ServiceNow Integration with VirtualWisdom

Introduction

Connecting monitoring and IT Service Management (ITSM) processes has become critical to ensure efficient and effective management of IT performance and availability issues. Without it, issues can easily fall between the gaps.   Virtual Instruments has developed a set of integrations with ServiceNow® to ensure nothing falls through those cracks.

1. The integration between VirtualWisdom and ServiceNow enables Incidents to be automatically created, updated and closed within ServiceNow. For instance, Incident updates in ServiceNow update the corresponding case in VirtualWisdom. A case combines one or more alarms of the same type to reduce the recurring-alarm noise that most monitoring systems create when integrated with IT service desk incident management processes.   VirtualWisdom can automatically create incidents for application or infrastructure issues covering:
    - IT infrastructure performance, availability, health or error states (such as CRC errors)
    - The health of VirtualWisdom itself (such as a fan failure in the appliance or hardware probes)

2. ServiceNow integrates with VirtualWisdom alarms, adding enhanced REST API access to reports, analytics, and case management CMDB.

3. VirtualWisdom also enables discovery / importation of applications directly from local and cloud instances of ServiceNow Business Service, Manual Service and Technical Services. After an application is created, you can drill down to see topology, application components, and FC conversations. This integration provides the ability to configure Tier Mapping to associate business criticality to VirtualWisdom tiers. VirtualWisdom alarm thresholds are automatically associated with each tier, simplifying the initial VirtualWisdom set-up. The application and the entire supporting infrastructure are included in this tiering set-up.

Two-way integration – details

ServiceNow Integration with VirtualWisdom is a two-way integration and bi-directional synchronization, which happens as cases are opened and closed, and as progress and updates are logged into either system.

This two-way integration is enabled via the ServiceNow API. When VirtualWisdom opens a case, a ServiceNow incident is opened at the same time. Bi-directional synchronization happens as progress and updates are logged in either system. When an incident is closed in ServiceNow, its case is closed in VirtualWisdom. When a VirtualWisdom Health alert is closed in VirtualWisdom, it's closed in ServiceNow.
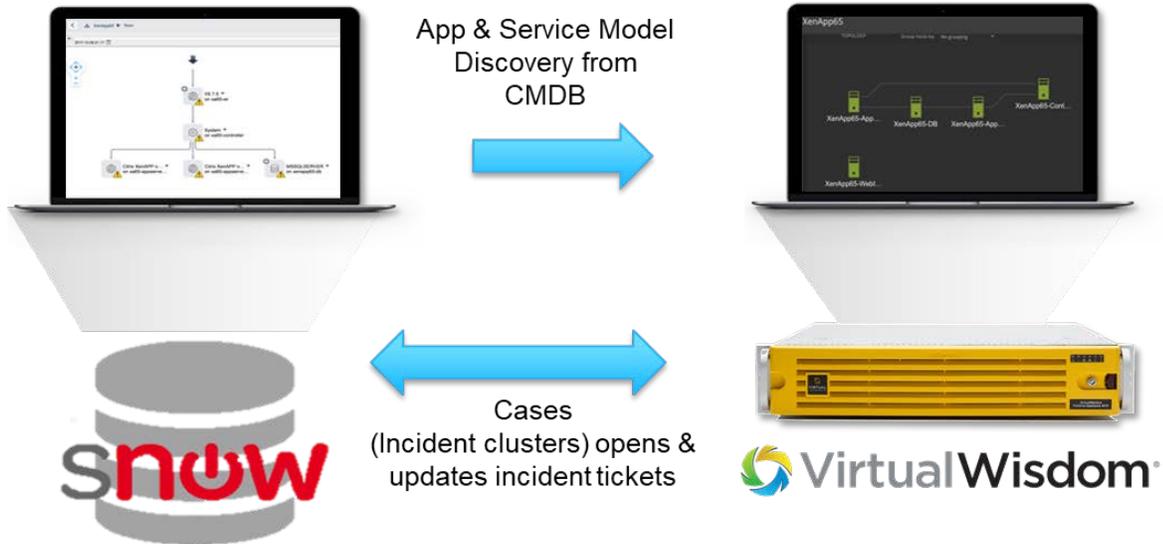
When a health alert or an alarm case is triggered in VirtualWisdom based on a certain rule, an "incident ticket" is opened in the ServiceNow system if it does not already exist. The ServiceNow incident includes "VirtualWisdom" in the short description. In VirtualWisdom, open cases now include the ServiceNow incident number (figure 1).

