knowledge14®

April 27–May 1, 2014 • Moscone Center • San Francisco, CA

# Lab Guide

## Discovery 201:

## Custom Probes and Sensors

Aleck Lin & Doug Schulze

Lab instance: https://**<<name>>**.lab.service-now.com

Login / Passwords:

admin / Knowledge14

itil / Knowledge14

employee / Knowledge14

## Lab Prerequisites

Skills needed for this lab are a core understanding of the ServiceNow Discovery technology, comprehension of TCP/IP protocols, IP networking and base understanding of the ServiceNow core platform. Lastly, some basic JavaScript knowledge is helpful.

## Lab Agenda

- Discovery basics
- SNMP basics
- Discovery of an device using SNMP
    - Classify using SNMP
    - Write custom SNMP probes and sensors
    - Classify using SNMP System OID
- Discovery identifiers
- Q & A

## SNMP Basics

SNMP stands for Simple Network Management Protocol. It is typically used to for network devices, such as routers, switches, printers, UPS, servers.

SNMP devices expose management data as variables (identified by OIDs), which are organized in hierarchies. These hierarchies and other metadata (such as type and description of the variable) are described by MIBs (Management Information Bases).

MIB (Management Information Base) typically consists of many managed objects (aka variables). There are two types of managed object

- Scalar object, which defines single object instance
- Tabular object, which defines multiple related object instances that are grouped in MIB tables.

OIDs, or Object Identifiers are what uniquely identify managed objects in a MIB hierarchy.

www.oid-info.com is a great site to look up OID information.

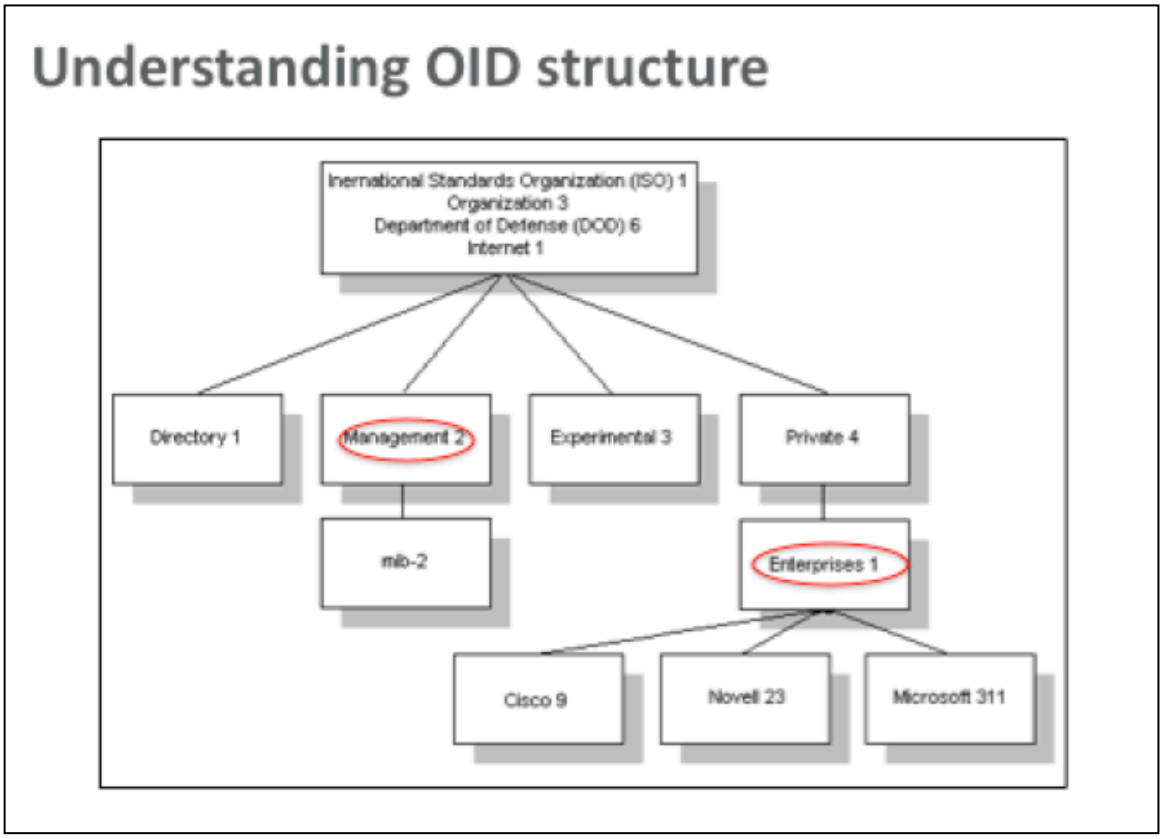
©2014 ServiceNow, Inc. All rights reserved.

## Understanding OID Structure

Typically assume the path of ISO(1).Identified-organization(3).dod(6).internet(1).

And most MIBs that we'd care about are in the level below marked in red.

- Directory (1)
- Mgmt(2)
- Experimental(3)
- Private(4)
- Security(5)
- snmpV2(6)
- Mail(7)
- Features(8)




©2014 ServiceNow, Inc. All rights reserved.

## What Kind of Device Is It?

"SNMP MIB-2" MIB (RFC 1213) is what we'll use…

ISO(1).Identified-organization(3).dod(6).internet(1).Mgmt(2).mib-2(1).system(1)

- sysDescr(1) -- Scalar object
- sysObjectID(2)
- sysUpTime(3)
- sysContact(4)
- sysName(5)
- sysLocation(6)
- sysServices(7)
- sysORLastChange(8)
- sysORTable(9) -- Tabular object

To access an object, for example, the sysDescr object. The OID would be 1.3.6.1.2.1.1.1**.** Typically one would use command line tools to retrieve the object value through clients such as snmpwalk, snmpget.

For example, the following command:

```
snmpwalk -v 2c -c public xxx.xxx.xxx.xxx 1.3.6.1.2.1.1.1
```

would return a result such as:

```
iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0 = STRING: Cisco PIX Firewall 6.0
```

©2014 ServiceNow, Inc. All rights reserved.

## Example of a Cisco PIX 520 Firewall

```
monster-MacBook:~ aleck.lin$ snmpwalk -v 2c -c public ec2-54-215-108-151.us-west-
1.compute.amazonaws.com
SNMPv2-MIB::sysDescr.0 = STRING: Cisco PIX Firewall 6.0
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.392
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (129600000) 15 days, 0:00:00.00
SNMPv2-MIB::sysContact.0 = STRING: Jalasoft
SNMPv2-MIB::sysName.0 = STRING: JalaFWPix525 - 10.160.234.164 - V2*
SNMPv2-MIB::sysLocation.0 = STRING: Undisclosed Location
SNMPv2-MIB::sysServices.0 = INTEGER: 64
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (253) 0:00:02.53
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.2 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIB
SNMPv2-MIB::sysORID.5 = OID: SNMPv2-SMI::enterprises.9
SNMPv2-MIB::sysORID.6 = OID: SNMPv2-SMI::enterprises.9.9.48
SNMPv2-MIB::sysORID.7 = OID: SNMPv2-SMI::enterprises.9.9.147
SNMPv2-MIB::sysORID.8 = OID: IANAifType-MIB::ianaifType
SNMPv2-MIB::sysORID.9 = OID: SNMPv2-SMI::enterprises.9.18.2.1
SNMPv2-MIB::sysORID.10 = OID: SNMP-TARGET-MIB::snmpTargetMIB
SNMPv2-MIB::sysORID.11 = OID: SNMP-COMMUNITY-MIB::snmpCommunityMIB
SNMPv2-MIB::sysORID.12 = OID: SNMP-NOTIFICATION-MIB::snmpNotificationMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module for SNMPv2 entities.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module to describe generic objects for
network interface sublayers. This MIB is an updated version of MIBIIs ifTable and
incorporates the extensions defined in RFC 1229.
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP implementations.
SNMPv2-MIB::sysORDescr.4 = STRING: The SNMP Management Architecture MIB
SNMPv2-MIB::sysORDescr.5 = STRING: The Structure of Management Information for
theCisco enterprise.
SNMPv2-MIB::sysORDescr.6 = STRING: MIB module for monitoring memory pools
SNMPv2-MIB::sysORDescr.7 = STRING: MIB module for monitoring Cisco Firewalls.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module which defines the IANAifType
textual convention and thus the enumerated values of the ifType object defined in
MIBIIs ifTable.
SNMPv2-MIB::sysORDescr.9 = STRING: The Cisco QOS Policy PIB for provisioning QOS
policy.
SNMPv2-MIB::sysORDescr.10 = STRING: This MIB module defines MIB objects which
provide mechanisms to remotely configure the parameters used by an SNMP entity for
the generation of SNMP messages.
```

©2014 ServiceNow, Inc. All rights reserved.

## Lab Exercise 1 – Discovery the Firewall

In this lab, we will learn how to classify a SNMP device that Discovery does not find out of the box.

A firewall device is available for the purpose of this lab.

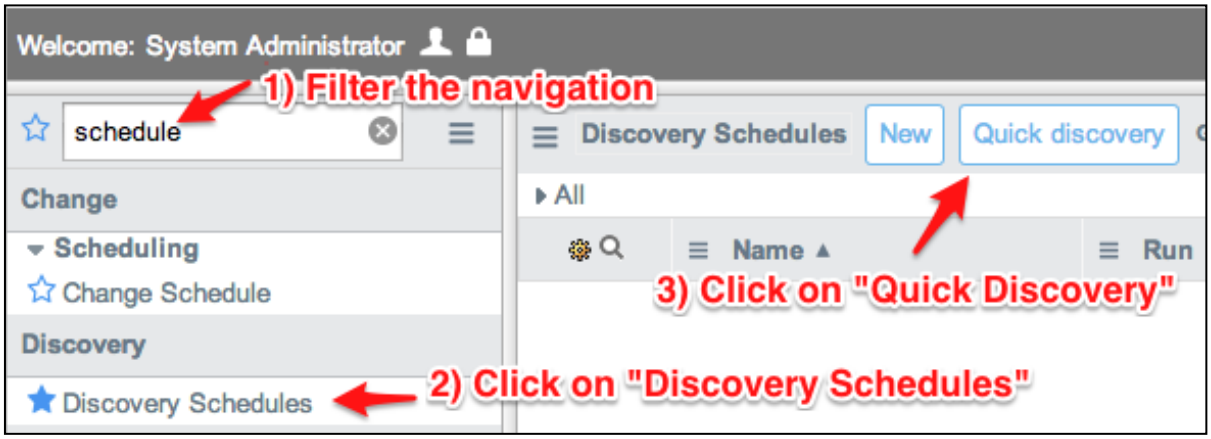
## Start a Discovery

To start off the lab, a discovery run is obviously needed, so here we go.

1. Filter the navigation with **schedule**.

2. Click **Discovery Schedules**.

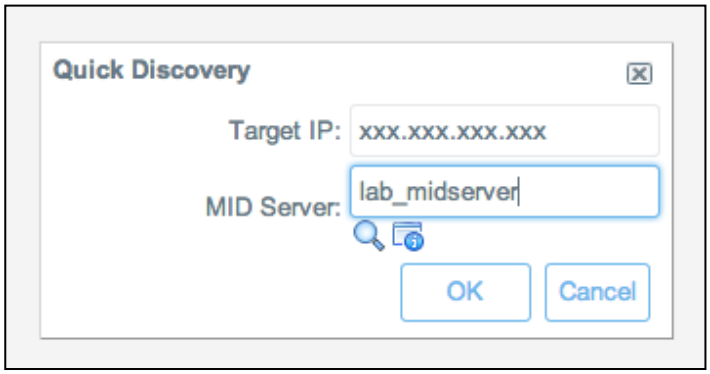
3. Click **Quick Discovery**.



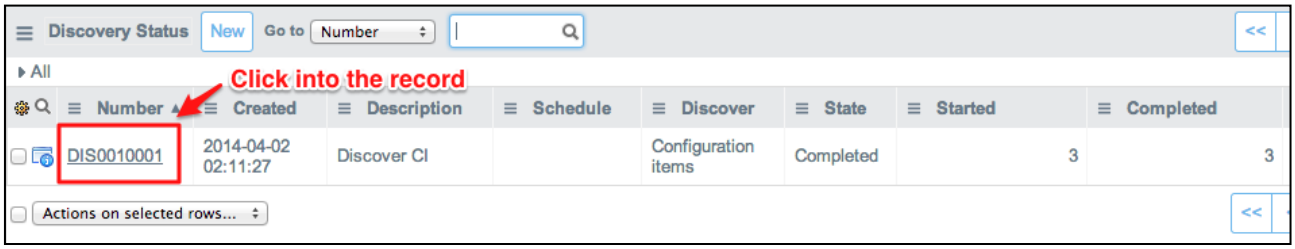

4. In the center of the browser, a pop-up box will show up. Enter the **Target** IP with the IP address given and select the MID server **lab_midserver1**.

©2014 ServiceNow, Inc. All rights reserved.

5. Click **OK** to start the discovery.




6. After clicking OK, the navigation will take you directly to the Discovery status record the represent the Discovery.

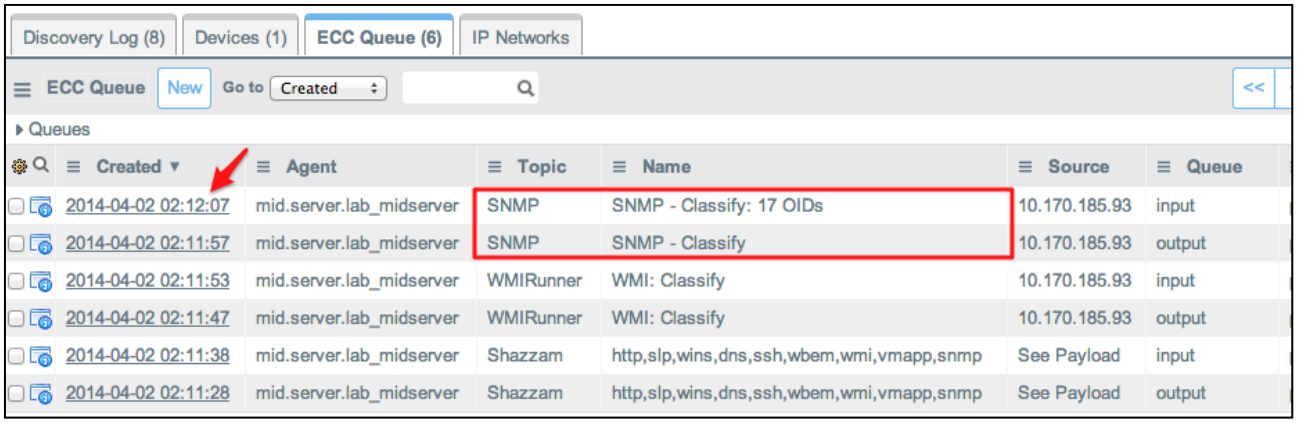



## What's Happening?

Discovery found SNMP port and launched SNMP classify probe, but stopped afterwards because it couldn't find any match in the SNMP classifications.

©2014 ServiceNow, Inc. All rights reserved.

Let's take a look at what we found by drilling into the SNMP – Classify input ECC queue record.



