Worksoft Certify Technical Note

Integrating Worksoft Certify with ServiceNow

Worksoft Certify® integrates with ServiceNow® to allow users to submit incidents into the ServiceNow system that were found in the Certify Result Viewer. ServiceNow is an IT incident management system that allows users to capture and organize IT incidents, assign work, and follow team activities.

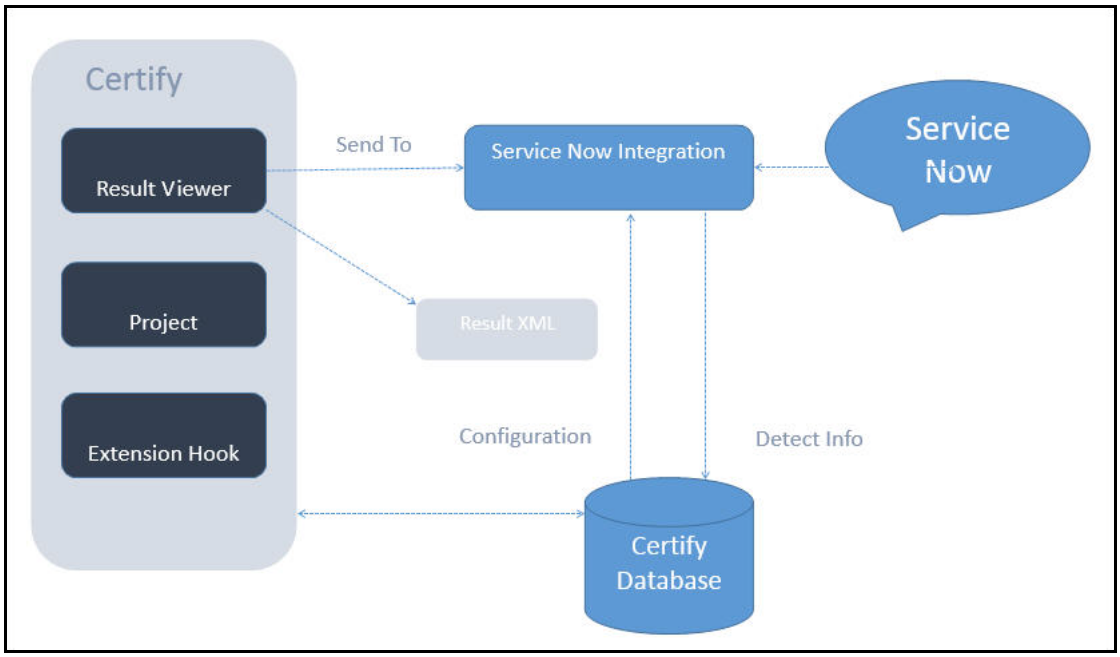
With the integration software, you are able to create ServiceNow incidents and populate all of the incident's fields by using information from Certify results and processes. The incident is then imported into a ServiceNow system where you are able to edit and refine the incident. After the incident is submitted to ServiceNow, you are unable to see the details of the incident in Certify.

In order to integrate Certify with ServiceNow, you will need to do the following:

- Create an Extension hook in Certify
- Configure ServiceNow
- Map ServiceNow fields

Integration Architecture

The following diagram shows an overview of how this integration works.



In the Certify Result Viewer, a user right-clicks on a failed step and selects **Send To > ServiceNow**. Certify generates a result XML file and an image file that is sent to the ServiceNow Integration tool.

The Integration tool completes the following tasks:

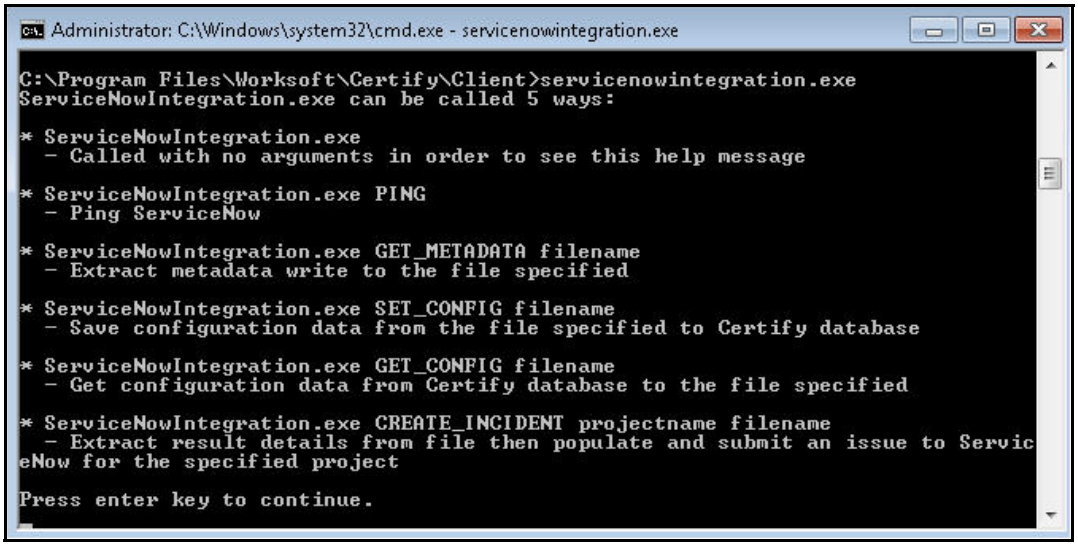
- Reads the result file
- Queries the Certify database for details of the target ServiceNow system, including the URI, user name, password, and field mapping
- Generates a ServiceNow incident
- Populates fields for the incident in ServiceNow by using Certify process and results data
- Submits the incident to ServiceNow which provides back an ID for a new incident
- Records the incident ID into the Certify database
- Launches ServiceNow to allow users to do additional editing on the new incident

ServiceNow Integration Command Line Modes

The ServiceNow Integration tool is implemented using a standalone command line executable. This executable has five modes of operation:

- PING
- GET_METADATA
- SET_CONFIG
- GET_CONFIG
- CREATE_INCIDENT

When you start the ServiceNow Integration executable without any arguments, you will see a summary of all five modes with a description.



PING Mode

ServiceNow Integration executable is started with the PING mode. In this mode, ServiceNow configuration stored in Certify is retrieved, and an attempt will be made to connect with the ServiceNow system. Any conditions resulting in an error will be shown to the user.

GET_METADATA Mode

You will use the GET_METADATA mode to create a configuration file template. This mode extracts metadata and writes to a specified file.

The GET_METADATA mode also helps identify fields that are needed for ServiceNow incidents. The output file includes details about projects, fields, and values from your ServiceNow instance.

SET_CONFIG Mode

The SET_CONFIG mode saves configuration data from a specified file and stores the data to a Certify database.

The attribute CREATEDEFECT has two possible values—Yes and No. The value of this attribute determines if a defect or incident is created. If the value is Yes, then a defect is created, and if the value is No, then an incident is created. The default value is No.

Example:

This XML file does not have any style information associated with it.

```
<DETAILS>
	<USERNAME>obaid.ullah</USERNAME>
	<PASSWORD>worksoft</PASSWORD>
	<URI>https://worksoftsandbox.service-now.com</URI>
	<CREATEDEFECT>no</CREATEDEFECT>
	<FIELDS>
		<FIELD>
			<NAME>caller</NAME>
			<VALUE/>
			<VALUEMAPPING>username</VALUEMAPPING>
		</FIELD>
		<FIELD>
			<DISPLAYEDNAME>affected user</DISPLAYEDNAME>
			<NAME>caller_id</NAME>
			<VALUE/>
			<VALUEMAPPING>username</VALUEMAPPING>
		</FIELD>
		<FIELD>
			<NAME>impact</NAME>
			<VALUE/>
		</FIELD>
		<FIELD>
			<NAME>urgency</NAME>
			<VALUE/>
		</FIELD>
		<FIELD>
			<NAME>contact_type</NAME>
			<VALUE/>
		</FIELD>
```

```
            <FIELD>
                  <NAME>opened_by</NAME>
                  <VALUE/>
                  <VALUEMAPPING>username</VALUEMAPPING>
            </FIELD>
            <FIELD>
                  <NAME>category</NAME>
                  <VALUE/>
            </FIELD>
            <FIELD>
                  <NAME>subcategory</NAME>
                  <VALUE/>
            </FIELD>
            <FIELD>
                  <NAME>configuration_item</NAME>
                  <VALUE/>
            </FIELD>
            <FIELD>
                  <NAME>state</NAME>
                  <VALUE/>
            </FIELD>
            <FIELD>
                  <NAME>assignment_group</NAME>
                  <VALUE/>
                  <VALUEMAPPING>username</VALUEMAPPING>
            </FIELD>
            <FIELD>
                  <NAME>owner</NAME>
                  <VALUE/>
                  <VALUEMAPPING>username</VALUEMAPPING>
            </FIELD>
            <FIELD>
                  <NAME>description</NAME>
                  <VALUE/>
                  <VALUEPATH>
                  CertifyResults/LogTestStep/LogTestStepDetails/Narrative
                  </VALUEPATH>
            </FIELD>
            <FIELD>
                  <NAME>short_description</NAME>
                  <VALUE/>
                  <VALUEPATH>
                  CertifyResults/LogTestStep/LogTestStepDetails/Narrative
                  </VALUEPATH>
            </FIELD>
      </FIELDS>
</DETAILS>
```

The password field is specified in clear text, but it is encrypted when it is stored in the Certify database.

GET_CONFIG Mode

The GET_CONFIG mode extracts configuration details from the Certify database and stores the details in a specified file.

The password will not be decrypted to prevent anyone from finding out the ServiceNow password. If the mapping file is updated and needs to be saved back to Certify, you are able to do one of the following to protect your password:

- Omit the password tag.

  Password field in the database will not be updated.
- Provide the correct clear-text value for the password.

CREATE_INCIDENT Mode

The CREATE_INCIDENT mode extracts result details from the result file, queries the Certify database for details of the target ServiceNow system, and generates a ServiceNow incident. If the integration was successful, then details of the ServiceNow incident will be associated with the result in the Certify database.

An entry will be created in a table called External incident, and the entity ID field will be the ID of the result log header. Details will be added to a child table called External Incident Details, and these details will include the ID and key of the ServiceNow incident. If a value for a field cannot be determined, then the default value Unknown will be used.

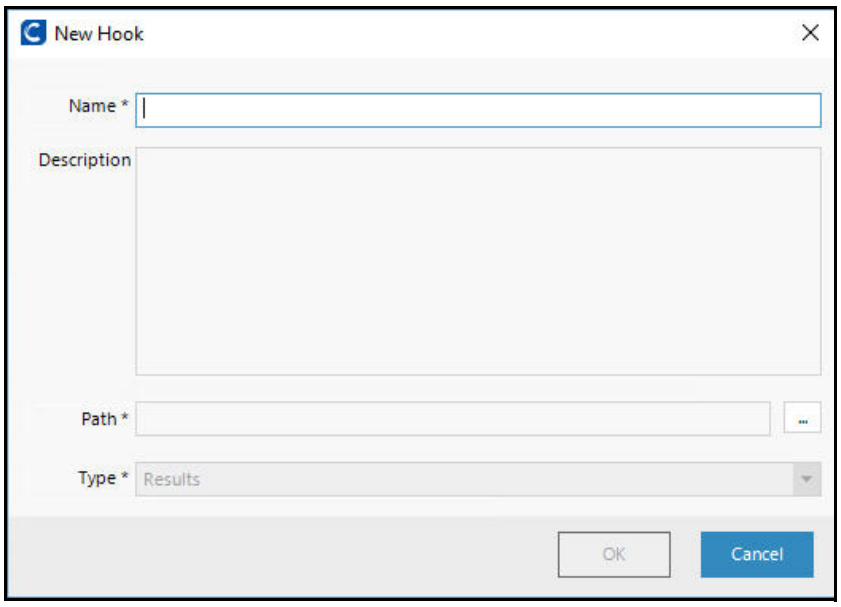
Creating an Extension Hook in Certify

The ServiceNow integration is implemented by creating an Extension hook in Certify and associating the hook to a Certify project.

▶ *To create a hook:*

1. In the Certify Navigation pane, click **Extensions**.
2. In the Navigation tree, select **Extensions > Hooks > Result**.
3. Right-click in the Summary pane and select **New Hook**.

   The New Hook dialog box appears.



4 In the Name field, type **`ServiceNow`**.

5 In the Description field, type **`ServiceNow Hook`**.

6 In the Path field, type the path where the **ServiceNowIntegration.exe** file is found in the Worksoft Certify client folder: **`. . .Worksoft\Certify\Client\servicenowintegration.exe`**.

7 Click **OK**.

▶ *To add a hook to a project:*

1 In the Certify Navigation pane, click **Projects**.

The Projects window appears.

2 In the Summary pane, select a project.

3 Click the **Hooks** tab.

4 Right-click in the Hooks tab and select **Add Hook**.

The Select Hooks dialog box appears.

5 Select a hook in the Summary pane.

6 Click **OK**.

The hook is added to the project and appears in the Hooks tab. Also, the ServiceNow option appears in the right-click menu option **Send To** in the Results Viewer Summary pane.

Configuring the ServiceNow Connection

In order for you to integrate with ServiceNow, you will need to do the following tasks:

- Create a configuration file for the ServiceNow Integration executable. The file requires a URI, user name, and password. This information gets stored in the Certify database along with details of which fields to populate in a ServiceNow incident.
- Save the configuration file in the Certify database.
- Verify the ServiceNow connection.

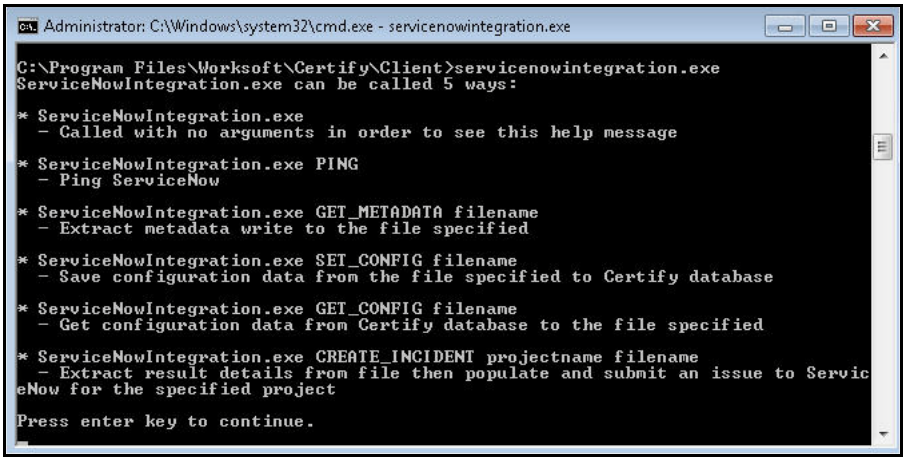
▶ *To create a configuration file:*

1 Open the Command Prompt window and navigate to the folder where ServiceNow Integration file is located.

Example: **`. . .Worksoft\Certify\Client\servicenowintegration.exe`**

2 Run the ServiceNow integration executable without any parameters.

All available ServiceNow modes display.



3 Execute the ServiceNow Integration executable again with the GET_METADATA mode to create a configuration file template.

Example:

```
ServiceNowIntegration.exe GET_METADATA "c:\temp\ServiceNowTemplate.xml"
```

4 Open the new XML file in a text editor.

5 Add the following ServiceNow information:

- User name
- Password
- URI

Example:

```
<DETAILS>
<USERNAME>myusername</USERNAME>
<PASSWORD>worksoft</PASSWORD>
<URI>https://worksoftsandbox.service-now.com</URI>
</DETAILS>
```

6 Save the updated configuration file. You are able to rename the file, but it needs to be saved as an XML file.

You now need to save the configuration file to the Certify database.

▶ *To save the configuration file to the Certify database:*

1. Open the Command window and navigate to the ServiceNow Integration executable.
2. Execute the ServiceNow Integration executable with the SET_CONFIG mode to upload the configuration file to the Certify database.

   Example:

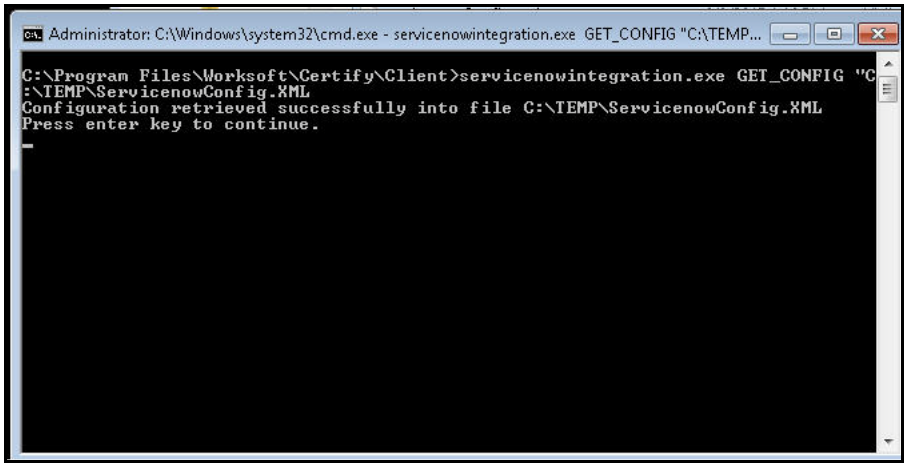
   ```
   ServiceNowIntegration.exe SET_CONFIG C:\temp\ServiceNow
   configuration.XML
   ```

   If there are errors, then the command window will indicate the source of the problem.
3. To retrieve the ServiceNow configuration that is now stored in Certify, run the executable with the GET_CONFIG mode to retrieve the configuration.

   Example:

   ```
   ServiceNowIntegration.exe GET_CONFIG C:\temp\ServiceNowConfig.xml
   ```

   The configuration file is stored in Certify.



The next step is to verify the ServiceNow connection.

▶ *To verify the ServiceNow connection:*

In the Command Prompt window, execute ServiceNowIntegration.exe with the following command:
`. . .Worksoft\Certify\Client\servicenowintegration.exe PING`

The ServiceNow credential is retrieved from the Certify database and connects to a remote ServiceNow system. If there are errors, they will be shown to the user as why it was unable to connect.

Mapping ServiceNow Fields

When an incident is created and submitted into ServiceNow, it must have values in the required fields. You will need to identify required fields, optional fields, and values by consulting your ServiceNow administrator.

You can also run the ServiceNow Integration executable with the GET_METADATA mode to identify needed fields. The output file includes details about projects, fields, and values from your ServiceNow instance.

Mapping information is specified in a text file that is subsequently loaded into the Certify database. The text file has the following structure:

```
<DETAILS>
  <FIELDS>
    <FIELD>Field 1 details</FIELD>
    <FIELD>Field 2 details</FIELD>
    <FIELD>Field 3 details</FIELD>
  </FIELDS>
  <USERNAME>myuserid</USERNAME>
  <PASSWORD>worksoft</PASSWORD>
  <URI>https://worksoftsandbox.service-now.com</URI>
</DETAILS>
```

Username and password fields are optional. Theses fields need to be loaded into Certify one time, and they do not need to be loaded with field definitions.

Each field and value is identified by the node named as Name and Value respectively. Sometimes a name in name field does not match with the corresponding field name displayed in ServiceNow UI. In such an instance, the node <DISPLAYNAME> is used to display the UI name. The value of this field shall not be used in any processing. The name is included only to help the end user to map the field in configuration with the corresponding name displayed in the UI.

Where to Get Data for ServiceNow Fields

As part of your implementation, you need to determine where to get data for the fields in your ServiceNow incidents. Data can be gathered from the following places:

- Hard-coded value

  Example:

  ```
  <FIELD>
    <NAME>caller</NAME>
    <VALUE>abc</VALUE>
  </FIELD>
  ```

  In this case, the User field will be identified by the value in the Value field.

- Value is mapped to another field in the XML file

  ```
  <FIELD>
    <DISPLAYEDNAME>affected user</DISPLAYEDNAME>
    <NAME>caller_id</NAME>
    <VALUE/>
    <VALUEMAPPING>username</VALUEMAPPING>
  </FIELD>
  ```

If no value is defined under in the Value field, then the value of the ValueMapping field is used to search corresponding fields in the XML file. In this particular case, username will be used as value for caller_id.

- Value retrieved from the Certify execution result using an XPath expression

```
<FIELD>
  <NAME>description</NAME>
  <VALUE> </VALUE<
  <VALUEPATH>
     CertifyResults/LogTestStep/LogTestStepDetails/Narrative
  </VALUEPATH>
</FIELD>
```

The Valuepath field will be used to extract a value from the XPath expression in the result XML file.

Save Field Mapping File to Certify

In the Command Prompt window, execute ServiceNowIntegration.exe to load your mapping file into the Certify database.

Example:

```
. . .Worksoft\Certify\Client\servicenowintegration.exe C:\temp\configuration.txt
SET_CONFIG
```

If there are errors, then the command window will indicate the source of the problem.

Submitting an Incident or Defect

After you have completed configuring the ServiceNow configuration, you are now able to submit an incident or defect to ServiceNow. You will use the Certify Result Viewer to submit them into ServiceNow.

▶ *To submit an incident or defect:*

1 In the Certify Result Viewer, select a process in the Navigation pane.

The Summary pane lists the steps of the process.

2 Right-click on a step and select **Send To > ServiceNow**.

Certify generates a result XML file and an image file that is sent to the ServiceNow Integration tool.

The ServiceNow Integration tool completes the following tasks:

- Reads the result file
- Queries the Certify database for details of the target ServiceNow system, including the URI, user name, password, and field mapping
- Generates a ServiceNow incident or defect
- Populates fields for the incident or defect in ServiceNow by using Certify process and results data
- Submits the incident or defect to ServiceNow which provides back an ID for a new incident or defect
- Records the incident or defect ID into the Certify database
- Launches ServiceNow to allow users to do additional editing on the new incident or defect

While the incident or defect is being constructed and submitted, the Command Prompt window shows the details of the progression.