURSDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| FRIDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| SATURDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |

| | |
|---|---|
| SUNDAY | Indicates the working hours of the day defined as hour to hour (i.e. 0700,1900).<br><br>A value of 0000,0000 indicates a non-working day. |
| **[AH DEFINITIONS]** | Header<br>Defines the values passed to ServiceNow when creating an incident ticket after hours |
| DEF | Defines the values to be submitted when creating an incident ticket.<br><br>Value<br>DEF=<incident field name>=<value to submit><br>incident field name: is the name of the field in the incident ticket to set<br>value to submit: is the value to submit when creating the incident ticket.<br><br>Note:<br>The definition includes predefined values for incident fields short_description and description. These definitions include place holders for the following<br>0 workflow name<br>1 task name<br>2 the agent that the task was executing on<br>3 the termination code<br>4 timestamp when the error occurred |
| **[WH DEFINITIONS]** | Header<br>Defines the values passed to ServiceNow when creating an incident ticket during working hours |
| DEF | Defines the values to be submitted when creating an incident ticket.<br><br>Value<br>DEF=<incident field name>=<value to submit><br>incident field name: is the name of the field in the incident ticket to set<br>value to submit: is the value to submit when creating the incident ticket.<br><br>Note:<br>The definition includes predefined values for incident fields short_description and description. These definitions include place holders for the following<br>0 workflow name<br>1 task name<br>2 the agent that the task was executing on<br>3 the termination code<br>4 timestamp when the error occurred |

*Table 1 : Agent.config definitions*

## Example Configuration.

```
[GENERAL]
LOG_FILES_DIRECTORY=LogFiles
DEBUG=OFF

[SERVICE NOW CONNECTION]
USE_PROXY=True
PROXY_ADDRESS=10.200.180.18
PROXY_PORT=8080
ADDRESS=dev39871.service-now.com
INCIDENT_URL=api/now/table/incident
ATTACHMENT_URL=api/now/attachment/file
USER=AfqItVm68q6k8K+P36el4A==
PASSWORD=3zXskIjsWA4DiGObwDe3eQ==

[OPCON API CONNECTION]
SERVER=50.17.60.164
PORT= 9001
USES_TLS=False
TOKEN=35f3b848-1991-40ad-be7f-9631b7da5eda

[OPCON CONNECTION]
PROFILE_NAME=OPCON
DAT_FILE_NAME=SMAODBCConfiguration.dat
```

```
USER=My5YBvYZ66+2Ao6qXnFnBw==
PASSWORD=3zXskIjsWA4DiGObwDe3eQ==

[RULES]
INCLUDE_JOBLOG_AS_ATTACHMENT=True

[TAG ROUTING]
TAG_END=TECH=subcategory=Operating System
TAG_END=FUNC=subcategory=Email
TAG_END=DEFAULT=subcategory=Operating System

[WORKING HOURS]
MONDAY=0800,1900
TUESDAY=0800,1900
WEDNESDAY=0800,1900
THURSDAY=0800,1900
FRIDAY=0800,1900
SATURDAY=0800,1100
SUNDAY=0000,0000

[AH DEFINITIONS]
DEF=short_description=OpCon Task Failure (schedule {0} job {1} server {2} error code {3})
DEF=description=Technical data of the Opcon batch (schedule ({0}) job ({1}) server ({2}) error code ({3}) date ({4})
DEF=assignment_group=Service Desk
DEF=state=2

[WH DEFINITIONS]
DEF=short_description=OpCon Task Failure (schedule {0} job {1} server {2} error code {3})
DEF=description=Technical data of the Opcon batch (schedule ({0}) job ({1}) server ({2}) error code ({3}) date ({4})
DEF=assignment_group=Incident Management
DEF=state=2
```

*Figure 9 :Agent.config file sample*

Figure 9 provides an example of a ServiceNow Agent.config file. In the example, a proxy server is used to submit the requests to ServiceNow.