Discovery Log (8) | Devices (1) | ECC Queue (6) | IP Networks

ECC Queue | New | Go to Created

Queues

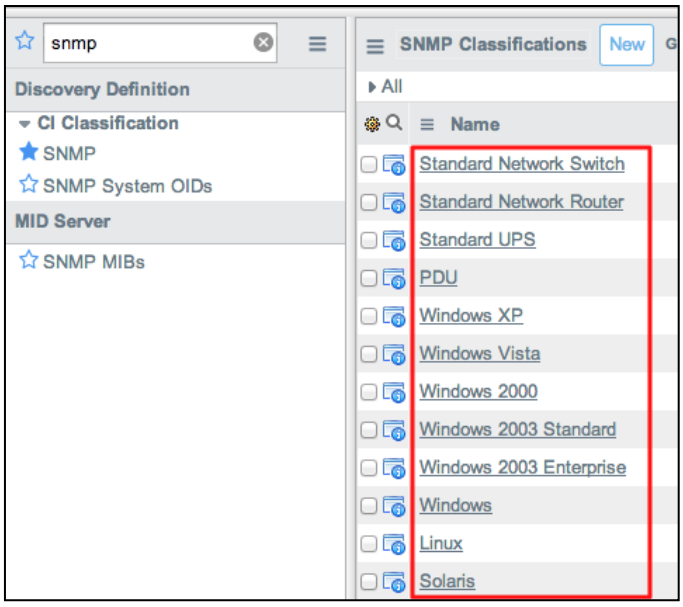
| Created | Agent | Topic | Name | Source | Queue |
|---|---|---|---|---|---|
| 2014-04-02 02:12:07 | mid.server.lab_midserver | SNMP | SNMP - Classify: 17 OIDs | 10.170.185.93 | input |
| 2014-04-02 02:11:57 | mid.server.lab_midserver | SNMP | SNMP - Classify | 10.170.185.93 | output |
| 2014-04-02 02:11:53 | mid.server.lab_midserver | WMIRunner | WMI: Classify | 10.170.185.93 | input |
| 2014-04-02 02:11:47 | mid.server.lab_midserver | WMIRunner | WMI: Classify | 10.170.185.93 | output |
| 2014-04-02 02:11:38 | mid.server.lab_midserver | Shazzam | http,slp,wins,dns,ssh,wbem,wmi,vmapp,snmp | See Payload | input |
| 2014-04-02 02:11:28 | mid.server.lab_midserver | Shazzam | http,slp,wins,dns,ssh,wbem,wmi,vmapp,snmp | See Payload | output |

We can see the basic info from the sysDescr OID that it is a **Cisco PIX Firewall 6.0**.




©2014 ServiceNow, Inc. All rights reserved.

7. Click the **SNMP** module under the **Discovery Definition** application menu. We'll notice that firewall is not on the list at all, so we'll need a SNMP classifier for the firewall device!




©2014 ServiceNow, Inc. All rights reserved.

## Create a Table for Firewall Device

Before creating a new SNMP classification for the firewall, we'll need to create a firewall table to properly store the CI record.

We'll create a **u_cmdb_ci_ip_firewall** table that will extend the **cmdb_ci_netgear** table.

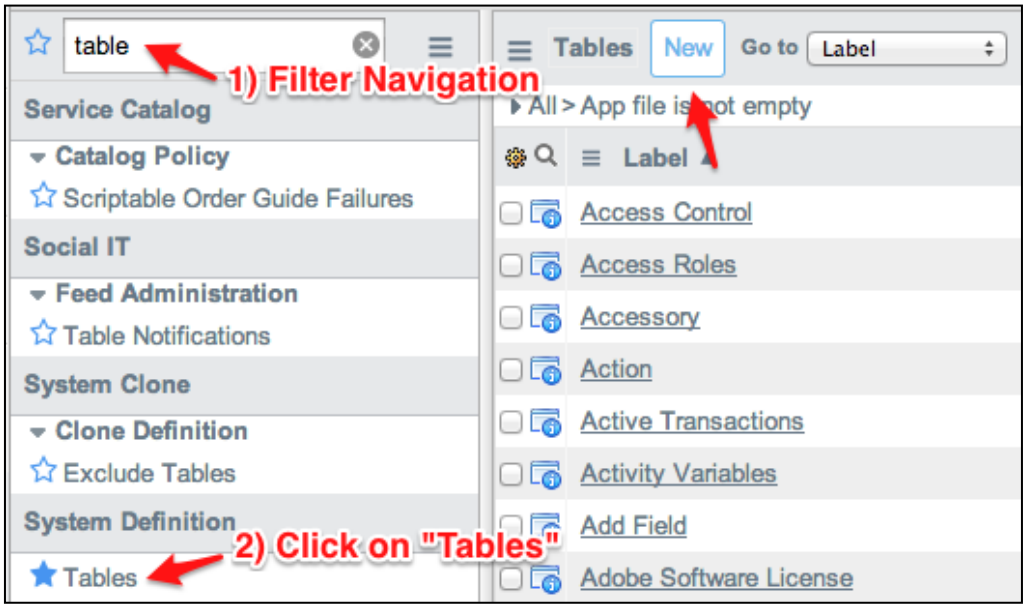
The **u_** is advised so that your table will never clash with the ones that ServiceNow create (or will create).

Let's switch gears to create the table first and we'll come back to create the new classification for firewalls.

1. Filter the navigation with **table**.

2. Click **Tables**.

3. Click **New**.




©2014 ServiceNow, Inc. All rights reserved.

4. Fill in the **Label** field with **IP Firewall**.

5. Fill in the **Name** field with **u_cmdb_ci_ip_firewall**.

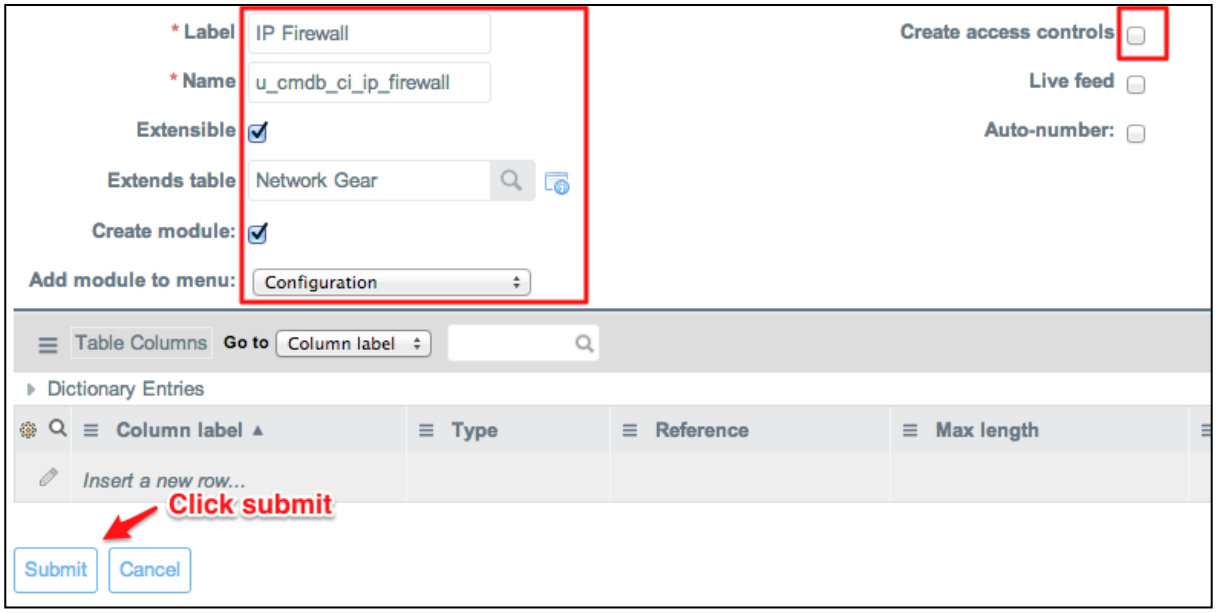
6. Check the **Extensible field**.

7. Select the **Extends Table** field with **Network Gear**.

8. Select the **Add module to menu** field with **Configuration**.

9. Deselect the **Create access controls** option.

10. Click **Submit**.




For more details regarding table creation, see wiki page
http://wiki.servicenow.com/index.php?title=Creating_a_Custom_Table

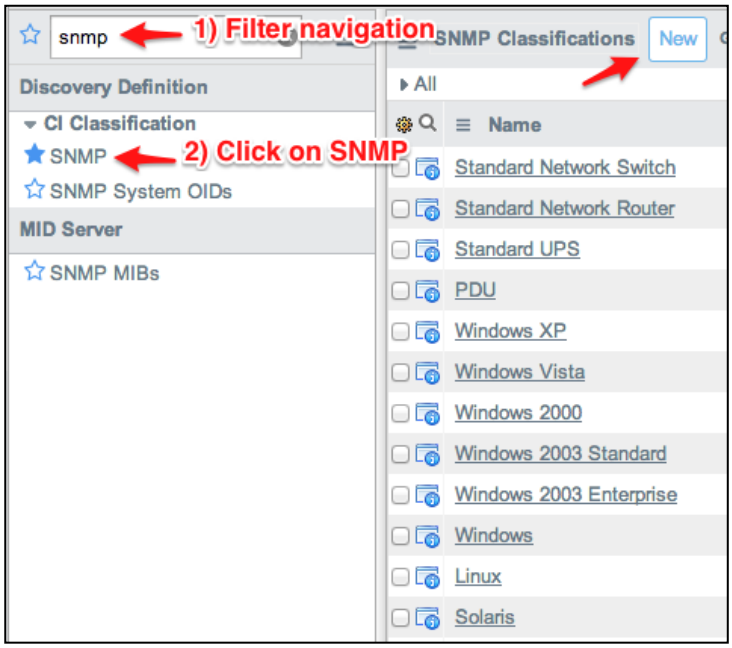
©2014 ServiceNow, Inc. All rights reserved.

## Create SNMP Classifier

1. Filter the navigation with **snmp**.

2. Click the **SNMP** module.

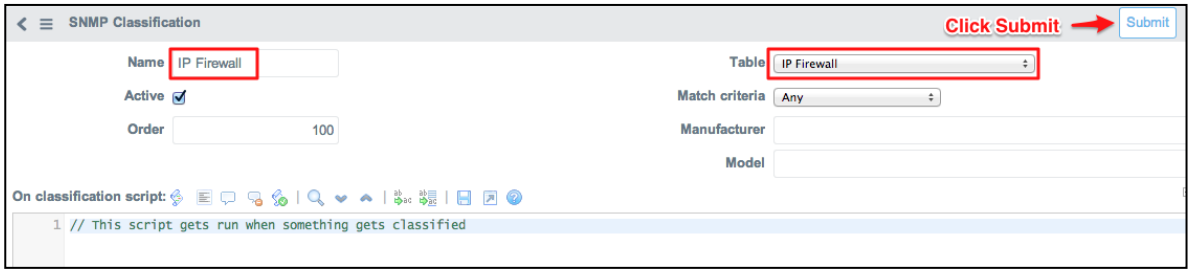
3. Click **New**.




4. Fill in the **name** field with IP **Firewall**.

5. Select the **Table** field with "**IP Firewall (u_cmdb_ci_ip_firewall)**.

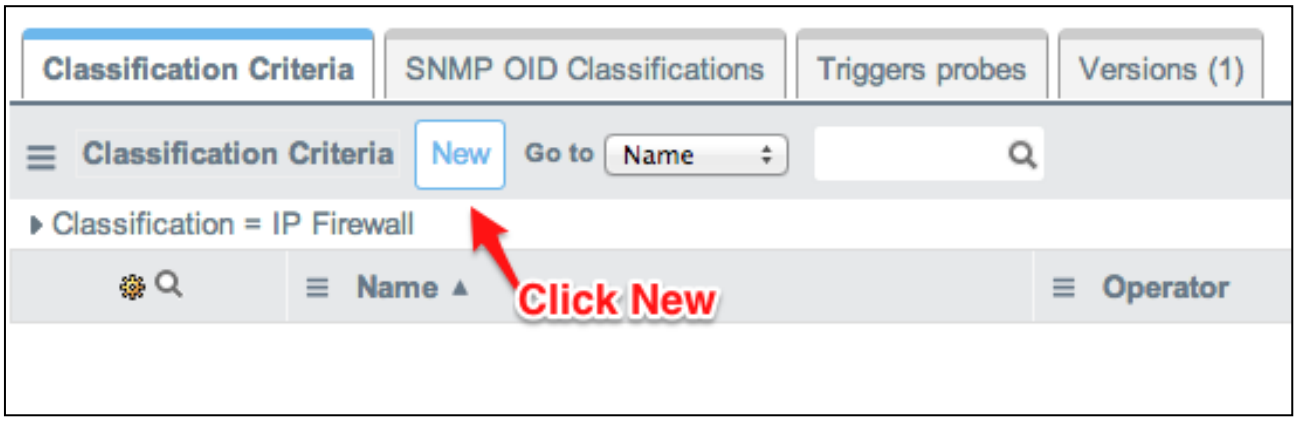
6. Click **Submit**




©2014 ServiceNow, Inc. All rights reserved.

7. Drill back into the record.

8. Click **New** under the **Classification Criteria** tab.

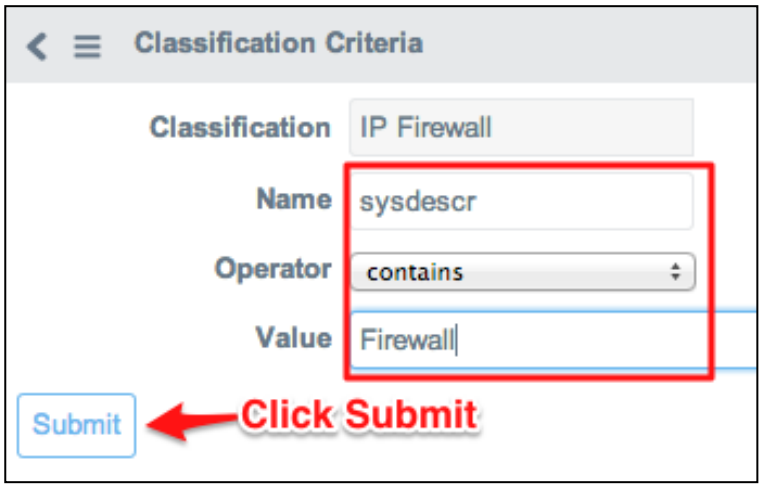



9. Fill in the **Name** field with "**sysdescr**".

10. Select the **Operator** field with **contains**.

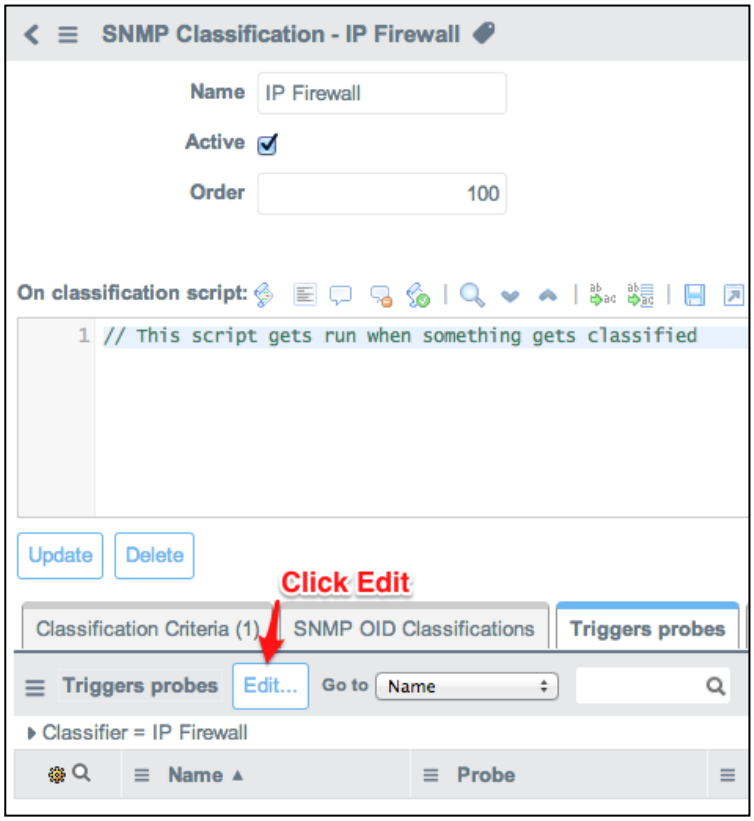
11. Fill in the **Value** field with **Firewall**.