Figure 1: VirtualWisdom Open Cases

The corresponding Service Now Incident has been opened, figure 2 below.

Figure 2: ServiceNow Incidents

Figure 3: ServiceNow Incident Record

All the details from the VirtualWisdom Case are in the Service Now Incident along with the threshold that triggered the case.
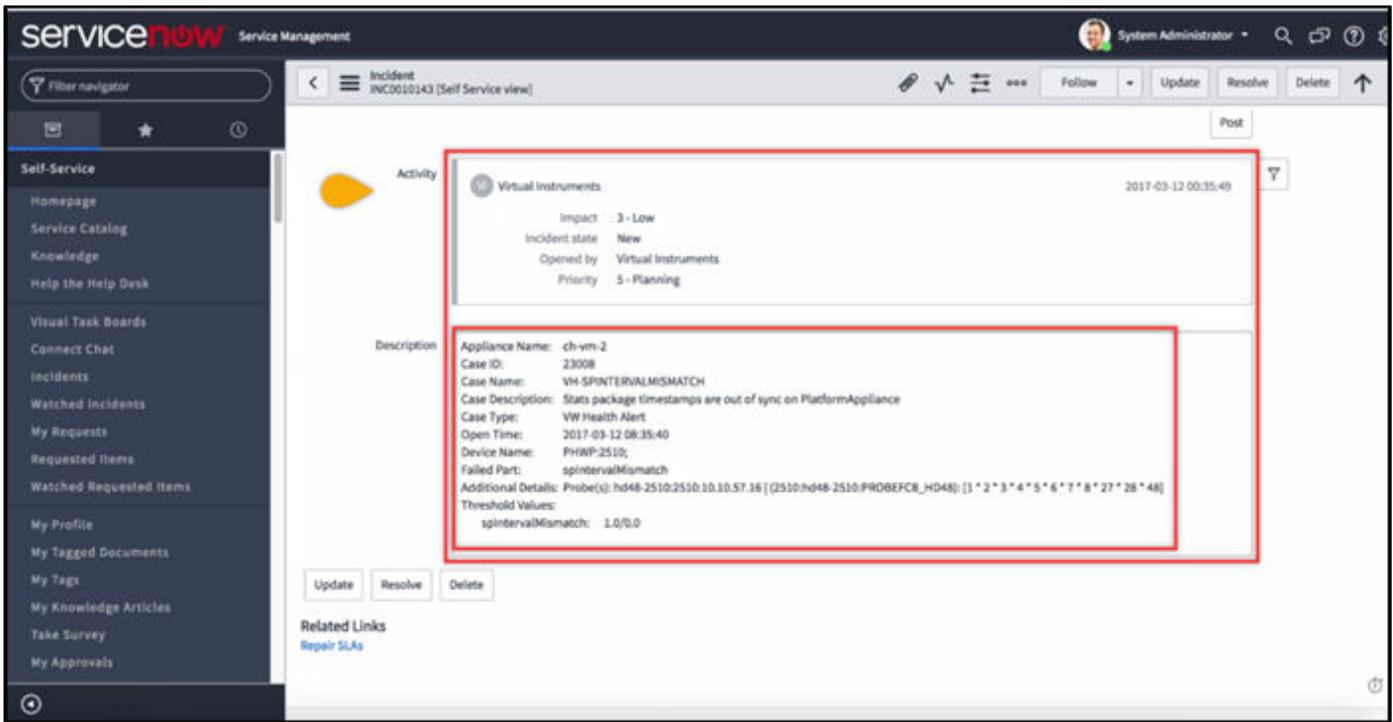
Figure 4: ServiceNow Incident Record (continued)

VirtualWisdom polls for recently closed ServiceNow incidents, every 30 seconds. A closed case in VirtualWisdom does not close a case in ServiceNow.

