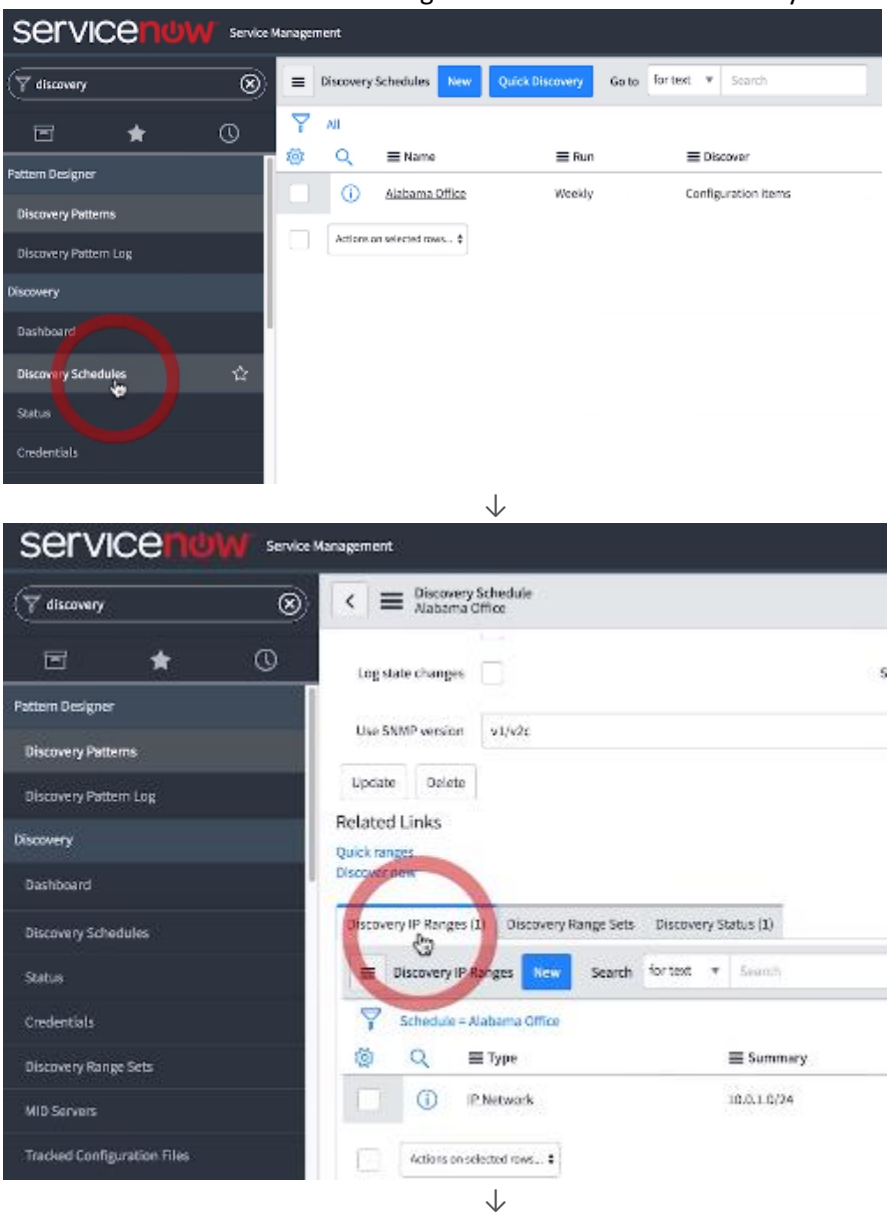
Step One: Determine the desired **IP Ranges** and **IP Addresses** to include on your network:

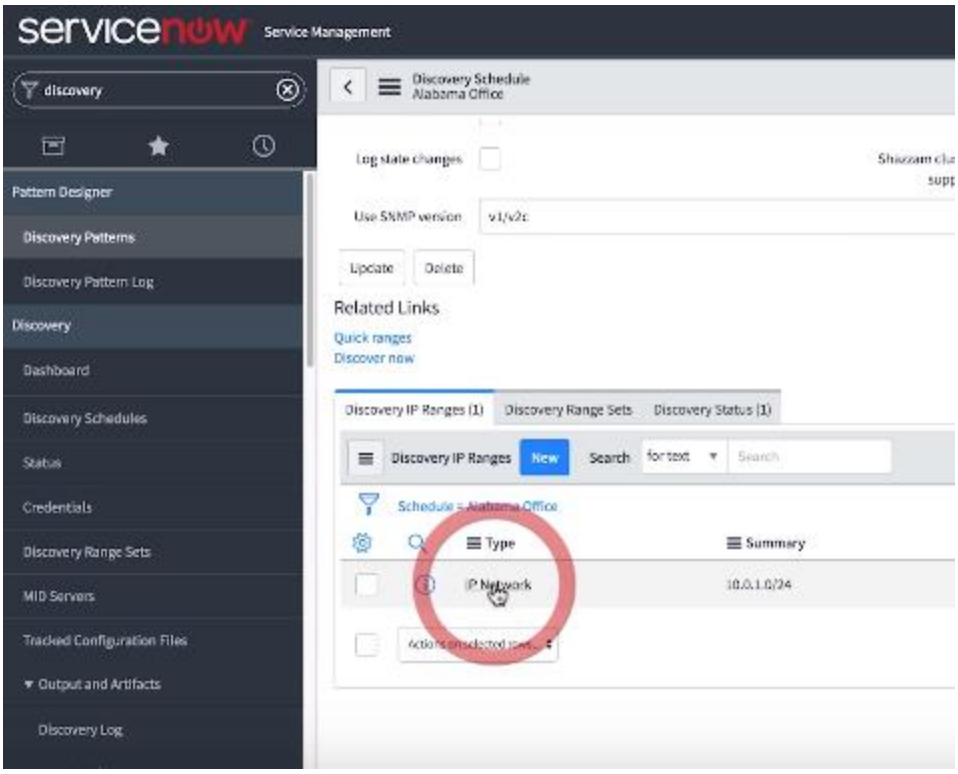
...make sure they are reachable by the MID Server.
The MID Server IP Range Auto Assignment Feature helps tremendously in helping us determine the ranges of our network.

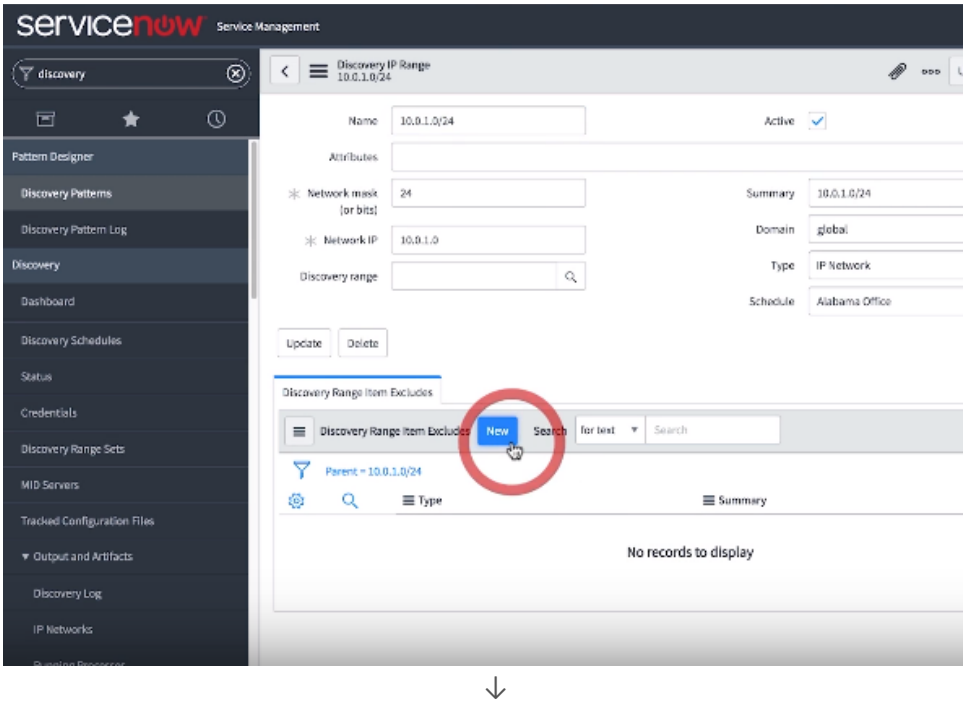
It's good practice to group our IP Ranges into **Range Sets**:

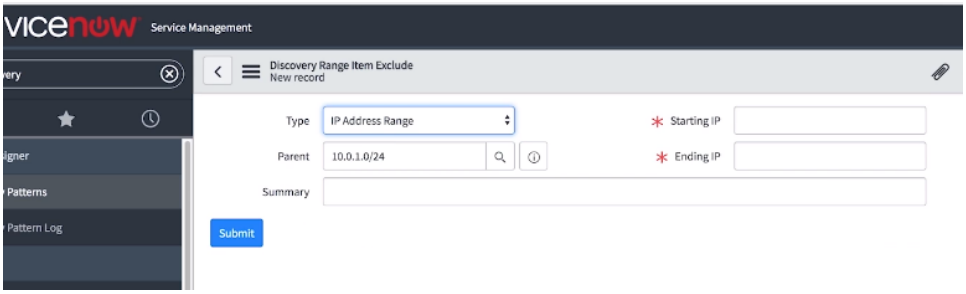
...Discovery will not scan anything outside of the range.