12. Click **Submit**.




©2014 ServiceNow, Inc. All rights reserved.

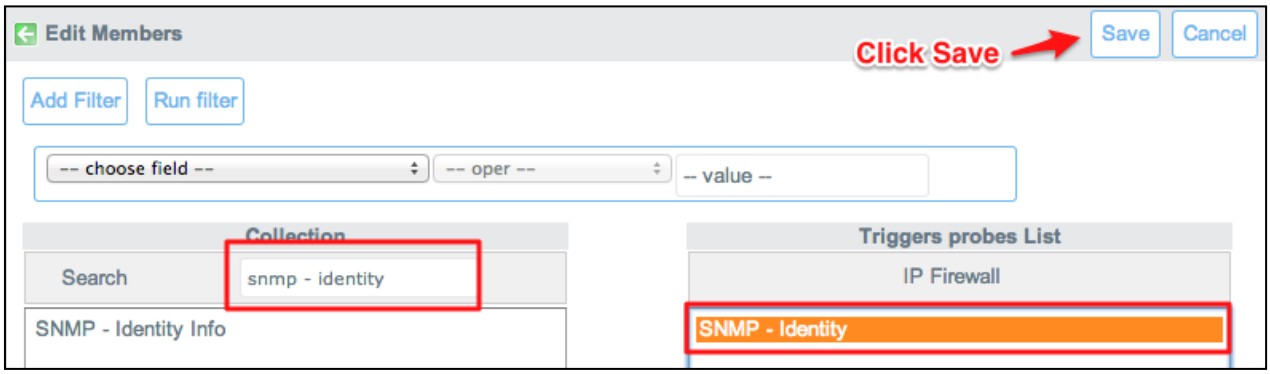
13. Click **Edit** under the **Triggers probes** tab.




14. Type **snmp – identity** in the“**search** box of the slush bucket.

15. Move the **SNMP – Identity** probe to the right side of the slush bucket.

16. Click **Save**.



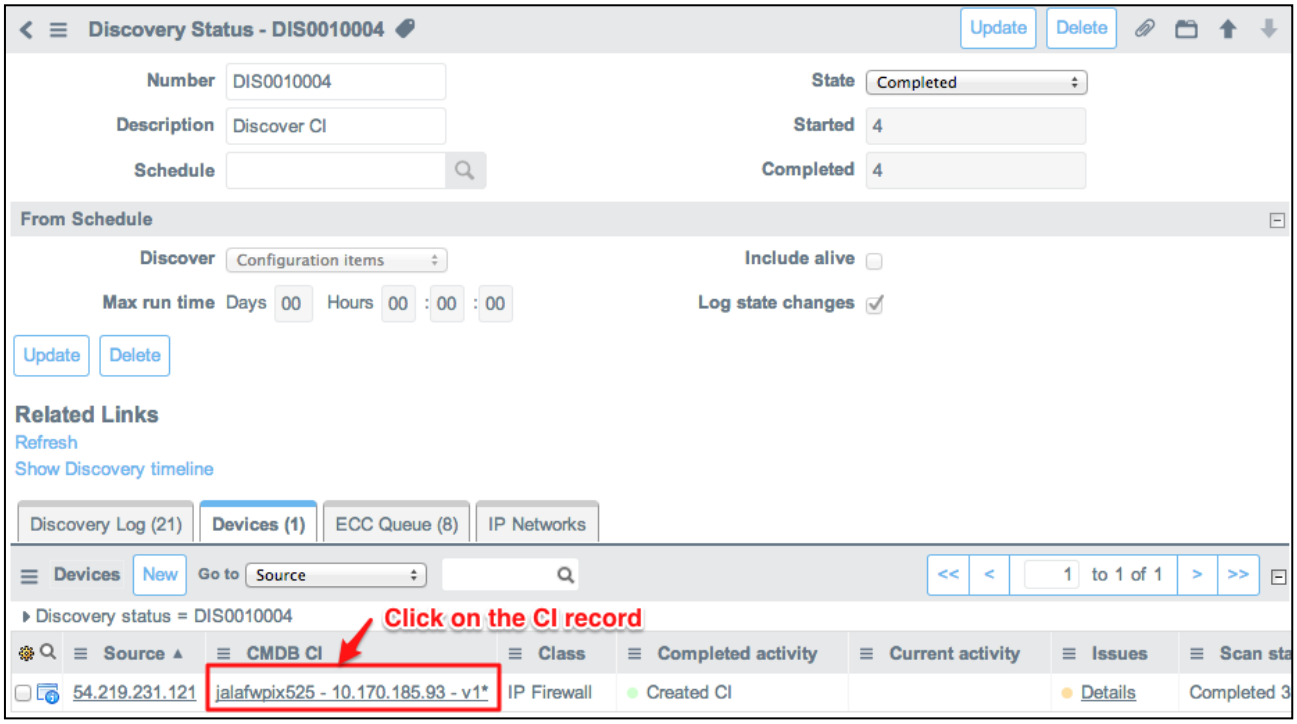

©2014 ServiceNow, Inc. All rights reserved.

## Kick off a New Discovery

Run Discovery against the host. Use Quick Discovery to kick off the Discovery against host. Refer to the section on "**Start a discovery**" for details.

## Discovery Result

We've successfully discovered the IP Firewall device. Let's drill into the **javafwpix525 – 10.170.185.93 – v1*** CI and see what we have found.




## Customize the Form Layout

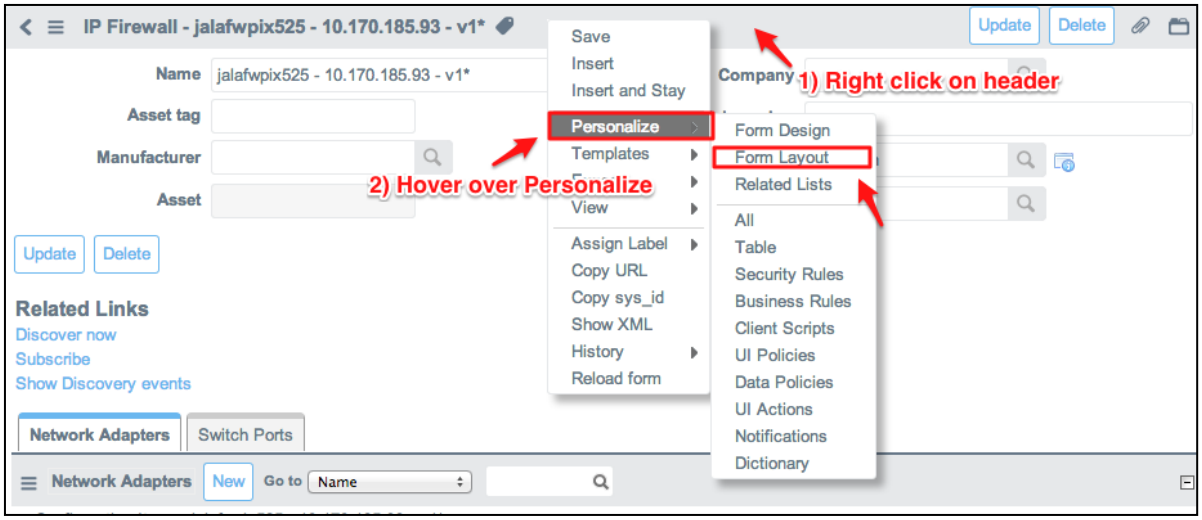
The out-of-the-box form layout isn't very exciting, so let's customize it by adding the **IP address** field and the **description** field to the form. This will also help us in the later exercises.

1. Right-click the header.

2. Hover over **Personalize**.

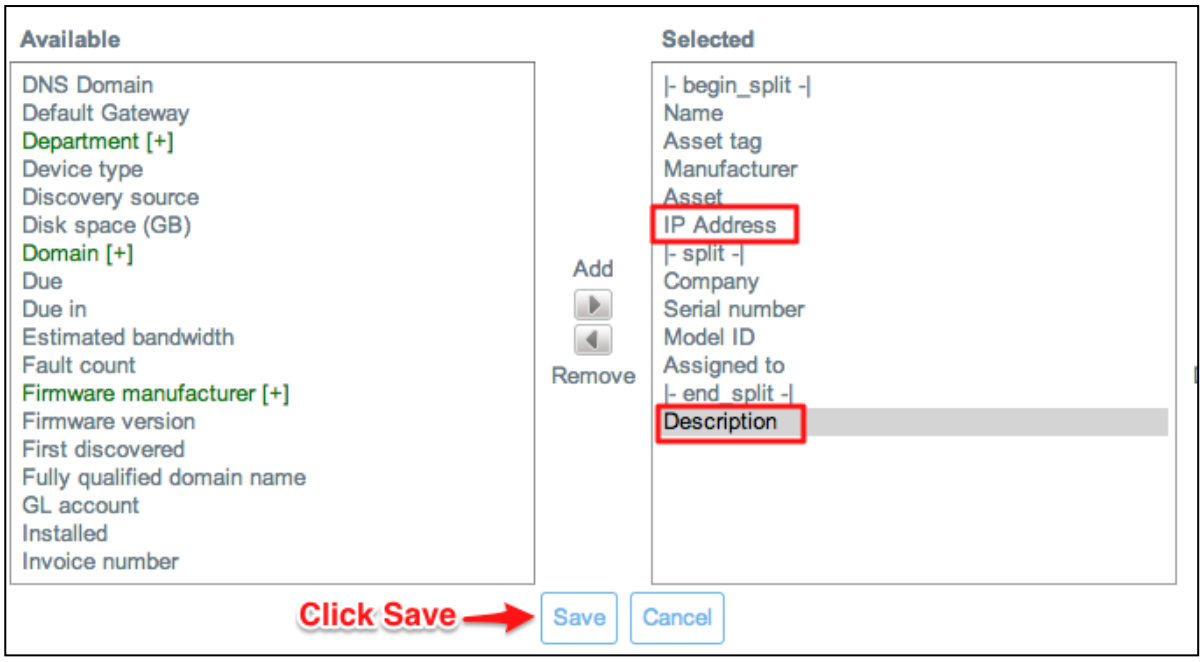
©2014 ServiceNow, Inc. All rights reserved.

3. Click **Form Layout**.



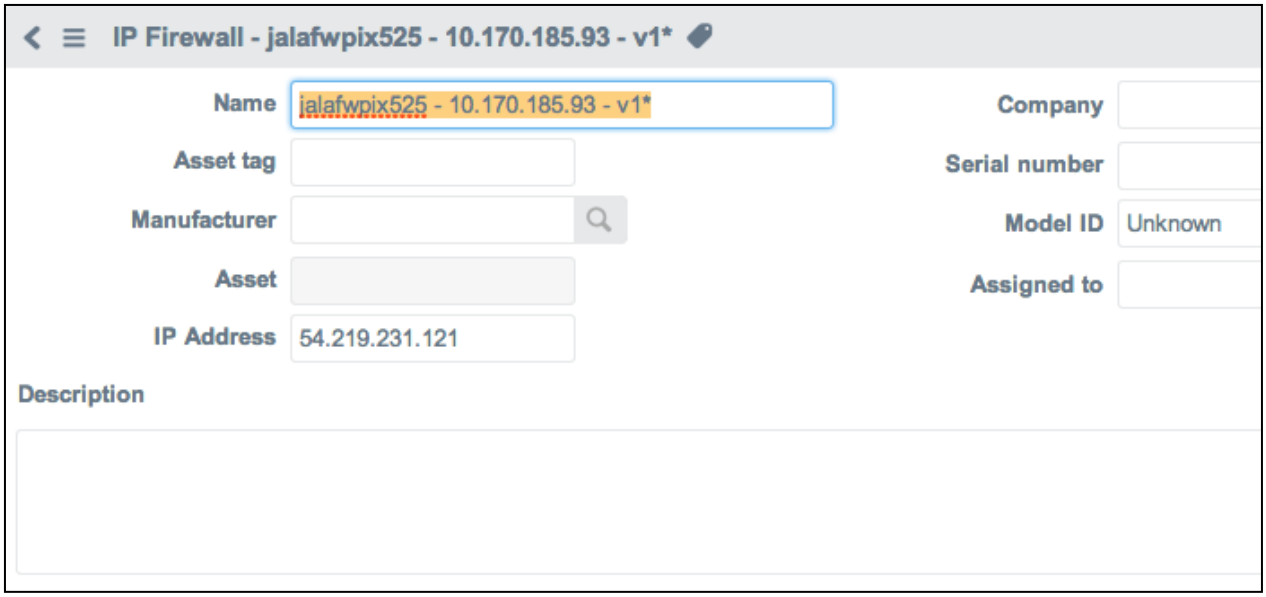

4. Move **IP address** and **Description** field to the right of the slush bucket.

5. Click **Save**.




©2014 ServiceNow, Inc. All rights reserved.

6. Now this is what the form should look like.




©2014 ServiceNow, Inc. All rights reserved.

# Lab Exercise 2 - Custom Probes and Sensors

In the following section we'll talk about how to create custom SNMP probes and sensors.

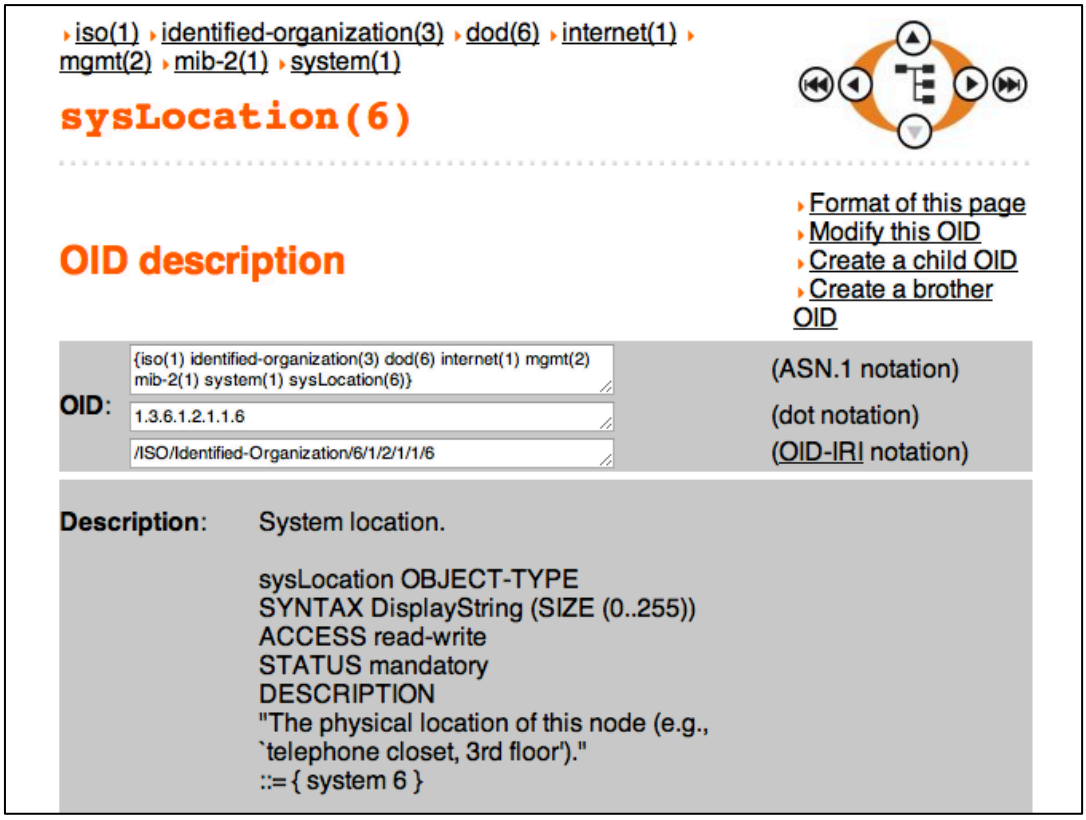
The goal is to help you figure out how you can leverage the Discovery tool to gather data that is meaningful to your organization.