The SERVICE NOW CONNECTION section provides the information about the connection to ServiceNow. The proxy server is defined using the USE_PROXY, PROXY_ADDRESS and PROXY_PORT statements and the ServiceNow connection is defined using the ADDRESS, INCIDENT_URL, ATTACHMENT_URL, USER and PASSWORD statements. User and Password values must be encrypted using the Enterprise Manager password encryption tool.

The OPCON API CONNECTION section provides the information about connecting to the OpCon System using the OpCon Rest-API so the job log can be retrieved and appended to the incident ticket using the ATTACHMENT_URL defined in the SERVICE NOW CONNECTION section. The SERVER statement defines the web server address and the PORT statement defines the web server port used. The USES_TLS statement indicates if the connection uses TLS. It should be noted that only if a certificate purchased from a certified certificate provider is used should a TLS connection be used as ServiceNow does not support connections to web servers using self-signed certificates. The TOKEN statement contains an application token (see OpCon Rest-API documentation on how to generate an application token).

The OPCON CONNECTION section provides the information about connecting to the OpCon System so the task information can be extracted and updated. The PROFILE_NAME statement defines the profile name when connecting to OpCon. The DAT_FILE_NAME statement defines the name of a SMAODBCConfiguration.dat file that contains the database access information for the OpCon system and the USER and PASSWORD statements define an OpCon user that has the appropriate privileges to submit the OpCon-API requests. User and Password values must be encrypted using the Enterprise Manager password encryption tool.

The RULES section defines rules that influence connector behavior. Currently only 1 rule is defined that indicates if the job log should be attached to the incident ticket.

The TAG ROUTING section defines if task tag definitions are to be used to submit values when creating the incident ticket. The TAG_END statement defines what value must be submitted if the user defined tag name ends in the matching value. When using TAG ROUTING, a special matching value of DEFAULT must be defined as this determines what to submit if there is no end match. In the example if the tag name ends with TECH, the field subcategory will be set to Operating System and if the tag name ends

with FUNC, the field subcategory will be set to Email. If there is no match, the field subcategory will be set to Operating System.

The WORKING HOURS section defines the working hours of the organization. These values are used to determine if the definitions associated with the WH DEFINITIONS (working hours) or AH DEFINITIONS (after hours) should be used when creating an incident ticket. The MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY and SUNDAY statements define the working hours for each day. The values are defined as starting work hour and ending work hour. In the example, the working hours are 0800 to 1900 Monday to Friday, 0800 to 1100 on Saturday and no working hours on Sunday.

The AH DEFINITIONS and WH DEFINITIONS sections define what values should be submitted when creating an incident ticket. The reason for different sections is that the recipients of tickets may be different for working hours or after hours. If the values are the same, then ensure that the values in the sections are the same.

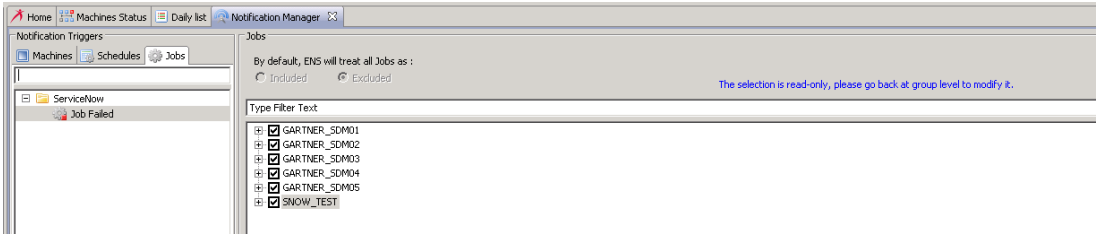
The DEF statement defines the field name and the value to be submitted when creating an incident ticket.
In the above example, during working hours, the incident ticket will be routed to the Incident Management group and after hours the incident ticket will be routed to the Service Desk.

The DEF statement includes two defaults short_description and description. These definitions include place holders for the workflow name, the task name, the agent name, termination code and the date time when the error occurred. In the above example the short_description definition *OpCon Task Failure (schedule {0} job {1} server {2} error code {3})* is converted to OpCon Task Failure (schedule WINTEST job PROPERTIES_TEST server BVHTEST01 error code 31001) when the incident ticket is created.