You can also define the desired ranges to exclude via the Discovery Schedules

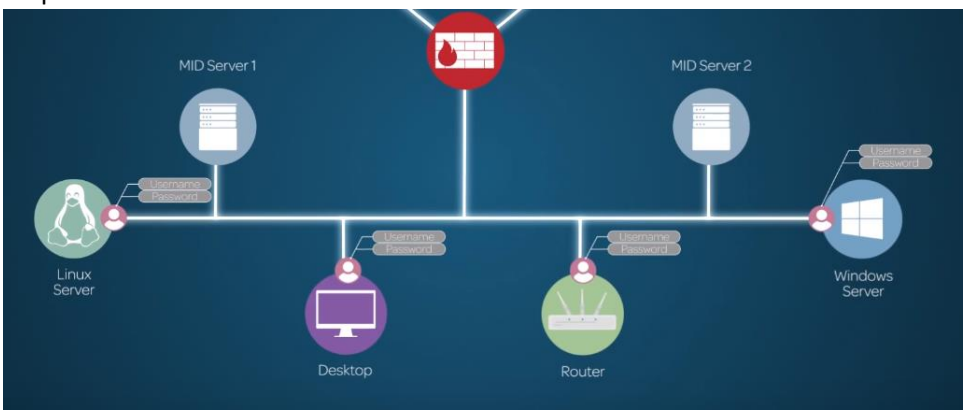



servicenow
Service Management
discovery
Pattern Designer
Discovery Patterns
Discovery Pattern Log
Discovery
Dashboard
Discovery Schedules
Status
Credentials
Discovery Range Sets
MID Servers
Tracked Configuration Files
Output and Artifacts
Discovery Log
Discovery Schedule
Alabama Office
Log state changes
Use SNMP version
v1/v2c
Update
Delete
Related Links
Quick ranges
Discover now
Discovery IP Ranges (1)
Discovery Range Sets
Discovery Status (1)
Discovery IP Ranges
New
Search
for text
Schedule = Alabama Office
Type
Summary
IP Network
10.0.1.0/24


servicenow
Service Management
discovery
Pattern Designer
Discovery Patterns
Discovery Pattern Log
Discovery
Dashboard
Discovery Schedules
Status
Credentials
Discovery Range Sets
MID Servers
Tracked Configuration Files
Output and Artifacts
Discovery Log
IP Networks
Discovery IP Range
10.0.1.0/24
Name
10.0.1.0/24
Active
Attributes
Network mask (or bits)
24
Network IP
10.0.1.0
Discovery range
Summary
10.0.1.0/24
Domain
global
Type
IP Network
Schedule
Alabama Office
Update
Delete
Discovery Range Item Excludes
Discovery Range Item Excludes
New
Search
for text
Parent = 10.0.1.0/24
Type
Summary
No records to display

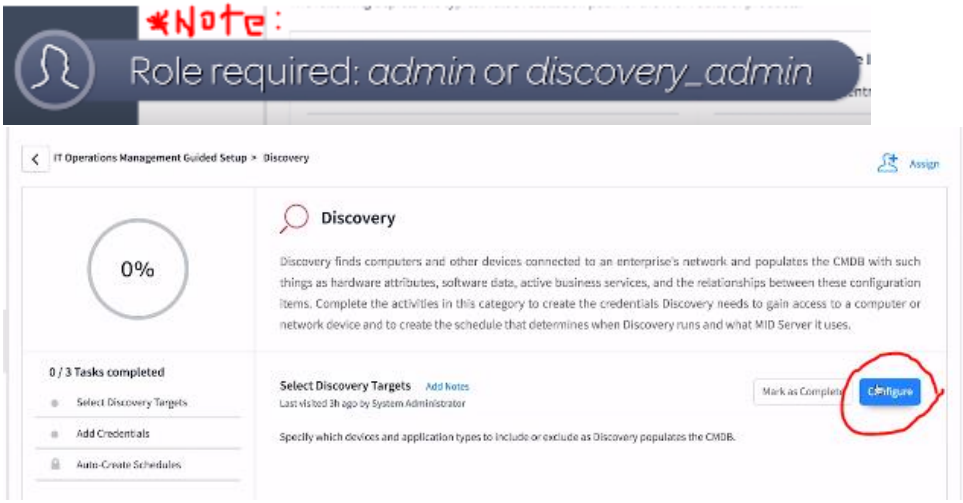

Service Management
Discovery Range Item Exclude
New record
Type
IP Address Range
Starting IP
Parent
10.0.1.0/24
Ending IP
Summary
Submit
Patterns
Pattern Log

Step Two: Obtain the List of Credentials of the desired Devices to Discover within the Network:

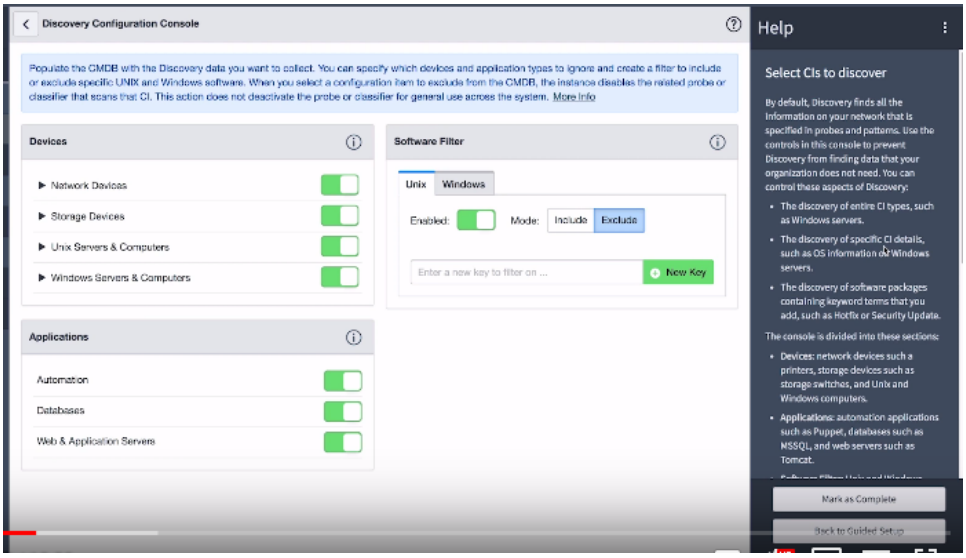


...the MID Server uses the login credentials to query these devices... otherwise, they won't be discovered.

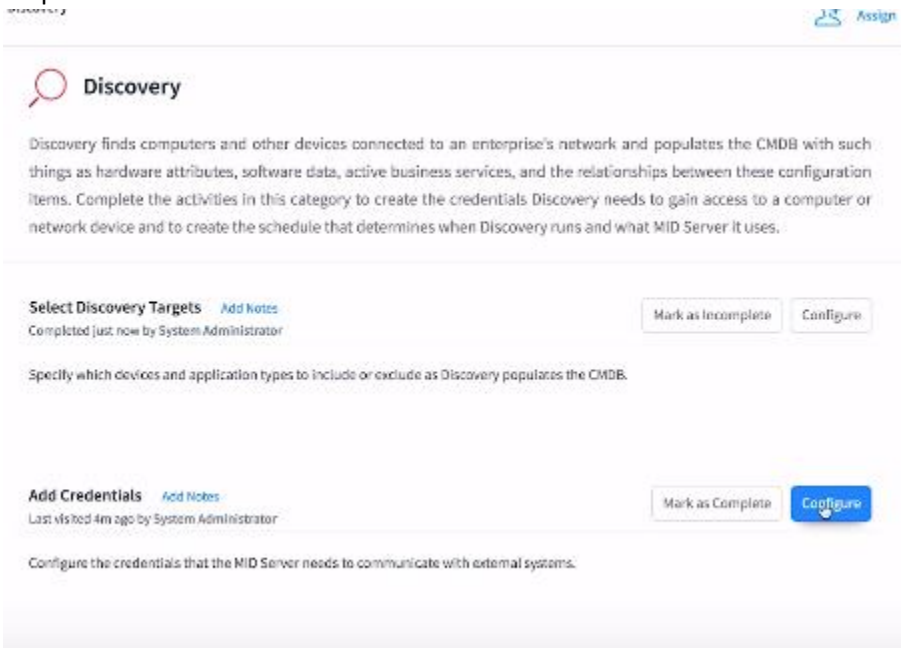
Step Three: Select Discovery Targets (make sure MID Server is installed at this point):

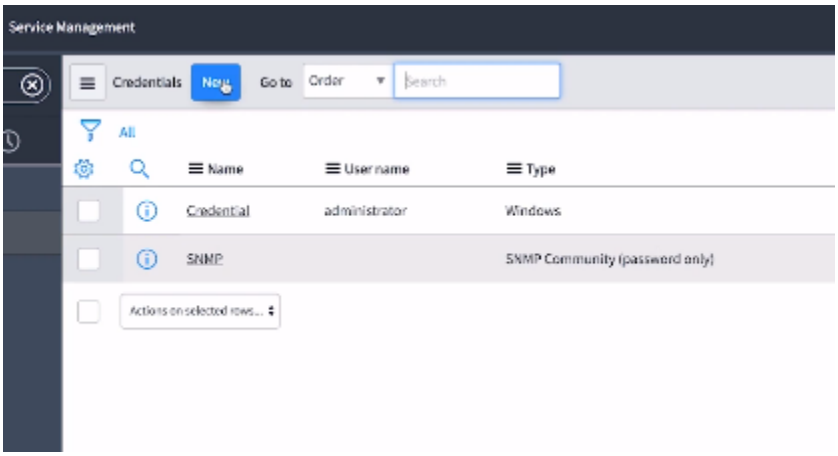


Specify the device types, application types, and software from each category to include/exclude:

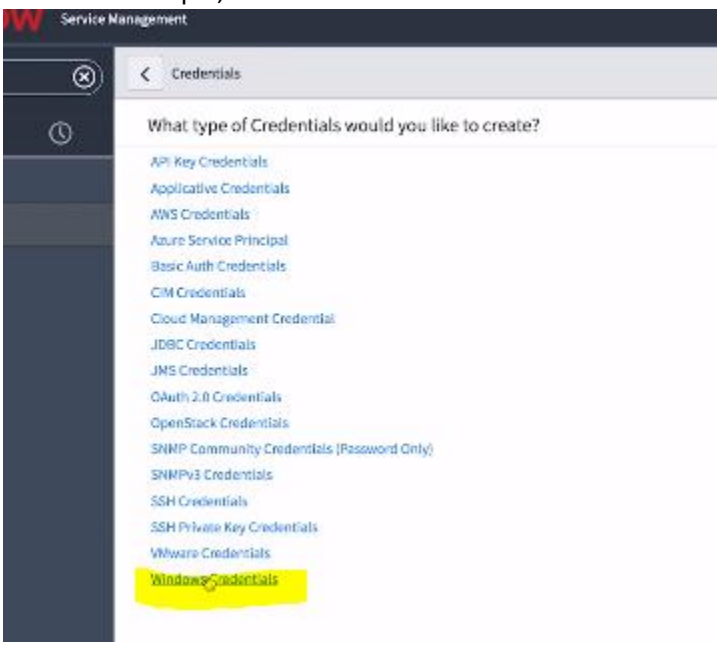


Step Four: Add Credentials:



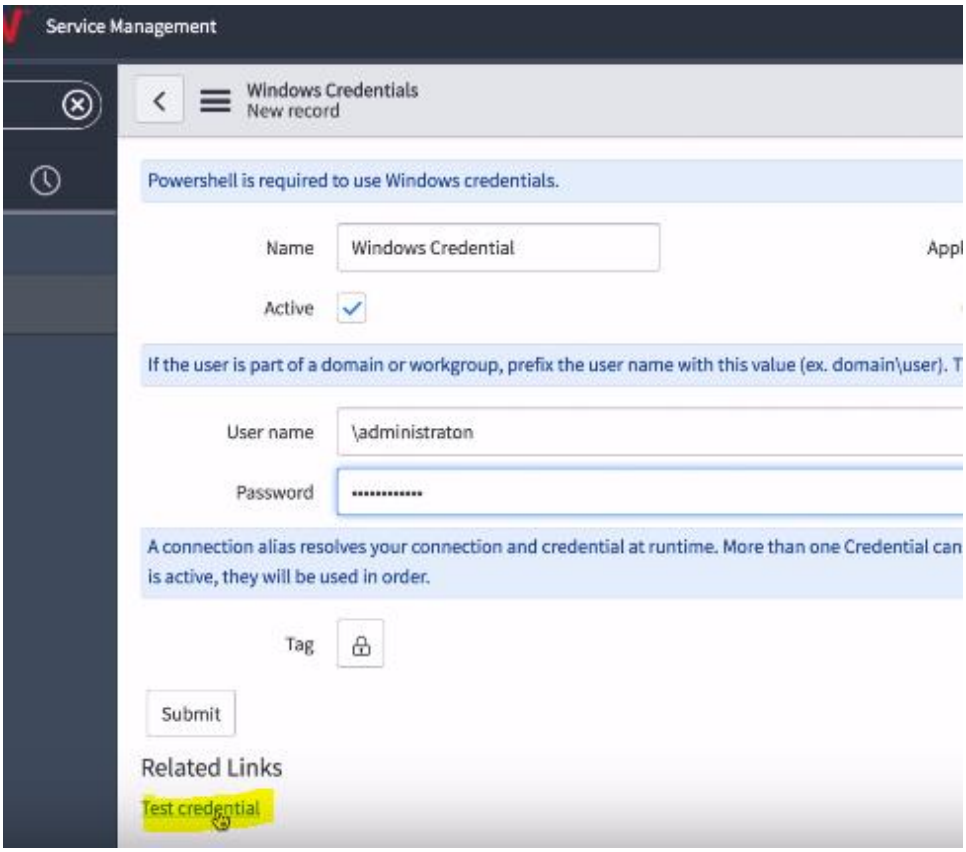


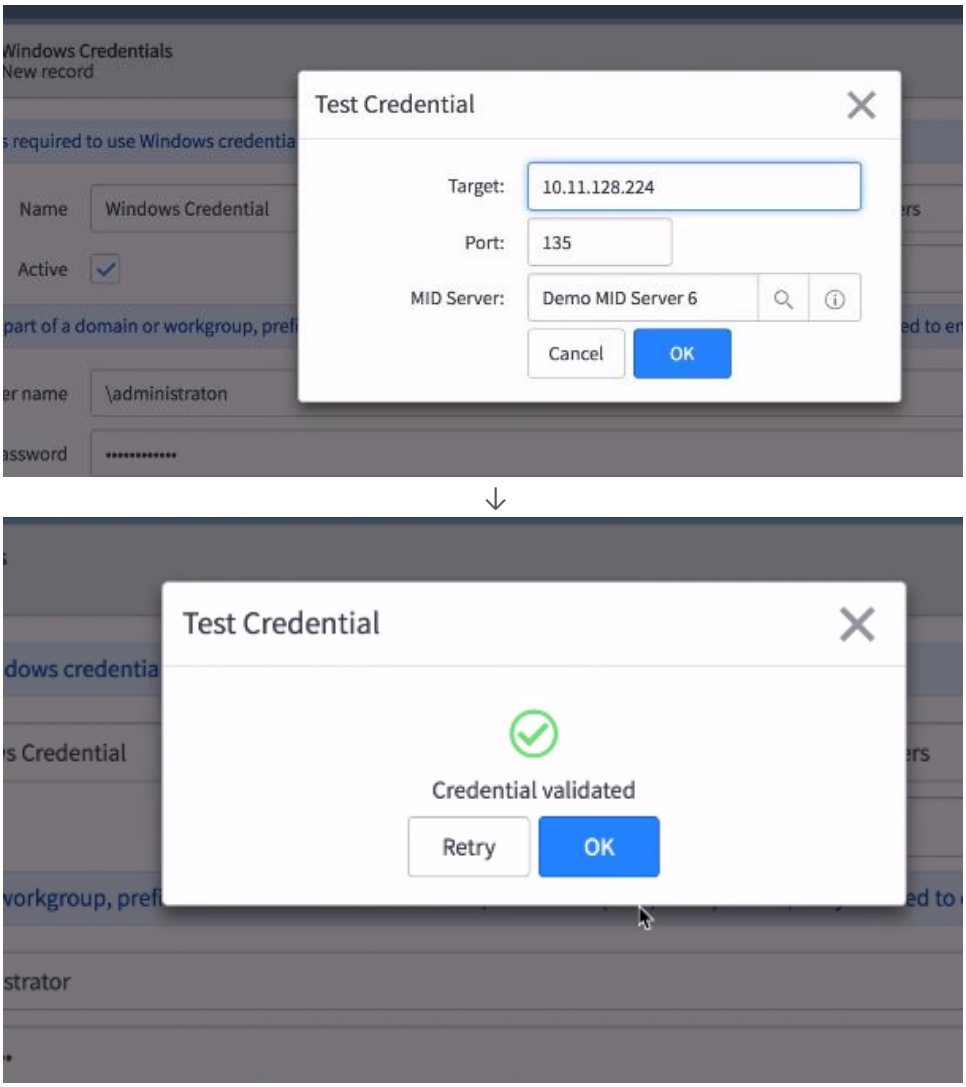
...for this example, it's a Windows credential:



...for Windows Discovery, the credentials should be a domain user with local admin privileges to the desired targets of Discovery.

Often, we use a single service account to make management easier. It can be valid across several servers in a Windows environment. Now let's test it:

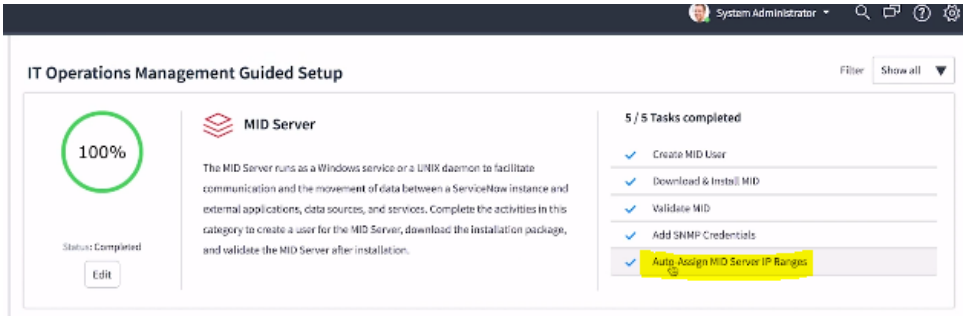




...now we mark this step as Complete.

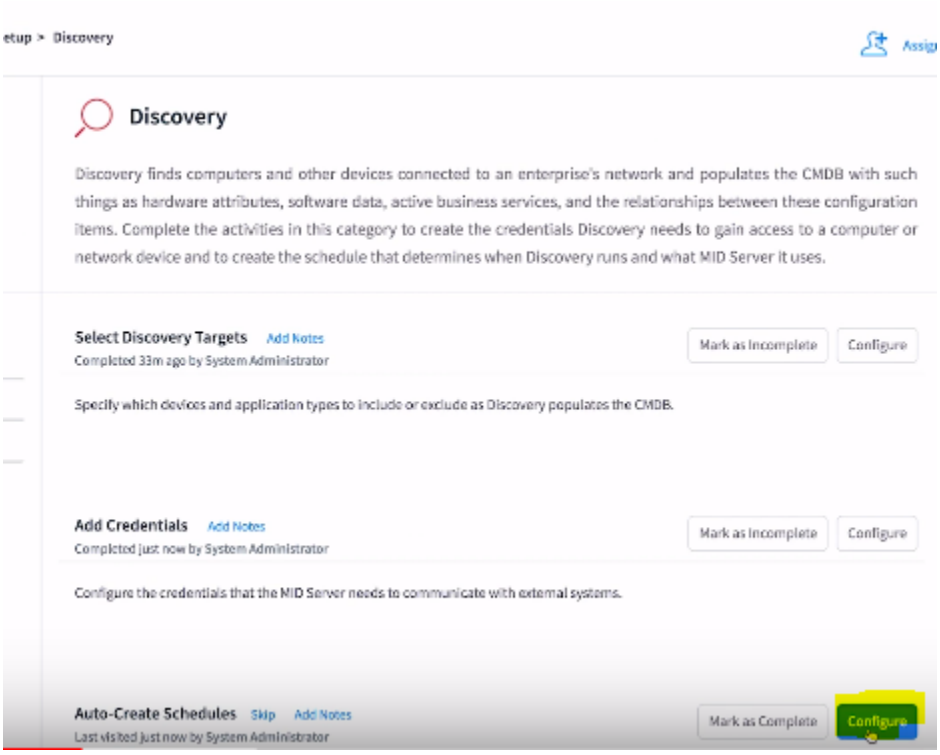
Step Five: Auto-Create a Schedule for Discovery:

***Note**: this is only possible if you already used the Auto-Assign MID Server IP Ranges:

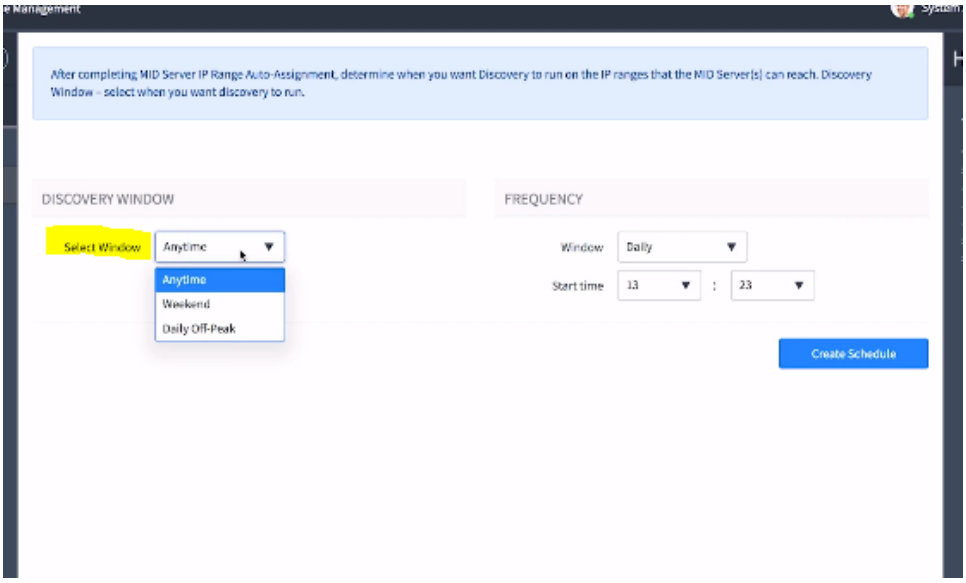


...otherwise, you will need to configure a schedule manually.

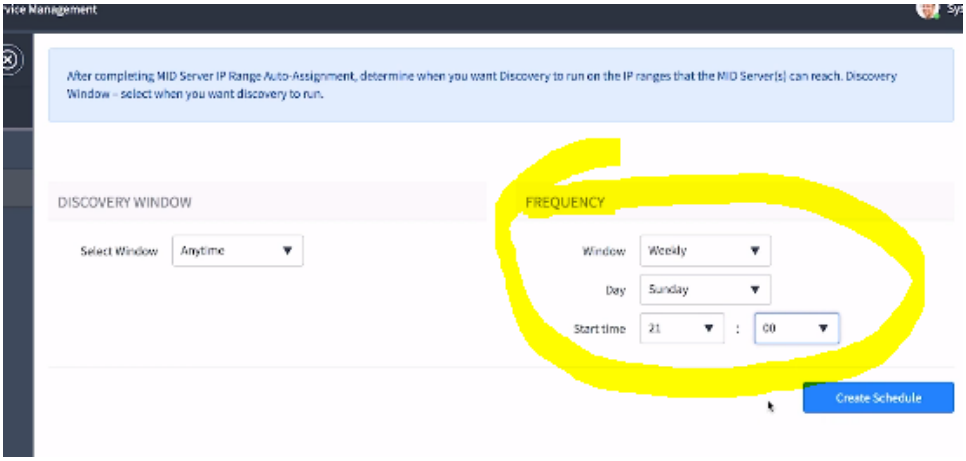
To Auto-Create a Schedule, select Configure:



...select the window in which you want the desired Schedule to execute. You can select the time options is applicable.

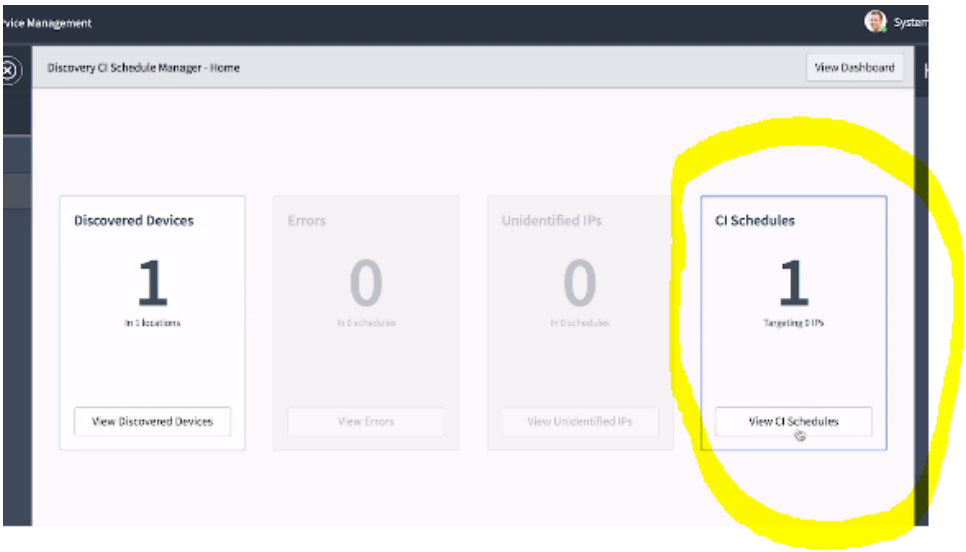


Let's say we want to schedule it every Sunday night at 09:00 pm:

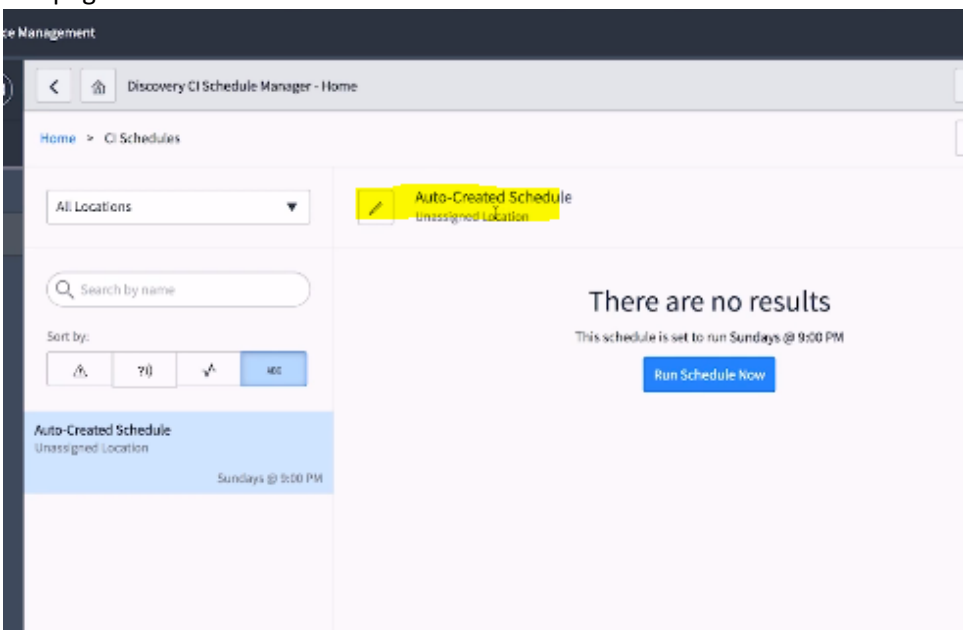


...select Create Schedule.

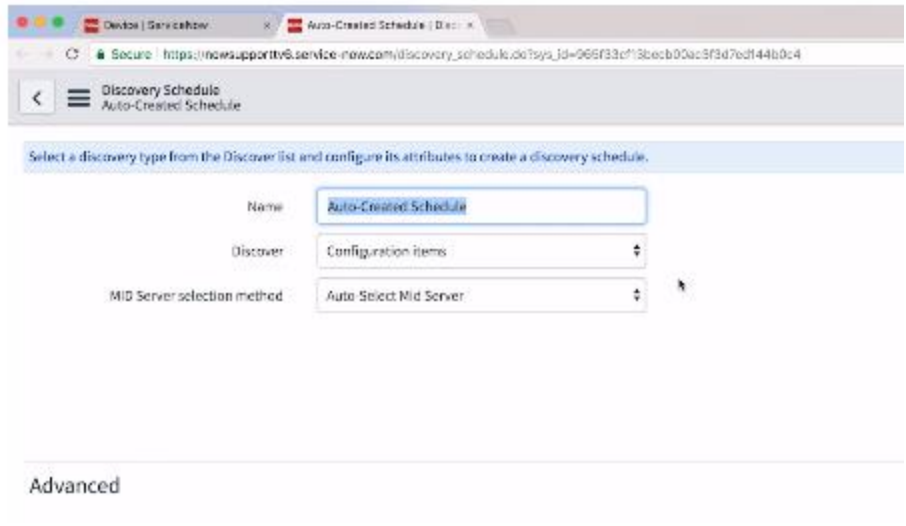
Now we see that the CI Schedule Manager opens:



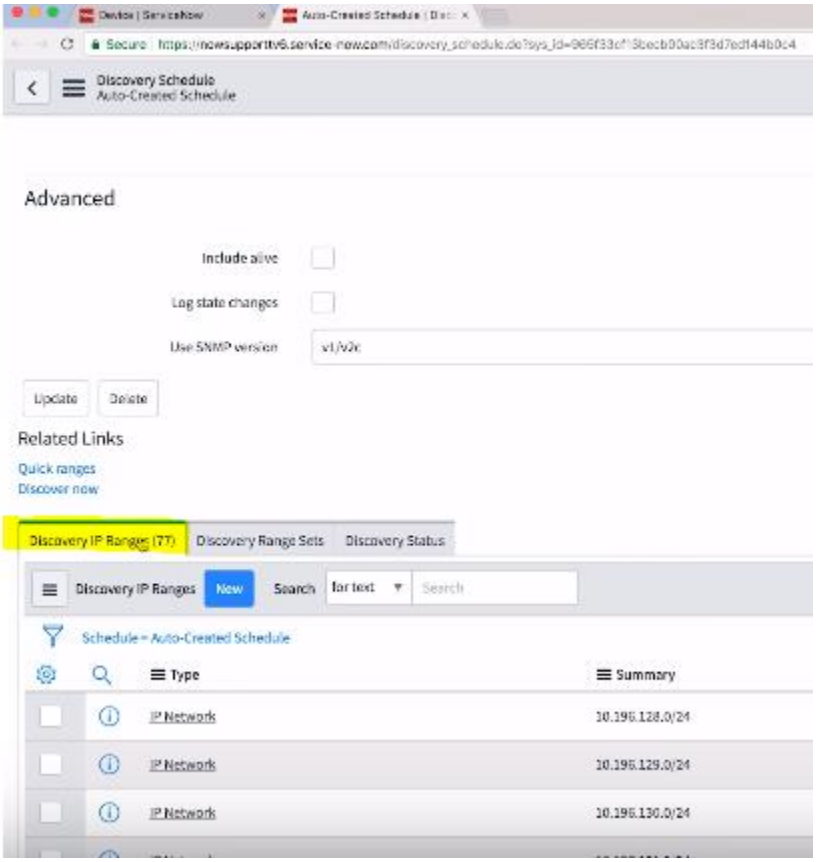
...we can also see the Schedule we just created. If we want to edit the schedule, we can access it here on this page:



↓

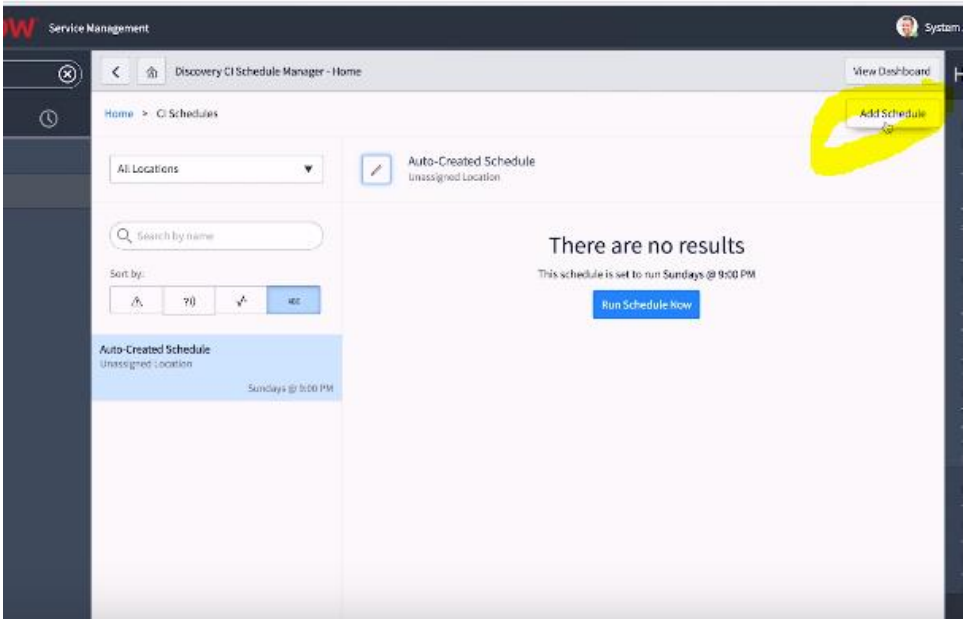


↓

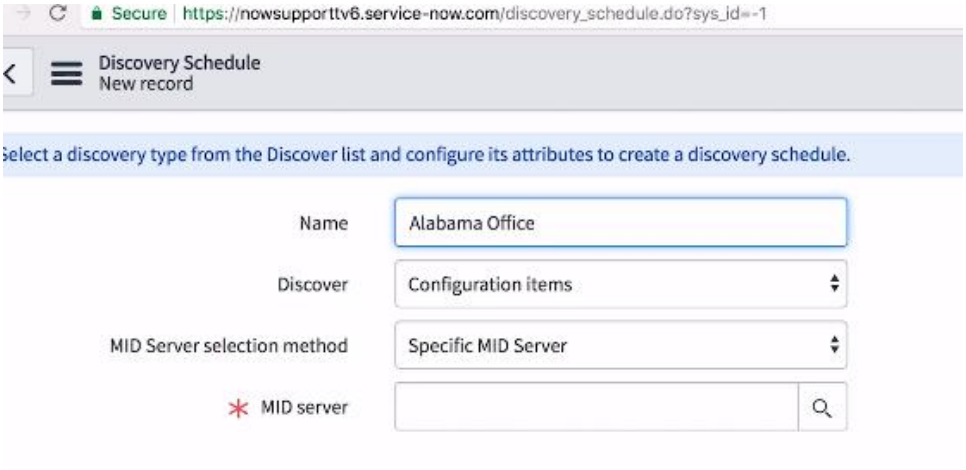


...we see how much of a time saver it is; all the Discovery IP Ranges are automatically configured!

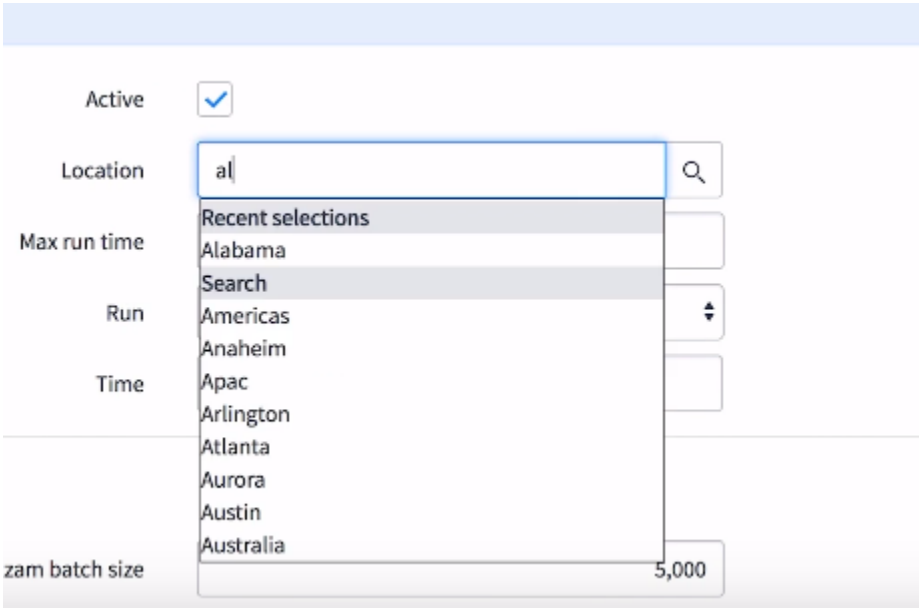
If we wish to create a Schedule manually:



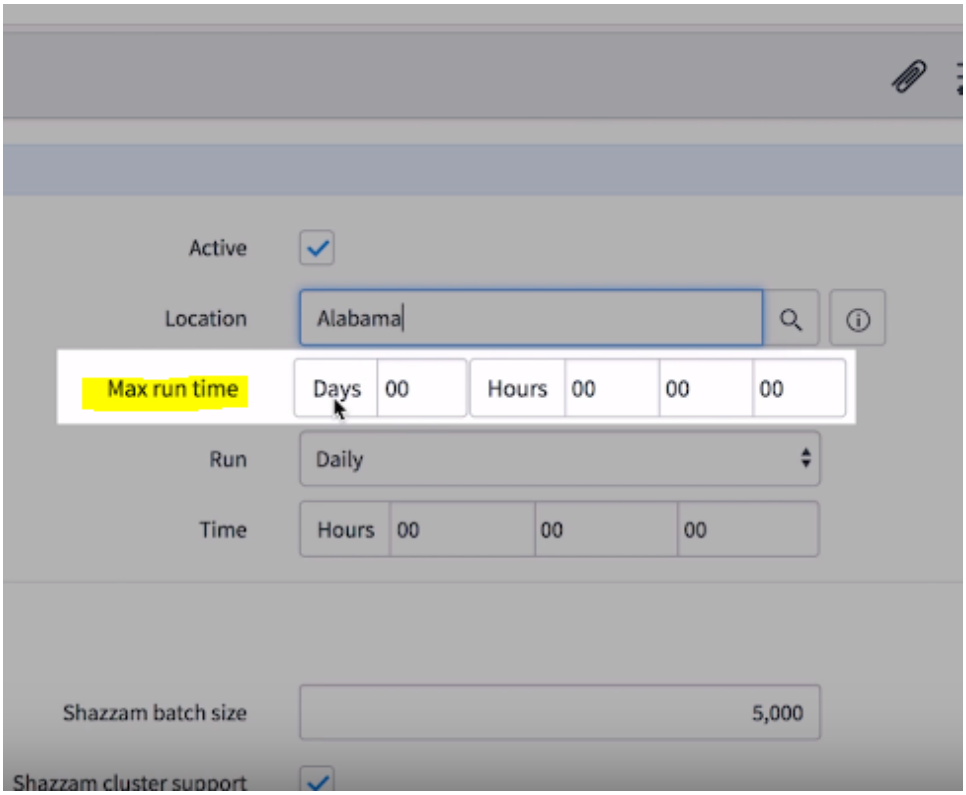
...since we configured our MID Server with Discovery and IP Ranges were assigned, we let Discovery Auto-Select the MID automatically:



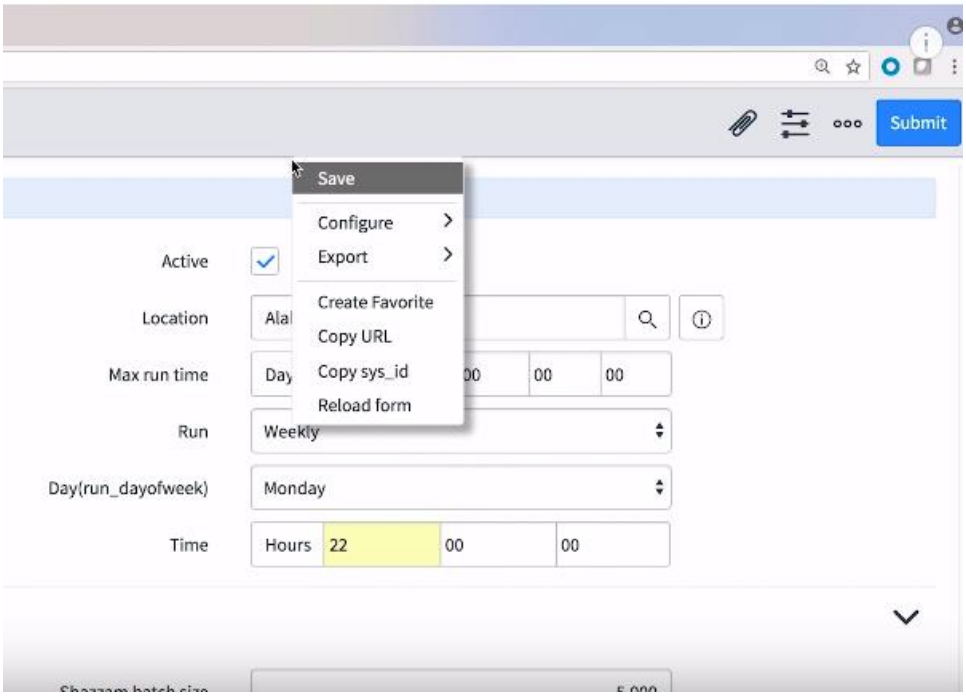
...we can enter a name for the location in the Schedule, which will also populate the location field in the CMDB on all CI's discovered by the Schedule:



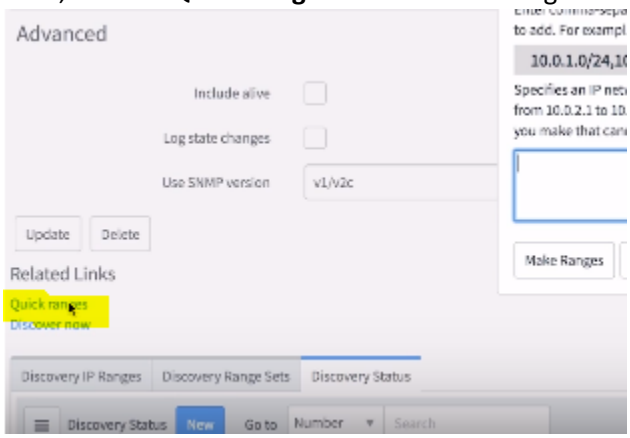
We can put a limit on how long a Discovery can run... we may leave it at zero (unlimited amount of time) in order to fully conduct the Discovery however long it needs until it is completely done:

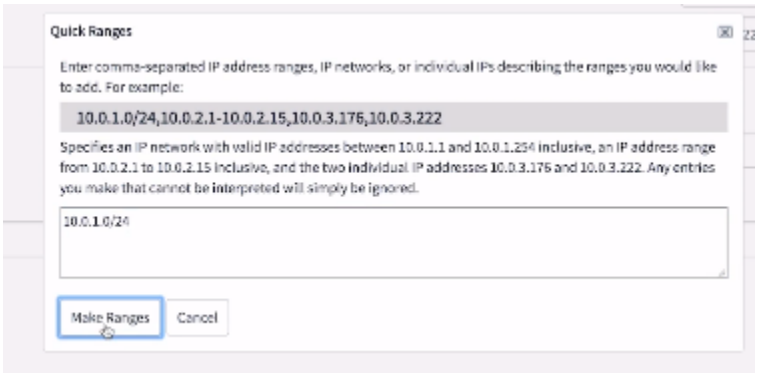


...next, right-click on the header and save:


Submit
Save
Configure
Export
Create Favorite
Copy URL
Copy sys_id
Reload form
Active
Location
Max run time
Run
Weekly
Day(run_dayofweek)
Monday
Time
Hours
22
00
00

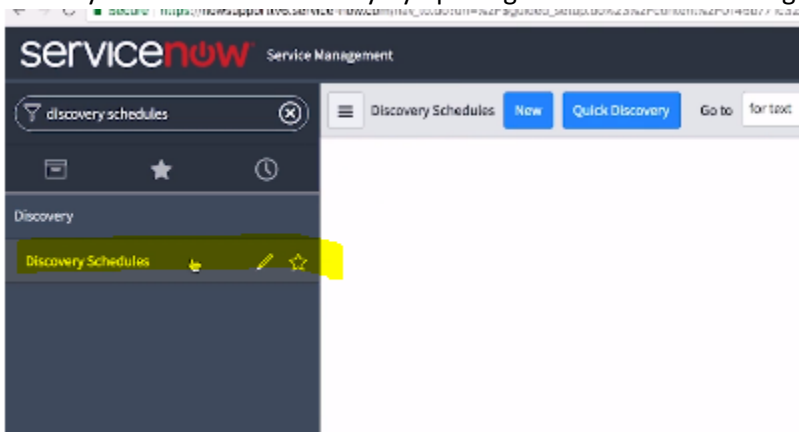
Next, click on **Quick Ranges** to add the IP Range we want:

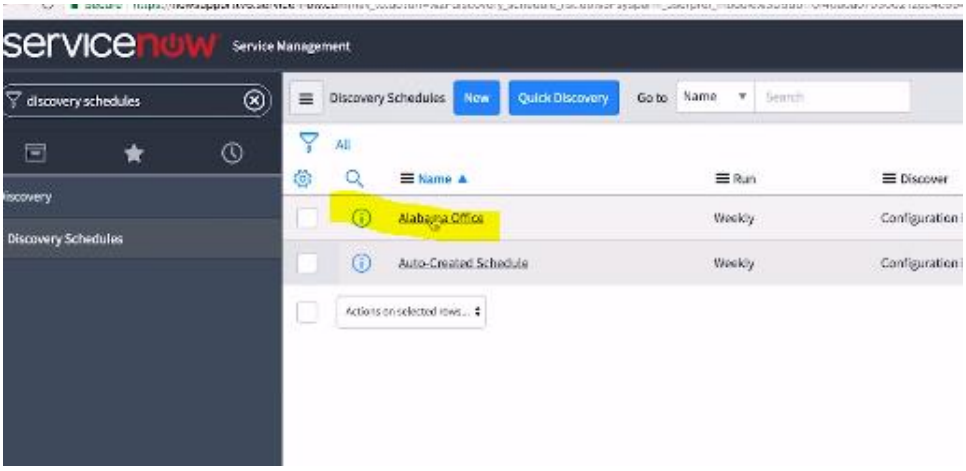


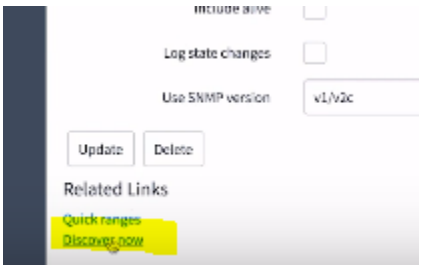


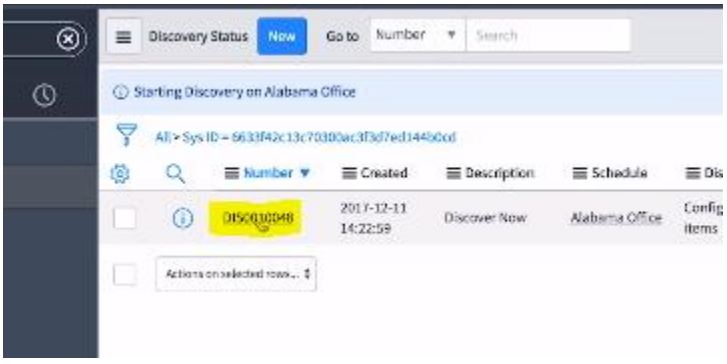
...mark as Complete.

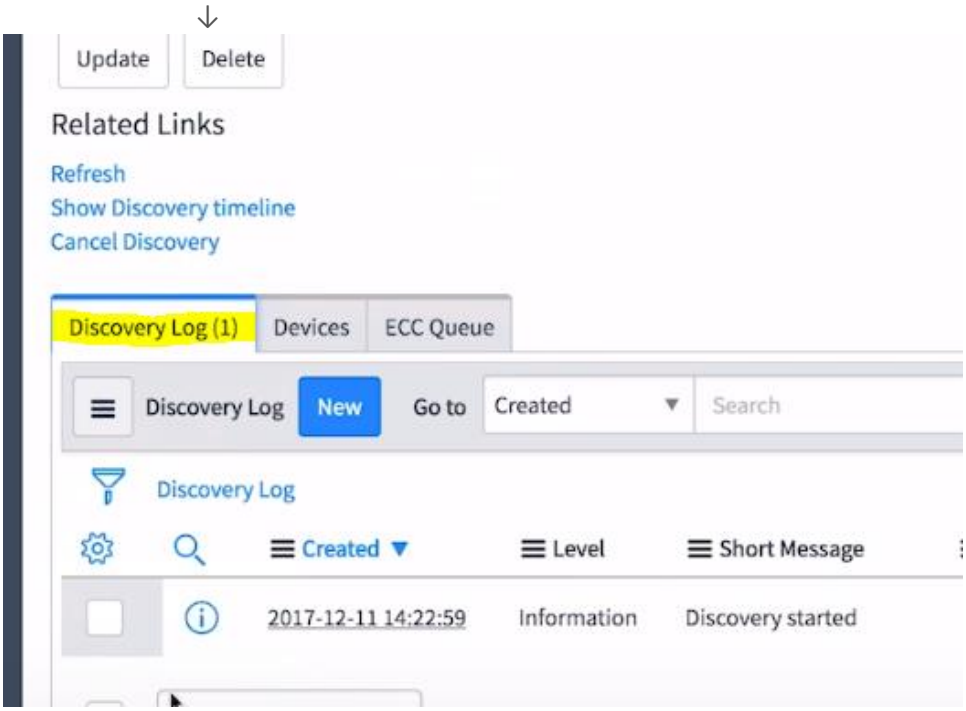
You may now test the Discovery by opening Schedule and selecting Discover Now :