When the incident ticket is acted upon in ServiceNow, the user would typically "close" the ticket. This, in turn, will allow the alert to be cleared in the VirtualWisdom system – closing the corresponding case, if VirtualWisdom detects that the fault has been cleared.

Customers are not required to login to the VirtualWisdom system to act on the case.

How to integrate

To integrate VirtualWisdom with ServiceNow, the user needs to provide the following information in table 1.

OAuth client id OAuth client secret	VirtualWisdom uses OAuth 2.0 to obtain the access token from the ServiceNow server
Instance name	
Username Password	The user needs to have the ITIL role

Table 1.

Specific steps:

- Create a ServiceNow user with the "ITIL" role
- Configure OAuth 2.0 authentication
- Setup VirtualWisdom to integrate with ServiceNow

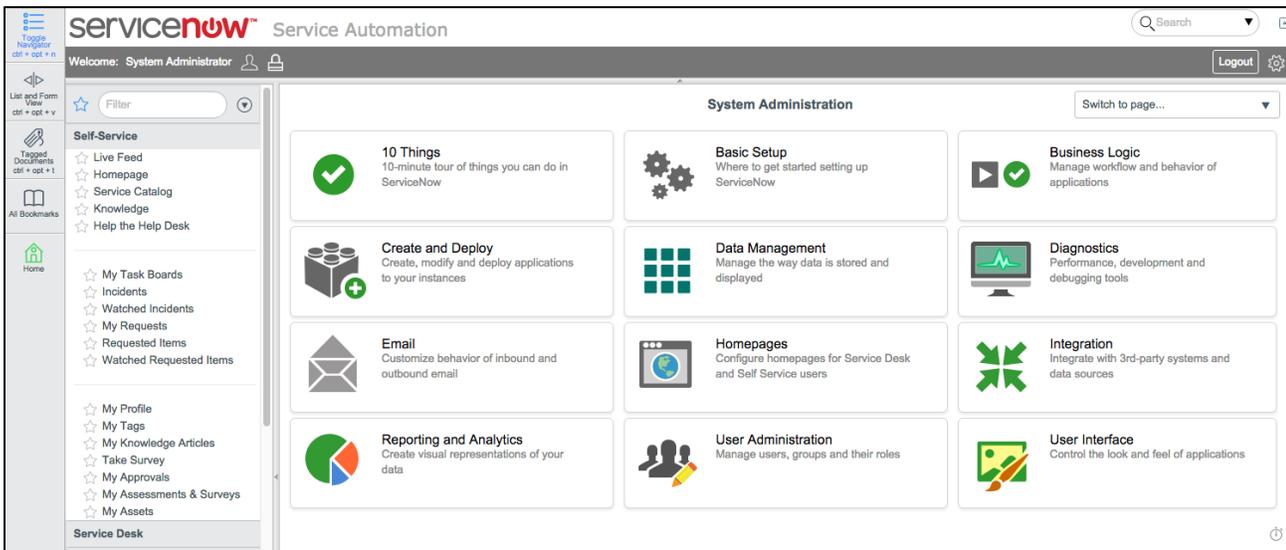## ServiceNow Configuration

Figure 5.

In ServiceNow, create a new user. Find User Administration in the navigation panel on the left of the main screen; scroll to the bottom of that panel. Click on it to expand and then select Users. Then click on the New button as shown below in figure 6.
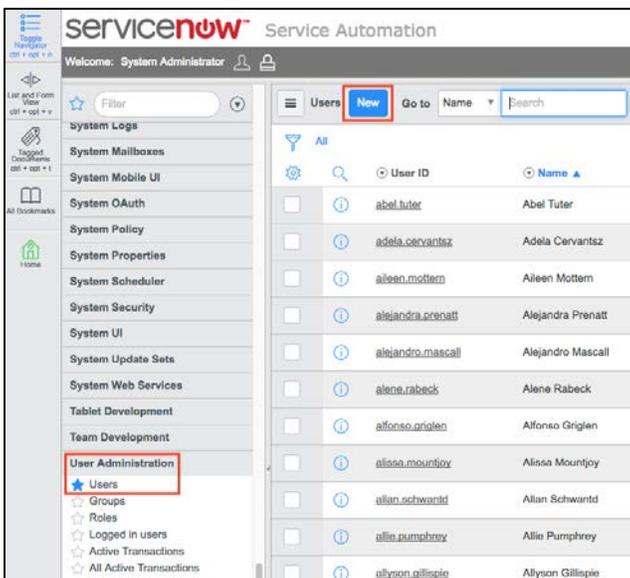

Figure 6.

Enter a User ID and Password, as shown in figure 7 below, and click on Submit. You can use anything you like for your ID and password, just write them down, because you'll need them later.

Figure 7.

After clicking Submit, you'll be taken back to the Users page and your newly minted User will be at the top of the page as shown below in figure 8.

Figure 8.

Click on the User ID again and then scroll down to the bottom of the resulting page as shown below.
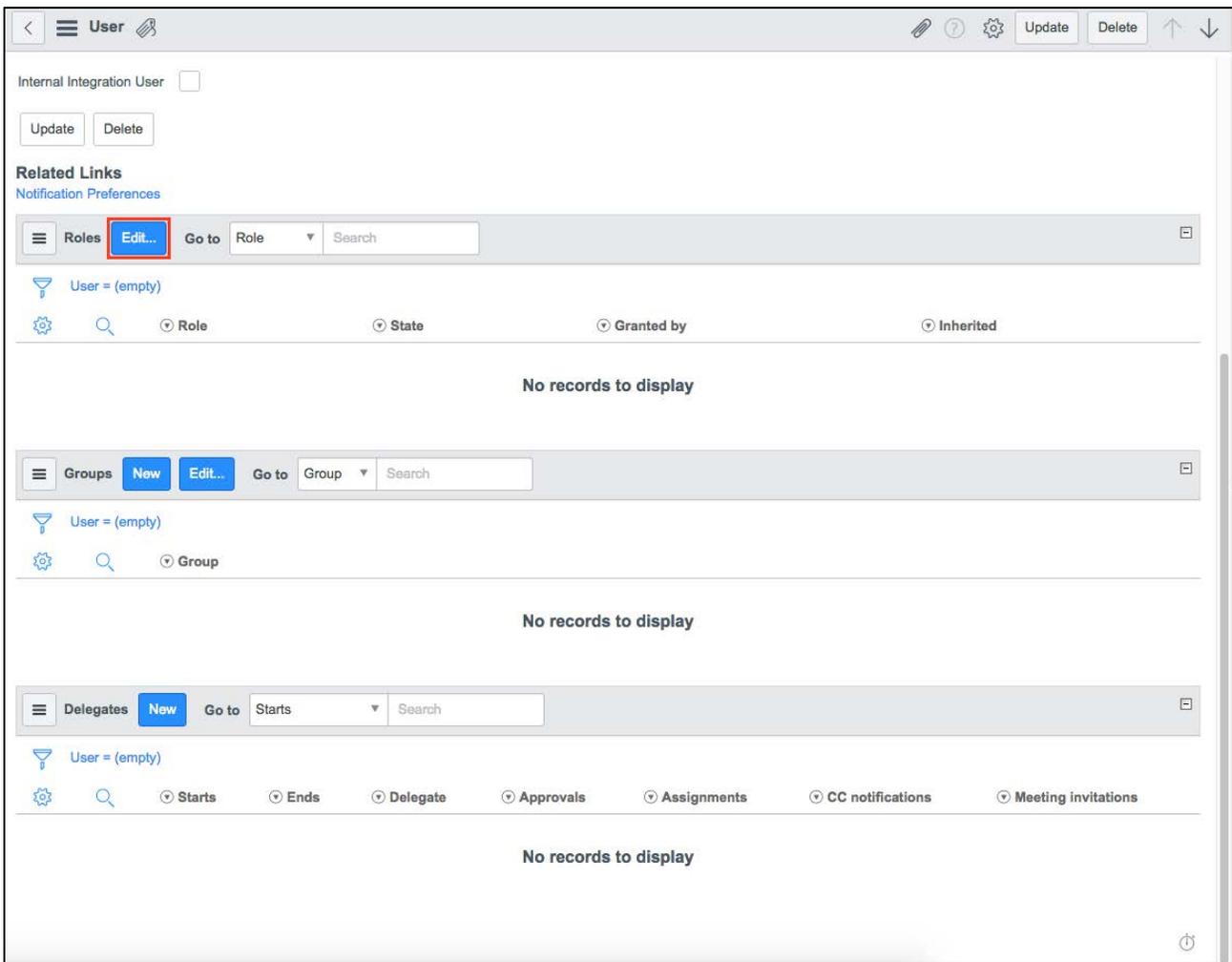

Figure 9.

Click on the Edit button next to the Roles category. It is on the resulting page where you will assign your new User the "Itil" role. Filter the Collection by typing "itil" in the search box. Then select "itil", click the right arrow button to add it to the Roles List and then click Save, as in figure 10, below.
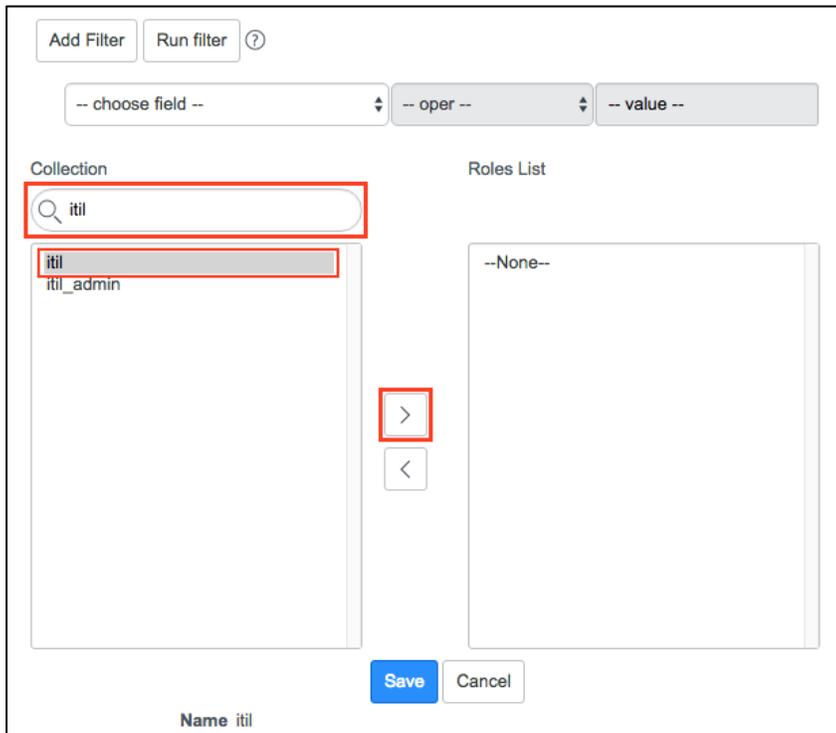

Figure 10.