Even though SNMP is the primary focus in this exercise, the general principle and techniques can be applied to writing other probes and sensors.

## Lab Exercise 2.1 – Gather Scalar OID Objects

In this exercise, we'll walk through how to build a probe to retrieve a scalar OID and a sensor to process the information and store it in the Firewall device.

The probe will use the following OID**, sysLocation. (www.oid-info.com)**



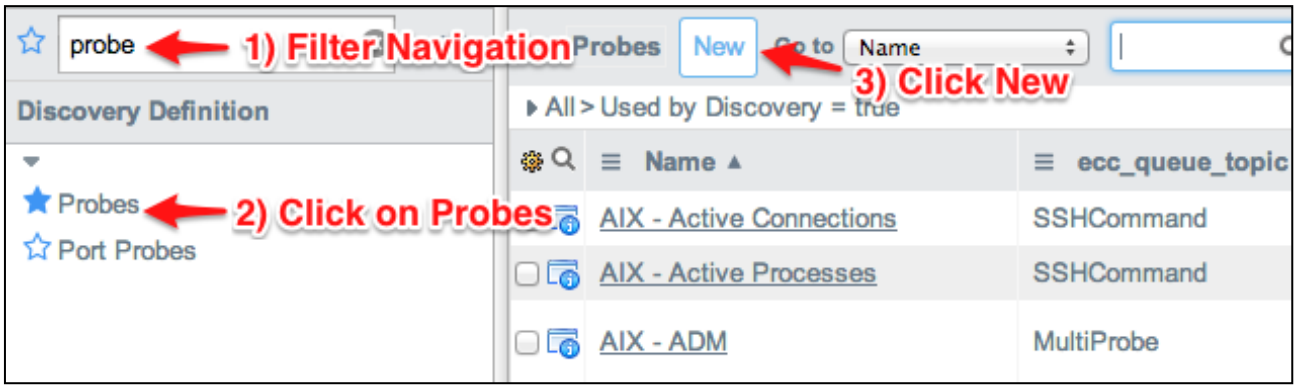

©2014 ServiceNow, Inc. All rights reserved.

## Build a Probe

1. Filter the navigation with **probe**.

2. Click the **Probes** module.

3. Click **New**.




©2014 ServiceNow, Inc. All rights reserved.

4. Fill in the **Name** field with **SNMP – Firewall**.

5. Select the **Probe Type** field with **SNMP Probe**.

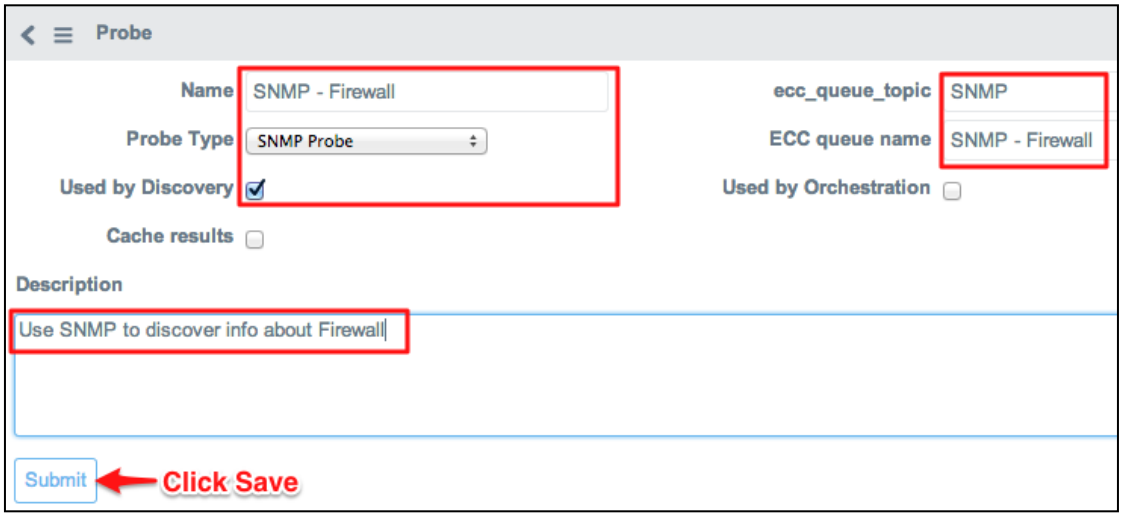
6. Fill in the **ECC queue topic** with **SNMP**.

7. Fill in the **ECC queue name** with **SNMP – Firewall**.

8. Fill in the **Description** with **Use SNMP to discover info about Firewall**.

9. Uncheck the **Use by Runbook** field.

10. Click **Submit**.




©2014 ServiceNow, Inc. All rights reserved.

11. Drill back to the probe record that was just created.

12. Click **New** under the **SNMP fields** tab.



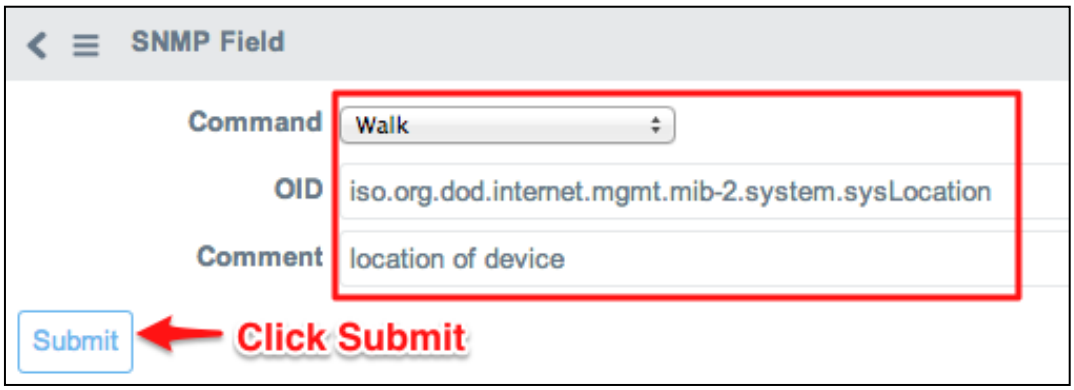

13. Select the c**ommand** field with **Walk**.

14. Fill in the **OID** field with:

```
iso.org.dod.internet.mgmt.mib-2.system.sysLocation
```

15. Fill in the **Comment** field with **location of device**.

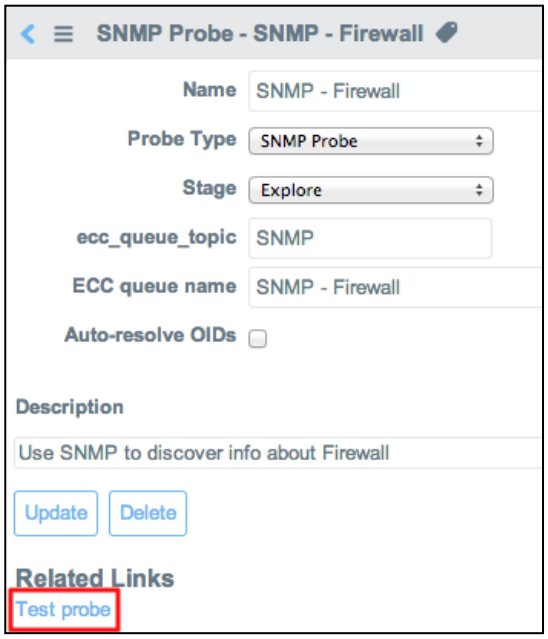
16. Click **Submit**.




©2014 ServiceNow, Inc. All rights reserved.

## Test the Probe

1. Click the UI action **Test Probe** to trigger a test probe.




2. Fill in the **Run probe against** with the target IP.

3. Fill in the **Using MID server** with **lab_midserver1**.

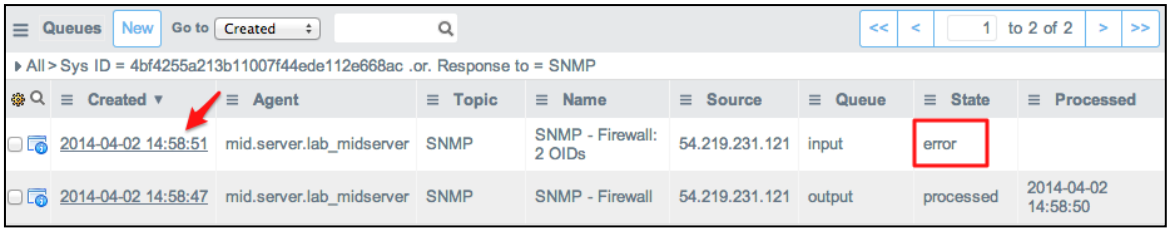
4. Click **OK** to start it.



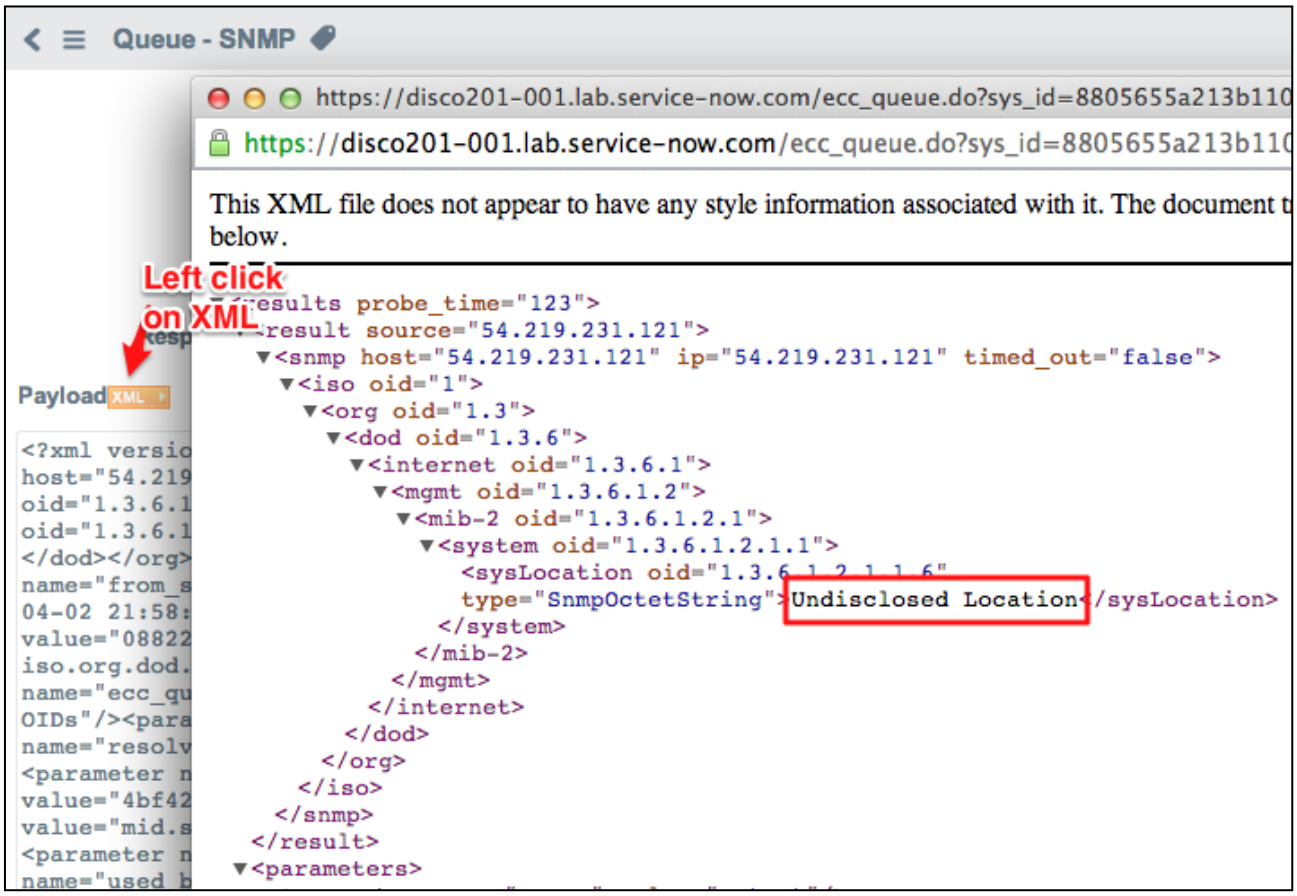

©2014 ServiceNow, Inc. All rights reserved.

After the test probe is done, it redirects the page to the ECC queue entries that represent the probe (output) and the result of the probe (input).

The state of the probe result (input) is error because there's no sensor for the probe yet.




Click the **ECC input entry** and observe that the payload of "Undisclosed Location" for the OID.



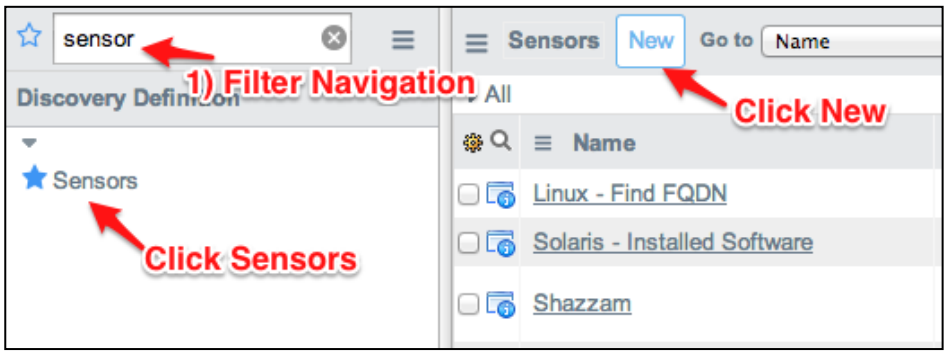

©2014 ServiceNow, Inc. All rights reserved.

## Build a Sensor

1. Filter the navigation with **sensor**.

2. Click the **Sensors** module.

3. Click **New**.




4. Fill in the **Name** field with **SNMP – Firewall**.

5. Select the **Reacts to probe** field with **SNMP – Firewall**.

6. Fill in the **Description** field with **Process Firewall** information"

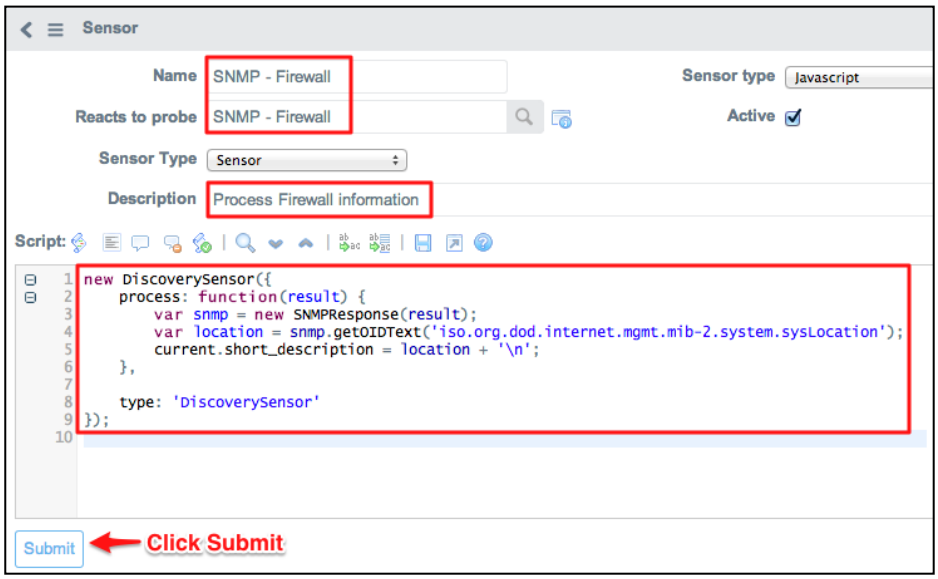
7. Fill in the "Script" field with the following piece of code.

```
new DiscoverySensor({
      process: function(result) {
            var snmp = new SNMPResponse(result);
            var location = snmp.getOIDText('iso.org.dod.internet.mgmt.mib-
2.system.sysLocation');
            current.short_description = location + '\n';
      },

      type: 'DiscoverySensor'
});
```

©2014 ServiceNow, Inc. All rights reserved.

8. Click **Submit** to save the record.

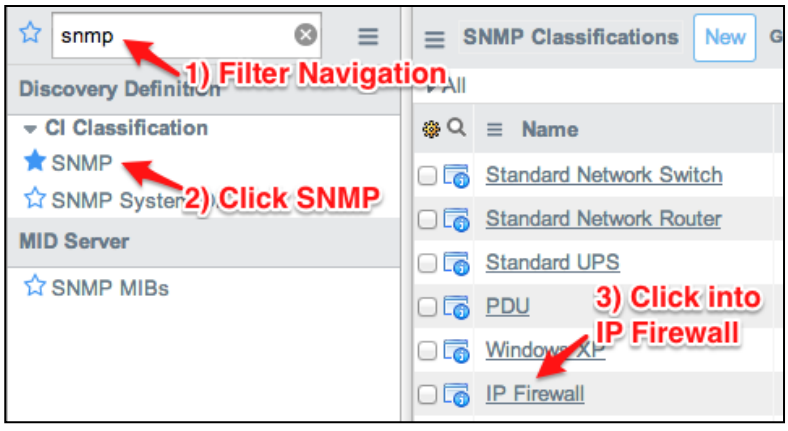



## Adding the Probe to the SNMP IP Firewall Classifier as an Exploration Probe

1. Filter the navigation with **snmp**.

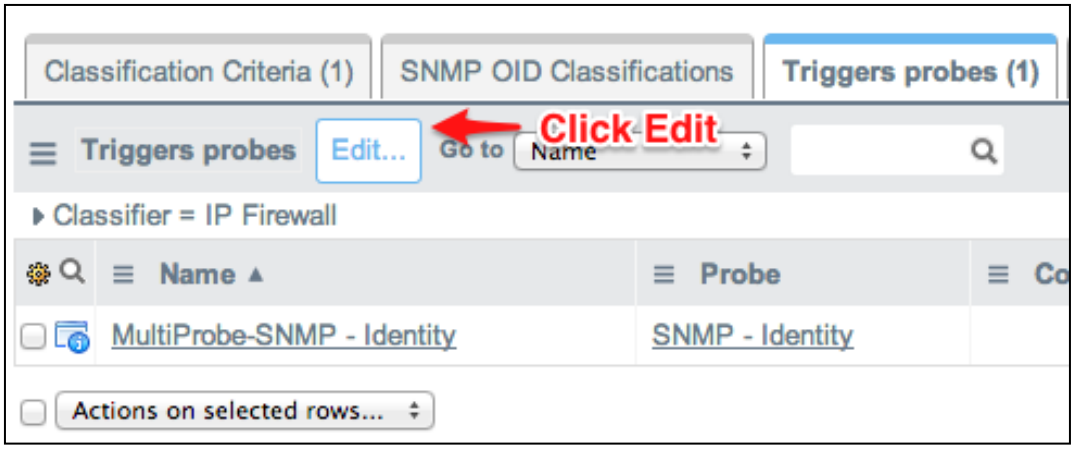
2. Click the **SNMP** module.

3. Click the **IP Firewall** record.




©2014 ServiceNow, Inc. All rights reserved.

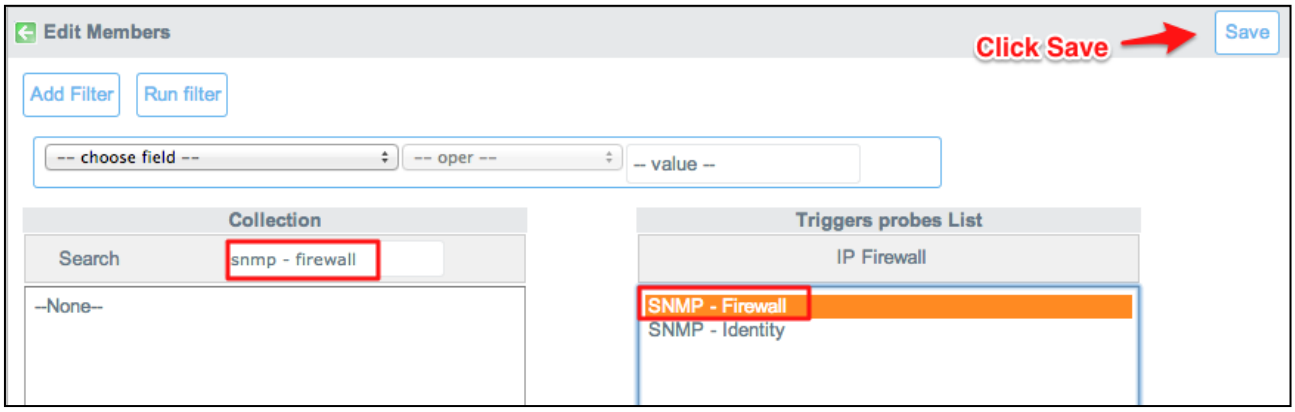
4. Click **Edit** under the **Triggers probes** tab.




5. Type **snmp – firewall** in the **Search** box of the slush box.

6. Move the **SNMP – Firewal**" record to the right side of the slush bucket.

7. Click **Save**.



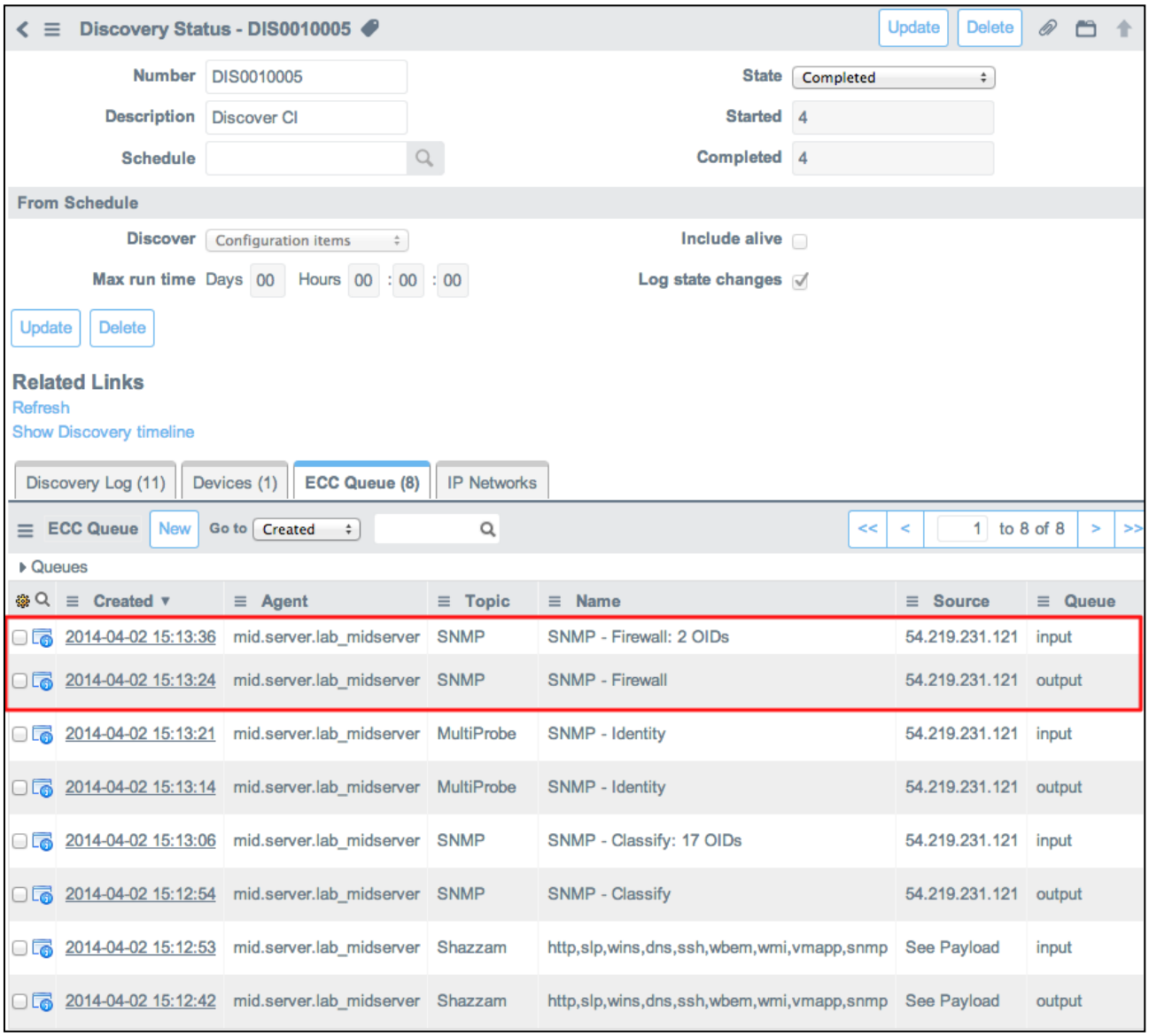

©2014 ServiceNow, Inc. All rights reserved.

## Kick off a New Discovery

Run Discovery against the host. Use Quick Discovery to kick off the Discovery against host. Refer to the section on **Start a discovery** for details.

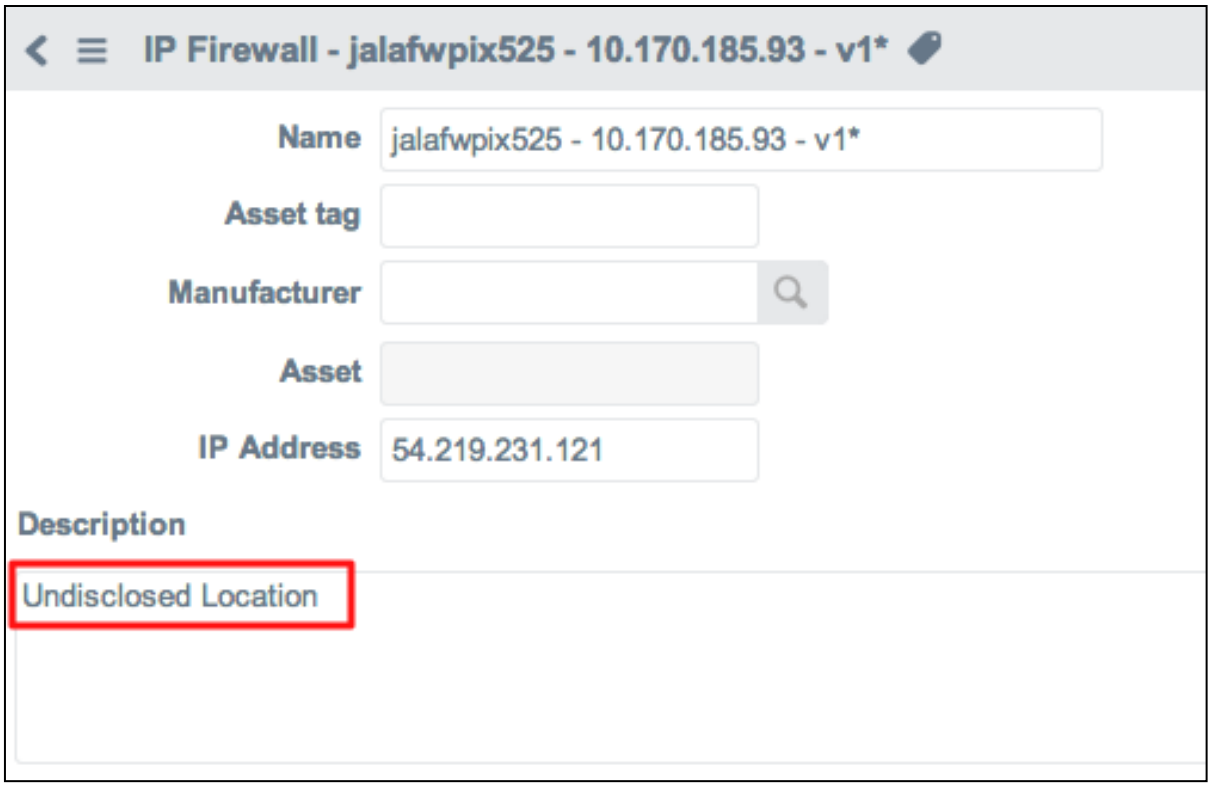
## Result

Observe that the Discovery run has launched the new probe.




©2014 ServiceNow, Inc. All rights reserved.

Go to the “Devices” related list and drill into the CI and observe that the value of the OID has indeed been added to the “Description” field.




## Lab Challenge - Add Additional Info from Other OIDs

Add **iso.org.dod.internet.mgmt.mib-2.system.sysContact** to the **asset_tag** field.

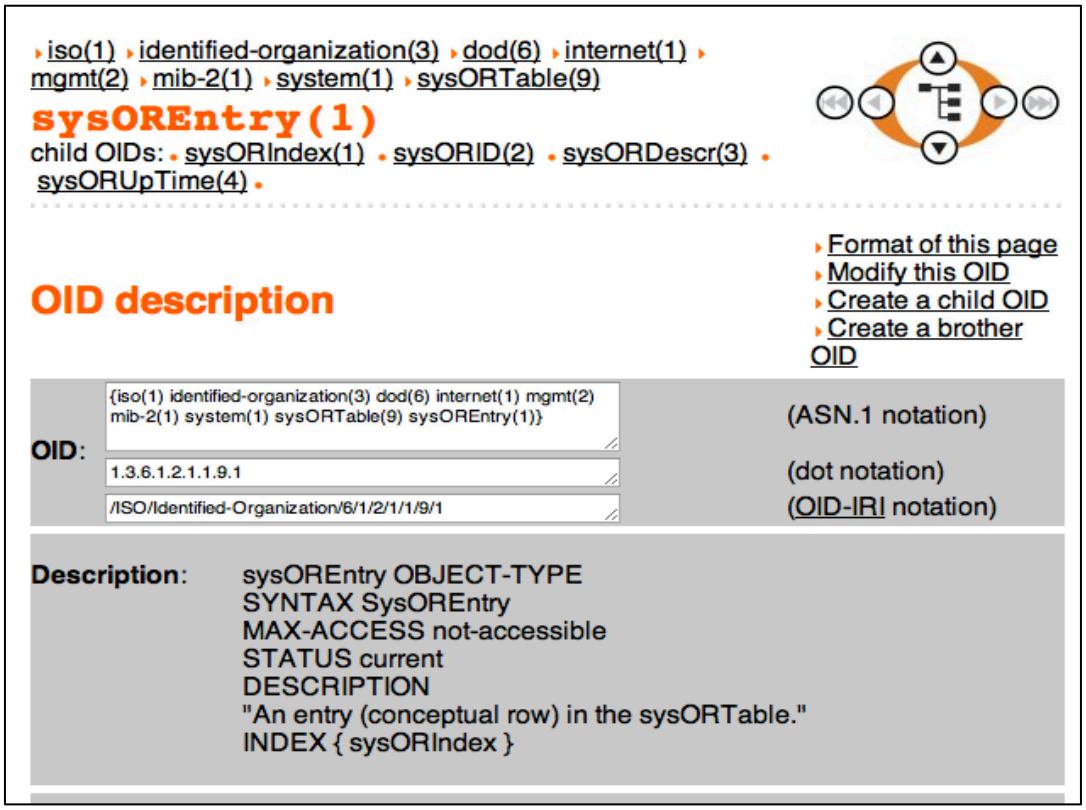
- Add the new OID to the probe we had created
- Modify the existing sensor to process the information
- Rerun discovery and see the result!

©2014 ServiceNow, Inc. All rights reserved.

## Lab Exercise 2.2 – Gather Tabular OID Objects

So far we have done the exercise around building a probe and a sensor for retrieving/processing scalar OID objects. Let's now continue to expand the probe and sensor for tabular OID objects. Here's the OID that we'll explore.

**Description of the sysOREntry table (www.oid-info.com)**

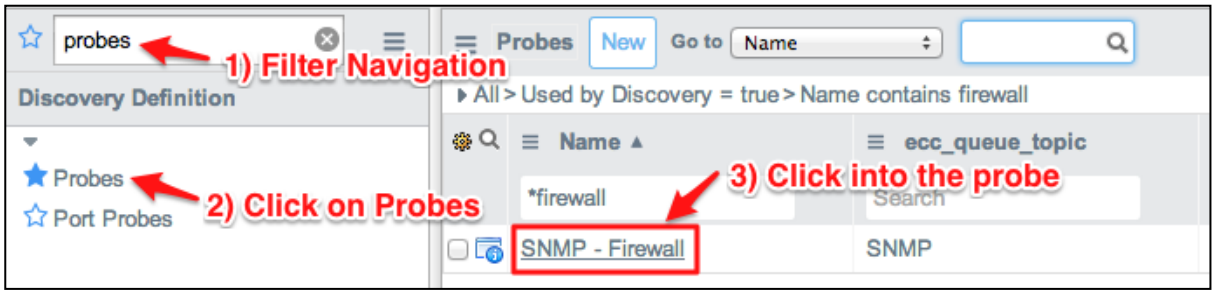



©2014 ServiceNow, Inc. All rights reserved.

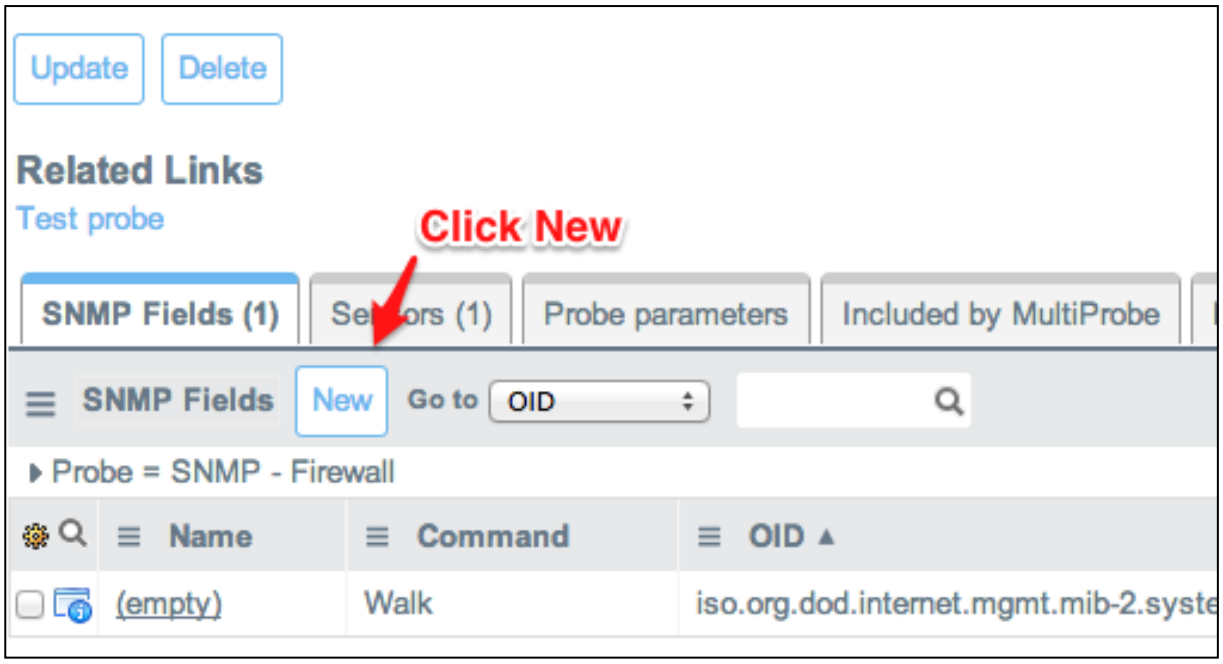
1. Filter the navigation with **probes**.

2. Click the **Probes** module.

3. Drill into the **SNMP – Firewall** probe record.




4. Click **New** under the **SNMP Fields** tab.




5. Select the **Command** field with **Table**.

©2014 ServiceNow, Inc. All rights reserved.

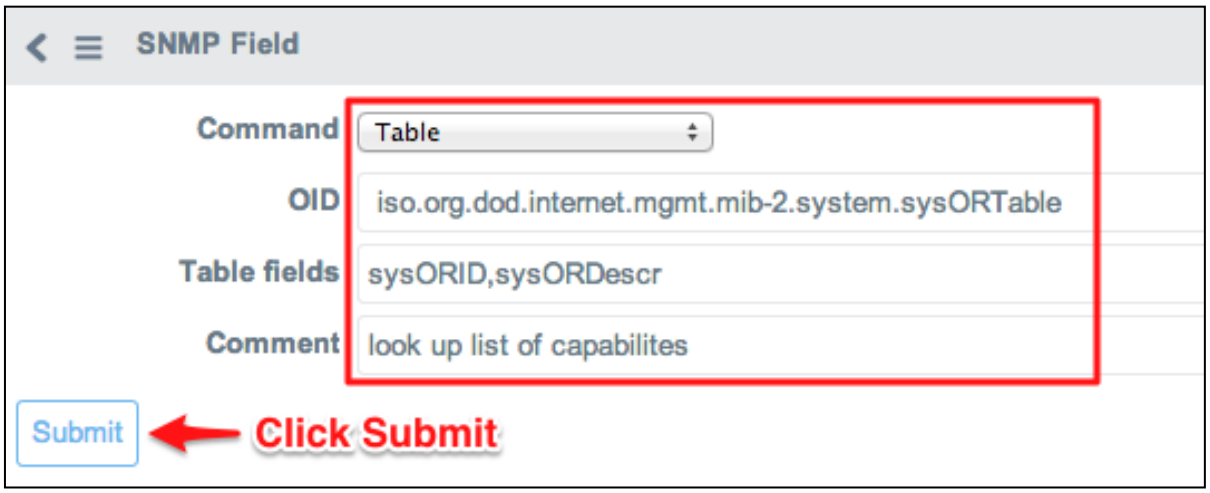
6. Fill in the **OID** field with the following OID:

```
iso.org.dod.internet.mgmt.mib-2.system.sysORTable
```

7. Fill in the **Table fields** field with **sysORID,sysORDescr**.

8. Fill in the **Comment** field with **look up list of capabilities**.

9. Click **Submit**.




©2014 ServiceNow, Inc. All rights reserved.

## Test the Probe Again

1. Click the UI action **Test Probe** to trigger a test probe.




2. Fill in the **Run probe against** with the target IP.

3. Fill in the **Using MID server** with **lab_midserver1**.

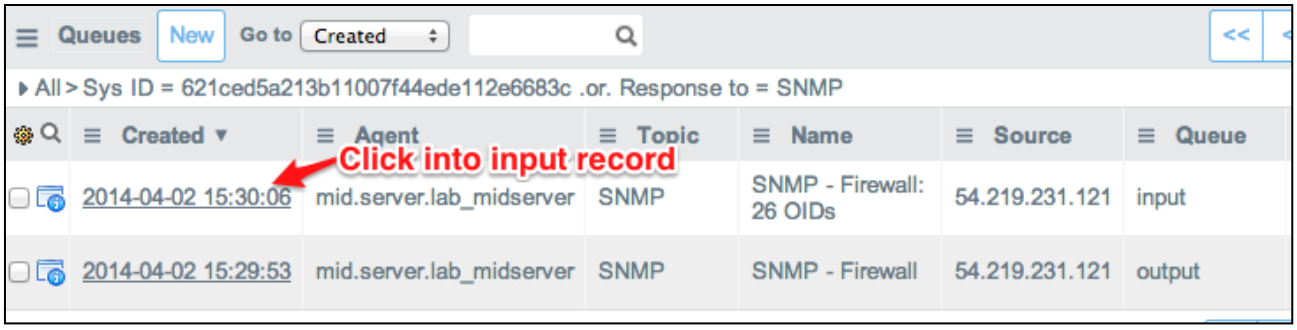
4. Click **OK**.




©2014 ServiceNow, Inc. All rights reserved.

5. You should be redirected to the ECC queue records of the probe results.

6. Click **the input ECC queue** record.




7. Click the **XML icon** to format the XML info.

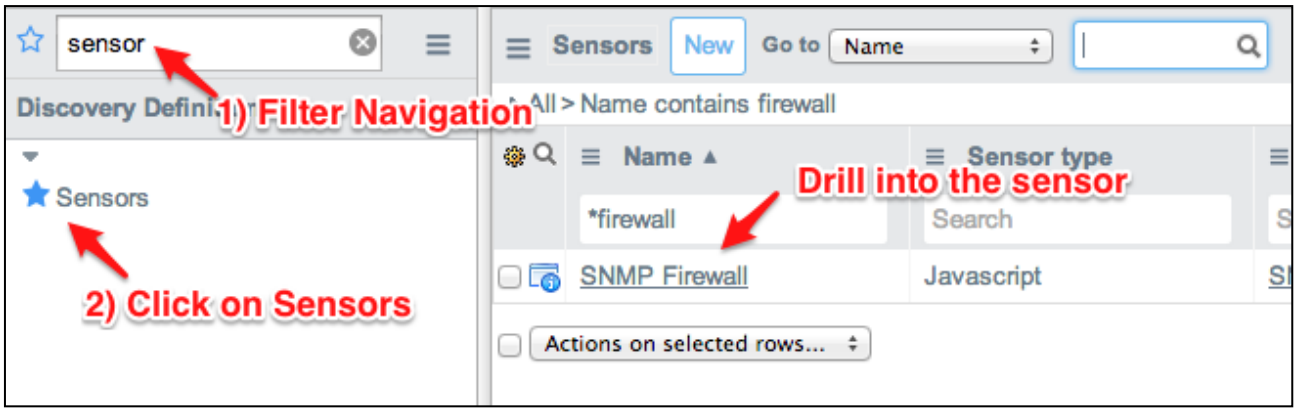
8. Observe that we have gotten back the results from the new OID.




©2014 ServiceNow, Inc. All rights reserved.

## Modify the Sensor

1. Filter the navigation with **sensor**.
2. Click the **Sensors** module.
3. Click the **SNMP – Firewall** sensor record.




4. In the **script** field, the following is what the code should look like in the end. The section in red is what is added to the original script.

```
new DiscoverySensor({
  process: function(result) {
        var snmp = new SNMPResponse(result);
        var location = snmp.getOIDText('iso.org.dod.internet.mgmt.mib-
2.system.sysLocation');
        current.short_description = location + '\n';

        var sysORObjs = snmp.getOIDTable('iso.org.dod.internet.mgmt.mib-
2.system', 'sysOREntry');
        var description = "";
        for (var i in sysORObjs) {
              var entry = sysORObjs[i];
              var id = entry['sysORID'];
              var desc = entry['sysORDescr'];

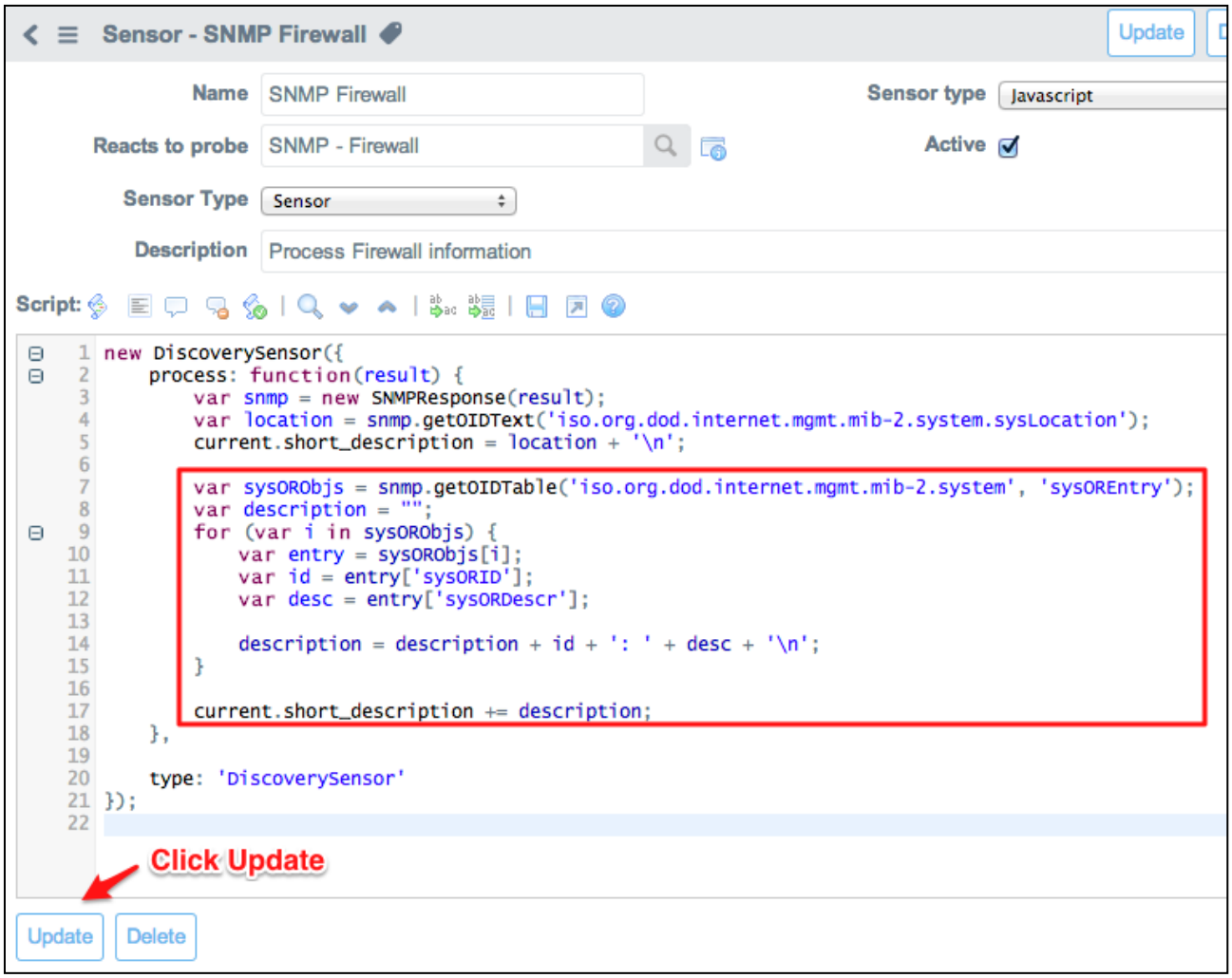
              description = description + id + ': ' + desc + '\n';
        }

        current.short_description += description;
  },

  type: 'DiscoverySensor'
});
```

©2014 ServiceNow, Inc. All rights reserved.

5. Click **Update** to save the record.



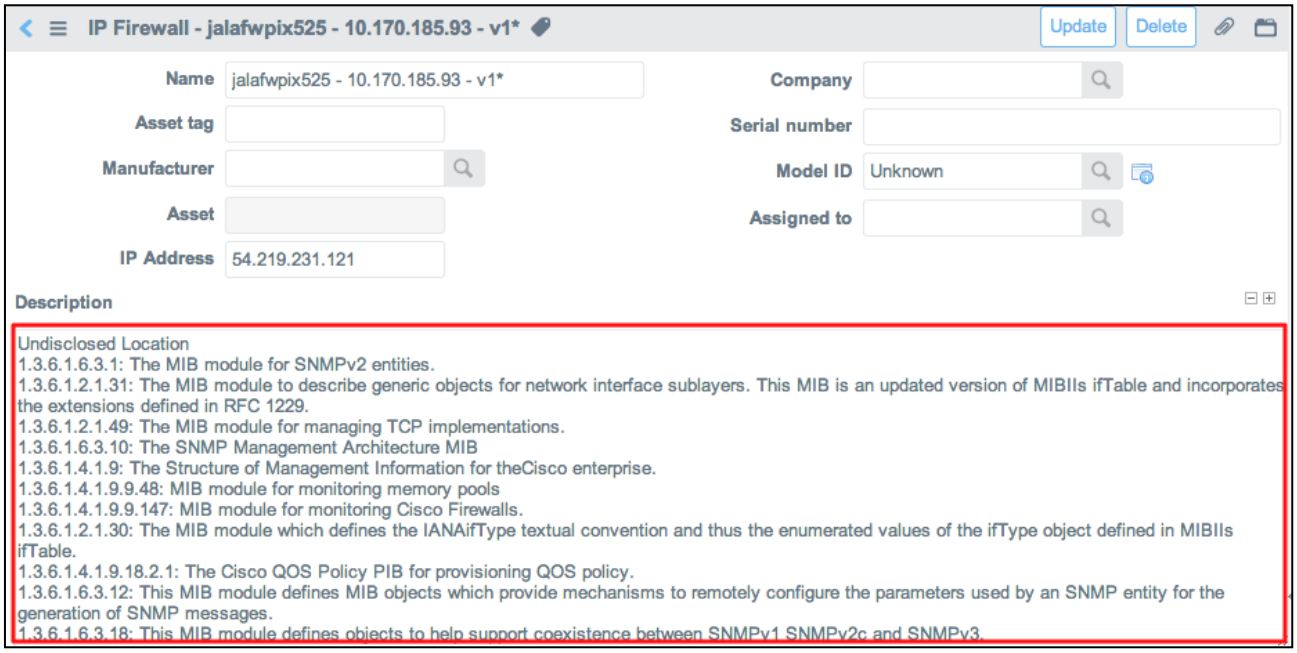

©2014 ServiceNow, Inc. All rights reserved.

## Kick off a New Discovery

Run Discovery against the host. Use Quick Discovery to kick off the Discovery against host. Refer to the section on **Start a discovery** for details.

## Result

Go to the “Devices” related list and drill into the CI and observe that the value of the OIDs (**sysORID** and **sysORDDescr**) have been added to the **Description** field.




©2014 ServiceNow, Inc. All rights reserved.

## Classify a SNMP Device

The trick to classify a particular SNMP device is to use something that is generic to the type of device.

What are possibilities?

- sysdescr
- Object ID
- An OID that that is mandatory from the RFC MIB.

## Lab Exercise 3 – Classify Using System OID

In our example, the system OID to use is **1.3.6.1.4.1.9.1.392**. We could use this ID to classify against the Firewall device.

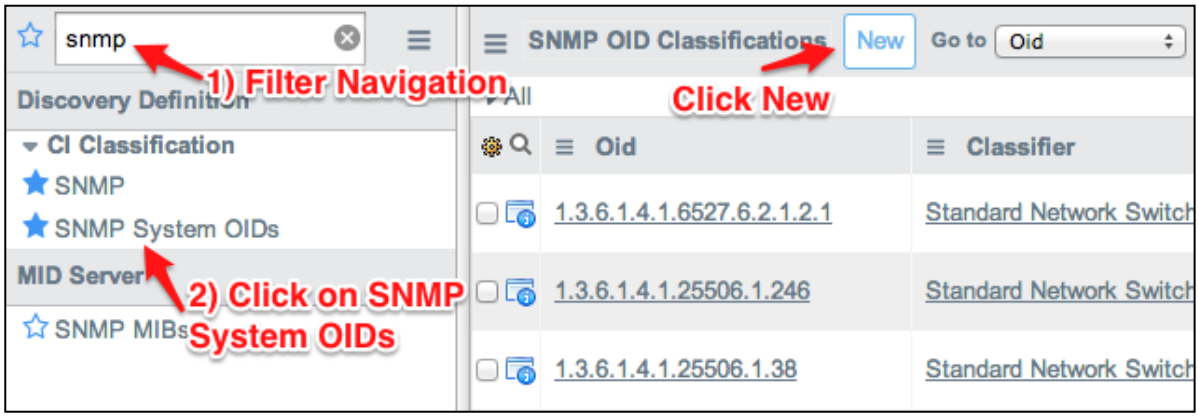



©2014 ServiceNow, Inc. All rights reserved.

1. Filter navigation with **snmp**.

2. Click the **SNMP System OIDs** module.

3. Click **New**.

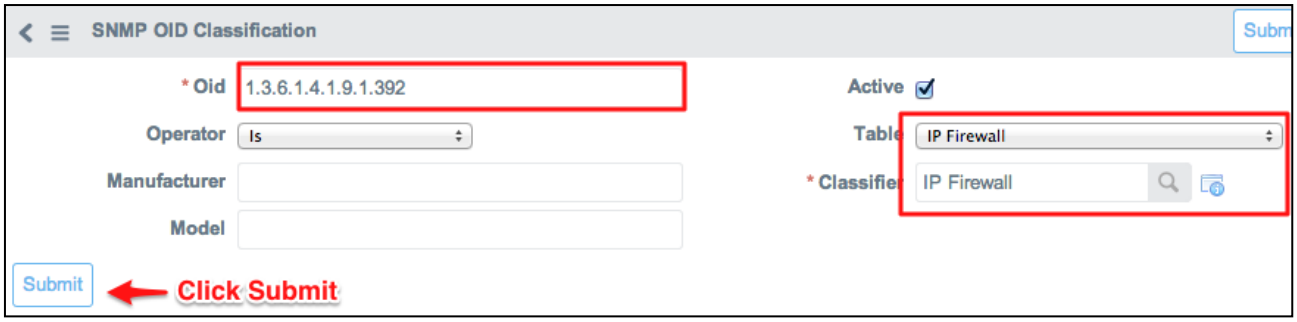



4. Fill in the **Oid** field with **1.3.6.1.4.1.9.1.392** .

5. Select the **Table** field with **IP Firewall [u_cmdb_ci_ip_firewall]**.

6. Select the **Classifier** with **IP Firewall**.

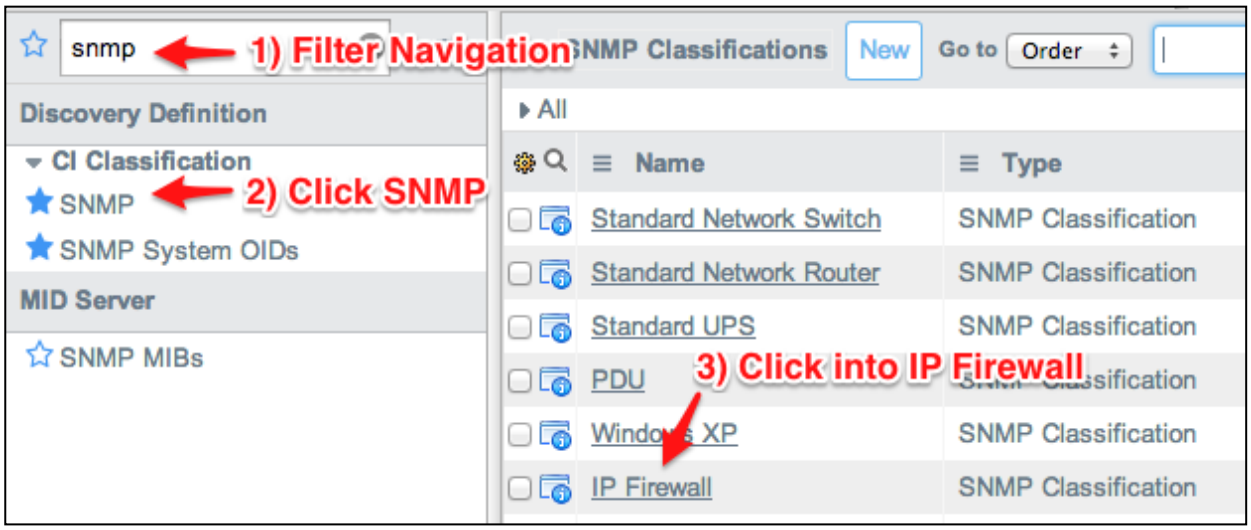
7. Click **Submit**.




©2014 ServiceNow, Inc. All rights reserved.

8. To prove to ourselves that the system OID classifier does indeed work, let's drill back into the IP Firewall record and delete the **Classification Criteria** that we've entered earlier.

   (1) Type snmp in the the text filter box
   (2) Click SNMP
   (3) Click IP Firewall record

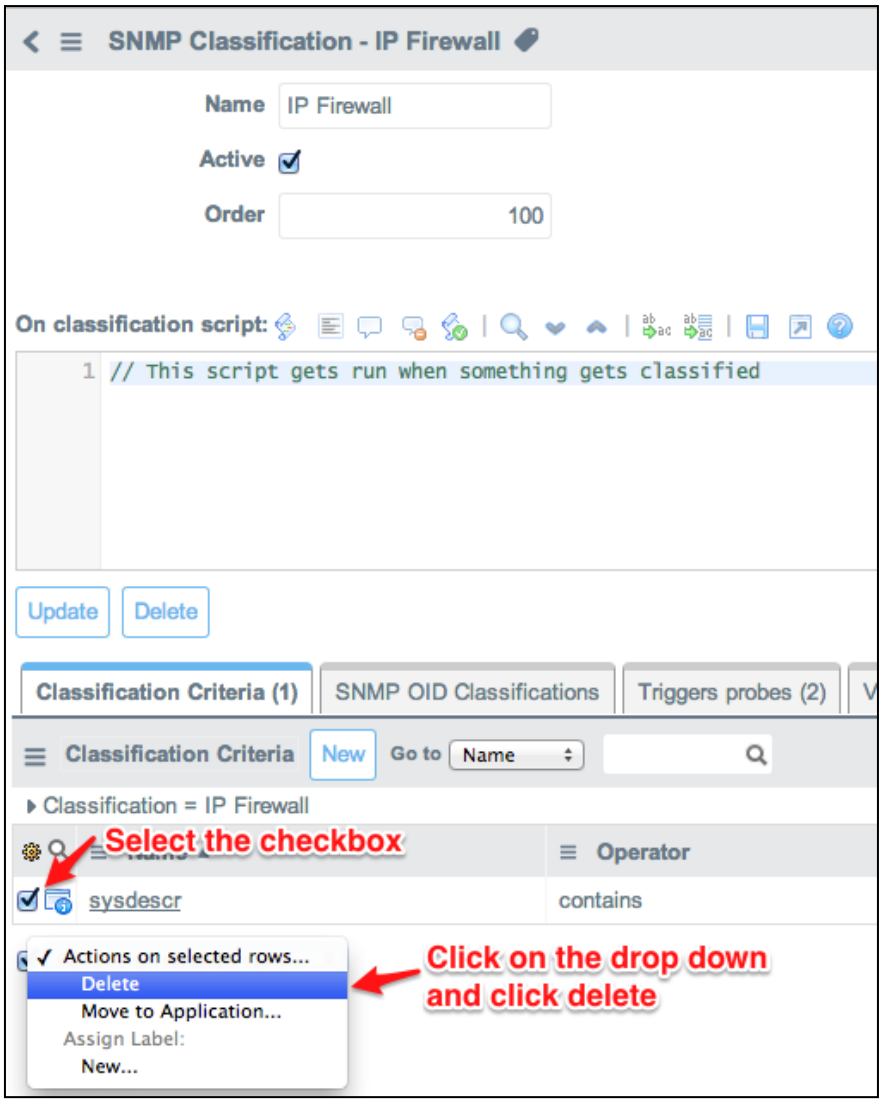



©2014 ServiceNow, Inc. All rights reserved.

9. Select the check box on the classification criteria that was created earlier.

10. Click the drop-down list and Click delete.

11. Click **OK** when the confirmation box pops up.



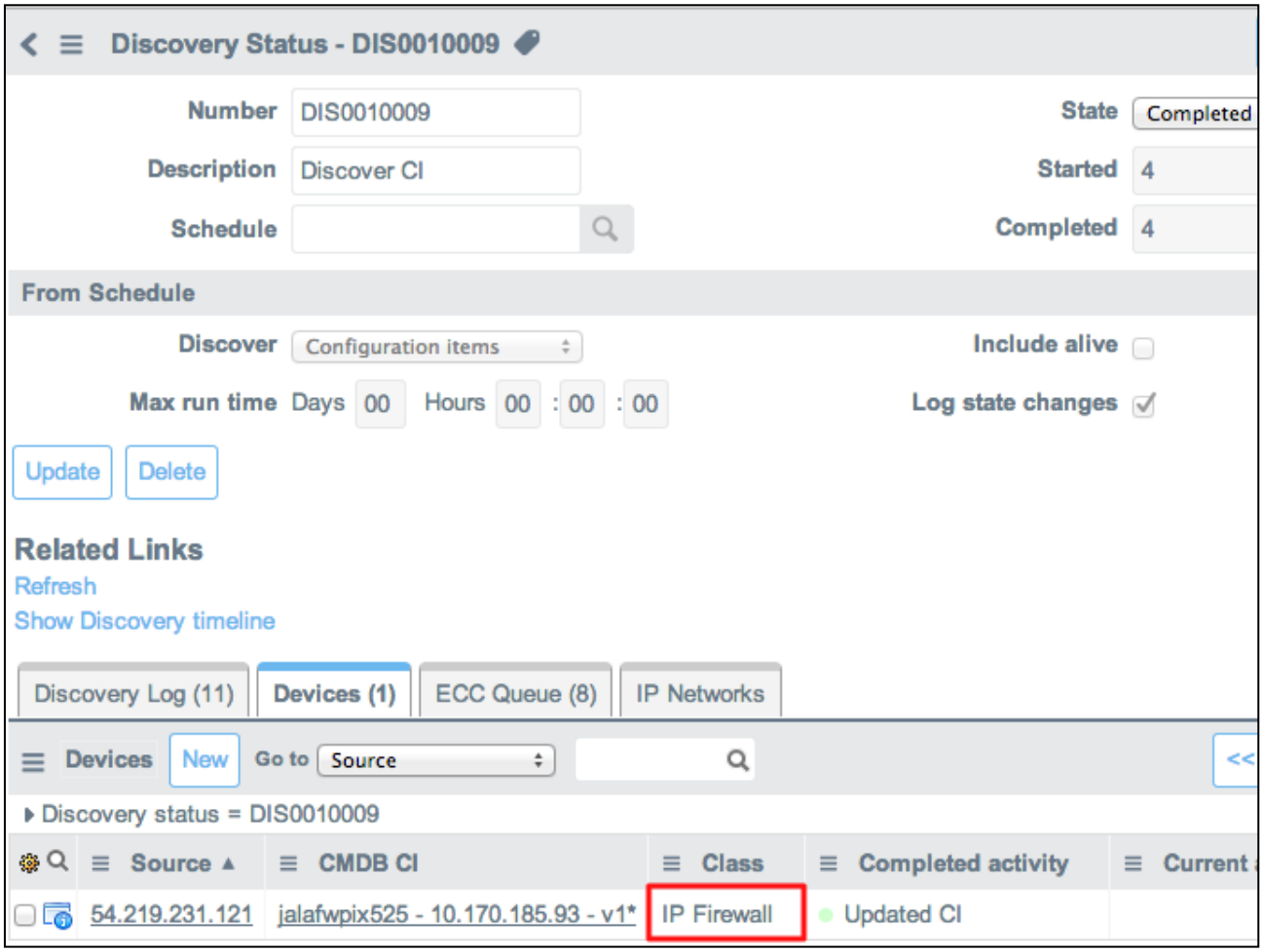

©2014 ServiceNow, Inc. All rights reserved.

## Kick off a New Discovery

Run Discovery against the host. Use Quick Discovery to kick off the Discovery against host. Refer to the section on **Start a discovery** for details.

## Result

Observe that the Discovery has again successfully classified the device as an IP Firewall device using the **system OID**.




©2014 ServiceNow, Inc. All rights reserved.

## Discovery Identifiers (CI Identifiers)

CI Identifiers are a set of rules that allows Discovery to determine if a discovered device is already in the CMDB based on discovered information such as “serial numbers”, “hostname” and “mac address”.

Its goal is to correctly determine the identity of a device and prevent the creation of duplicate CIs.

In this lab, we will talk about

- How to configure them
- What is the right for you
- How to customize the identifiers
- http://wiki.servicenow.com/index.php?title=Discovery_Identifiers

## How Does It Work? What Are the Rules?

- Discovery runs through each identifier to find a match based on its matching algorithm.
- The identifier chain will stop as soon as an identifier finds one and only one match.
- The identifier chain will not stop if there’s no match or multiple matches.
- If all identifiers fail to match and there are no multiple matches, a new CI will be created provided there’s matchable info.
- If all identifiers fail to match and there are multiple matches. Discovery logs duplicate CIs.

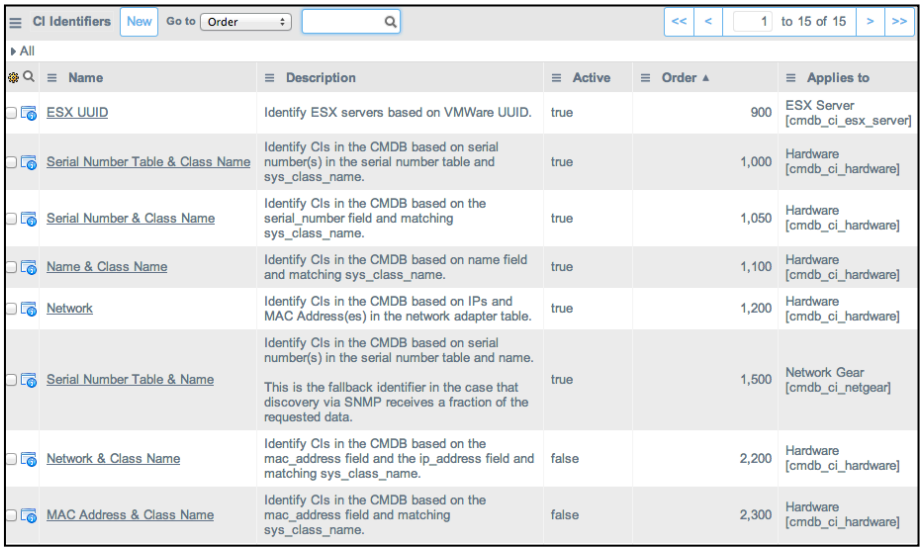
## Order Matters!

- Serial number(s)
- Name
- Network adapter(s) -- IP and MAC address

©2014 ServiceNow, Inc. All rights reserved.

## Understanding OOB Identifiers

Each identifier has its own algorithm in identifying a device in the CMDB. It is important to understand what works for your environment as the unique identifier for your devices. Out of the box, we have three major identifiers. They are **serial number**, **name** and **network**.



CI Identifiers | New | Go to Order | << < 1 to 15 of 15 > >>

All

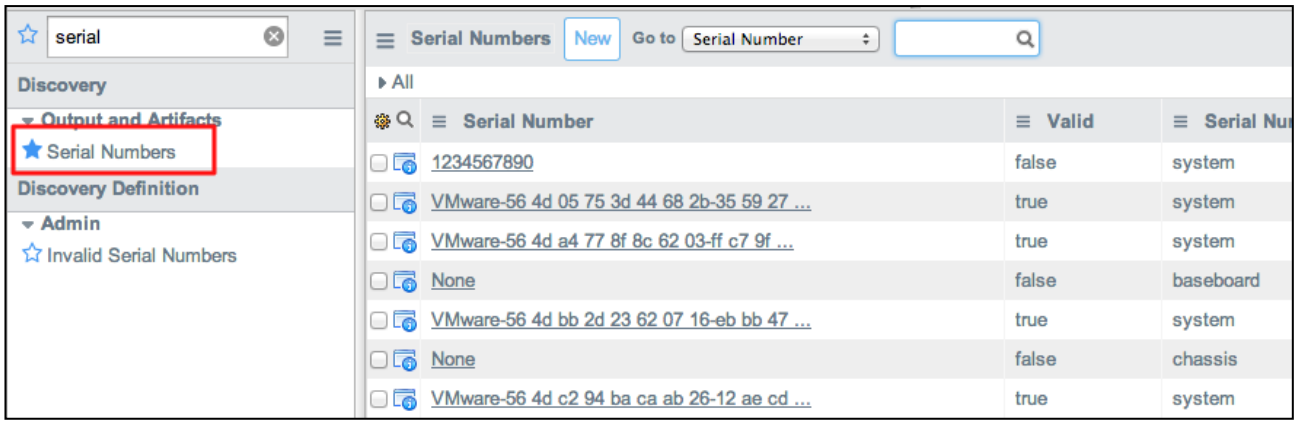
| Name | Description | Active | Order ▲ | Applies to |
|---|---|---|---|---|
| ESX UUID | Identify ESX servers based on VMWare UUID. | true | 900 | ESX Server [cmdb_ci_esx_server] |
| Serial Number Table & Class Name | Identify CIs in the CMDB based on serial number(s) in the serial number table and sys_class_name. | true | 1,000 | Hardware [cmdb_ci_hardware] |
| Serial Number & Class Name | Identify CIs in the CMDB based on the serial_number field and matching sys_class_name. | true | 1,050 | Hardware [cmdb_ci_hardware] |
| Name & Class Name | Identify CIs in the CMDB based on name field and matching sys_class_name. | true | 1,100 | Hardware [cmdb_ci_hardware] |
| Network | Identify CIs in the CMDB based on IPs and MAC Address(es) in the network adapter table. | true | 1,200 | Hardware [cmdb_ci_hardware] |
| Serial Number Table & Name | Identify CIs in the CMDB based on serial number(s) in the serial number table and name.<br>This is the fallback identifier in the case that discovery via SNMP receives a fraction of the requested data. | true | 1,500 | Network Gear [cmdb_ci_netgear] |
| Network & Class Name | Identify CIs in the CMDB based on the mac_address field and the ip_address field and matching sys_class_name. | false | 2,200 | Hardware [cmdb_ci_hardware] |
| MAC Address & Class Name | Identify CIs in the CMDB based on the mac_address field and matching sys_class_name. | false | 2,300 | Hardware [cmdb_ci_hardware] |

Here's an important distinction between the **serial number table** identifier and the **serial number field** identifier.

®2014 ServiceNow, Inc. All rights reserved.

## Serial Number Table Identifier

It identifies by matching the serial numbers in the serial number table (**cmdb_serial_number**) that belong to a CI. See the serial number table below.




## Serial Number Field Identifier

It identifies by matching the serial number field of the CI. See the example below.




©2014 ServiceNow, Inc. All rights reserved.

## The applies_to Class Type Matters!

The “applies_to” field on the identifiers can matter a lot when it comes to the group of CIs in the CMDB the identifier goes after. “cmdb_ci_hardware” is the default, which includes child table such as

- cmdb_ci_computer
- cmdb_ci_printer
- cmdb_ci_netg
- cmdb_ci_ups

For more, see **Tables** modules under **System Definition** menu

©2014 ServiceNow, Inc. All rights reserved.

# Lab Exercise 4 – Custom identifiers

## Scenario

My Solaris global zone and its non-global zones return the same serial number.

## Solution

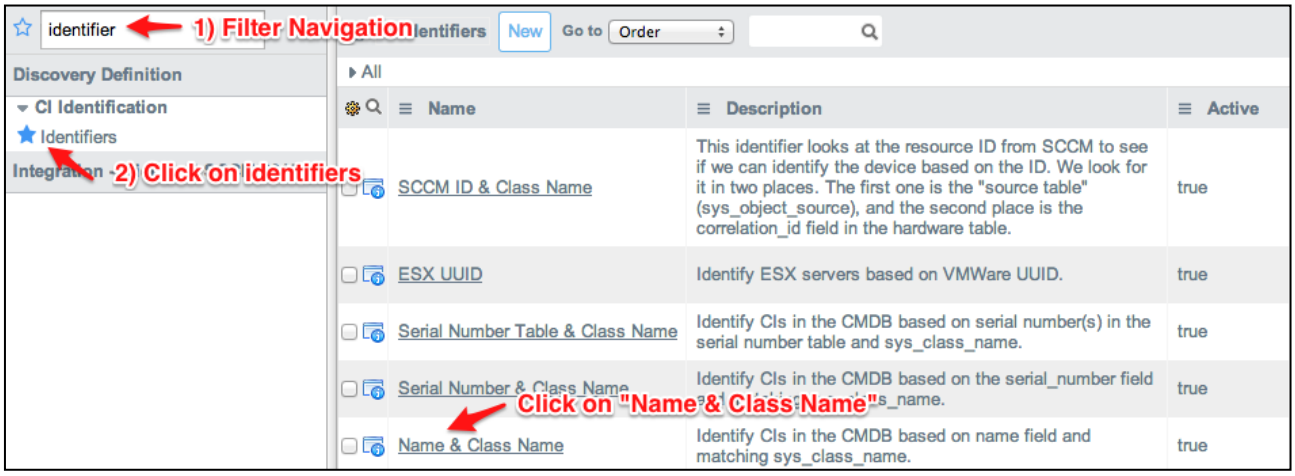
Have a separate identifier just for Solaris servers using the name value

## Here we go

1. Filter the navigation with **identifier**.

2. Click the **Identifiers** module.

3. Click the **Name & Class Name** identifier record.




©2014 ServiceNow, Inc. All rights reserved.

4. Change the **Name** field to **Name for Solaris**.

5. Change the **Order** field to **100**.

6. Change the **Applies to** field to **Solaris Server [cmdb_ci_solaris_server]**.

7. Modify the 4th line of the **Script field** from:

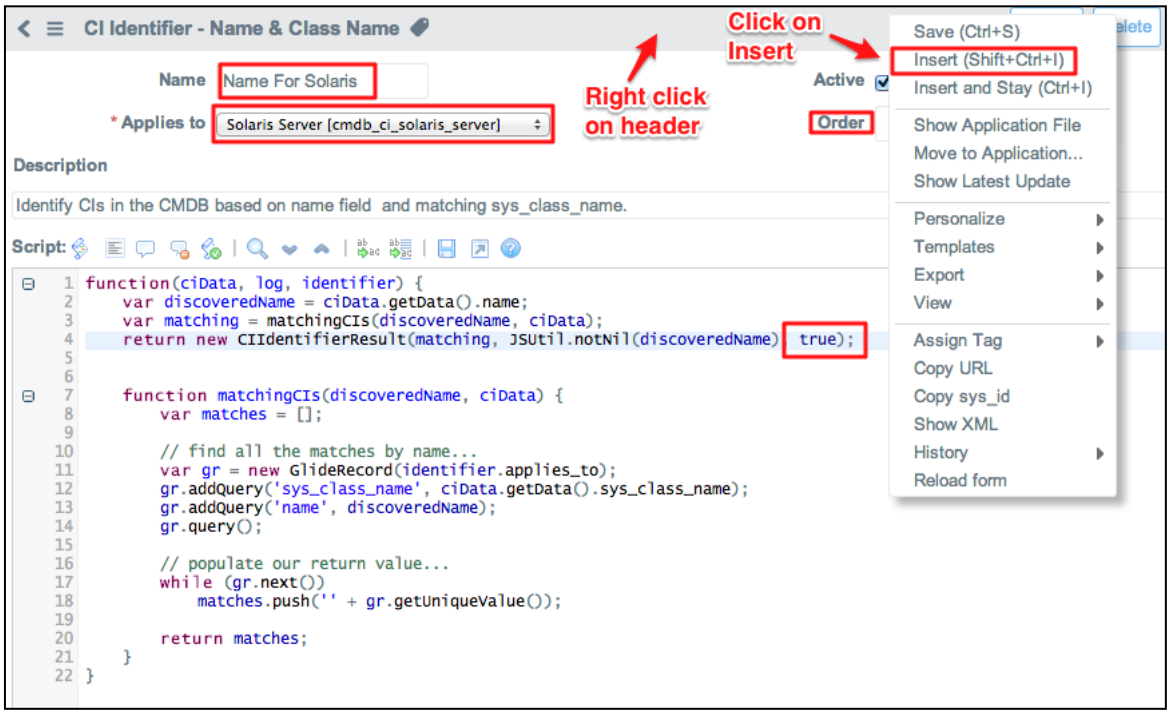
```
return new CIIdentifierResult(matching, JSUtil.notNil(discoveredName));
```

to

```
return new CIIdentifierResult(matching, JSUtil.notNil(discoveredName), true);
```

8. Right-click the gray header.

9. Click **Insert**.




©2014 ServiceNow, Inc. All rights reserved.

## Why Adding the 3rd Argument for CIIdentifierResult Class

The third argument will dictate whether the other identifiers continue to run after the current identifier (based on order)

See the **CIIdentifierResul**t script include for detail

## Lab Challenge – Create Your Own Identifier for the IP Firewall Devices

- Make an identifier using the name field for the IP Firewalls and make sure it will stop going through the other identifiers if the identifier fails to find a match.
- Run a Discovery and verify in the discovery logs that it indeed stops after the identifier.
- Tip: Change the existing Firewall CI name to ensure the identifier will fail.

## Additional Resources

Look up OID info
www.oid-info.com

Creating table in ServiceNow
http://wiki.servicenow.com/index.php?title=Creating_a_Custom_Table

Probes and Sensors
http://wiki.servicenow.com/index.php?title=Discovery_Probes_and_Sensors

CI Identifiers
http://wiki.servicenow.com/index.php?title=Discovery_Identifiers

©2014 ServiceNow, Inc. All rights reserved.