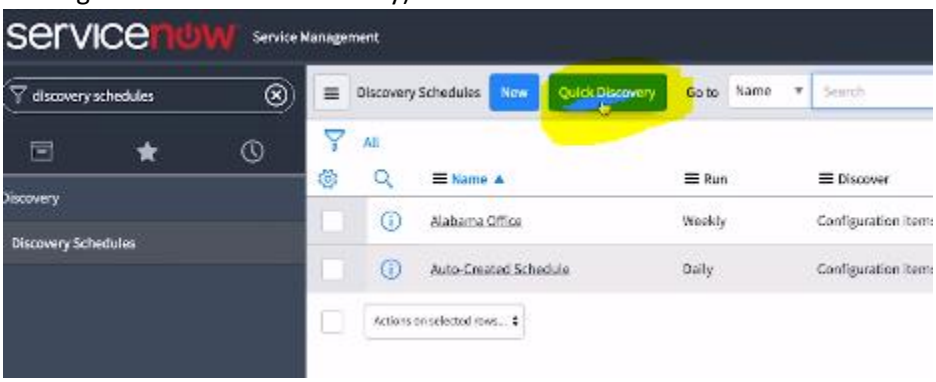




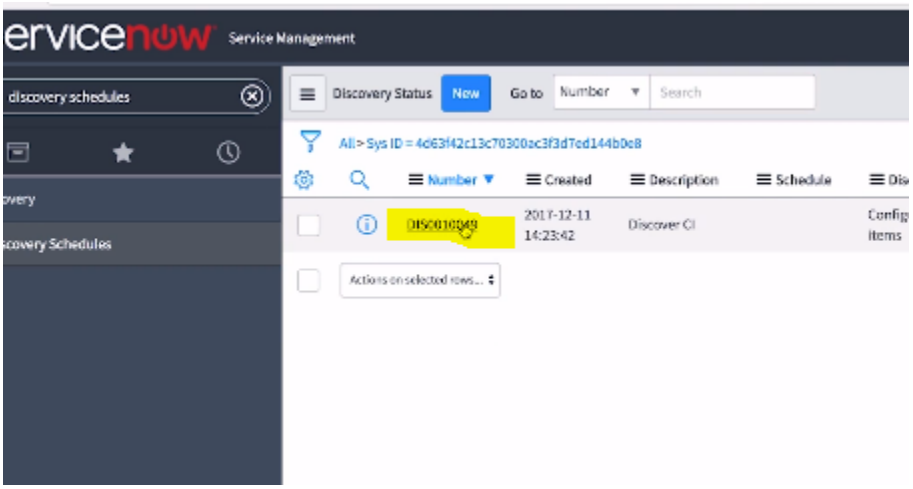


… ***Note**: you may also click on Refresh to see the most current status.

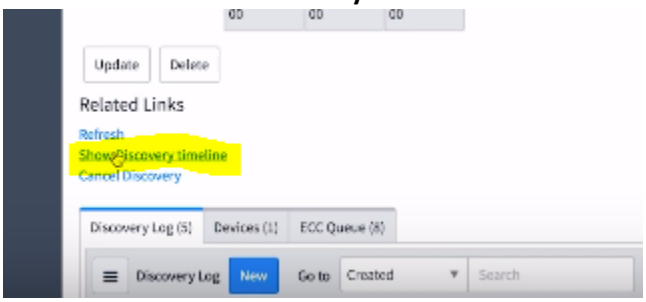
Quick Discovery allows you to discover a new device you just added to your network (as opposed to waiting for a scheduled Discovery):

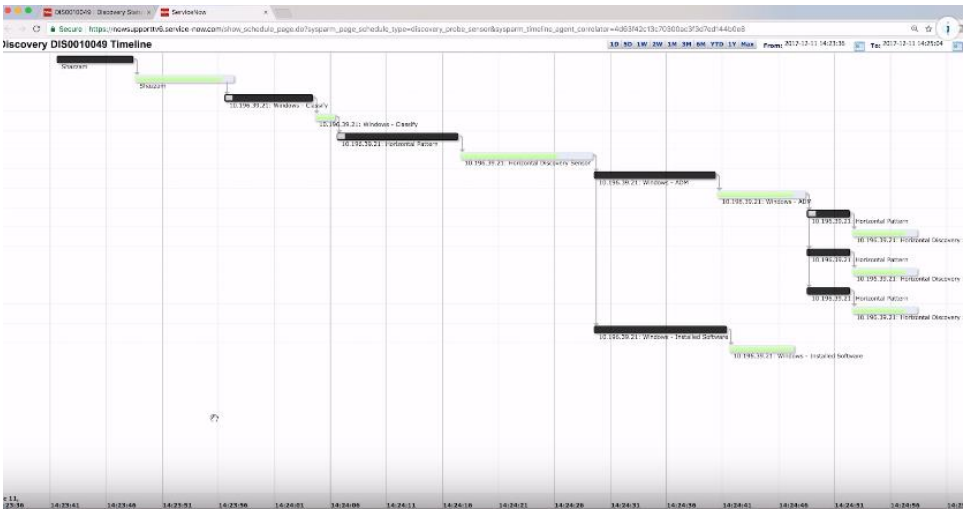


When we open the **Discovery Status** record...



...we can access the **Discovery Timeline**:

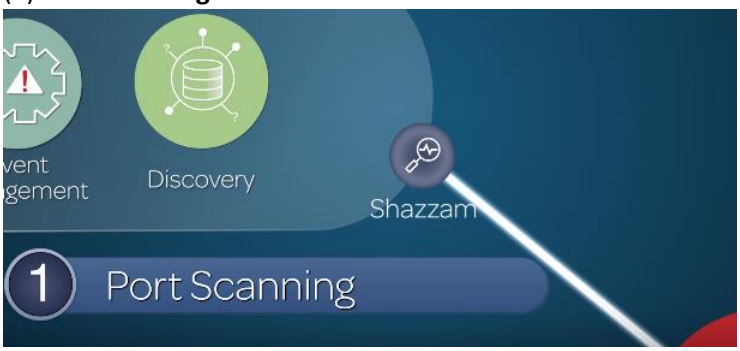




...here we can see the different phases of discovery, as well as their lengths of time.

What happens in each phase of Discovery?

(1) **Port Scanning**:

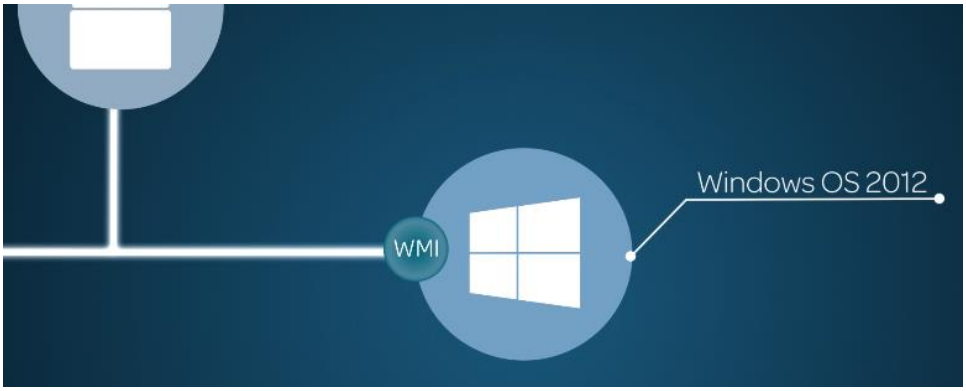


Discovery launches a **Shazzam** probe to scan the defined IP address(es) and identifies responsive (active) IP's and defined IP Port states.

For example, Windows Server:

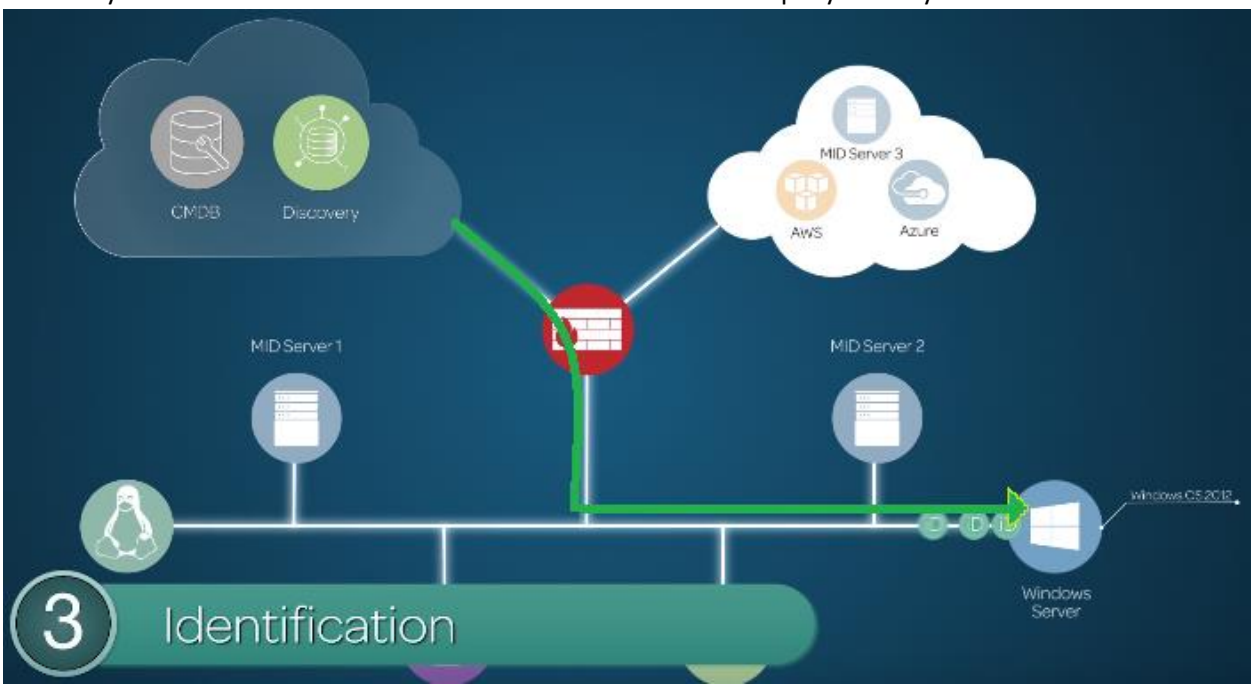
The probe finds an active IP that responds on port 135. So Discovery will assume it's a Windows device and launch the Windows Classification probe.