Back at the User page, you'll notice that a few additional roles have been added. That's normal.

Figure 11.

Click on the Update button in the upper right-hand corner of the User screen to save the role to the User.
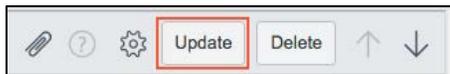

Figure 12.

Now you'll add OAuth capabilities to your instance. Find System OAuth in the navigation panel, select Application Registry, and then click on the New button as shown below.
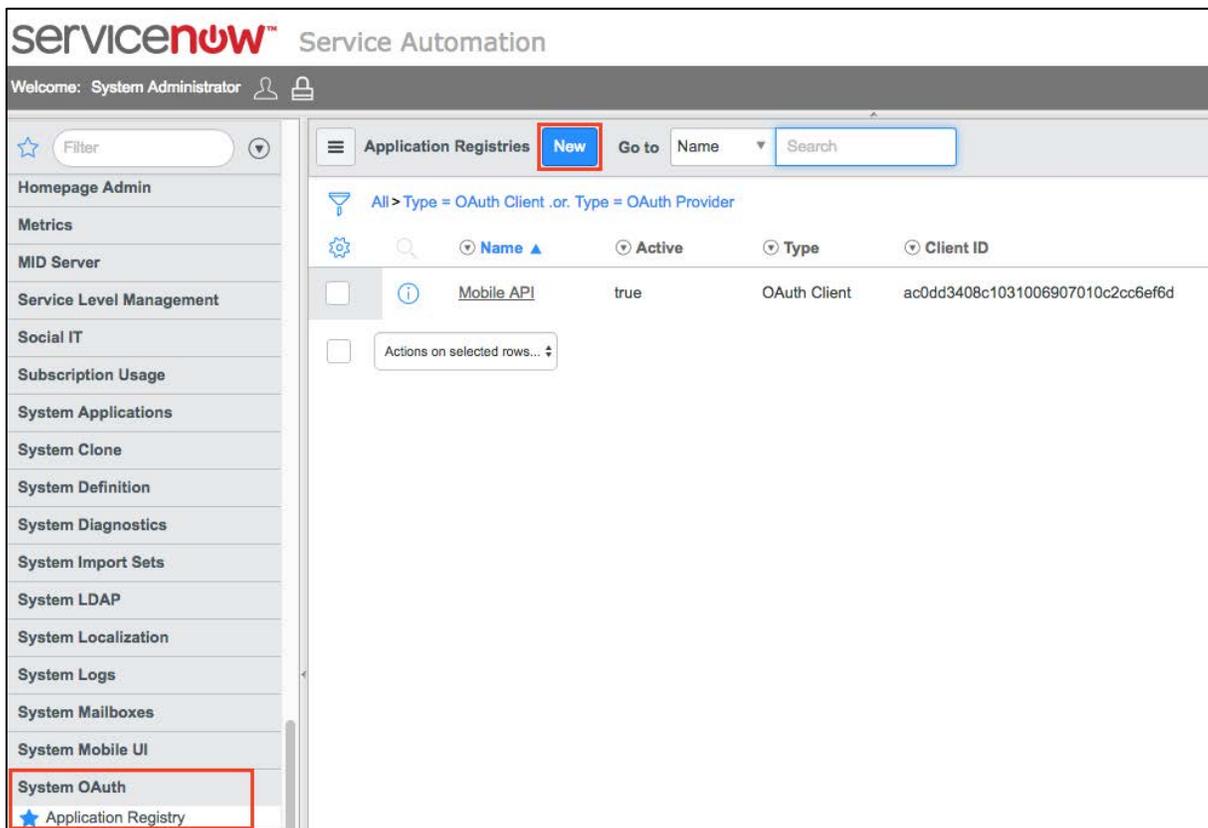

Figure 13

On the resulting page, click on the link shown below.

Figure 14.

Enter a name—you can use the same name as your User ID—and then click on Submit. There's no need to modify anything else on the page.
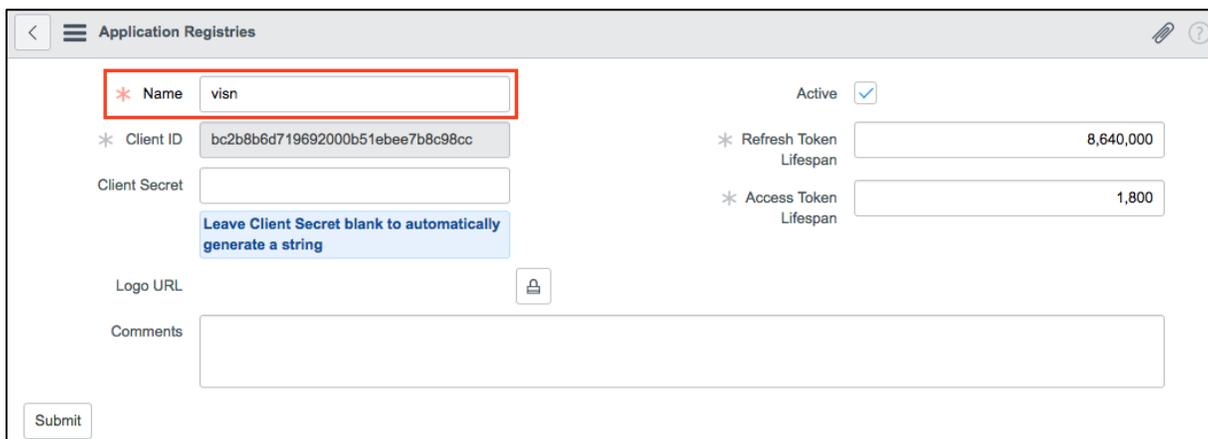

Figure 15.

Back on the Application Registries page, click on the new registry you just created. As shown below, click the lock icon next to Client Secret to reveal the secret. Copy these two pieces of information for later use with VW.

Figure 16.

We have all the information we need to configure ServiceNow integration on VirtualWisdom. From the Settings page, select Integration and click on the New button. Enter the numbered pieces of information from previous screenshots (the fields boxed in green) and then click on Save. That is all that is needed to get VirtualWisdom talking to ServiceNow.

Figure 17.

Please note the following:

1. Closing an alarm case in ServiceNow will trigger a close in VirtualWisdom. VirtualWisdom polls ServiceNow once every thirty seconds looking for closed incidents.

2. VirtualWisdom does not trigger the closing of alarm incidents in ServiceNow.

3. VirtualWisdom does trigger the closing of a VirtualWisdom health case in ServiceNow. A health alert is related to the VirtualWisdom instance itself.

4. Regarding health alerts: when an incident is closed in ServiceNow, the VirtualWisdom alert will not be closed until VirtualWisdom detects that the fault has cleared.

5. VirtualWisdom does not provide updates to incidents once created.

6. Both alarm and health alerts are sent to SNMP traps and to ServiceNow.

Case Information

ServiceNow Parameters	VirtualWisdom Parameters	Description
Short_description	VirtualWisdom, Rule Name, Entity Name	Set the short description to: VirtualWisdom-<Rule Name>-<Entity Name>
Description	Host Name, Case ID, Case Name, Case Description, Entity Type, Entity Name, Rule Name, Rule Type, Threshold Values, Exceeded Values, Open Time	The details of the case are stored in the description
Severity	Severity	The latest release of ServiceNow has 3 levels of severity: 1 – High 2 - Medium 3 – Low VirtualWisdom also has 3 levels of severity, named: FATAL – Critical WARNING – Moderate INFO – Non-disruptive

Table 2.

VIRTUAL INSTRUMENTS®

Sales
Sales@virtualinstruments.com
1.888-522.2557

Website
virtualinstruments.com