## OpCon Notification Manager Definition

Notification Manager is used to execute the ServiceNow Connector when a task completes with a failure condition. Using this approach allows the tasks to be added to the rule instead of defining a failure event on every task.

Using Notification Manager, select the *Jobs* tab and create a new Group called *Service Now*.
Once the Group has been created, select the *Service Now* Group, perform a '*right-click*' and select *Add Job Trigger*. In the *Add Job Trigger* selection, select *Job Failed*.



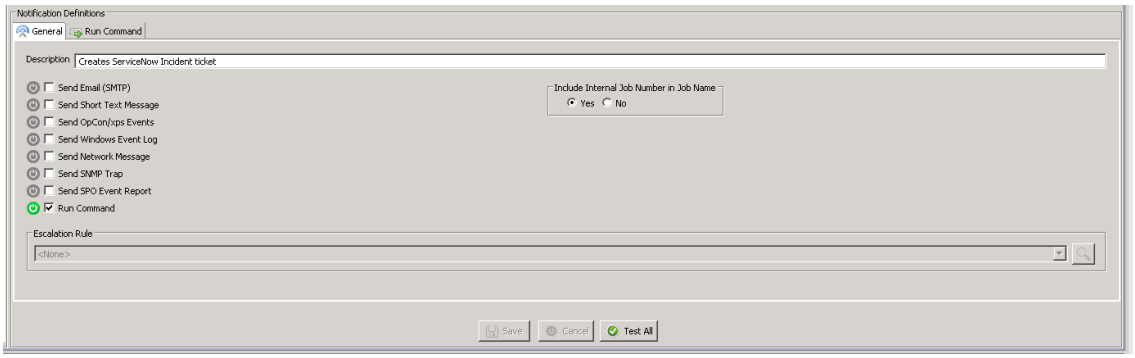



*Figure 10 : Notification Definitions Example*

In the Notification Definitions section, select *Run Command*. In the Run Command tab, enter the following:

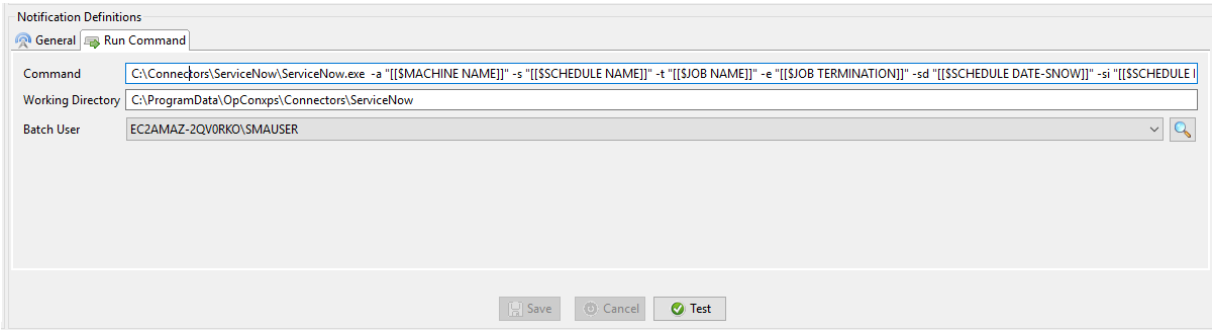



*Figure 11 : Run Command definition example*

C:\connectors\ServiceNow\ServiceNow.exe -a "[[$MACHINE NAME]]" -s "[[$SCHEDULE NAME]]" -t "[[$JOB NAME]]" -e "[[$JOB TERMINATION]]" -sd "[[$SCHEDULE DATE-SNOW]]" -si "[[$SCHEDULE ID]]" -sn "[[$SCHEDULE INST]]"

Where

- C:\connectors\ServiceNow\ServiceNow.exe is the installed location of the connector.
- C:\ProgramData\OpConxps\Connectors\ServiceNow is the location of the working directory.
- Batch user is a defined OpCon Batch user with administration rights.

The created Agent.config and .dat files must be placed in the c:\ProgramData\OpConxps\Connectors\ServiceNow.

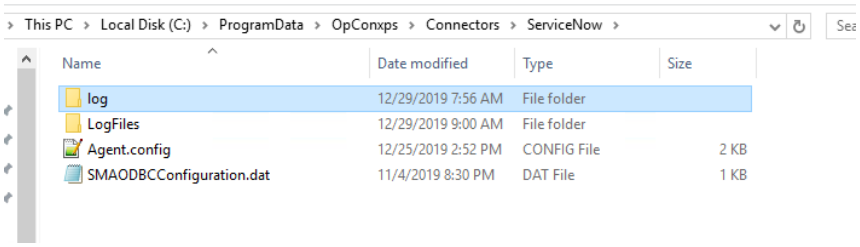



*Figure 12 : ServiceNow Connector ProgramData contents*

## ServiceNow SMA OpCon Application Installation

The ServiceNow SMA Application provides business rules and outbound Rest messages that can be imported into ServiceNow using the System Update Sets function.

To import the ServiceNow SMA OpCon Application, got to Retrieved Update Sets and select the *Import Update Set from XML* button.

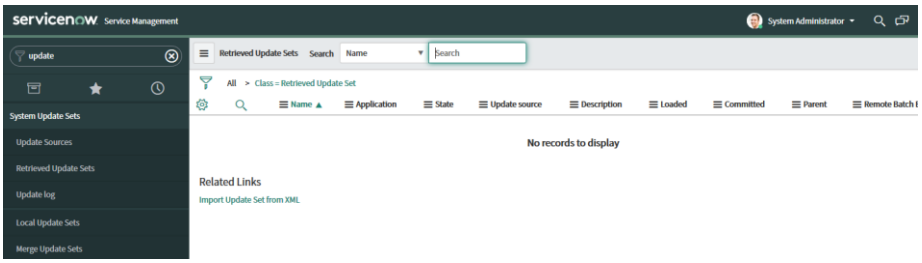



*Figure 13 : Loading Application using System Update Sets*

Now browse for the ServiceNow SMA OpCon Application file (should be in the application directory after connector installation).

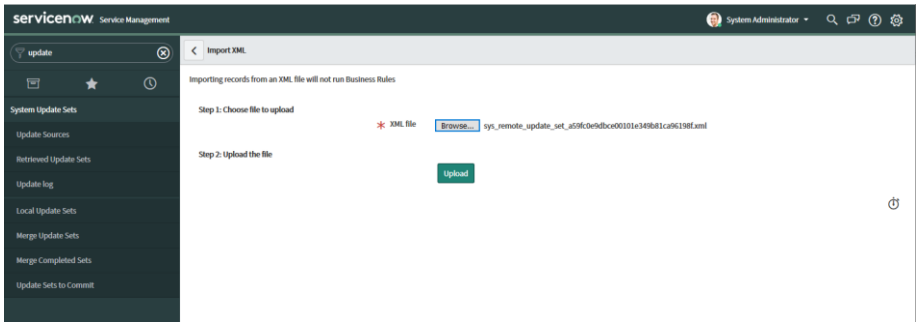



*Figure 14 : Uploading Application File*

Once the file has been found, select the *Upload* button.

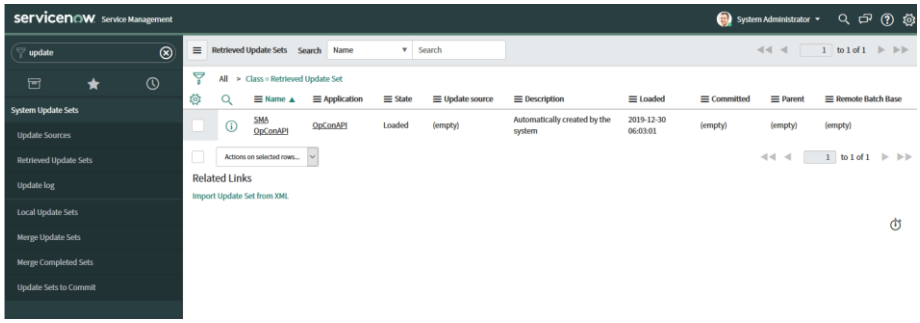



*Figure 15 : Loaded Application on Retrieved Update Sets List*

Once the upload is complete, the application will appear on the Retrieved Update Sets list. Select the application by 'clicking' on the name and the application information appears.

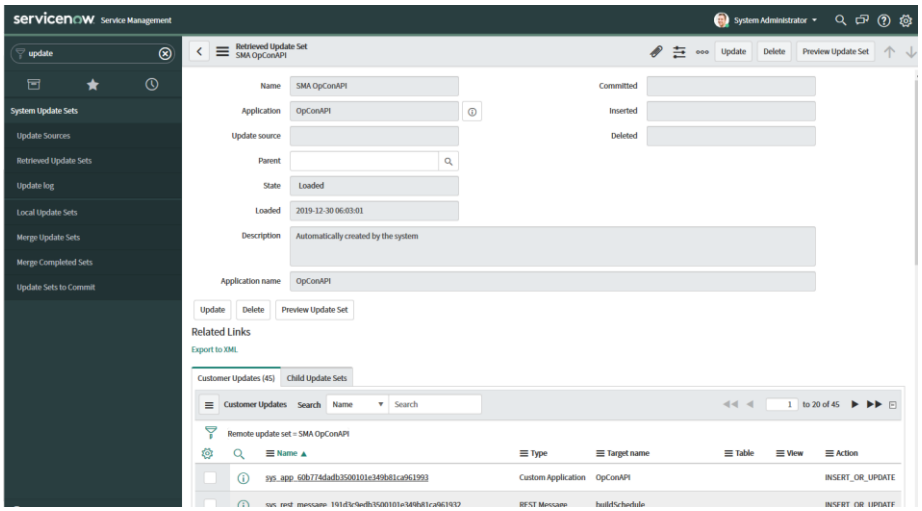



*Figure 16 : ServiceNow SMA OpCon Application Information*

Once the application information appears, select the Preview Update Set information. The process of previewing an Update Set detects problems that may occur if you commit the updates on the local instance. After you preview and before you commit an Update Set, follow this procedure to resolve all the problems that the preview process discovered. Once the indicates 100% succeeded, it is possible to commit the new application into the ServiceNow instance and make it available.

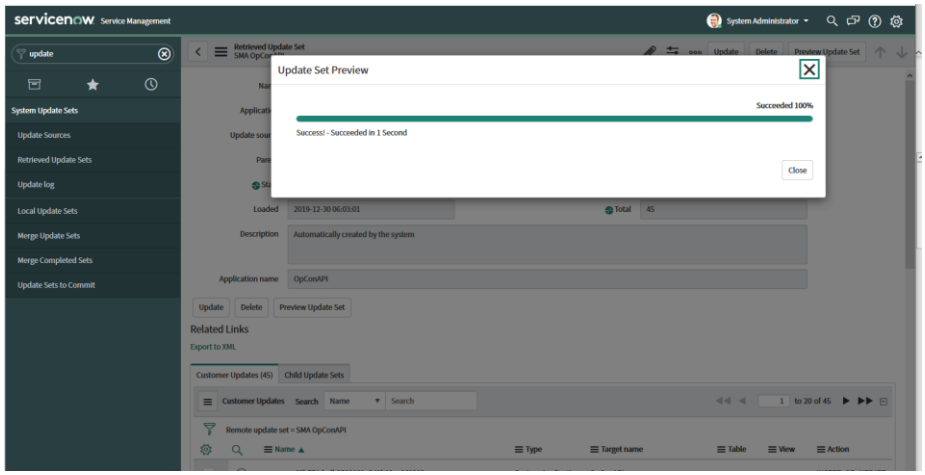



*Figure 17 : Update Set Preview success*

When the Update Preview Set had achieved a 100% success, the *Commit Update Set* button appears. Select this button to commit the update set and make it available in the ServiceNow instance.

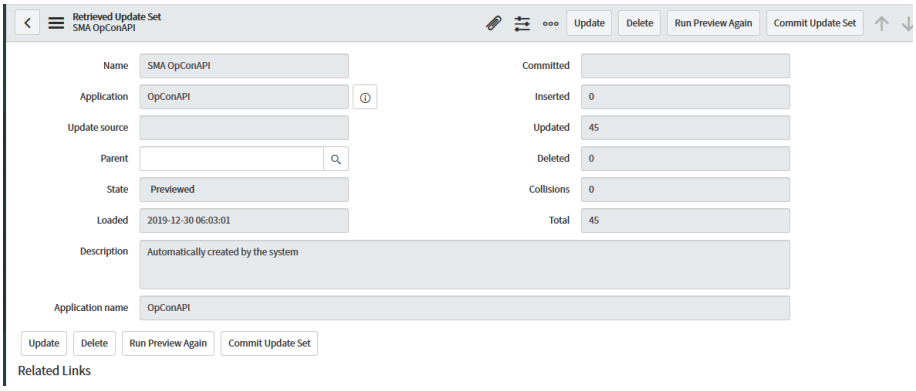



*Figure 18 : Commit Update Set*

Once the Update Set has been committed, the business rules and outbound rest messages are available in the ServiceNow instance. The business rules need to be marked as active to have any effect on the Incident table. Got to System Definition -> Business Rules and enter the name opcon in the search field and transmit. This will display the new installed rules.

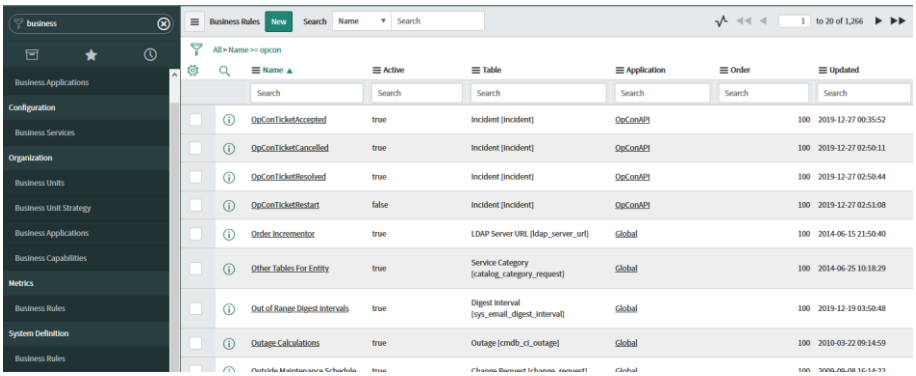



*Figure 19 : Installed OpConAPI Business Rules*

Select a rule and then mark the rule as Active for it to become effective.

The application import provided two rules that can be used when an Incident is Resolved. The task in OpCon can be set to Fixed (rule OpConTicketResolved) which means operations staff must release the task or it can be automatically restarted (rule OpConTicketRestart).

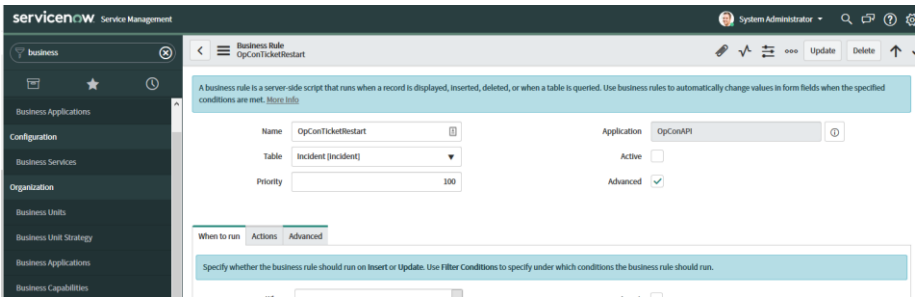



*Figure 20 : Setting Business Rule to Active state.*