(2) **Classification**:
Discovery continue to send probes to find the device type under each IP Address.
In our Windows Server example, Discovery sends the **WMI** probe, which is used to determine which Windows Operating System is running on the device:

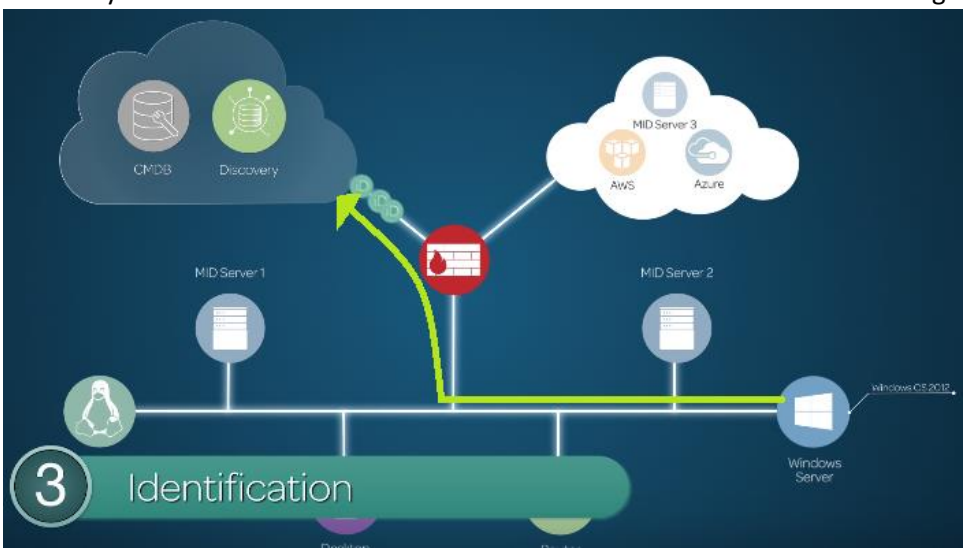


(3) **Identification**:

Discovery collects additional information about the device to uniquely identify it:



Discovery then uses CI Identification Rules to check the CMDB for the matching CI:

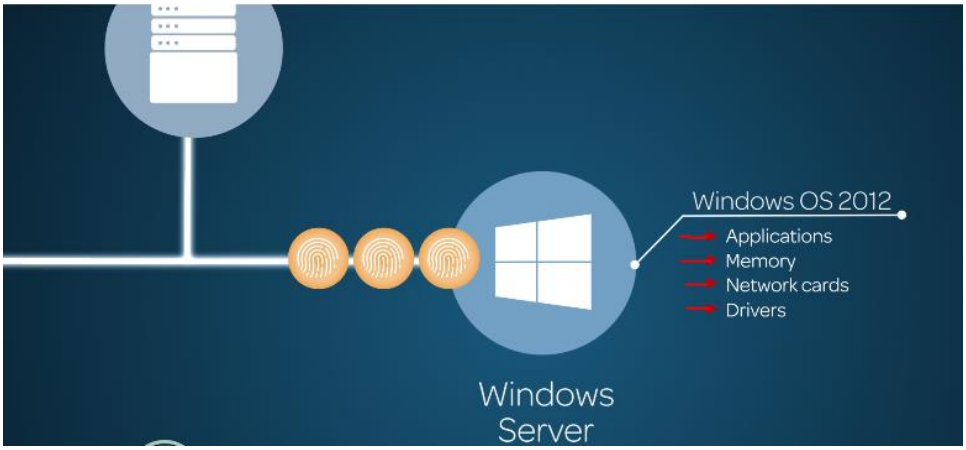


If a matching CI is found, it is updated.

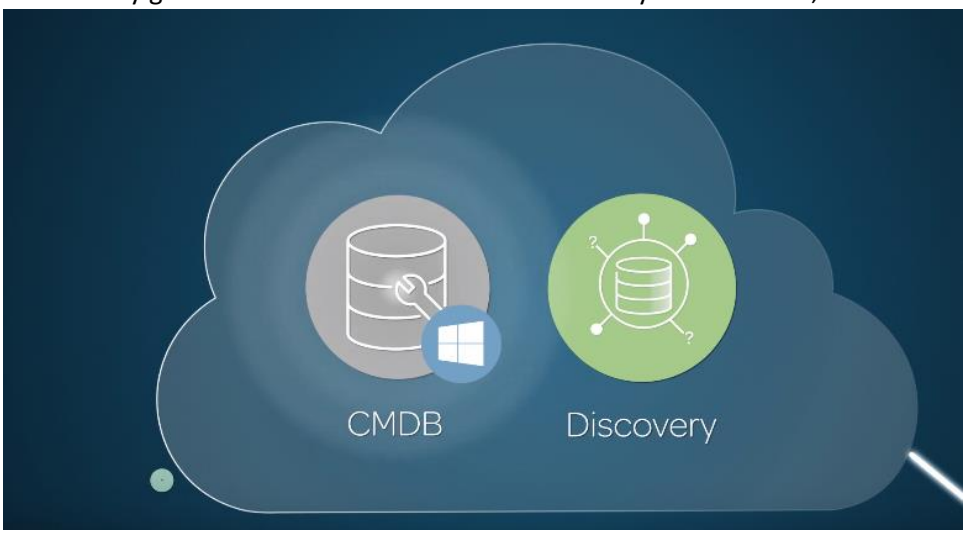
If a matching CI is not found, a new CI is created.

(4) **Exploration**:

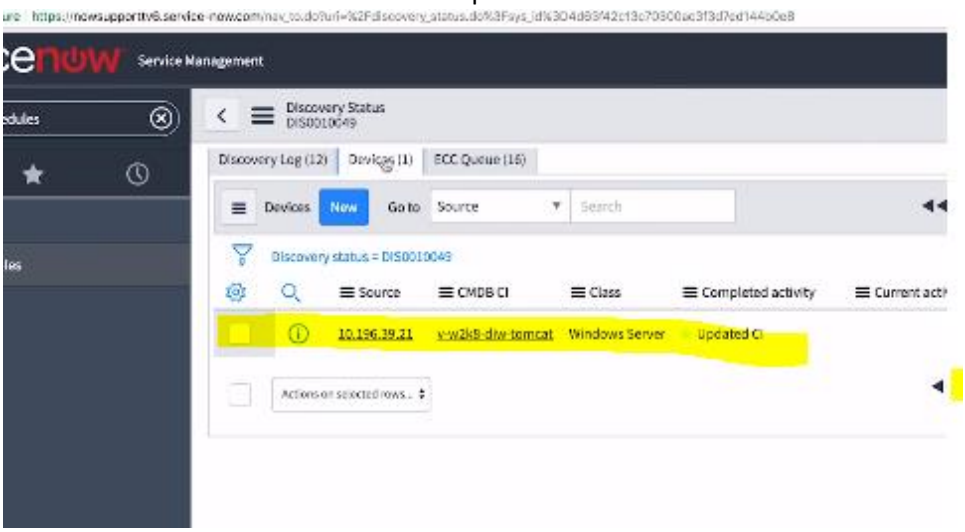
We gather additional information about the device, such as:



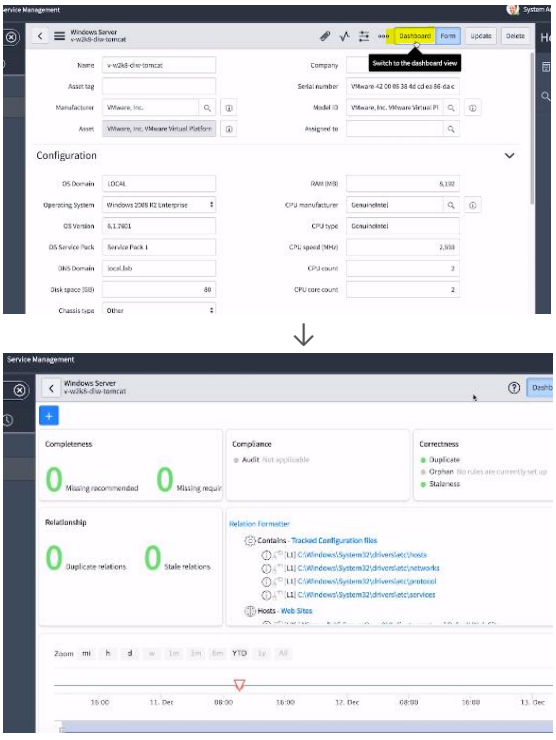
...the newly gathered information is sent via Discovery to the CMDB, which will be updated:



We can check to see if the CMBD was updated:



...for CI's that have changed, we can look at the timeline and view any incidents or changes in the list at the bottom:



We can also go to the Discovery Dashboard to see the current status of all Discovery activity: