REVATURE

ServiceNow – ITOM - Midserver

ITOM - Midserver

- Let look at the demo of creating Midserver
- Steps involved

  - Create a MID Server

  - Download and install MID Server

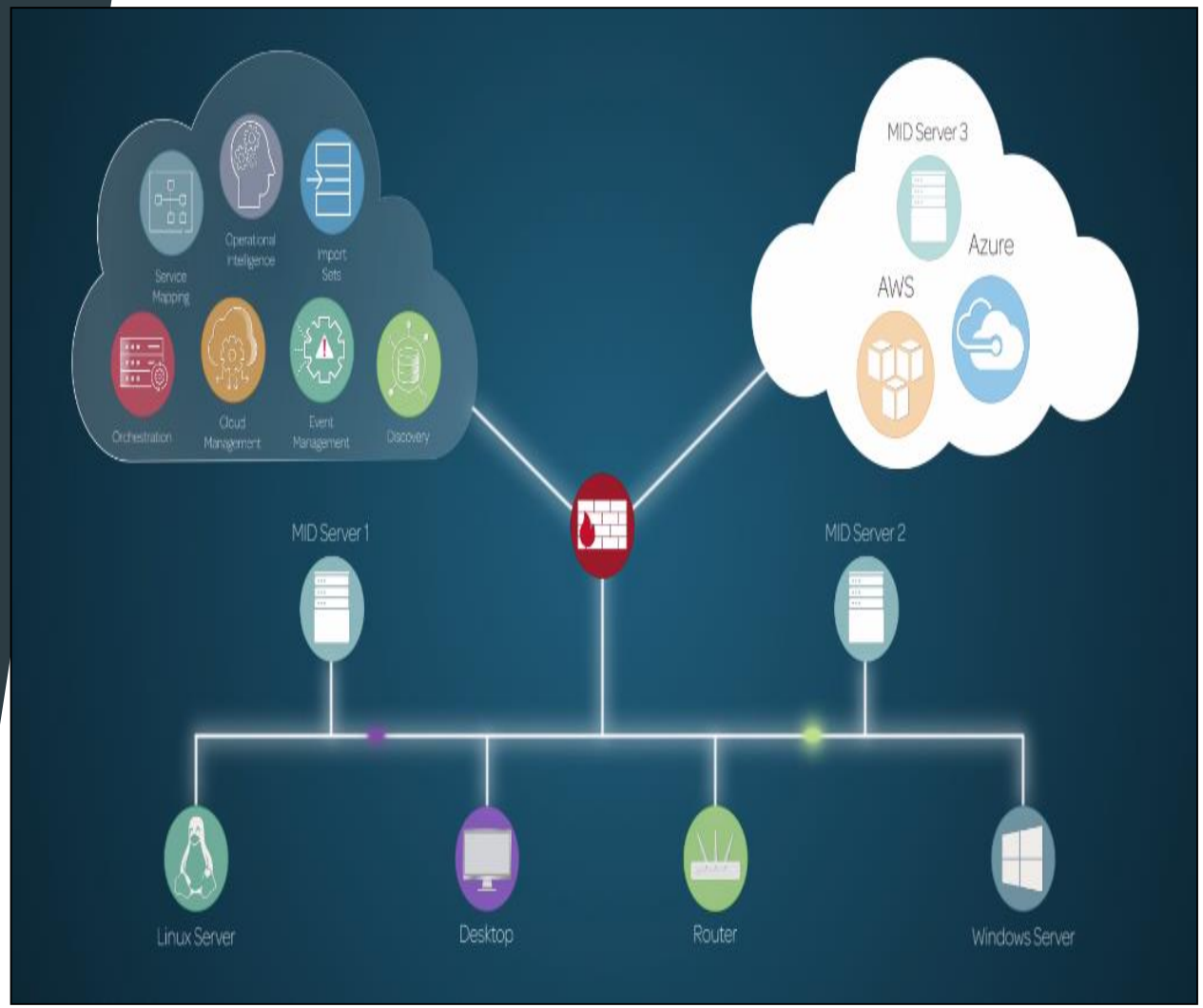
  - Validating the MID Server

  - Adding SNMP credentials

  - Assigning IP address ranges for subnets

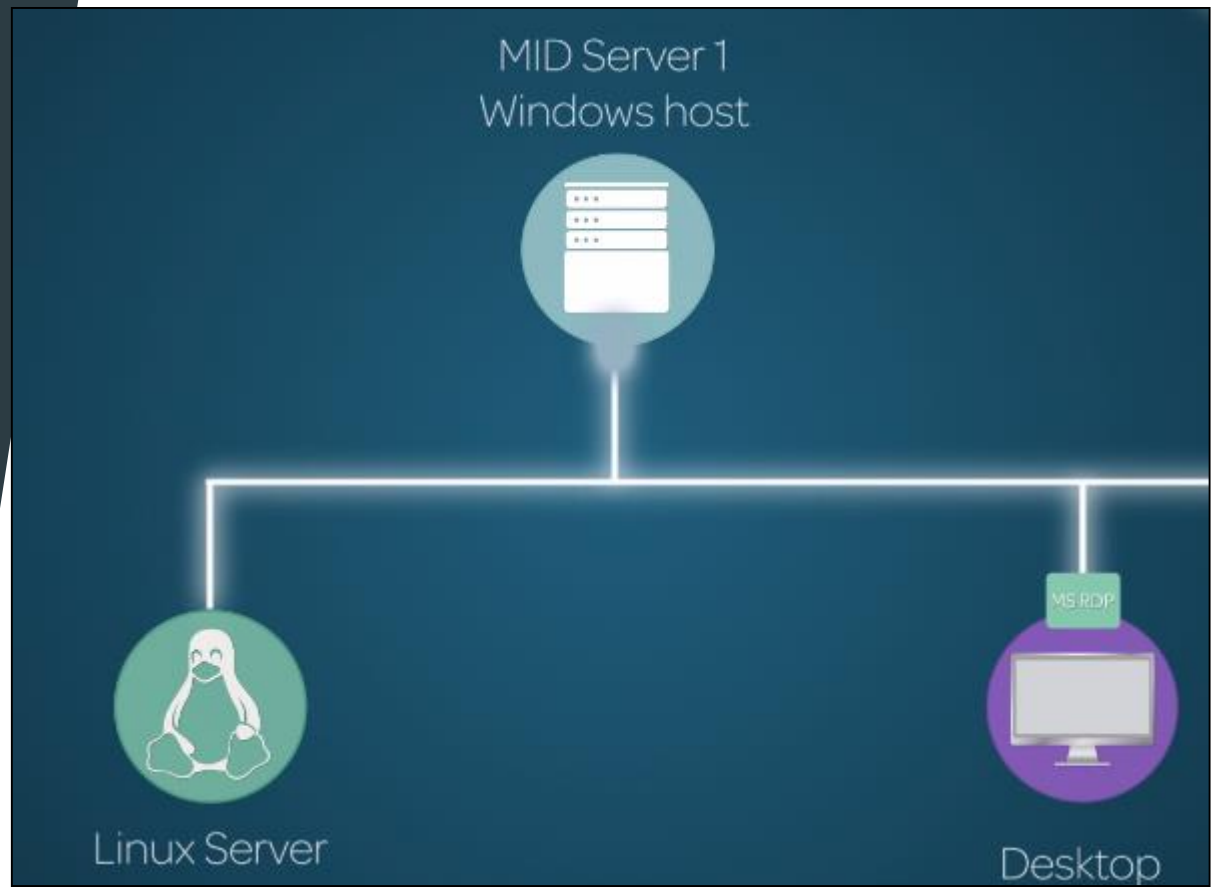
ITOM - Midserver

- Midserver enables SNOW applications to communicate with external systems on the enterprise local network or public cloud.
- The ITOM guided setup steps you through the process of installing Midserver and getting it ready to use
- Midserver can be installed on Windows or Linux OS hosts either on the enterprise network or on the cloud(AWS - EC2 running on VPC or Azure)



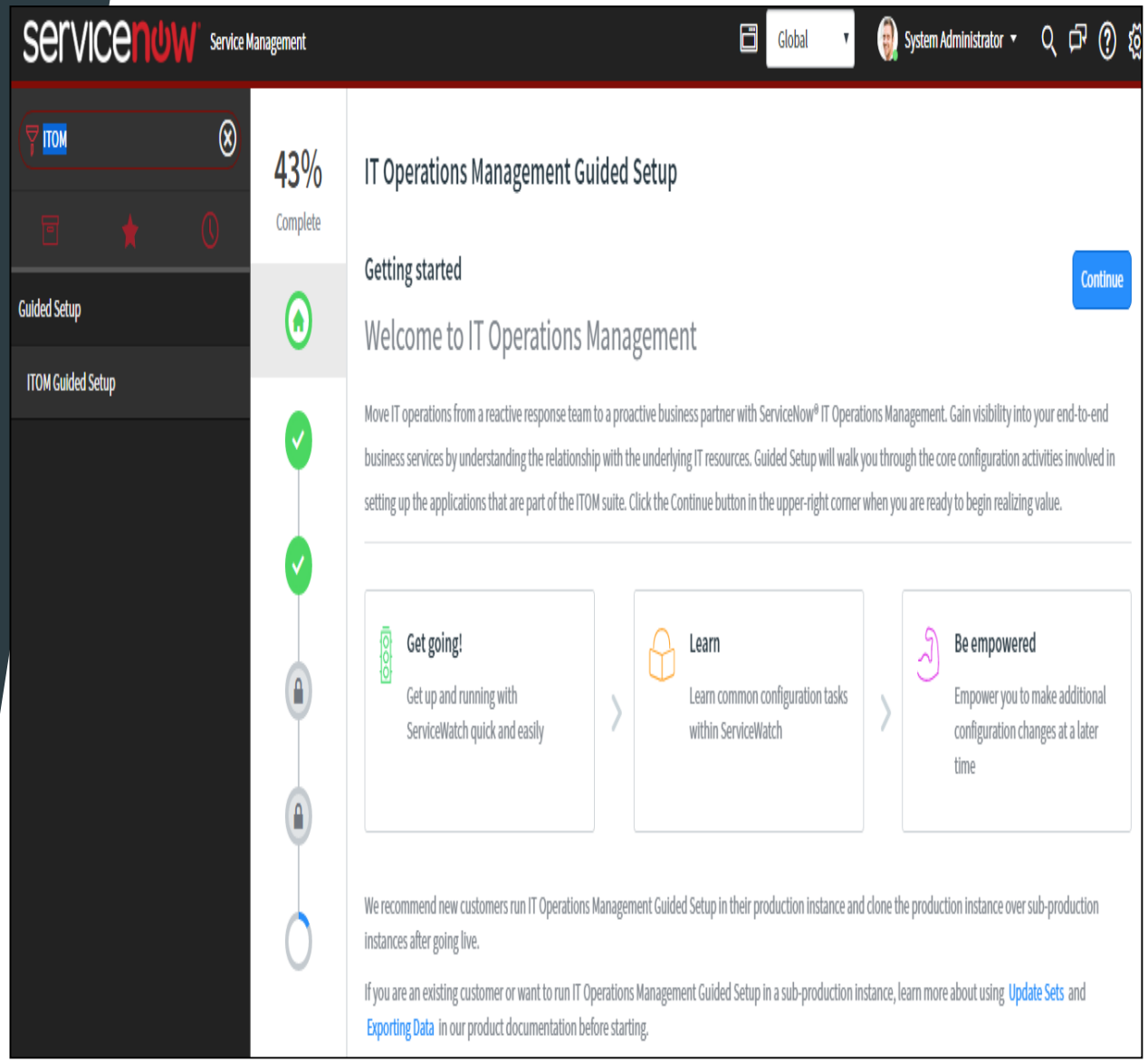
ITOM - Midserver

- For this demo we would need specifically need Windows host based Midserver to discover windows machine when working on desktop machine connected to Windows machine through Microsoft Desktop client



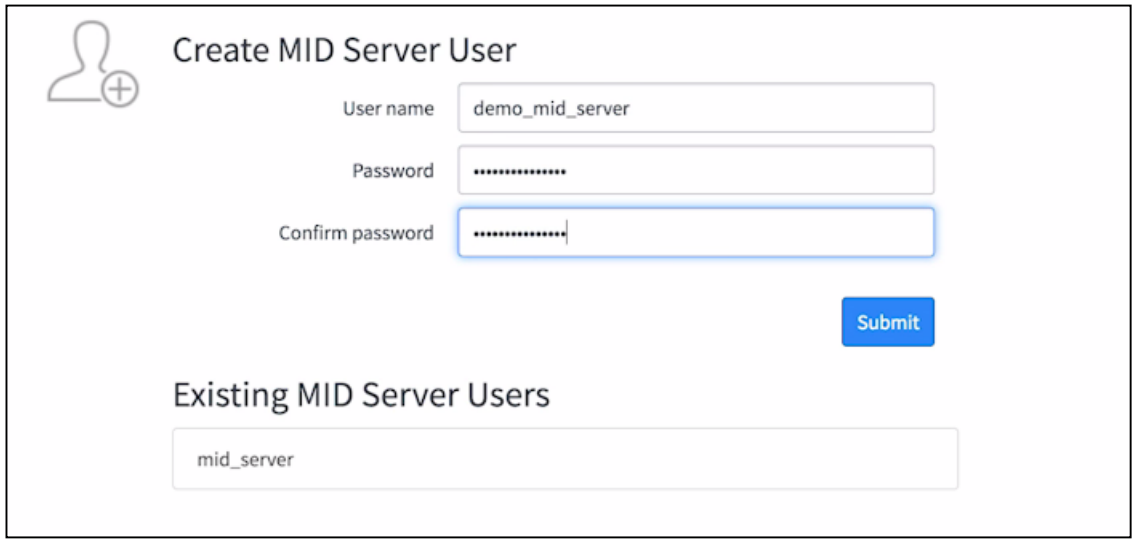
ITOM - Midserver

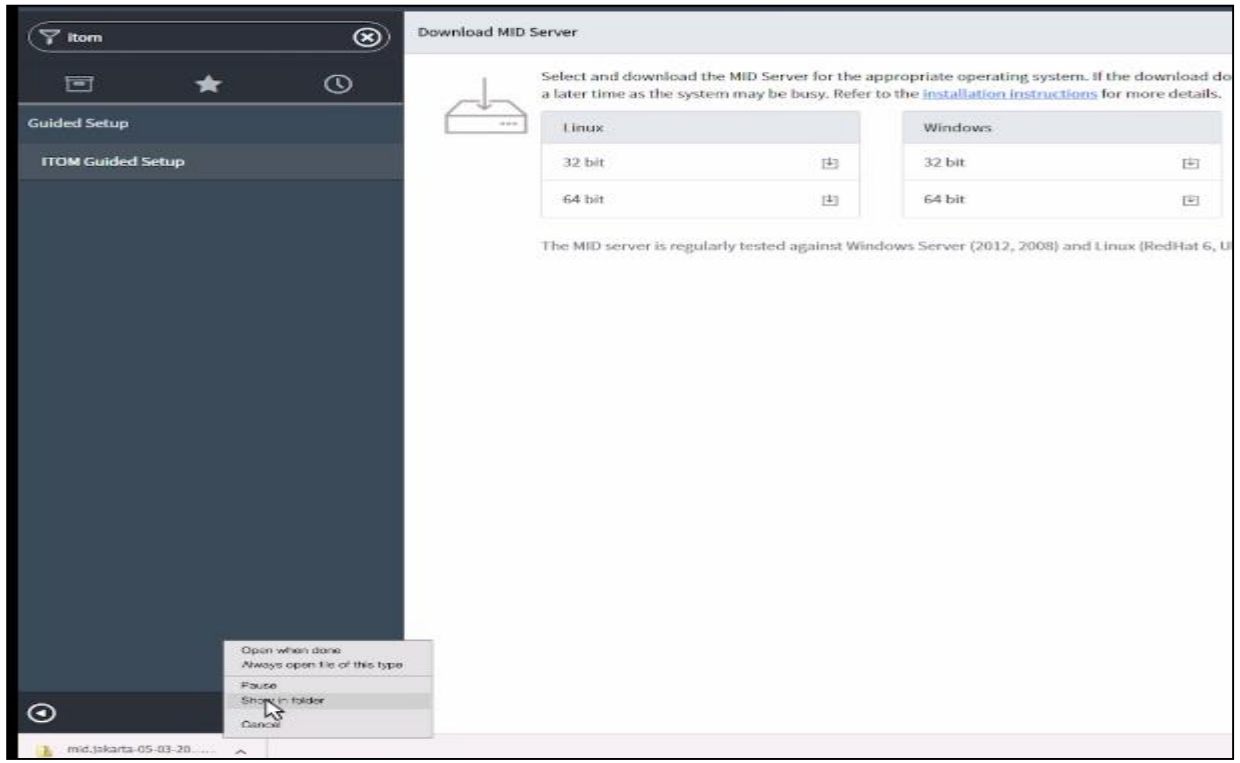
- Lets take the demo of installation and use of Midserver.
- Navigate to ITOM guided setup and get started
- Guided setup helps connect several ITOM apps
- We will navigate straight to MID server setup



ITOM - Midserver

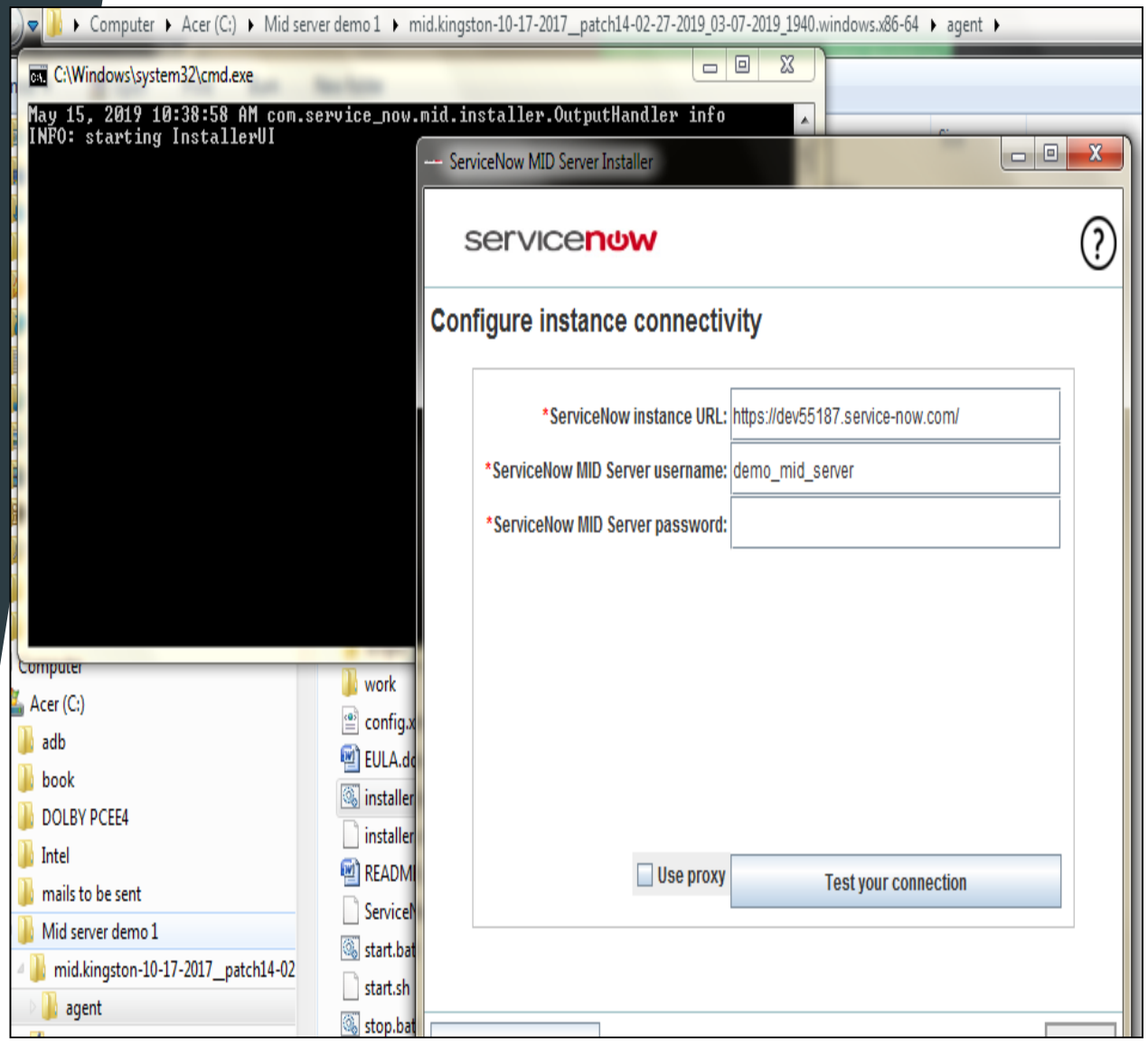
- First task is to create user account.
- Next task is to download and install MID server installer archive.Since we need to install in host machine log onto SNOW instance on host machine and click on configure and download 64 bit.
- Create a folder MID Server Demo and extract all to the same folder
- In the agent folder install the install batch file





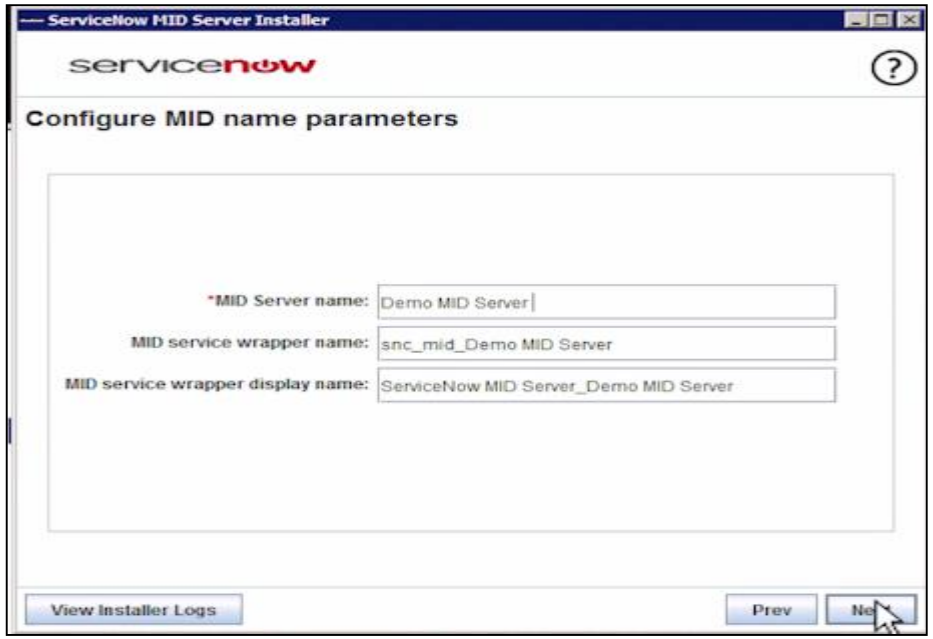
ITOM - Midserver

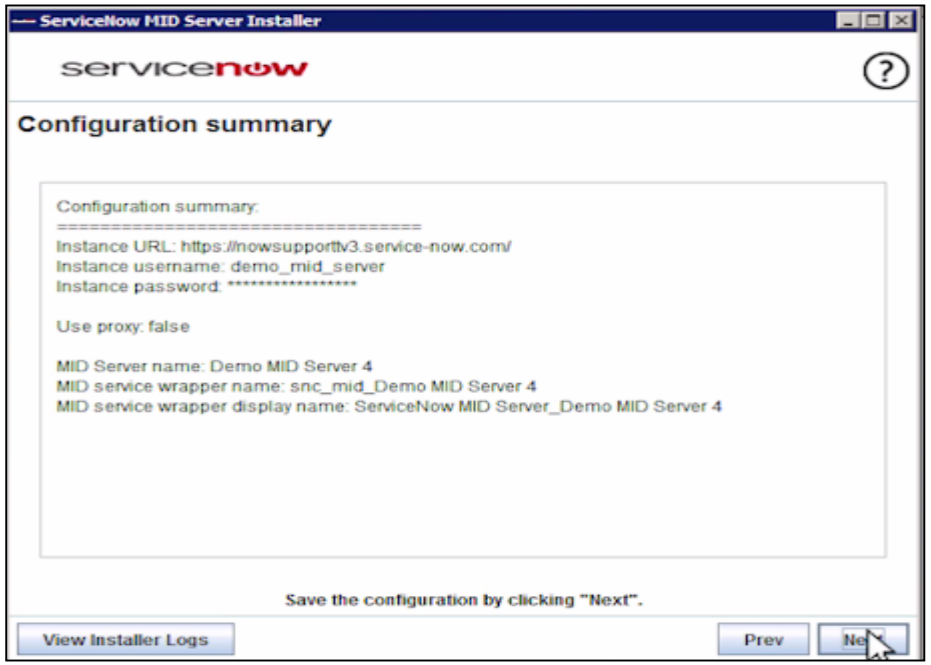
- After the installer has run login midserver username and password we created earlier in configuration step.
- Test our connection and verify it is tested successfully and continue to next step



ITOM - Midserver

- Give a name to Midserver Demo Midserver 1 and SNOW uses supplied values for other field.
- Verify the configuration summary and click next.



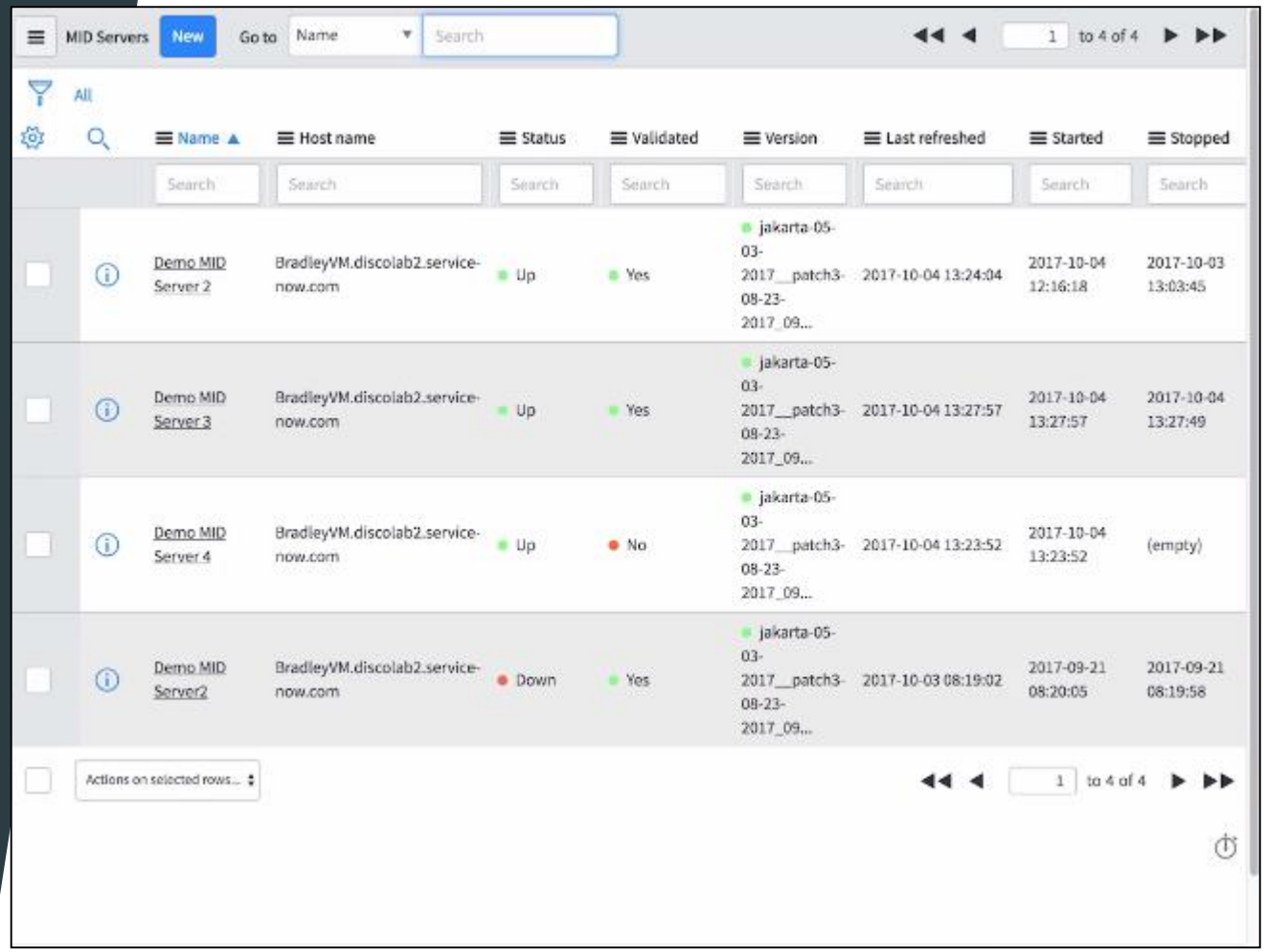


ITOM - Midserver

- Finally start the Midserver which completes the installation.Mark this complete.
- This complete setup is done on the host in Enterprise Network.Now switch back to local browser.
- Reload the page and mark the step as complete

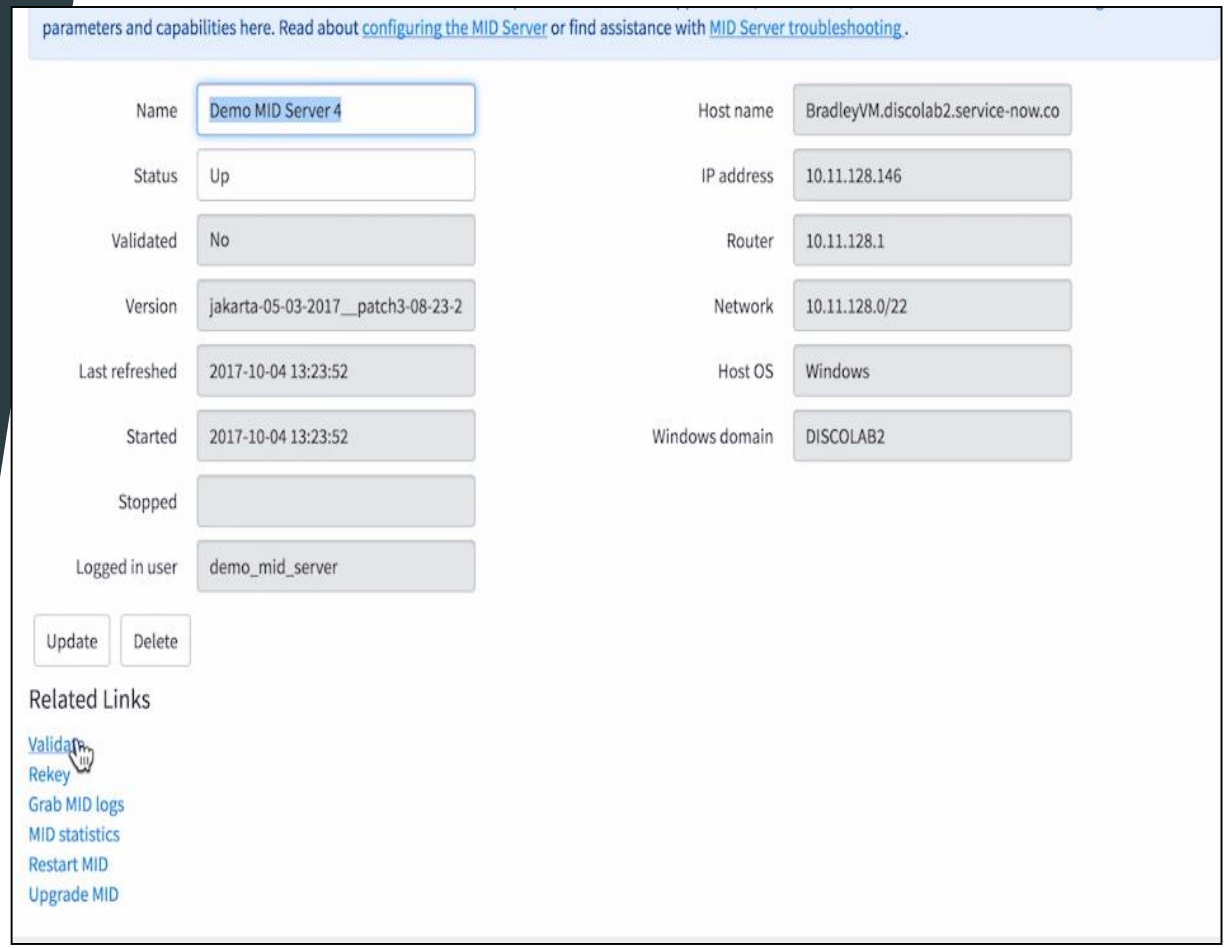
ITOM - Midserver

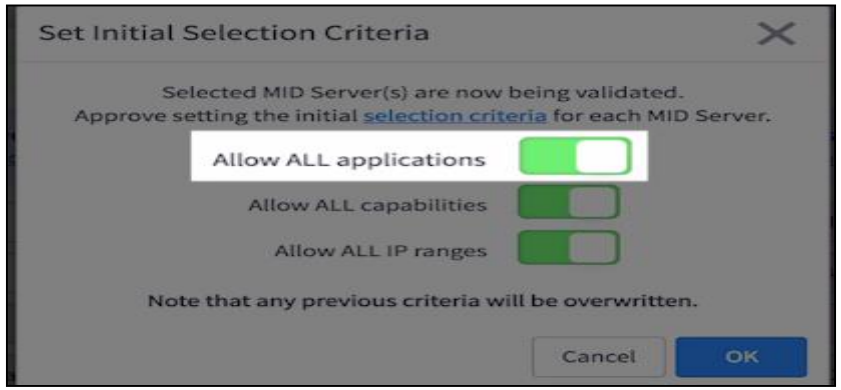
- Next step is Validate Midserver. This security features ensures only those midservers that are validated by the instance can communicate with the instance.
- Click configure and we can check list of midservers running on the server.



ITOM - Midserver

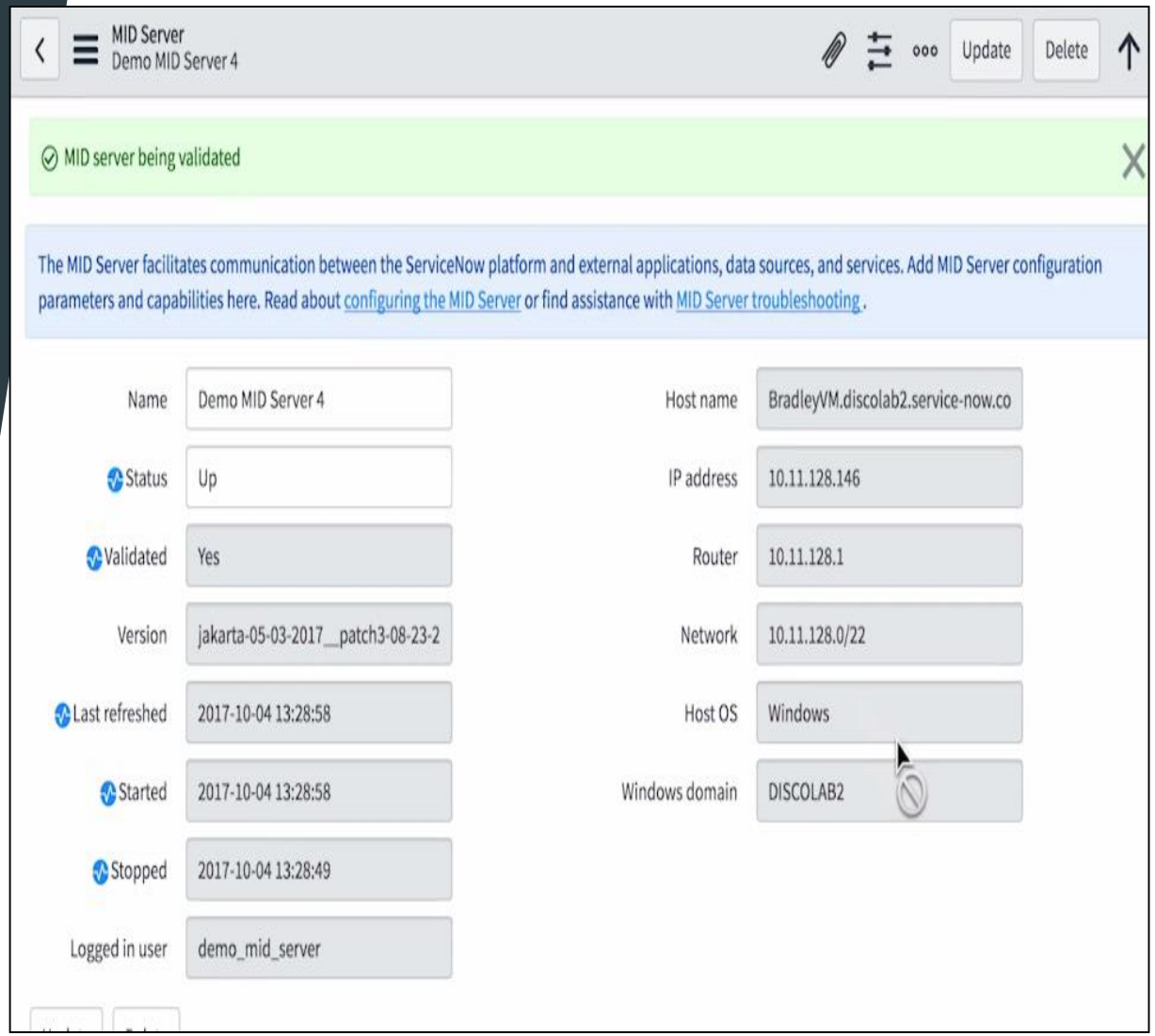
- Open the form for Midserver and Click on Validate.
- The selection criteria setting ensures which application can use the currently configured Midserver. The other Capabilities setting include SNMP,VM Ware,Power shell to be included.
- The other setting is which IP Addresses the Midserver can reach within the enterprise network or cloud





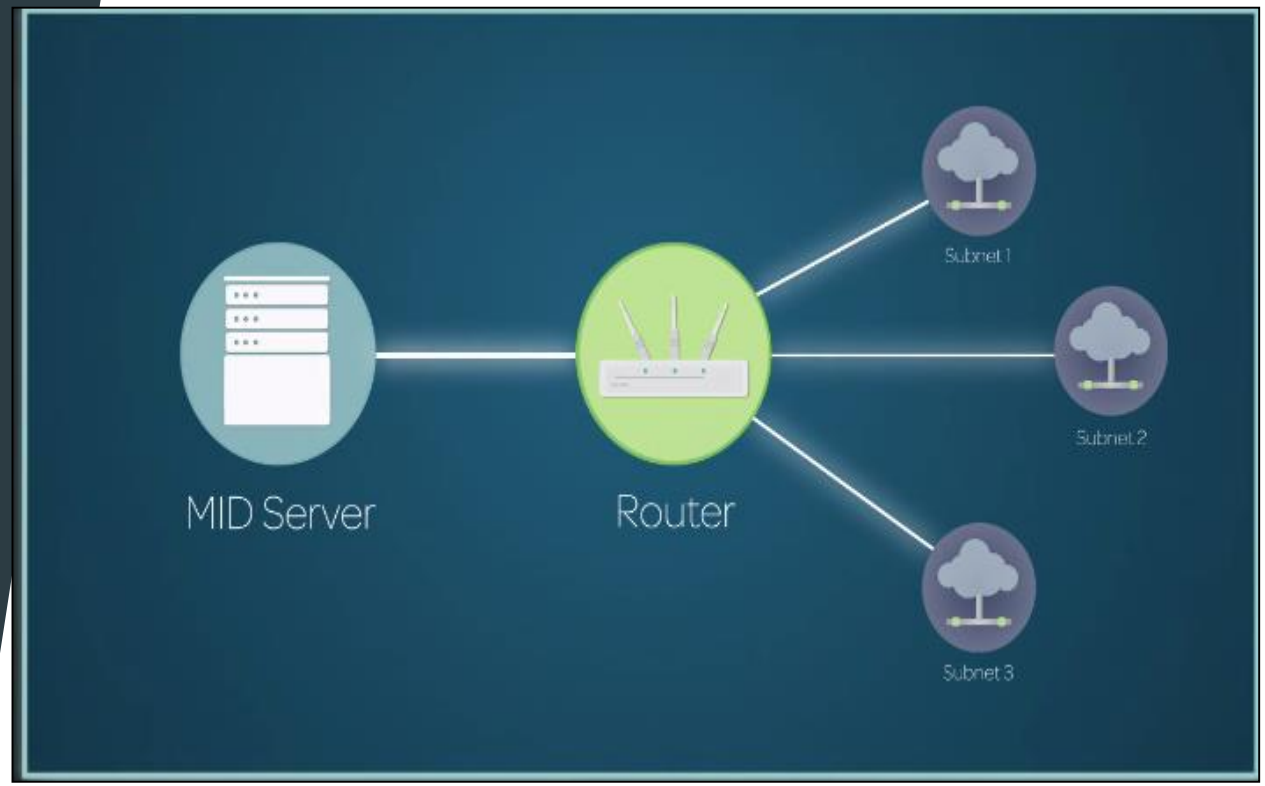
ITOM - Midserver

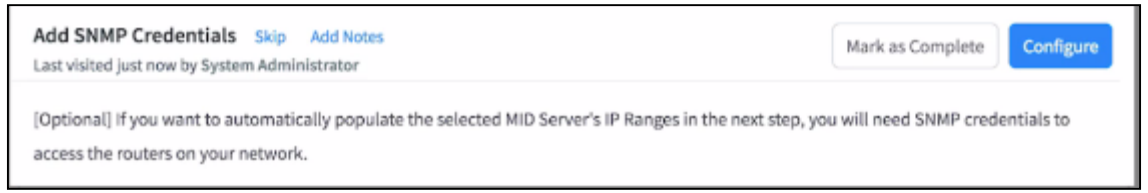
- Validation takes few minutes when the Midserver is validated we find the field in Midserver form having validated field yes populated



ITOM - Midserver

- We will go ahead and assign IP address ranges for subnetworks that the MID Server can connect to.Guided setup does that automatically by discovering subnets.
- Inorder to discover subnets MID server needs SNMP (Simple Network Management Protocol)credentials to log on to network devices.Ensure it has required persmissions as mentioned in MID server product documentation



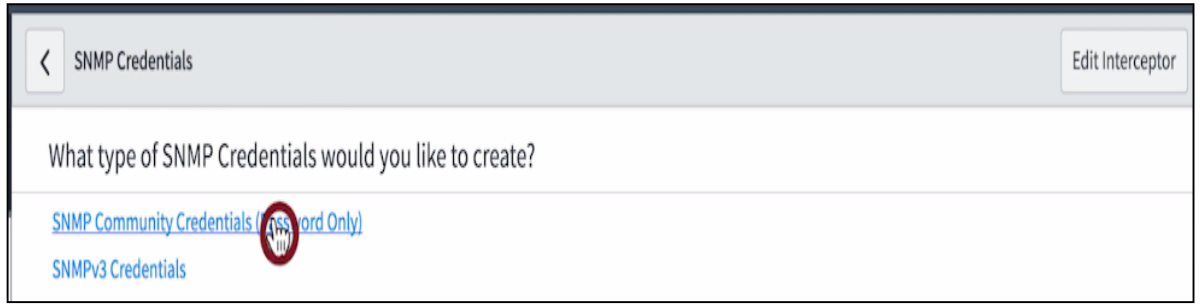


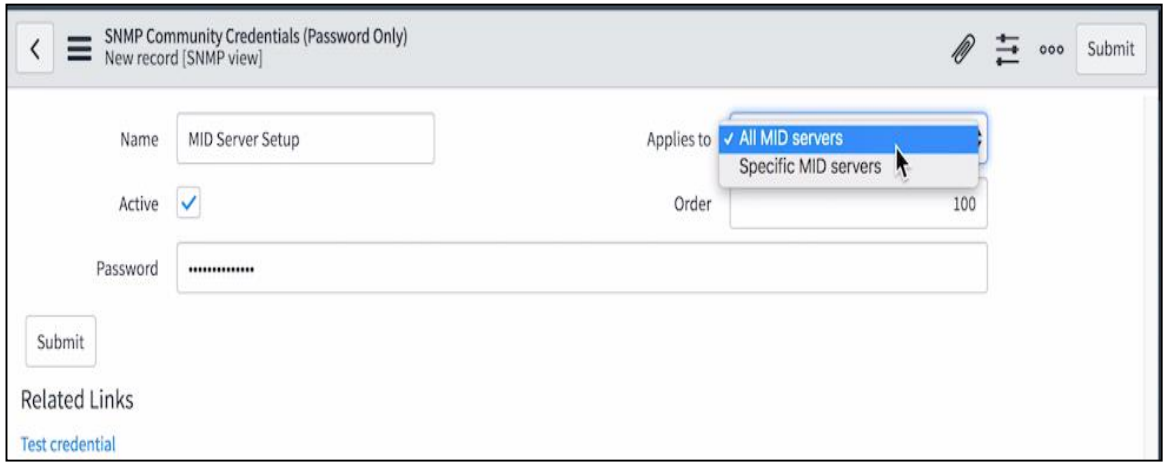
ITOM - Midserver

- Configure SNMP Credentials and click New Credentials and choose SNMP Community Credentials(password only) and give name for credentials
- Name : MID Server Setup

  Passoword:****

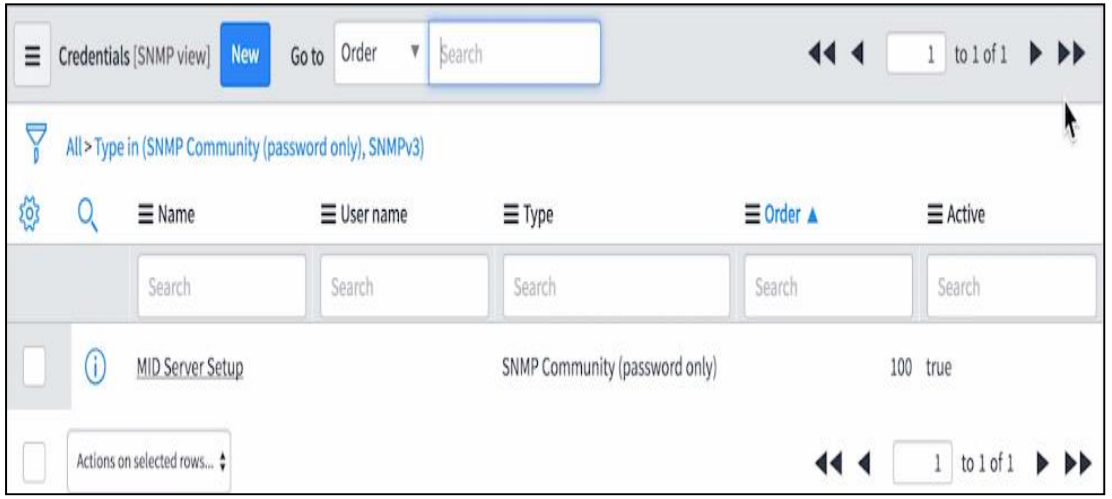
  We can choose specific MID servers
- Click Submit

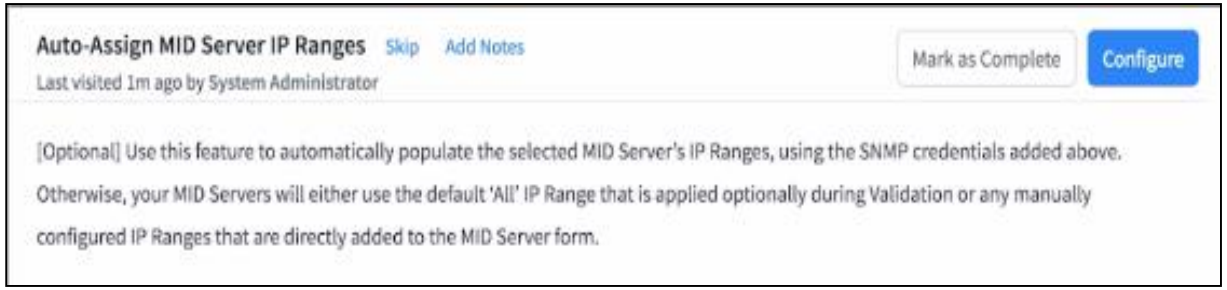




ITOM - Midserver

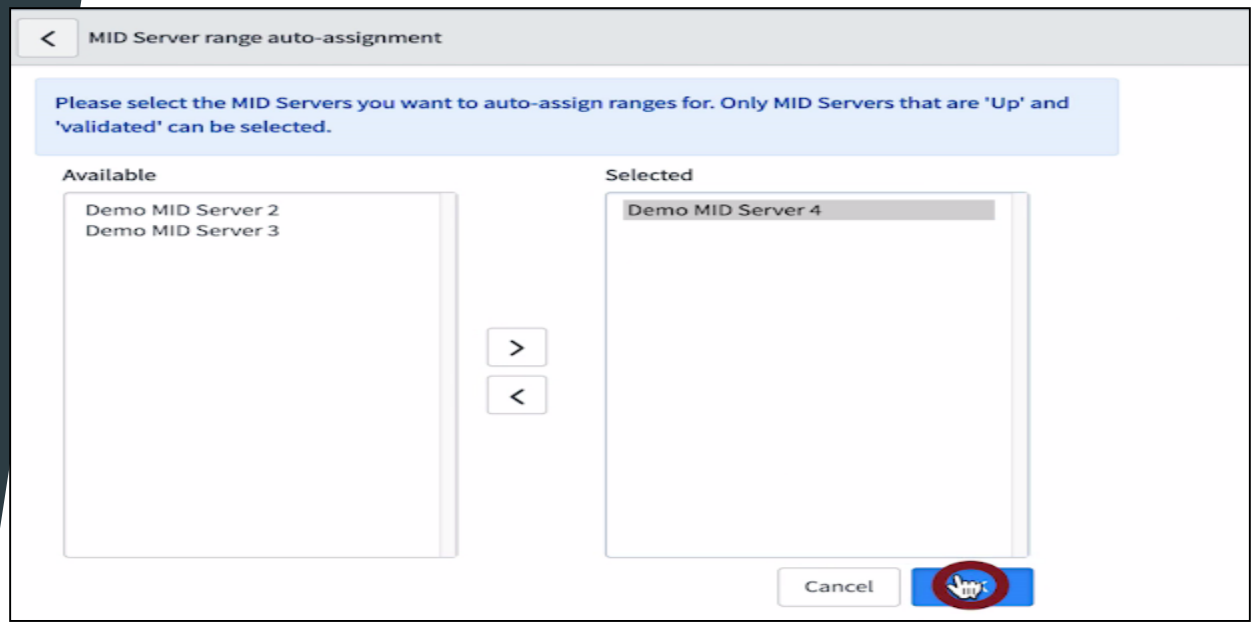
- We observe the new credentials submitted in the list.
- Now lets observe system automatically assigning IP ranges for MID Server.These are the subnets that midserver can reach inorder to interact with the endpoints.

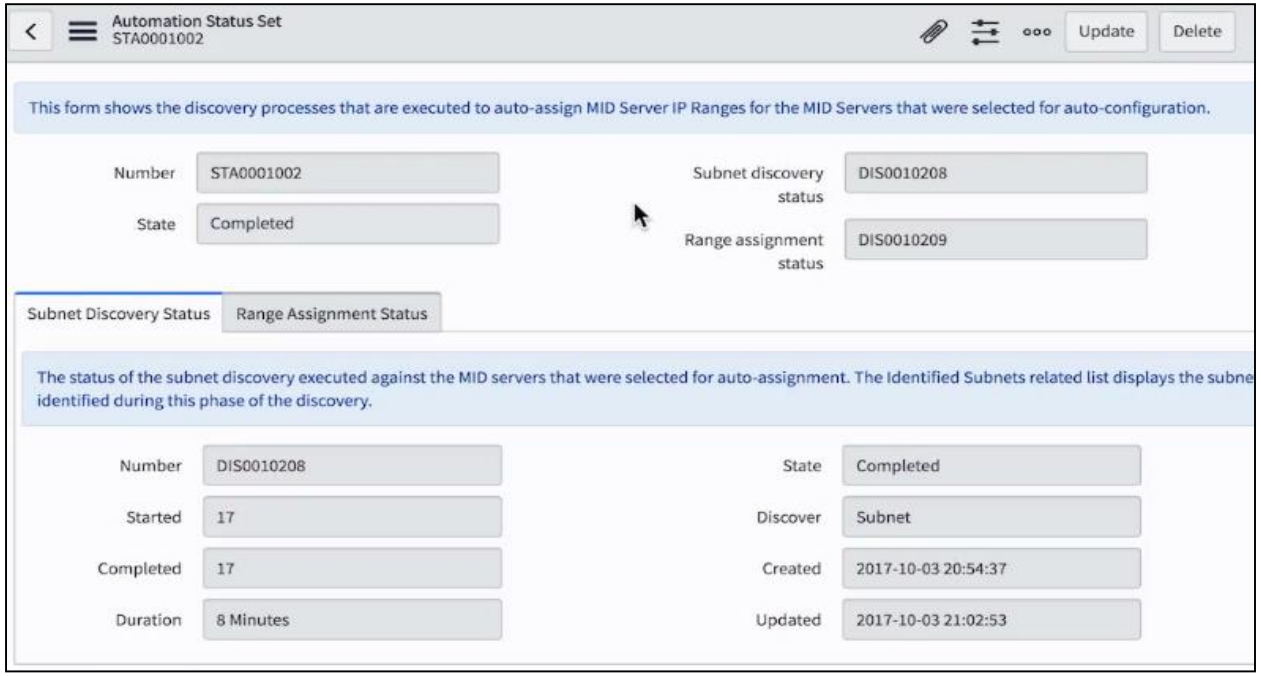




ITOM - Midserver

- **Configure it and choose the Demo mid server we created earlier.we can choose all MID servers which are validated**
- The next form helps in monitoring the process.The entire process can take few hours depending on size of network and would complete in state field in the Automation Status Set form





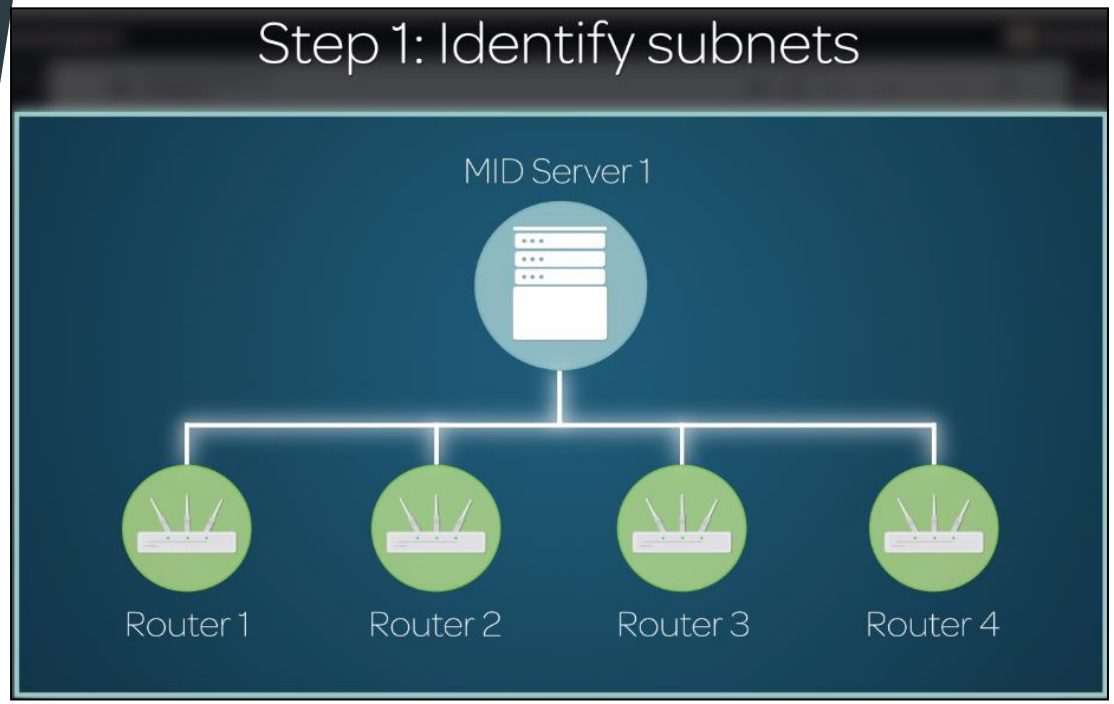
ITOM - Midserver

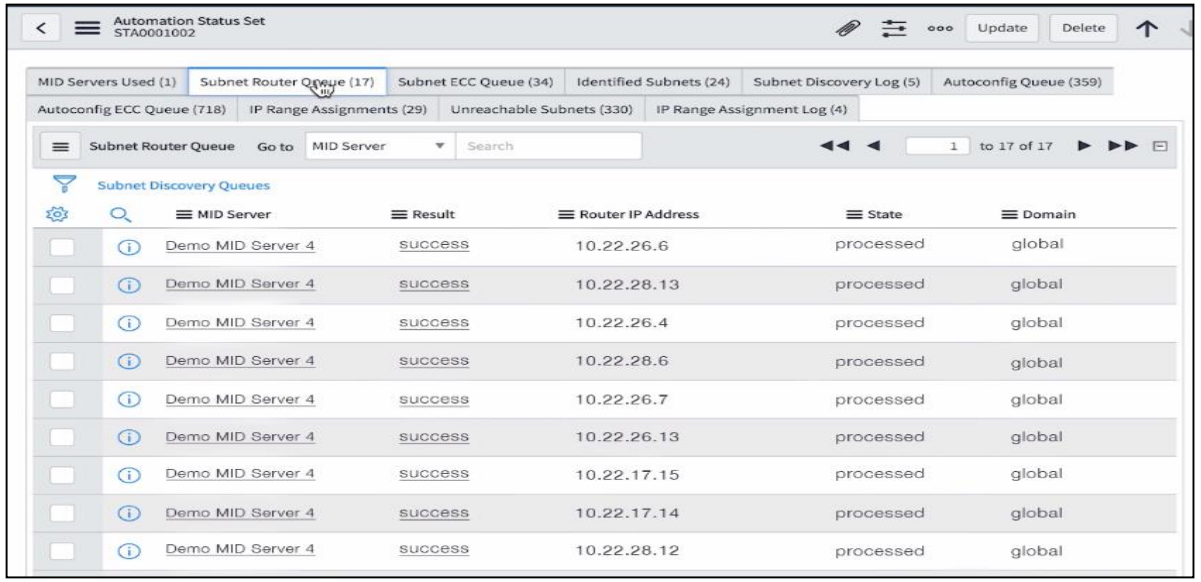
- The assignment process has 2 steps

  Step 1 : Identify the subnets that the MID server can access

  To achieve this MID Server searches the network for all the routers that it can login to using the SNMP credentials that we define in the previous task.

- The routers are listed in the related links in Subnet Router Queue

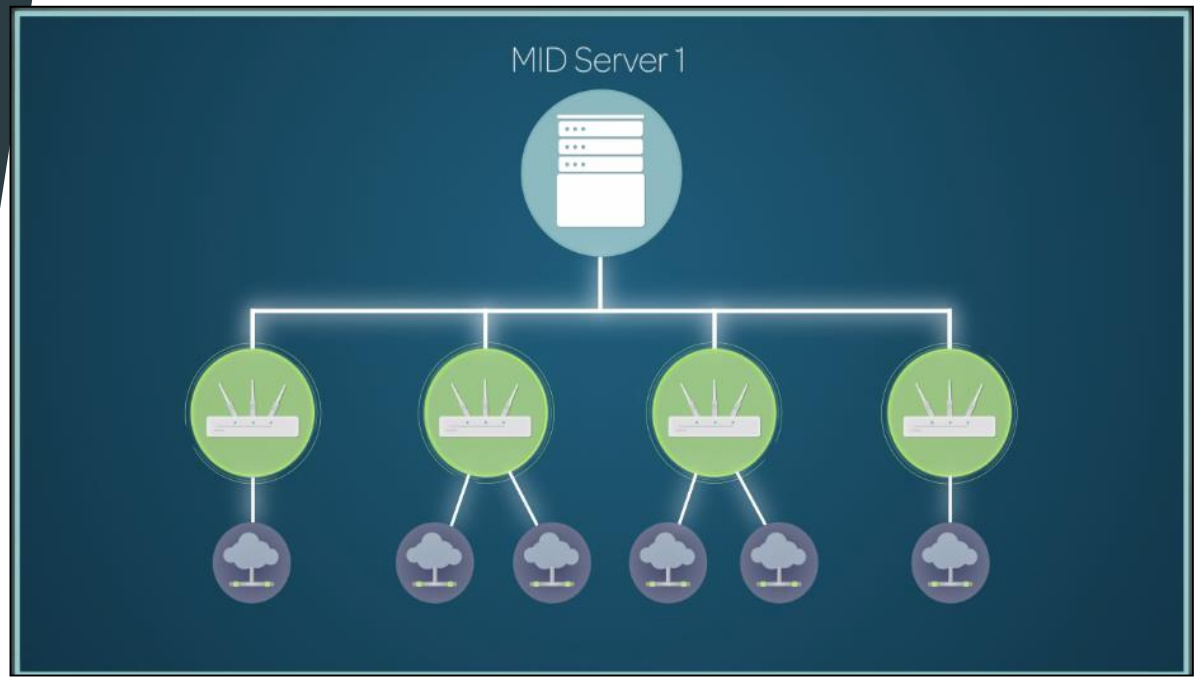


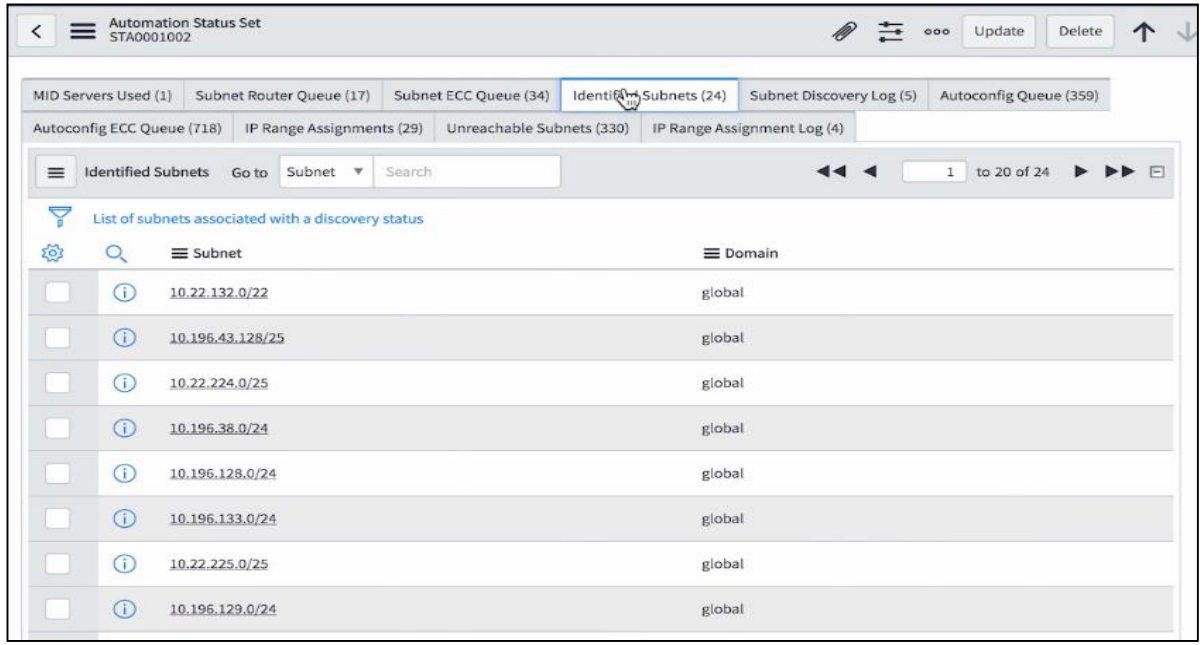


MID Server	Result	Router IP Address	State	Domain
Demo MID Server 4	success	10.22.26.6	processed	global
Demo MID Server 4	success	10.22.28.13	processed	global
Demo MID Server 4	success	10.22.26.4	processed	global
Demo MID Server 4	success	10.22.28.6	processed	global
Demo MID Server 4	success	10.22.26.7	processed	global
Demo MID Server 4	success	10.22.26.13	processed	global
Demo MID Server 4	success	10.22.17.15	processed	global
Demo MID Server 4	success	10.22.17.14	processed	global
Demo MID Server 4	success	10.22.28.12	processed	global

ITOM - Midserver

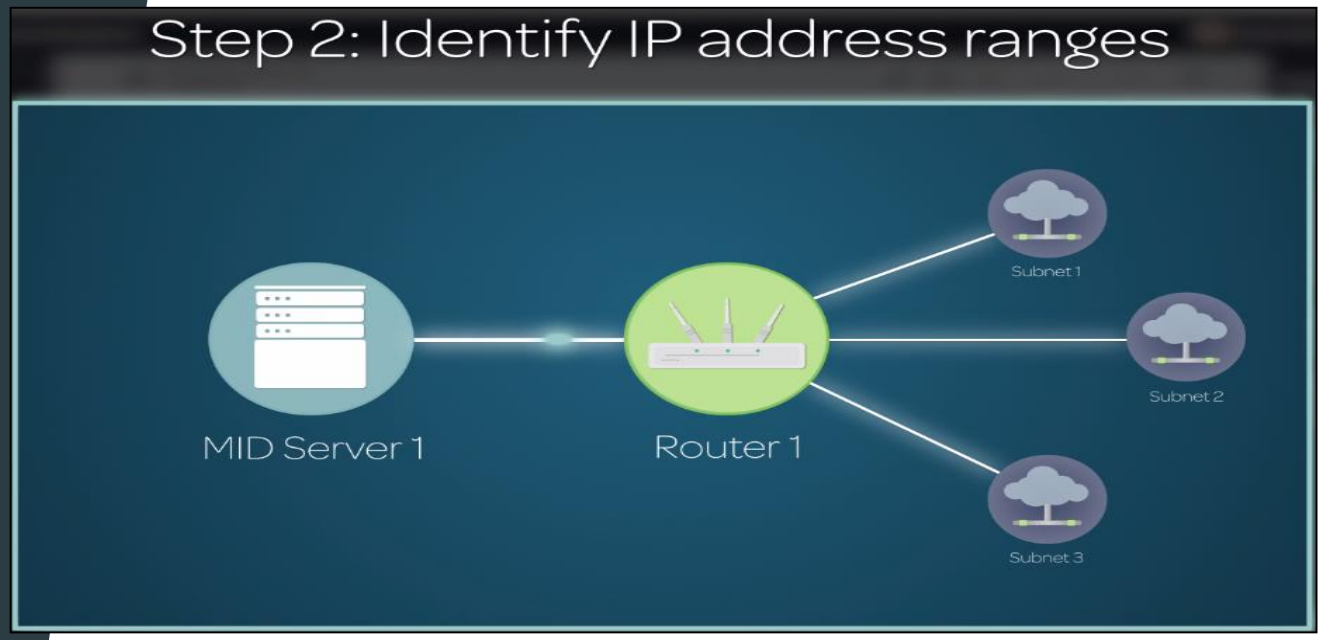
- Midserver reads the routing table on each Router to identify the subnets known to the Router.
- Those subnets are listed in the Identify Subnets tab of Related links

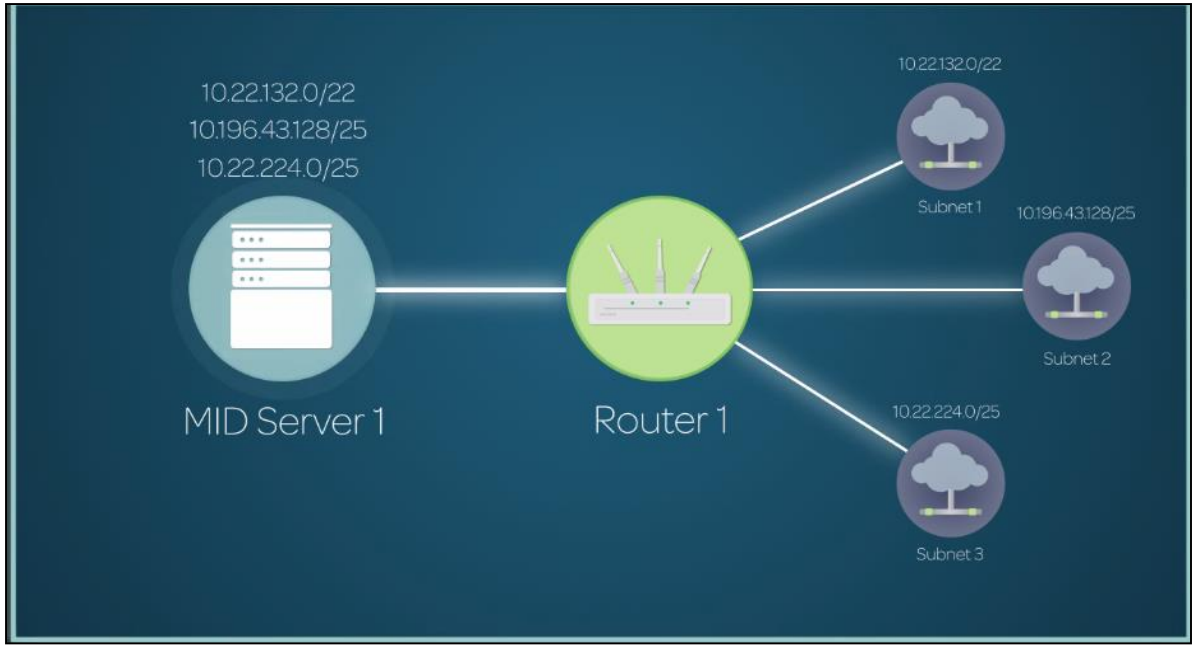




ITOM - Midserver

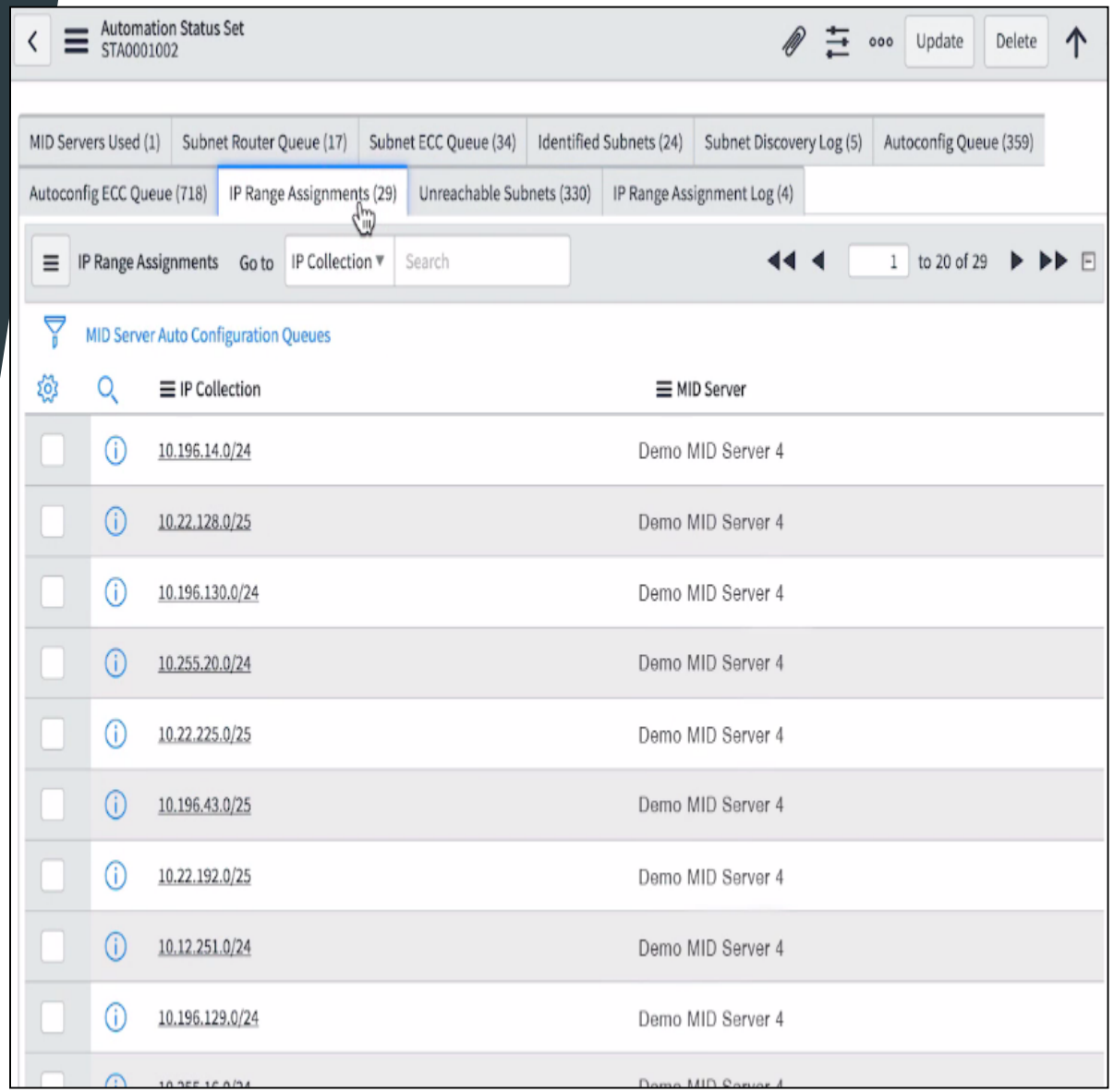
- Second step is Identify IP address ranges that can be reached by the MID Server and assign them to the MID server.
- In this step MID server tries to access each subnet for their IP Address.





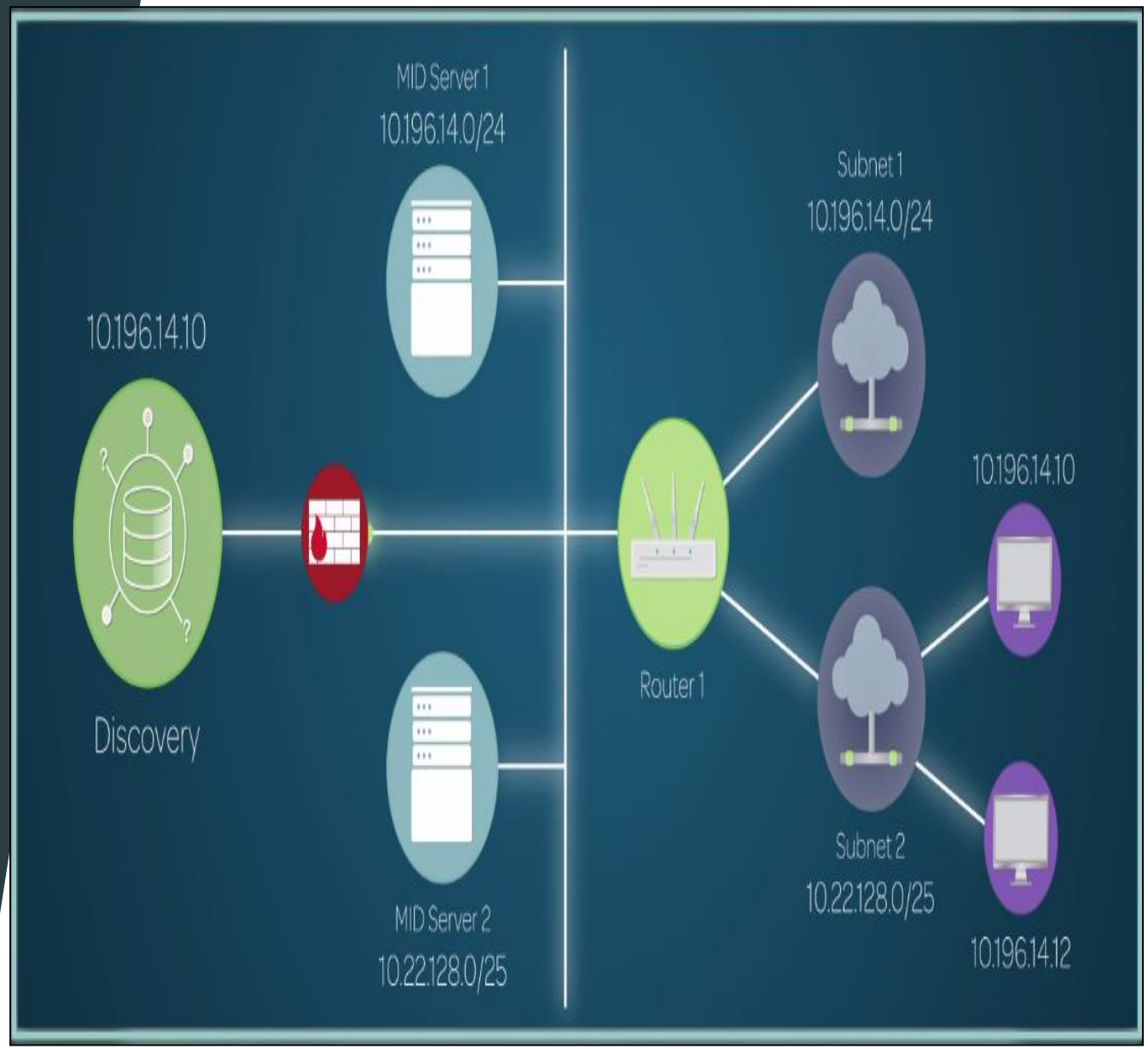
ITOM - Midserver

- Those IP address identified is listed in IP Range Assignments tab in Related links



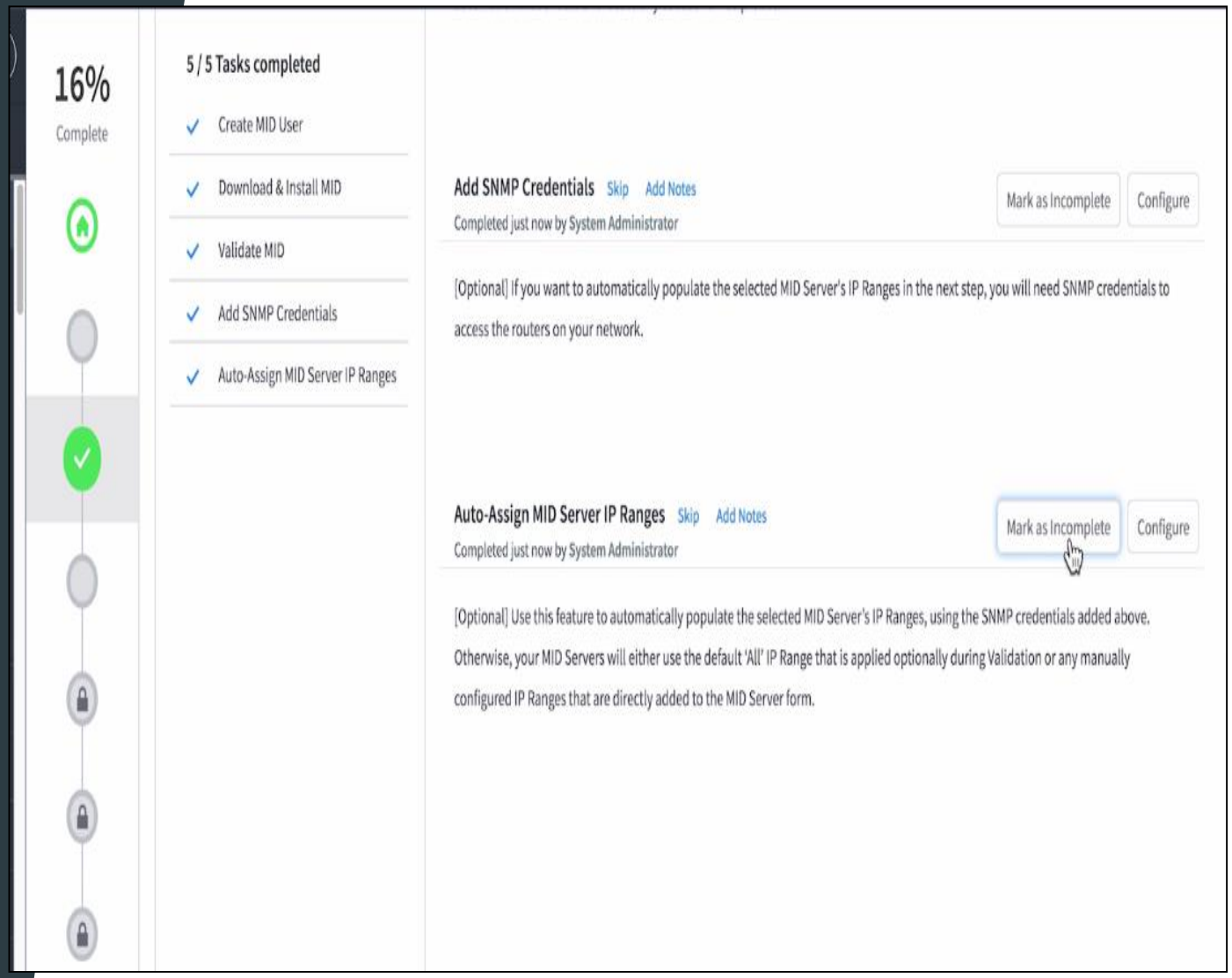
ITOM - Midserver

- When application like Discovery or service mapping needs to access particular target in the enterprise network,it chooses a MID server to include whose assigned ranges include the target address.
- If there any subnets that cannot be reached it populates in the Unreachable Subnets.(we may have to add another MID server to reach these subnets)



ITOM - Midserver

- **Mark the task for Auto Assign as complete**
- Now we can setup applications like Discovery and Event management which use the Midserver for its communication.



ITOM – Discovery with Service Mapping

- We will look at setting up Discovery and would be covering topics related to

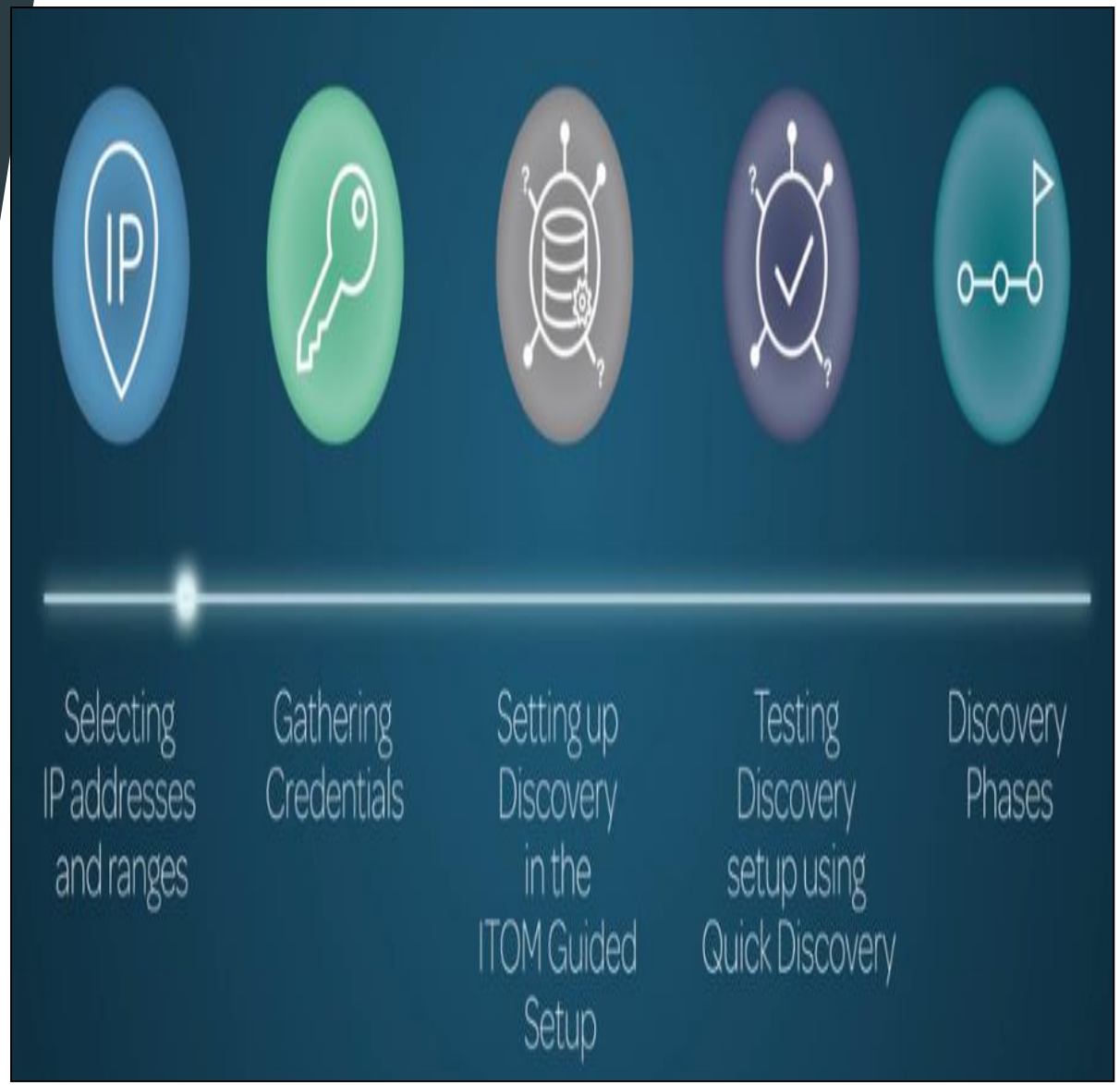
  - Selecting IP Addresses and ranges

  - Gathering Credentials

  - Setting up Discovery in ITOM Guided setup

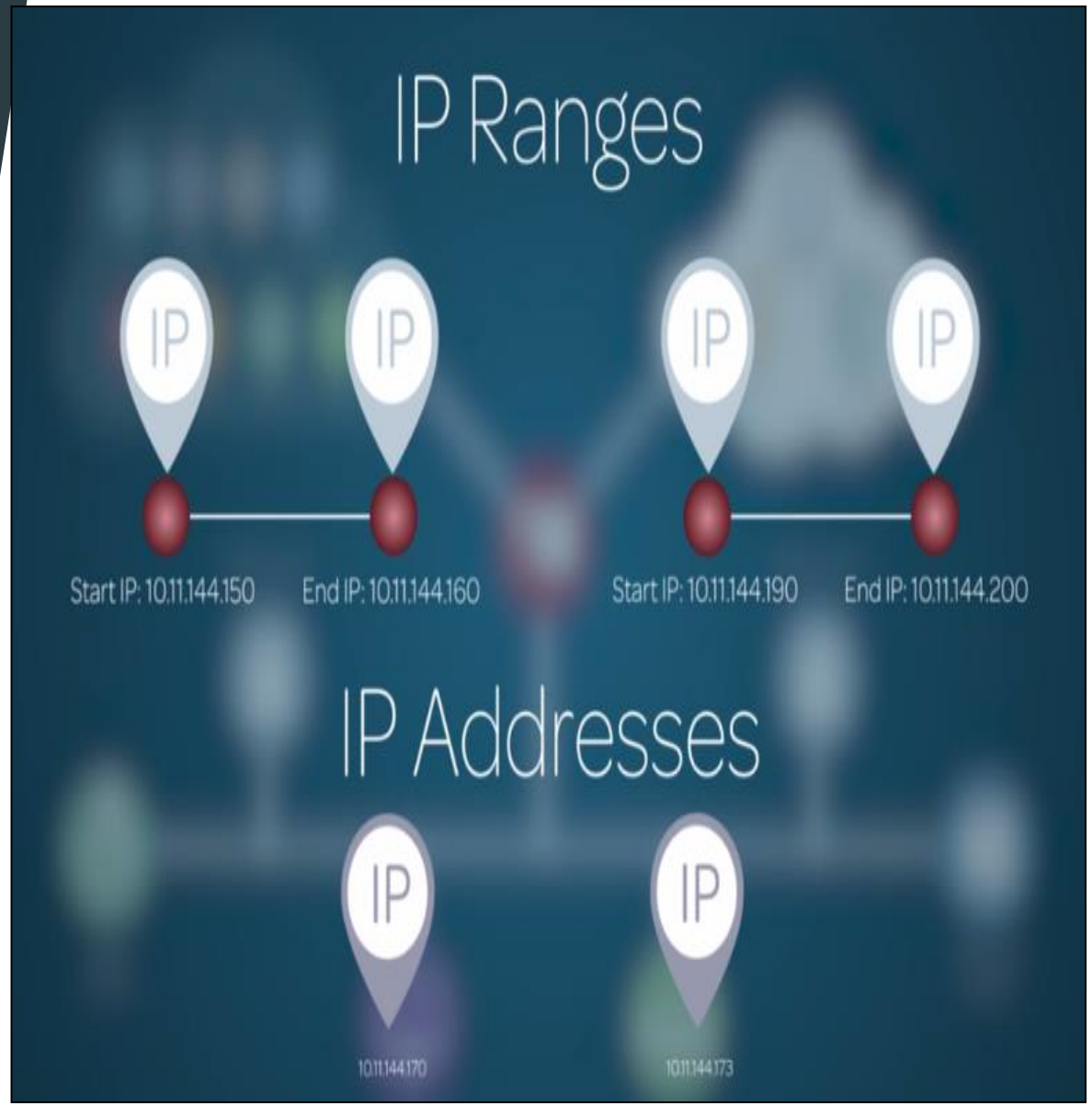
  - Testing Discovery setup using quick discovery

  - Discovery Phases



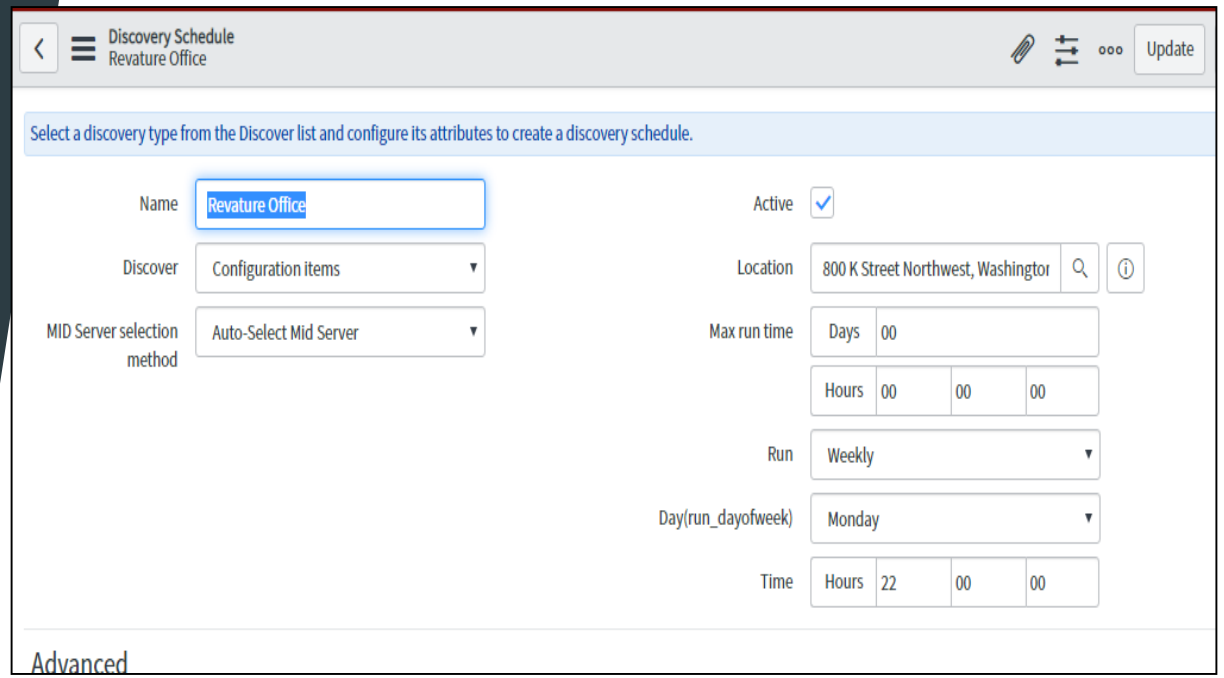
ITOM – Discovery with Service Mapping

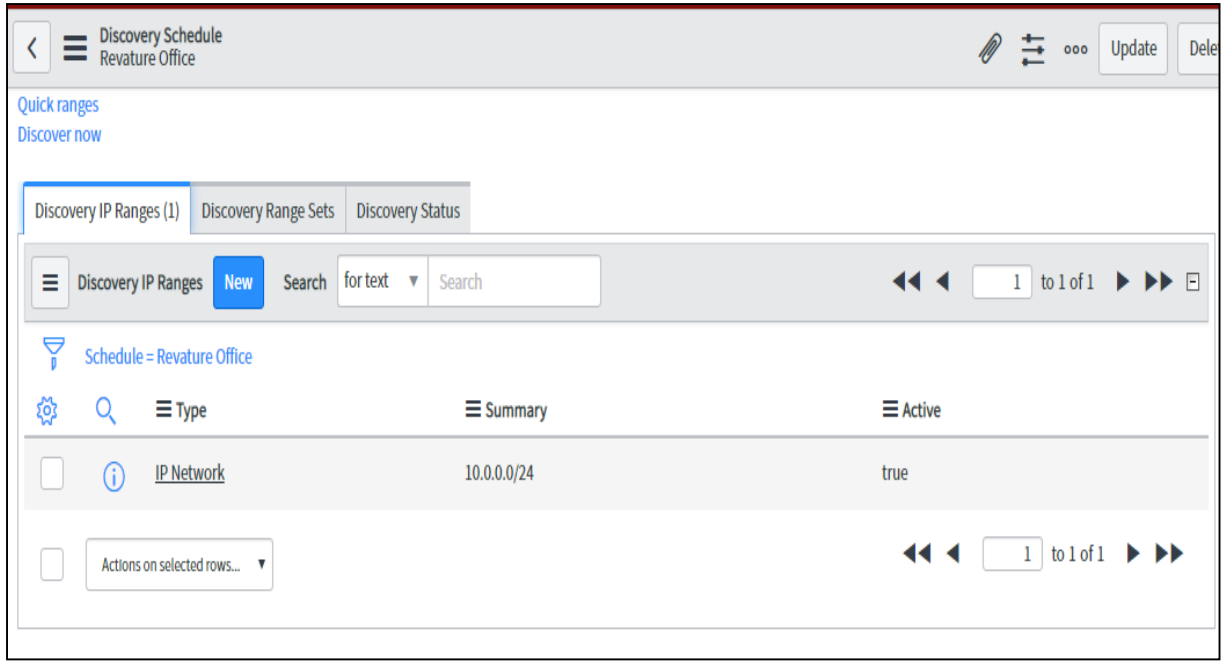
- To setup Discovery,we need to determine IP Ranges and IP Adresses in the network which you need to include in the Discovery.
- IP Auto Assignment feature helps identify IP Addresses reachable by Midserver
- Best practice is to include IP Addresses in Range set where it restricts SNOW discovery not to scan outside the range set



ITOM - Discovery

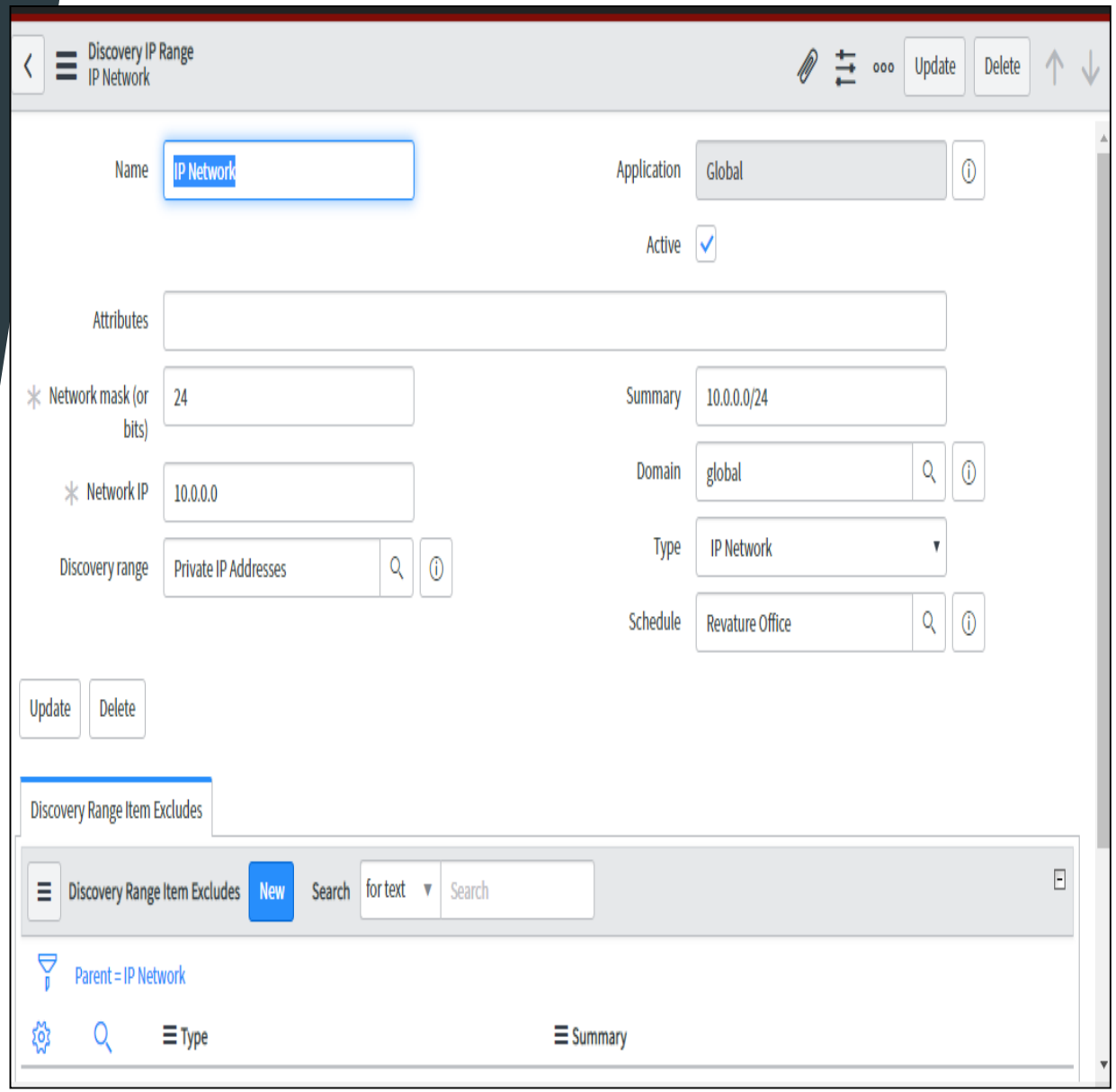
- Navigate to Discovery Schedules → Create new schedule in Discovery schedules
- Save it.
- In related links Discovery IP Ranges for a schedule add new IP network





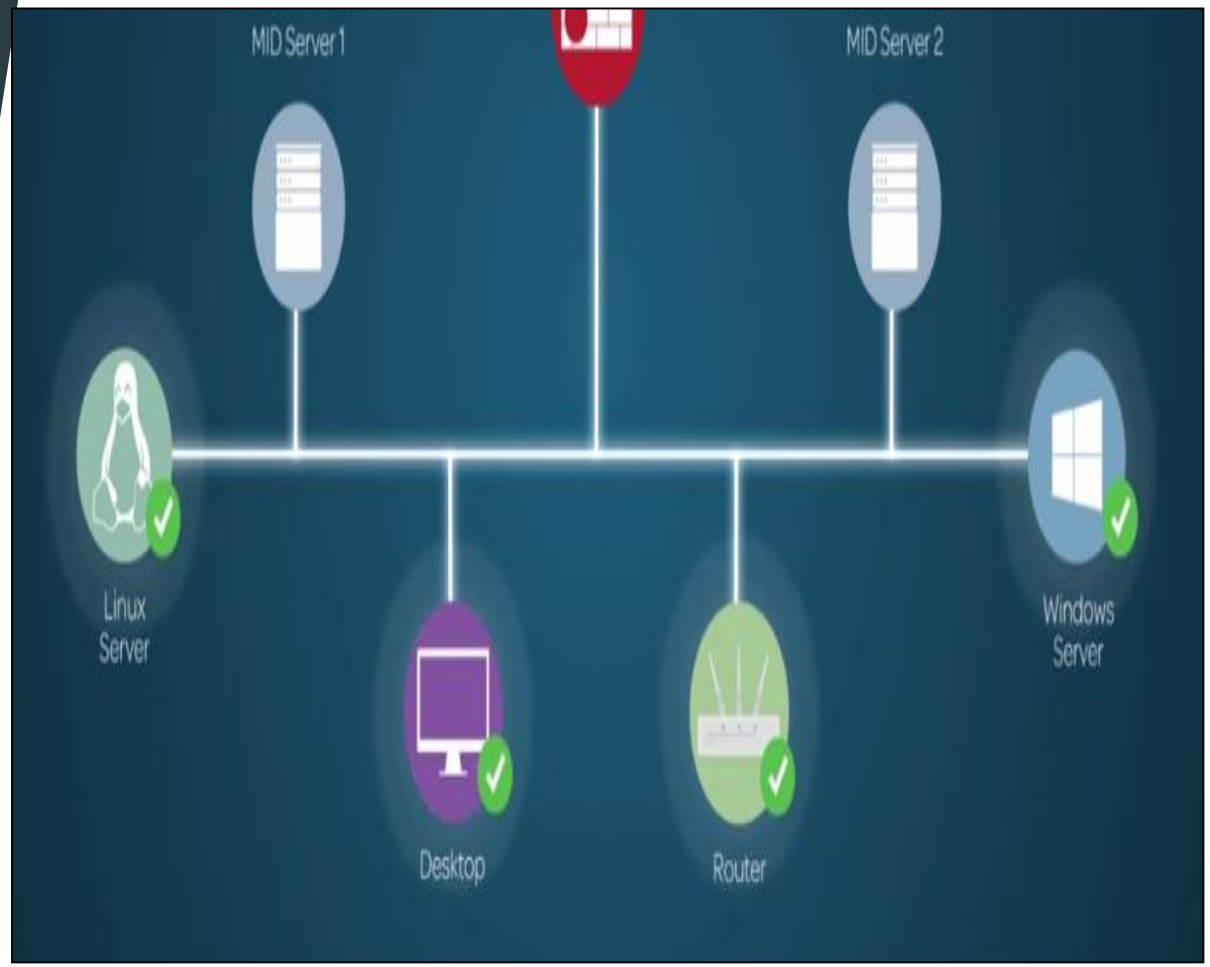
ITOM - Discovery

- After defining IP Range.we can exclude IP ranges for a schedule by including in related list of discovery Range Item Excludes.



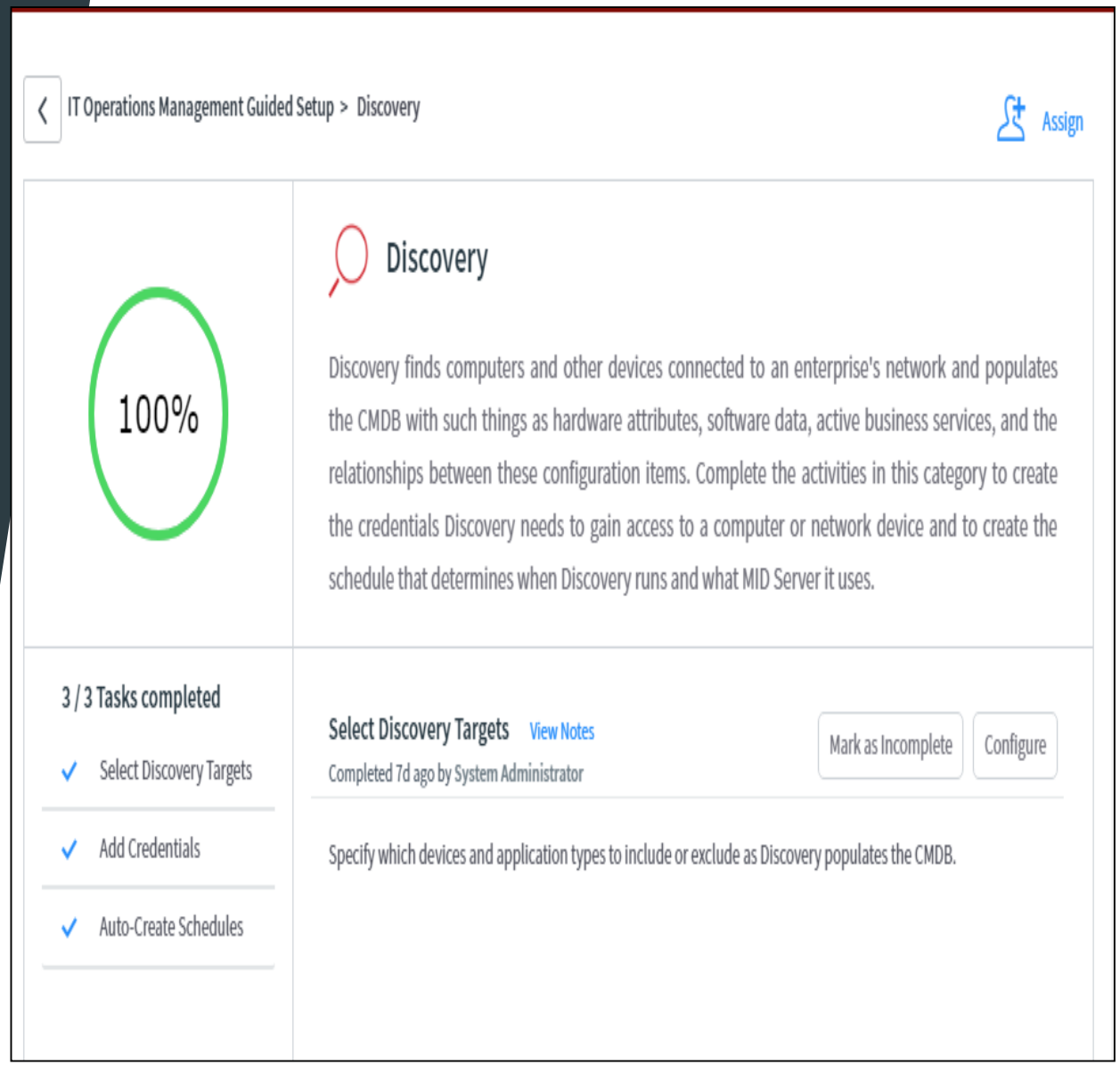
ITOM - Discovery

- Next step is to gather list of credentials for the devices on the network which you would want to discover including windows and unix computers.
- Midserver uses login credentials to query the devices otherwise it fails to discover them.



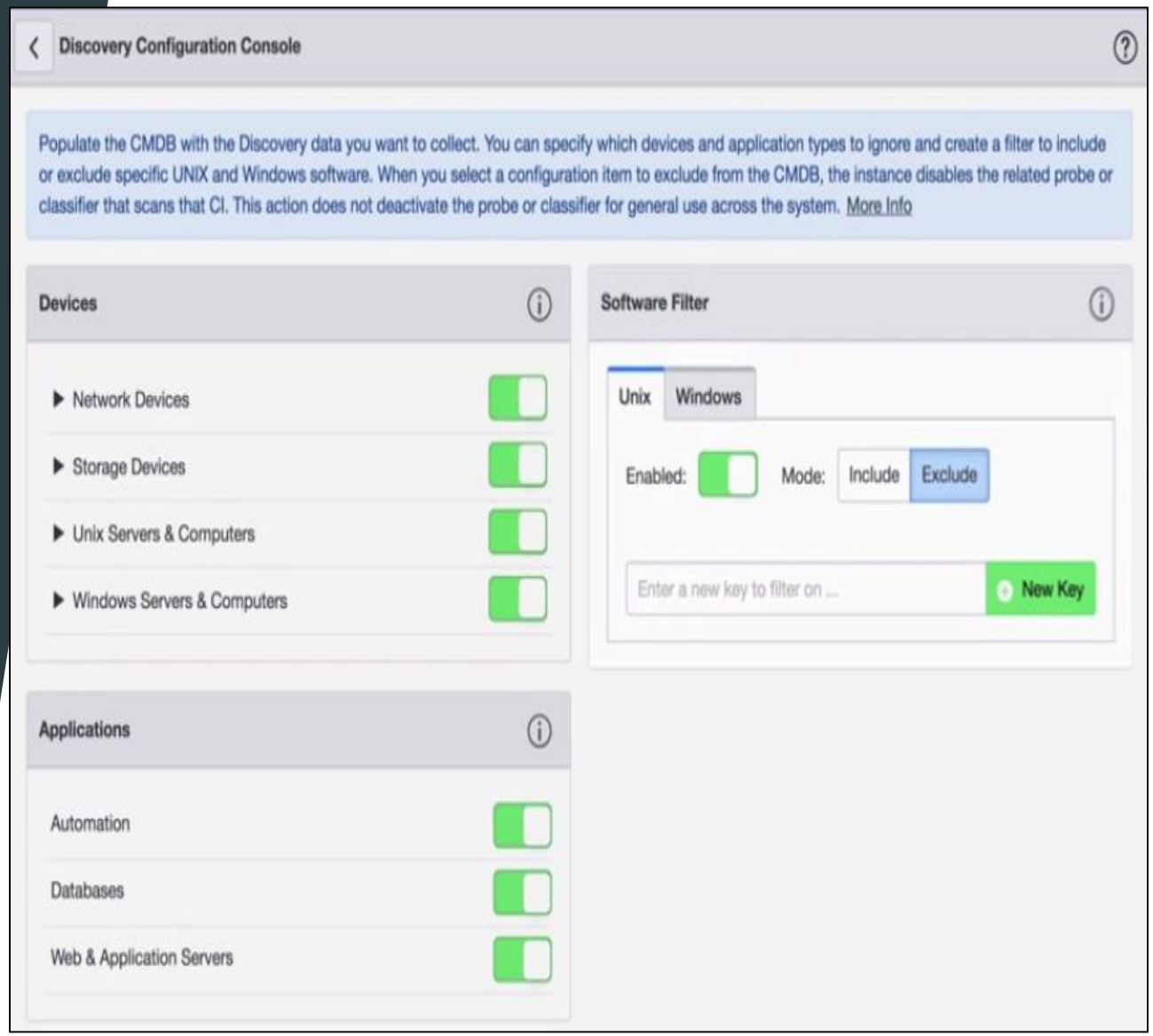
ITOM - Discovery

- Navigate back to ITOM guided setup.
- First step is to select Discovery targets



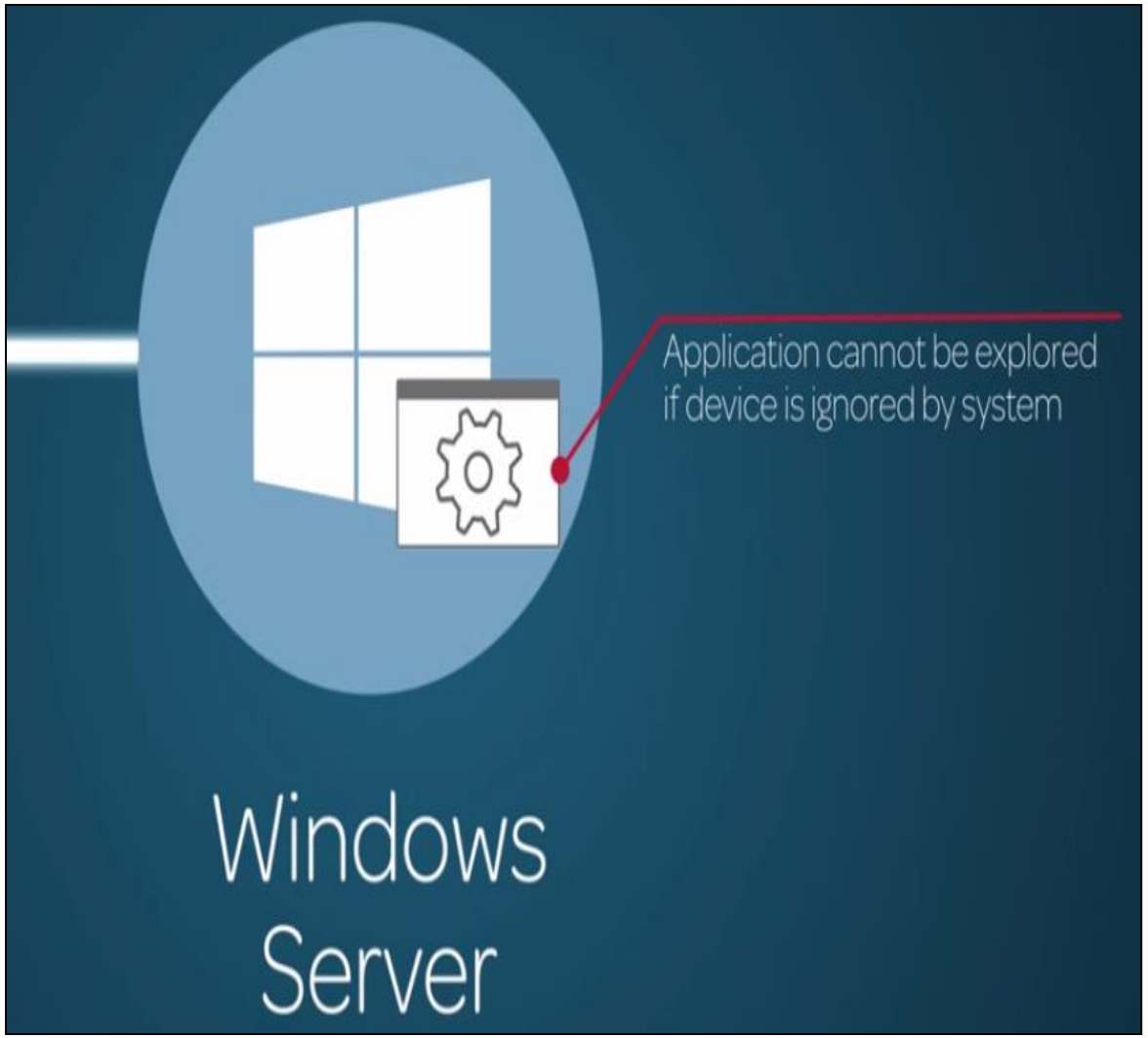
ITOM - Discovery

- We would normally specify which device types,Application types and software to include or exclude as Discovery populates the CMDB.By excluding items we can filter out what organization does not need.



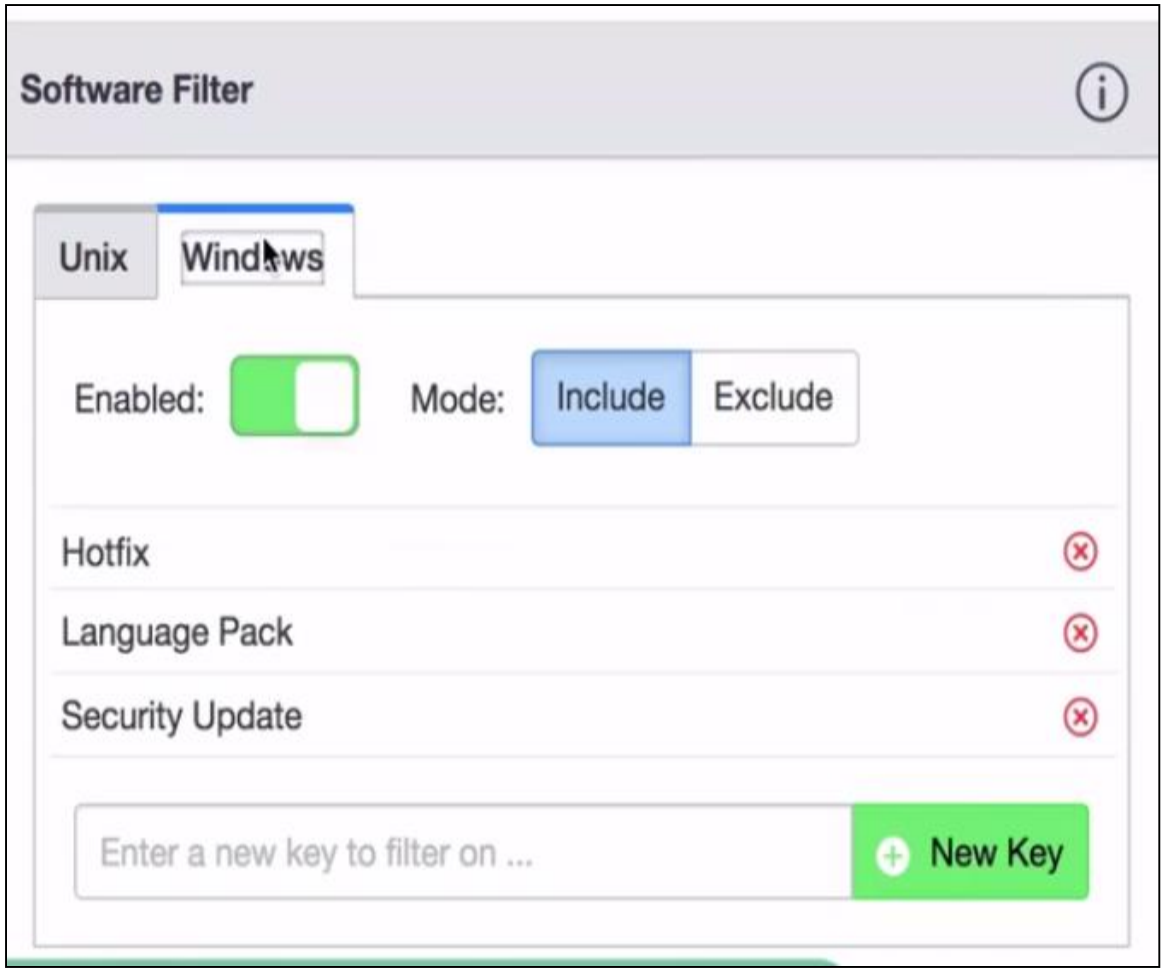
ITOM - Discovery

- In our example lets disable windows 200 and 2003 server that don’t exist.
- We can also disable applications but do keep in mind if the server is disabled applications under it would not be disabled



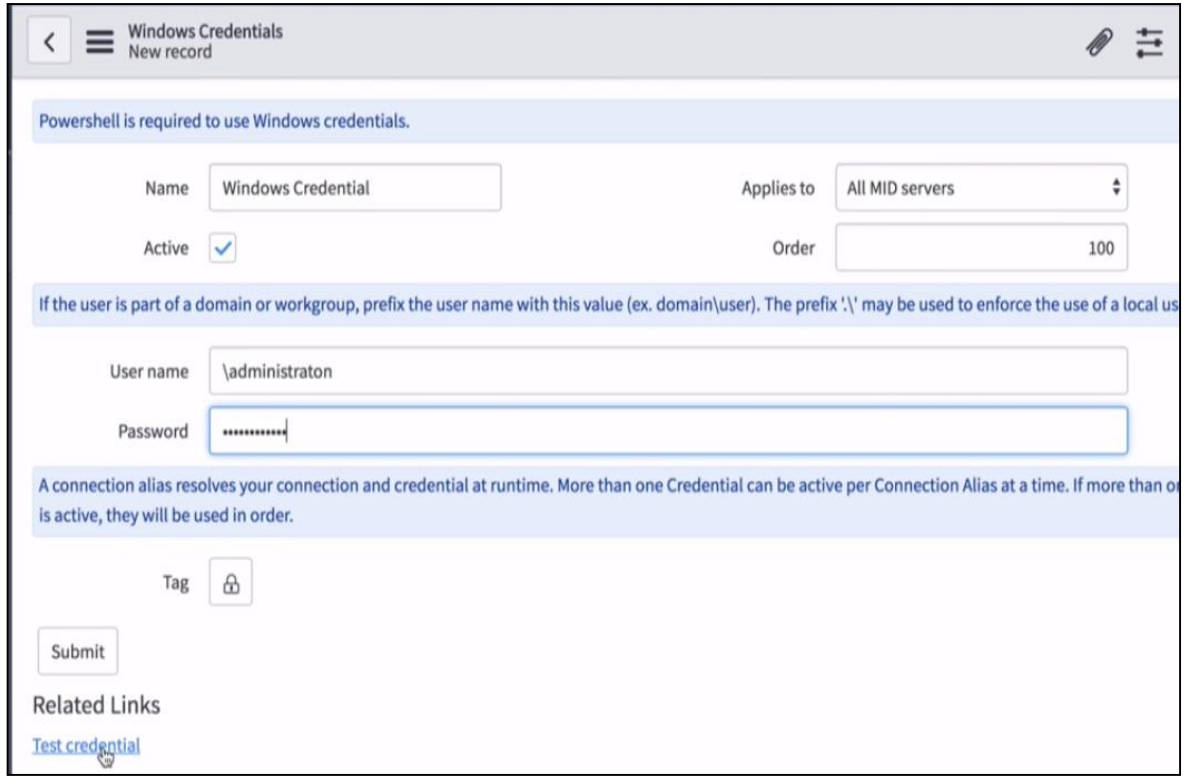
ITOM - Discovery

- Software filter allows you to filter the software's added to the CMDB using keywords.
- When the filter is disabled for the OS whole discovered softwares for that OS are not added to the CMDB conversely if the OS is enabled only softwares that includes or excludes with the specified keywords will be added to CMDB.
- In our example lets include by adding new key Hotfix,Language Pack and by Security update,critical update



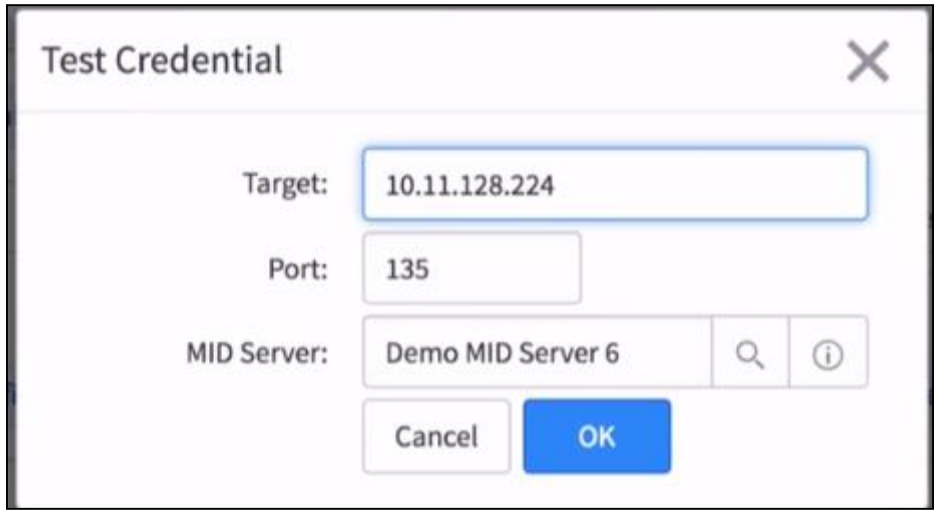
ITOM - Discovery

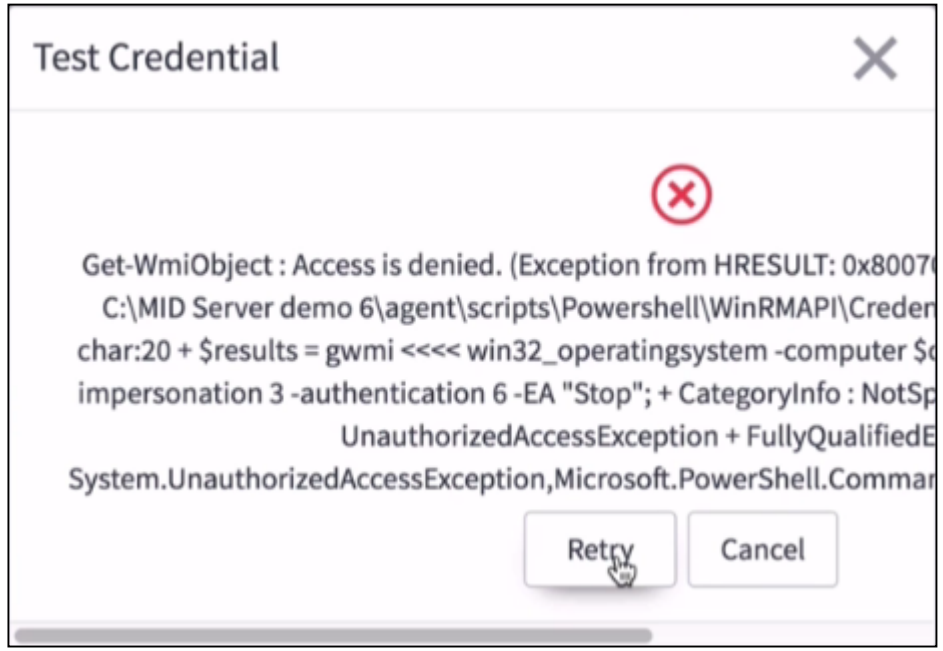
- Mark the step as complete and return to Guided setup.
- Next step is to add credentials.In our example lets add windows credentials
- For windows discovery credentials must be domain user with local admin privileges to the target you would need to discover.
- Many enterprise uses valid domain user like administrator(userid) as credentials for valid windows environment



ITOM - Discovery

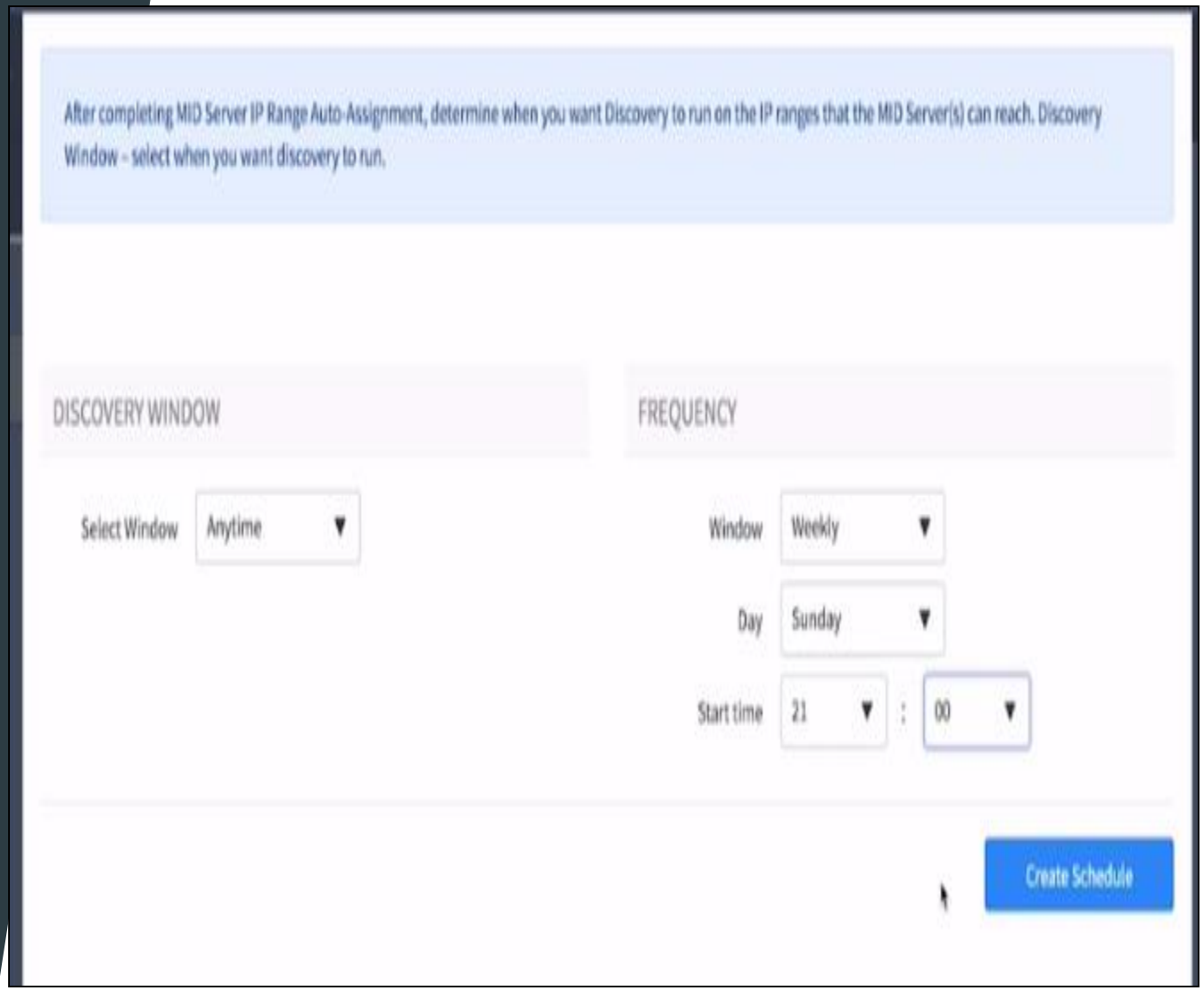
- **We can test credential for specific target on the specific IP address.The midserver and port field are pre-populated by system.**
- We can validate by inputting correct address
- As it is not running in domain access fails for the connection





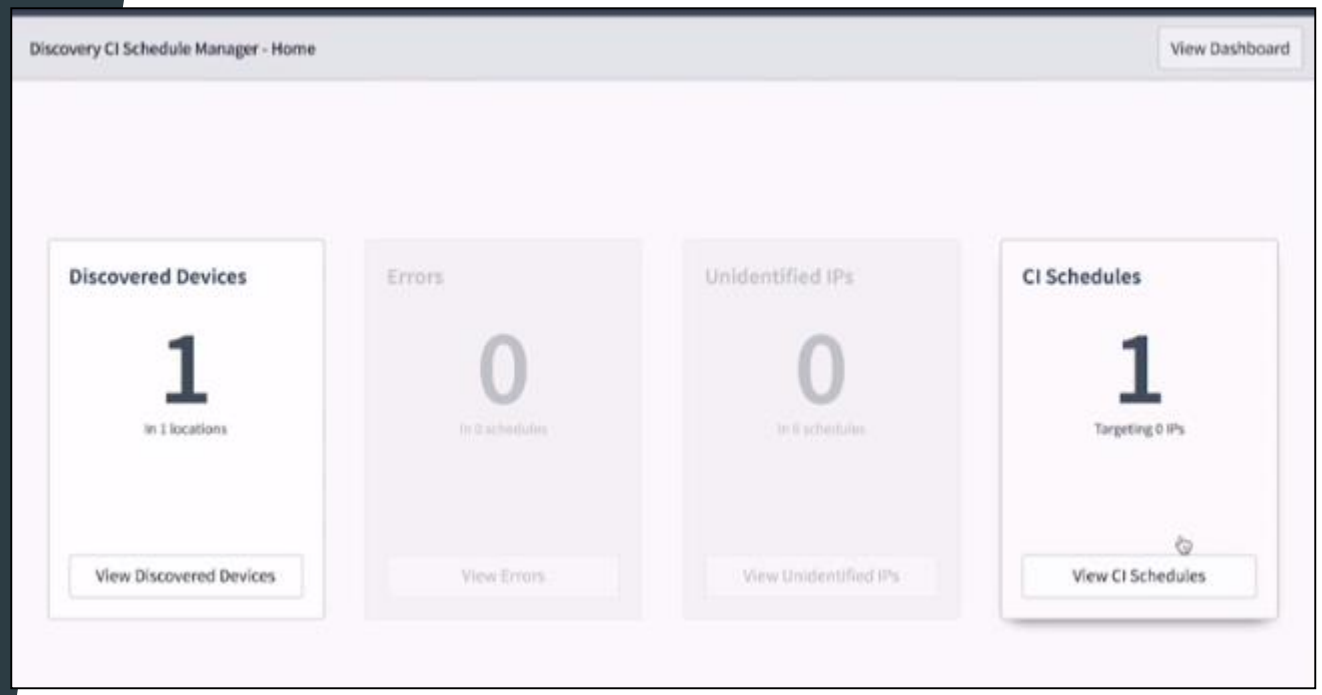
ITOM - Discovery

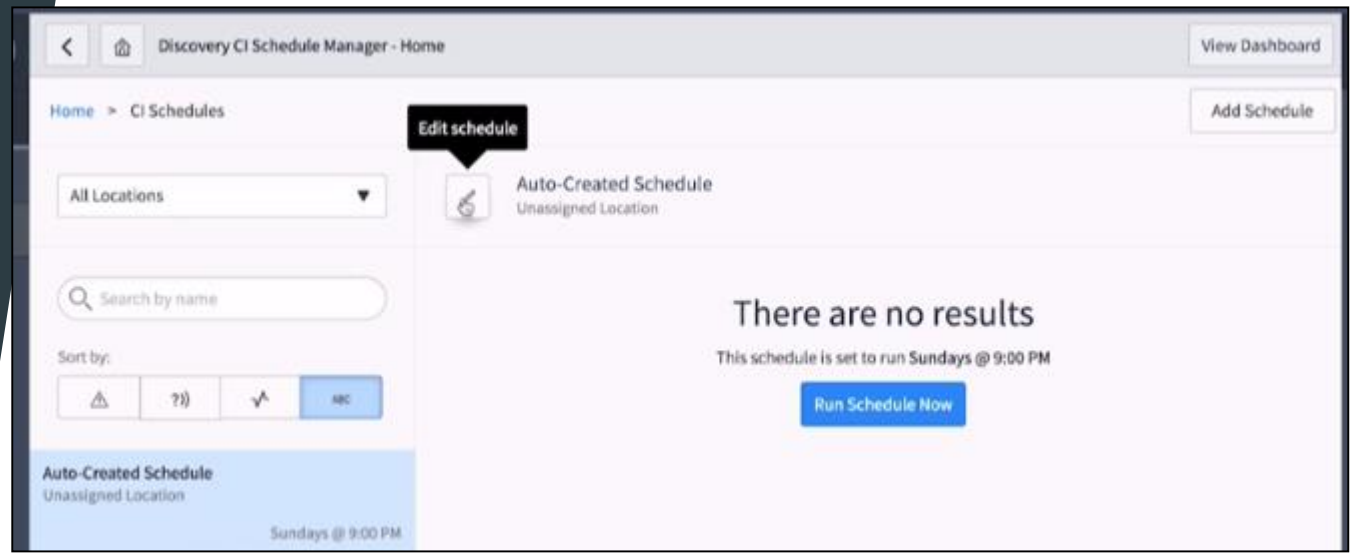
- Next step is to Auto create a schedule for discovery.
- Select the window you would want to run within and time options if its applicable.
- For demo lets create Window for weekly that runs Sunday at 9pm(SNOW uses 24 hr clock convention) relative to SNOW timezone settings.



ITOM – Discovery with Service Mapping

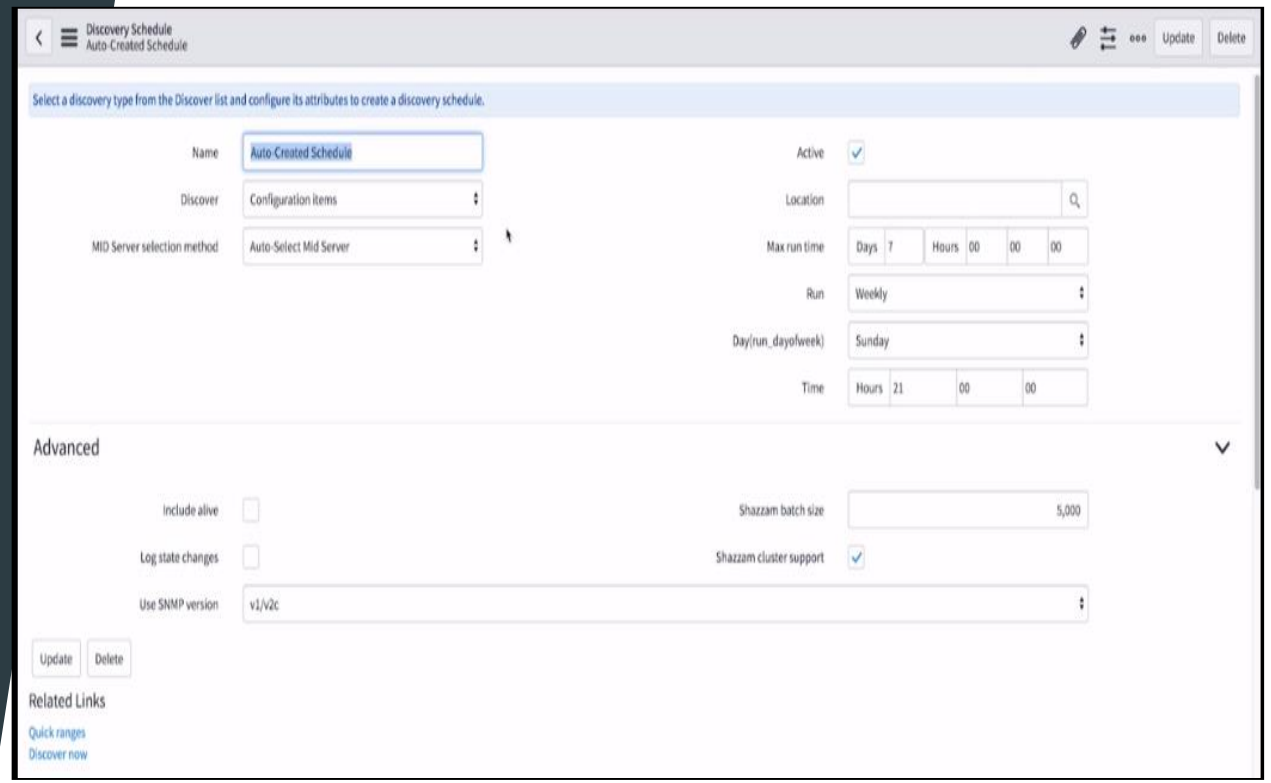
- When we create schedule the Discovery CI schedule manager opens.
- Click View CI Schedules to open page where we can see the schedule we just created by clicking on Edit Schedule which will open Auto created Schedule

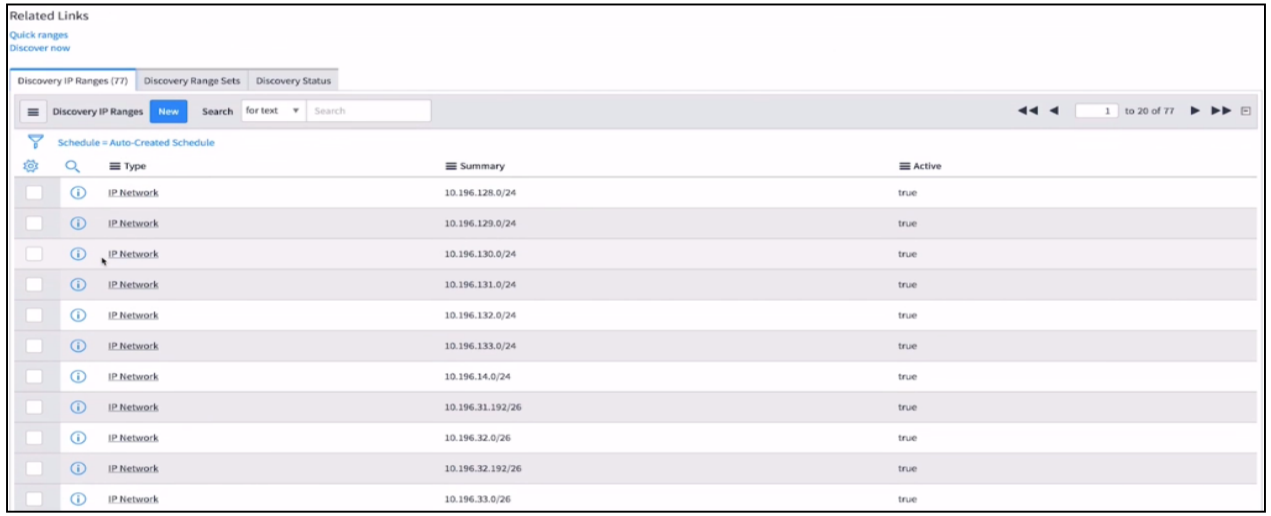




ITOM - Discovery

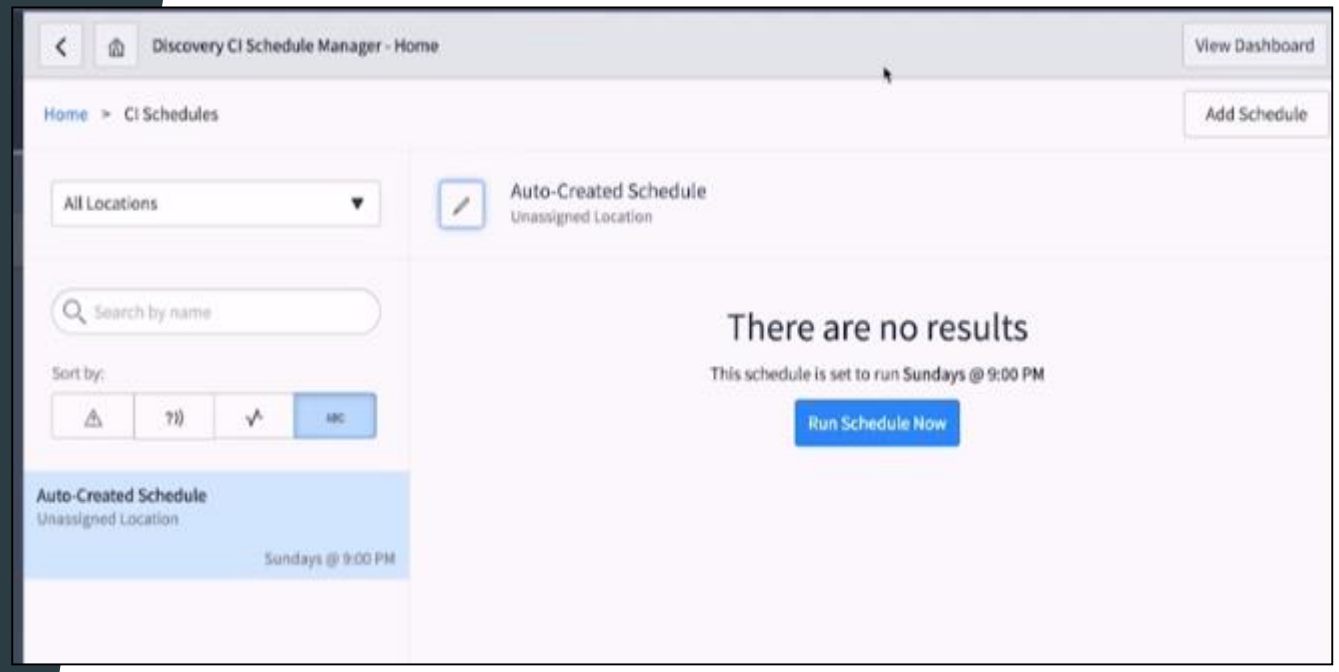
- Observing this schedule we can see this Auto created schedule as time saver i.e All the discovered IP ranges are automatically configured in Discovery IP ranges tab.

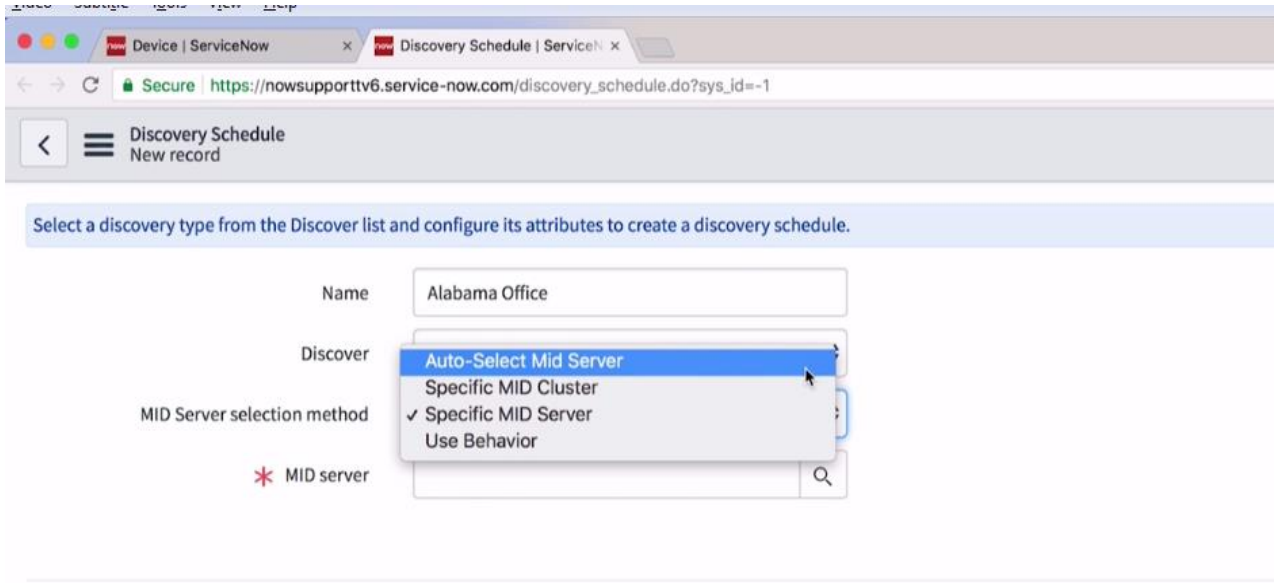




ITOM - Discovery

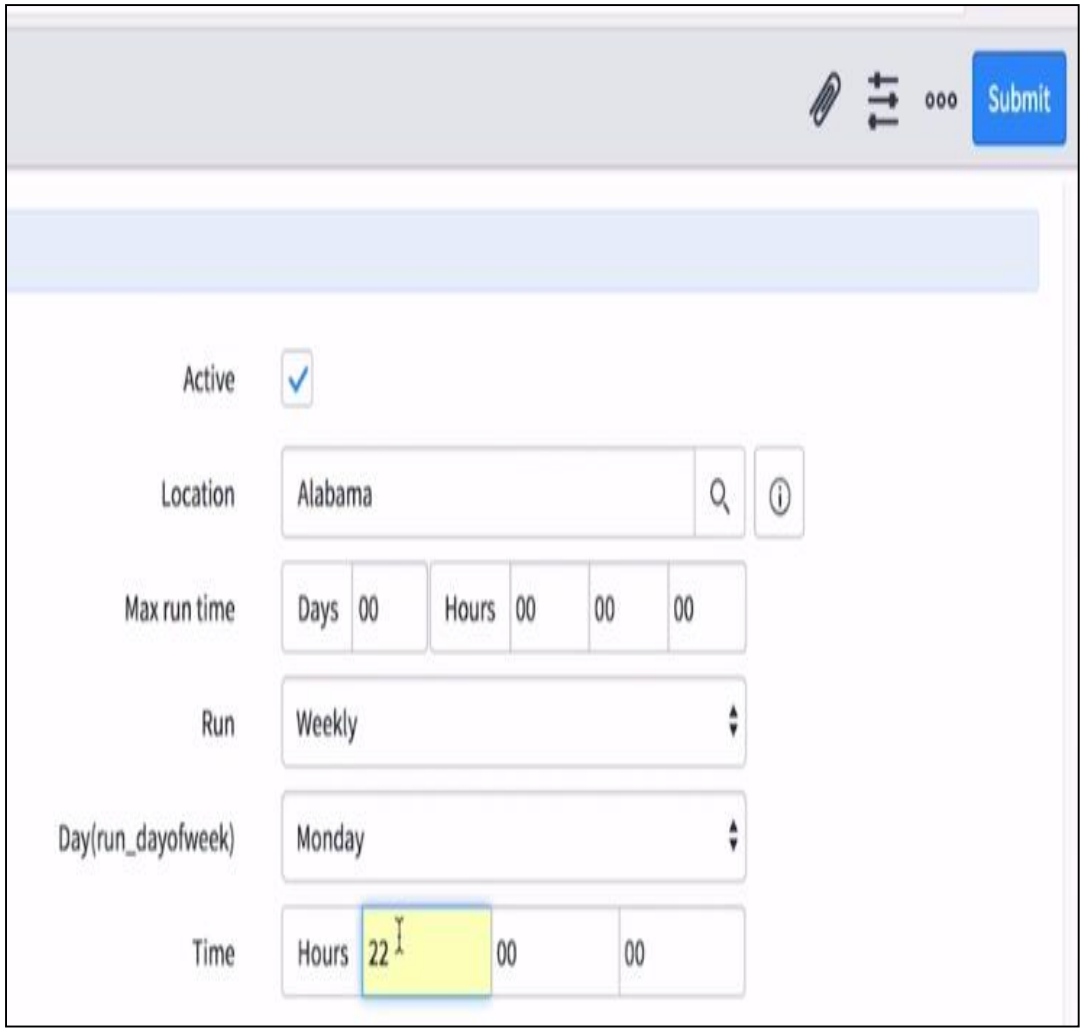
- Going back to Schedule manager ,we can also setup Discovery schedule manually by Add Schedule
- For our example lets create for discovering CI's for the specific subnets.With this type we can choose how the midserver is selected because we have configured our midserver with correct application discovery and IP ranges have been selected,we choose discover→Auto Select Mid server automatically.





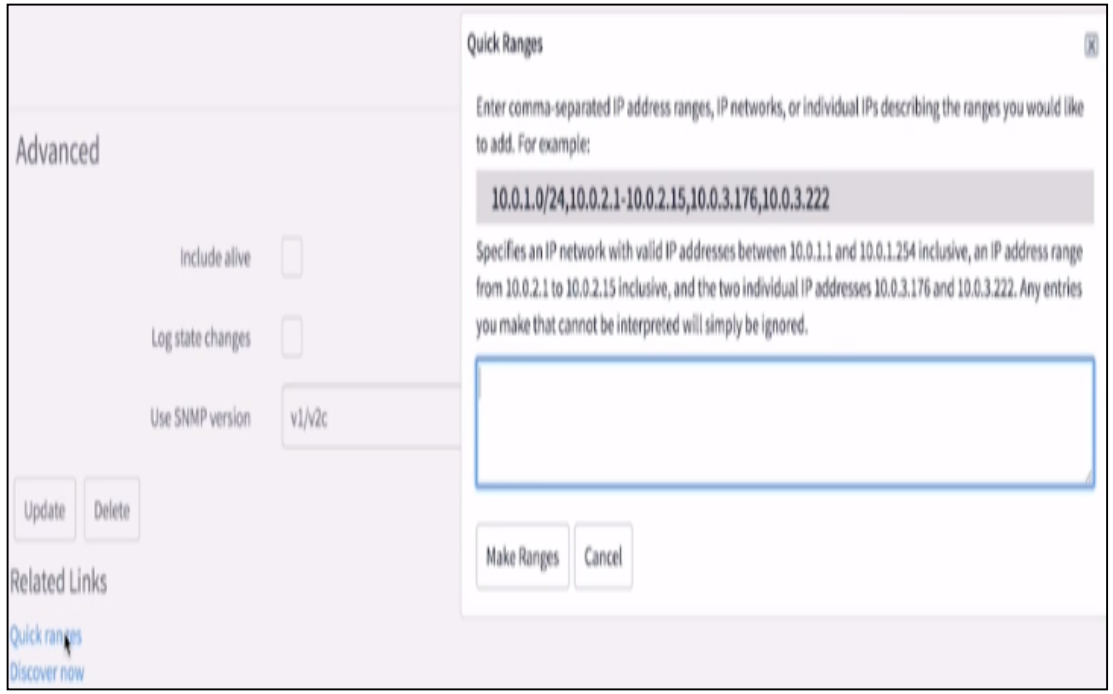
ITOM – Discovery with Service Mapping

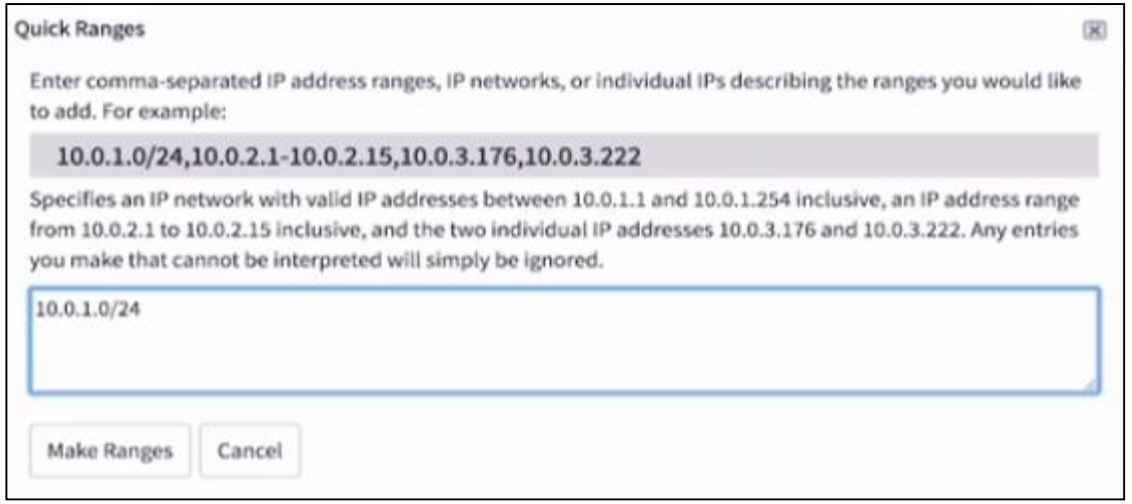
- We can enter the name for location Reston which will also populate the location field in CMDB on all Cis discovered by this schedule
- In Max run time we can put the duration of how long this discovery can run.00 lets it to complete till the end of discovery.
- Run:weekly
- Time : 21:00
- Save it



ITOM – Discovery with Service Mapping

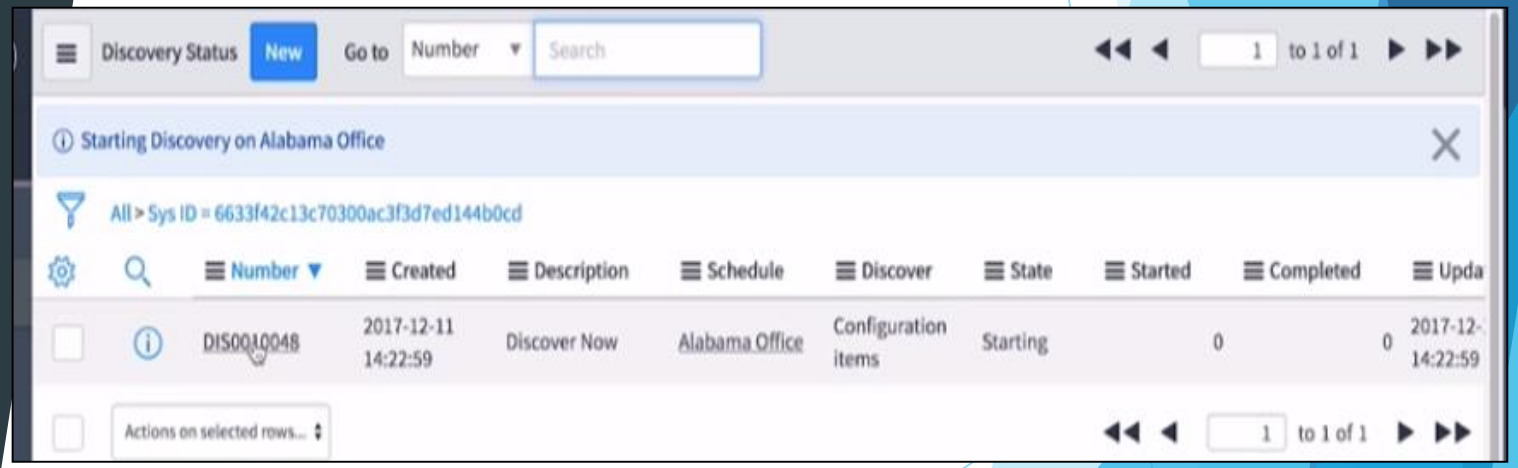
- Next we add the IP ranges we want using Quick ranges
- Use the same IP range of your system 10.0.1.189/24 and click Make ranges
- Update the Discovery schedule for Reston Office
- Mark the schedule task as competed





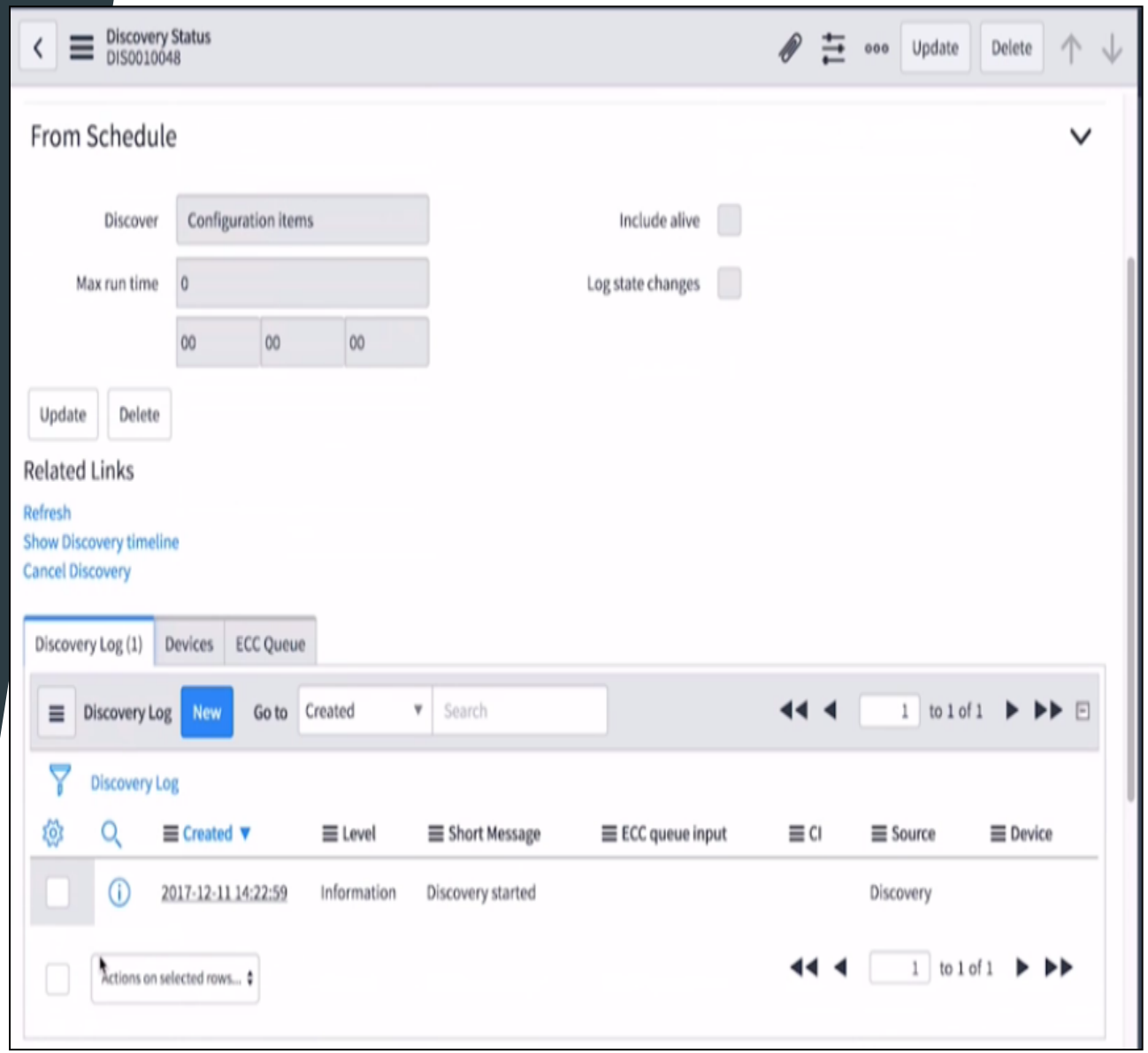
ITOM - Discovery

- Go back to Discovery schedule and press Discover now to watch the progress of Reston office discovery.



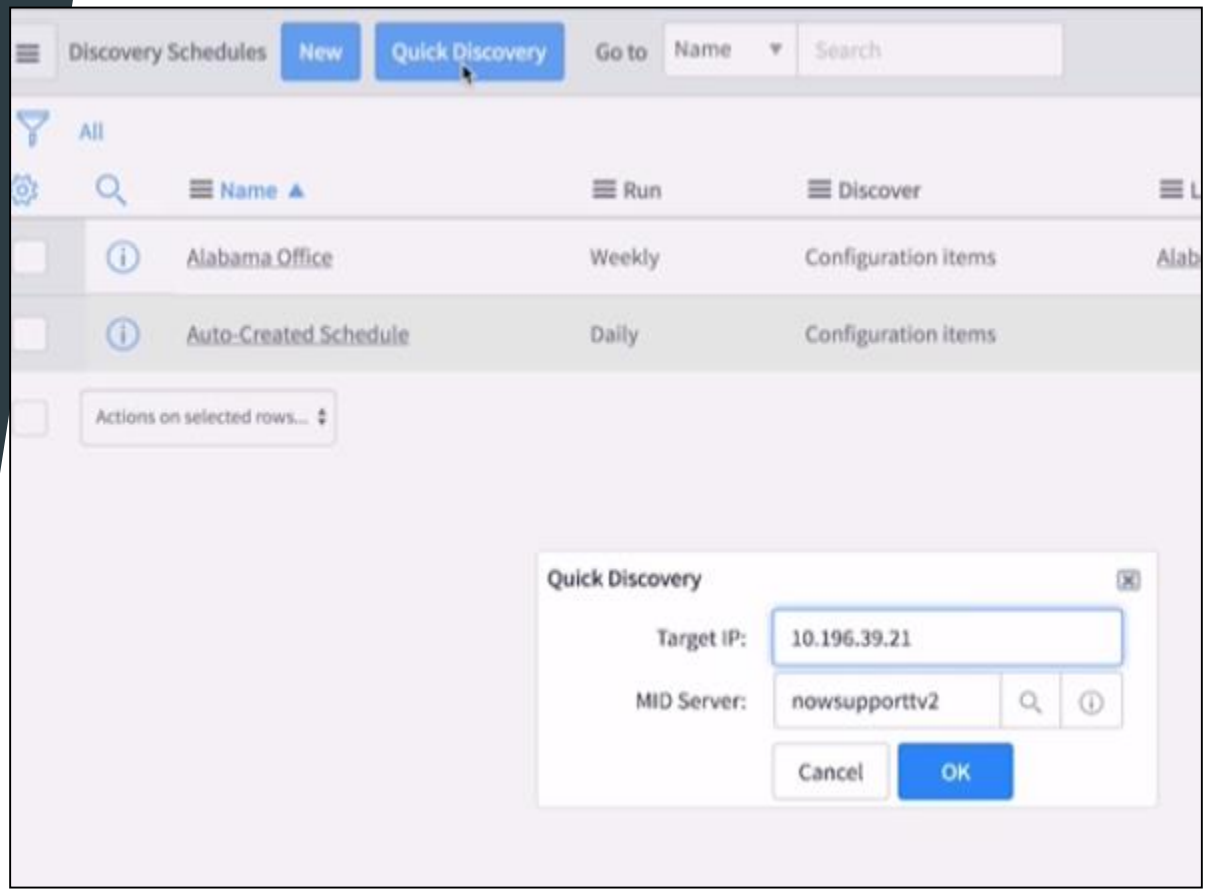
ITOM - Discovery

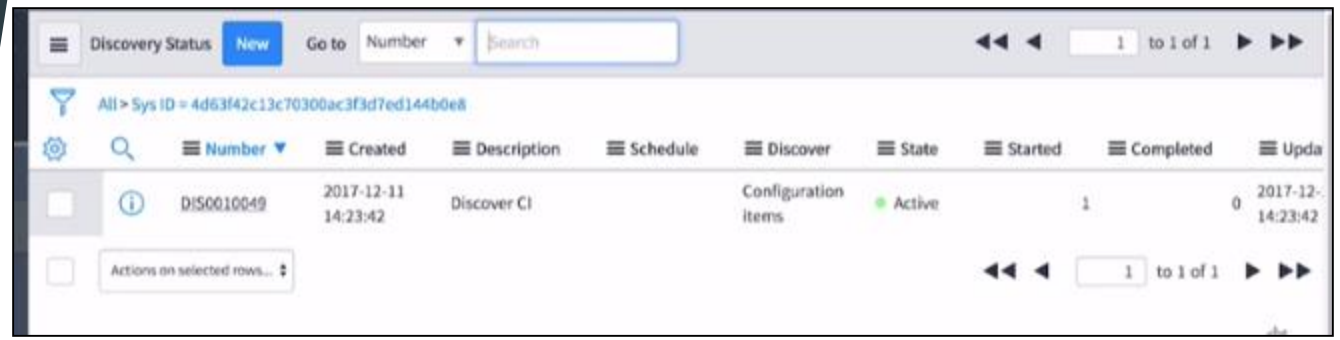
- **We click the status of Discovery to watch the progress**
- We can click refresh to check the udpdated status



ITOM - Discovery

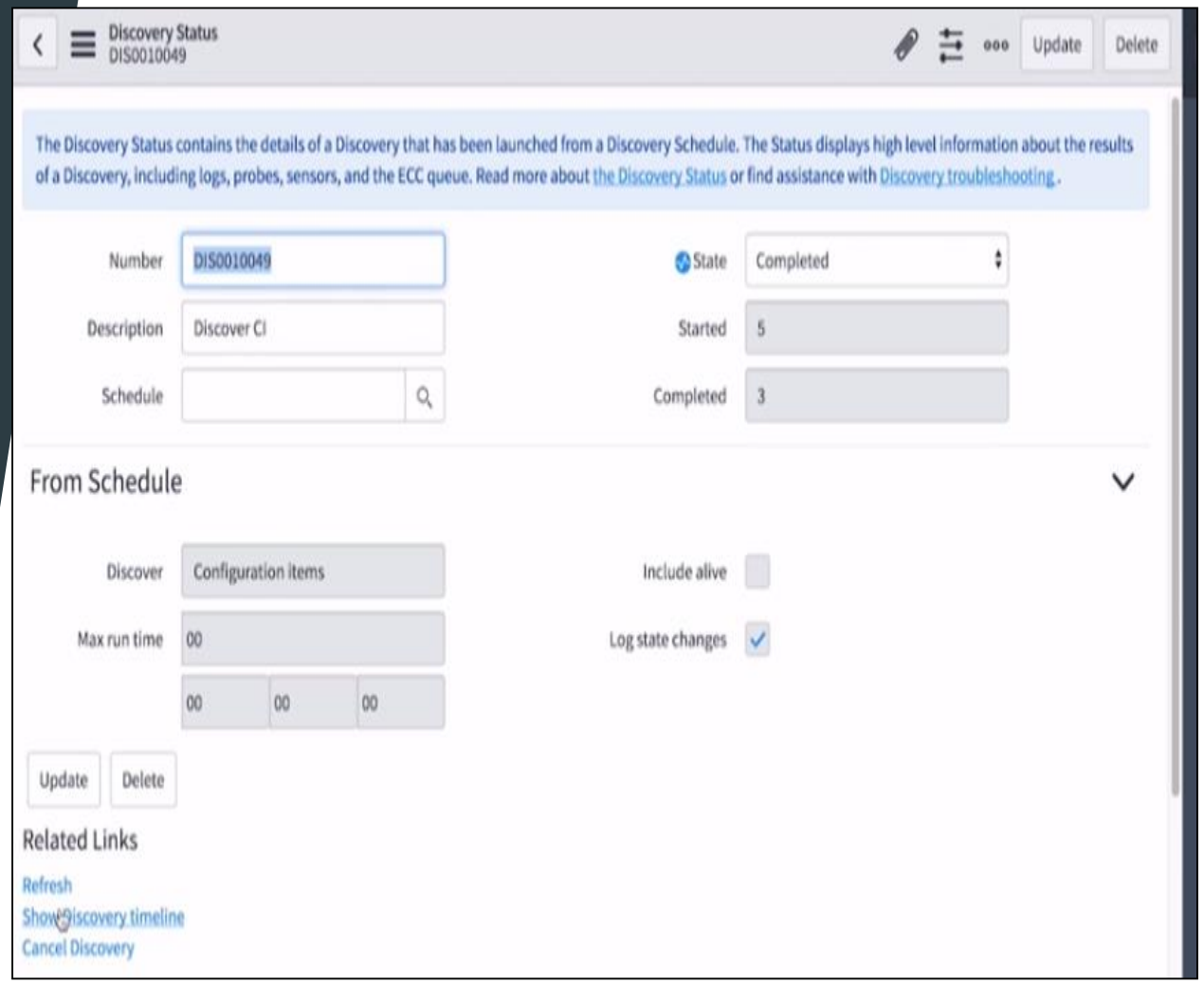
- Another tool is Quick discovery present on Discovery Schedules
- Lets put the target IP address and not the IP ranges.In this example as we are trying to discover our laptop in our company lets put target IP as IPv4 address in this case 10.0.0.189
- Click ok to start discovery process





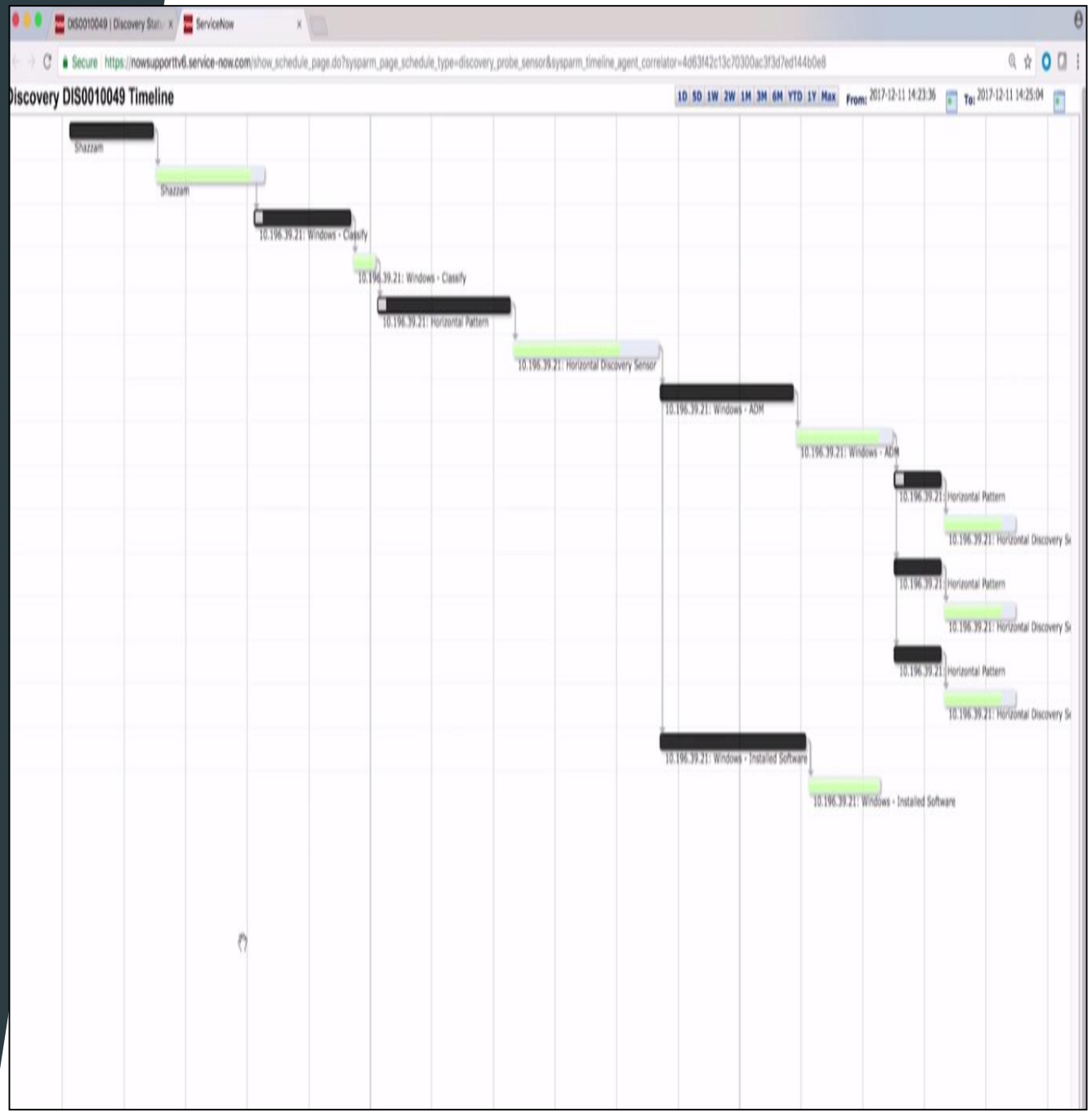
ITOM - Discovery

- When we open the discovery status record we can access the discovery timeline



ITOM - Discovery

- Here we can see the phases of Discovery and how long each one takes and what happens in each phase

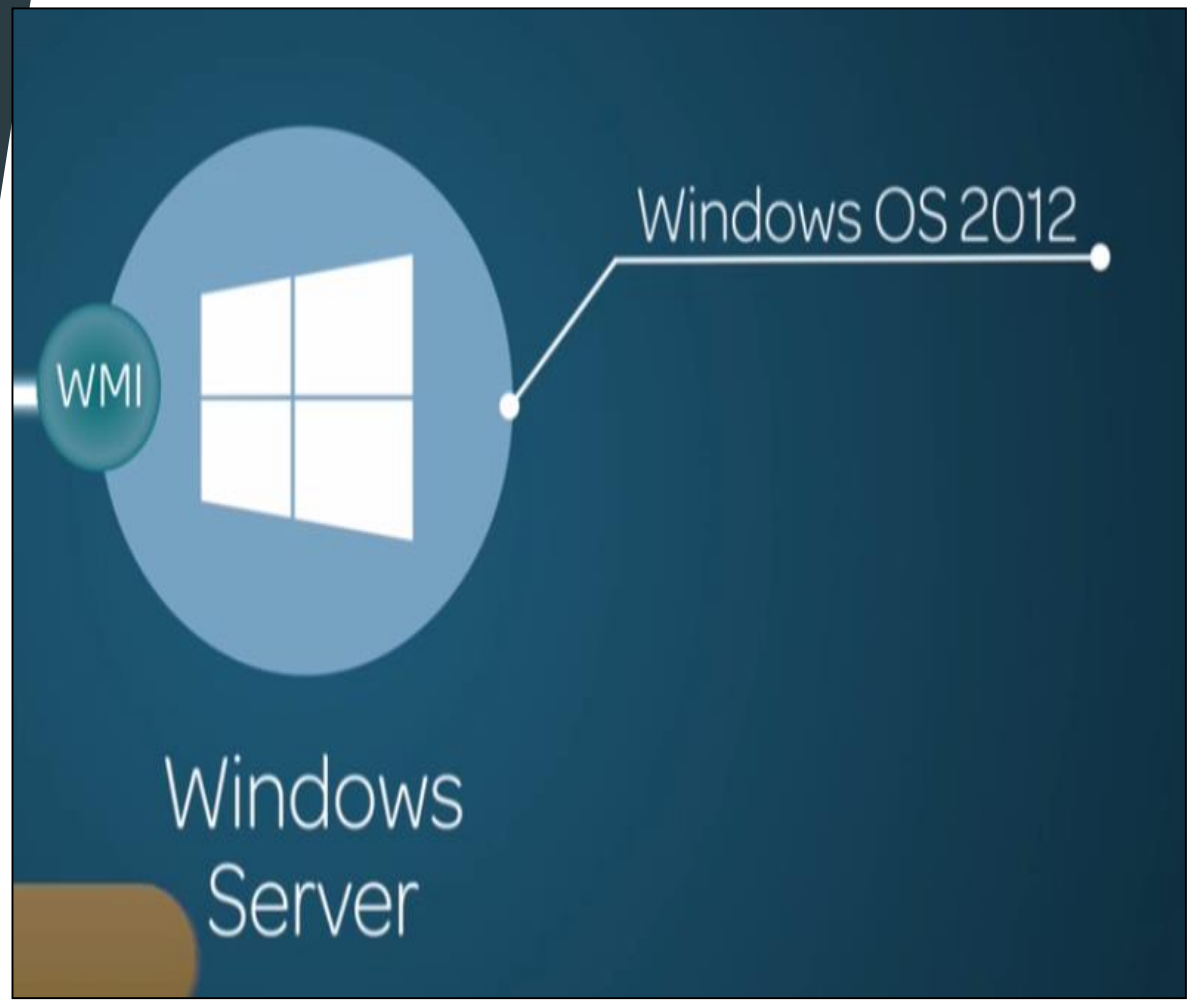


ITOM - Discovery

- Lets take a look on each phases
- First phase Port scanning takes place.Discovery launches a Shazzam probe to scan defined IP address and identify responsive IP and define discovery port state.
- In our demo the probe finds active IP on port 135 and discovery finds windows device and launch windows classification probe.

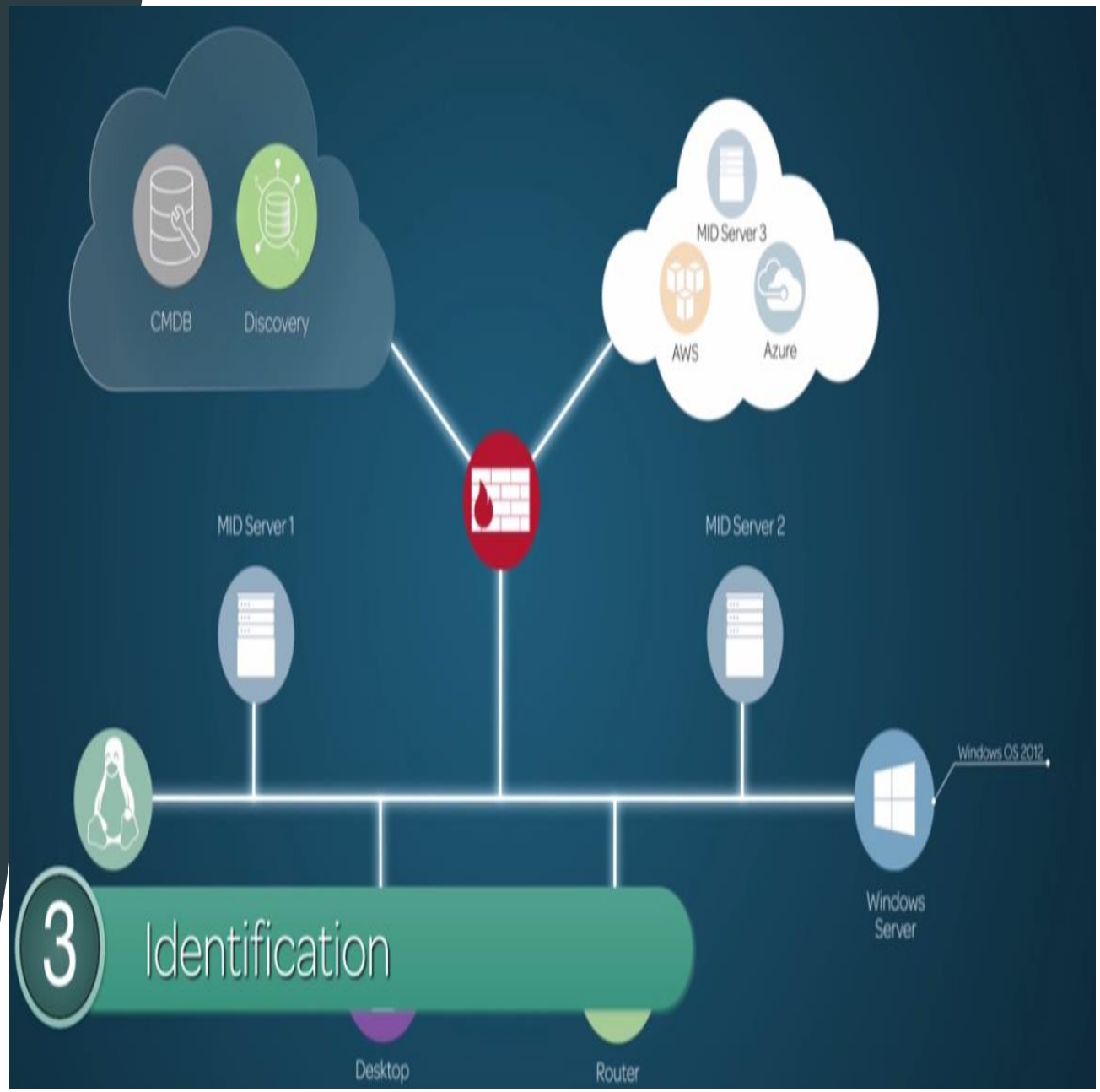
ITOM – Discovery with Service Mapping

- In the second phase discovery Classification discovery continues to send probes to find type of device in each IP address
- In windows discovery example discovery sends WMI used for Windows device OS 2012 to determine which OS is running on that device



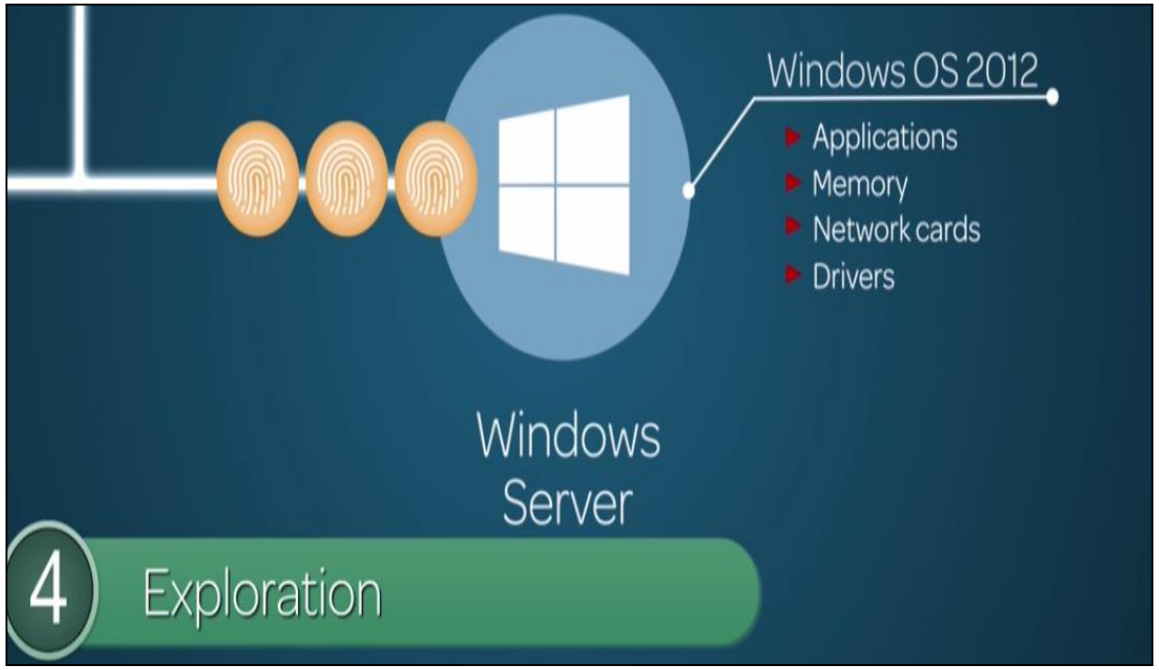
ITOM - Discovery

- In the third phase Identification Discovery collects additional information of the device to uniquely identify iD.
- Discovery then uses CI identification rules to check CMDB for matching Cis.
- If matching CI is found CMDB is updated.If matching CI is not found a new CI is created in CMDB



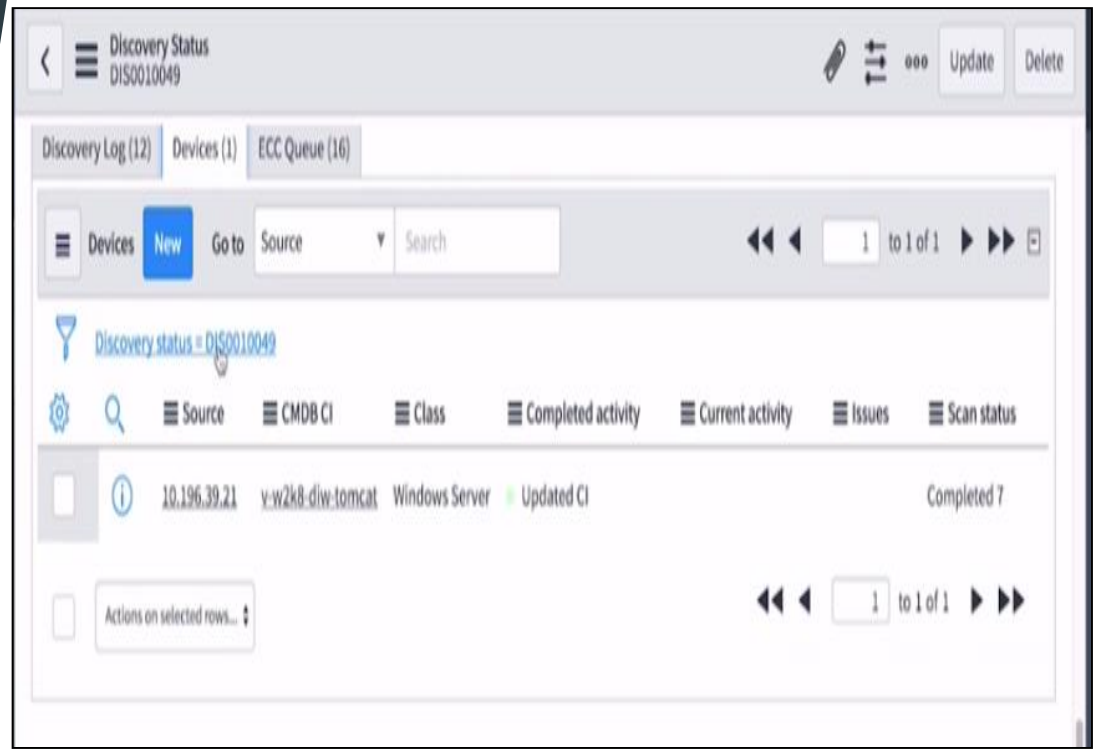
ITOM - Discovery

- Fourth phase the Exploration gathers additional information about the device like applications running on the device and attributes such as Applications,Memory,Network cards ,Drivers and more.
- Discovery process the results and updates the CMDB



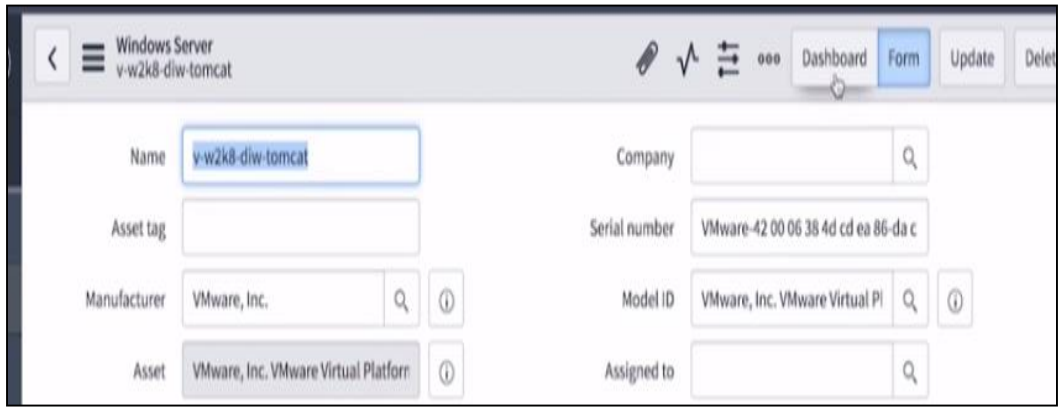
ITOM - Discovery

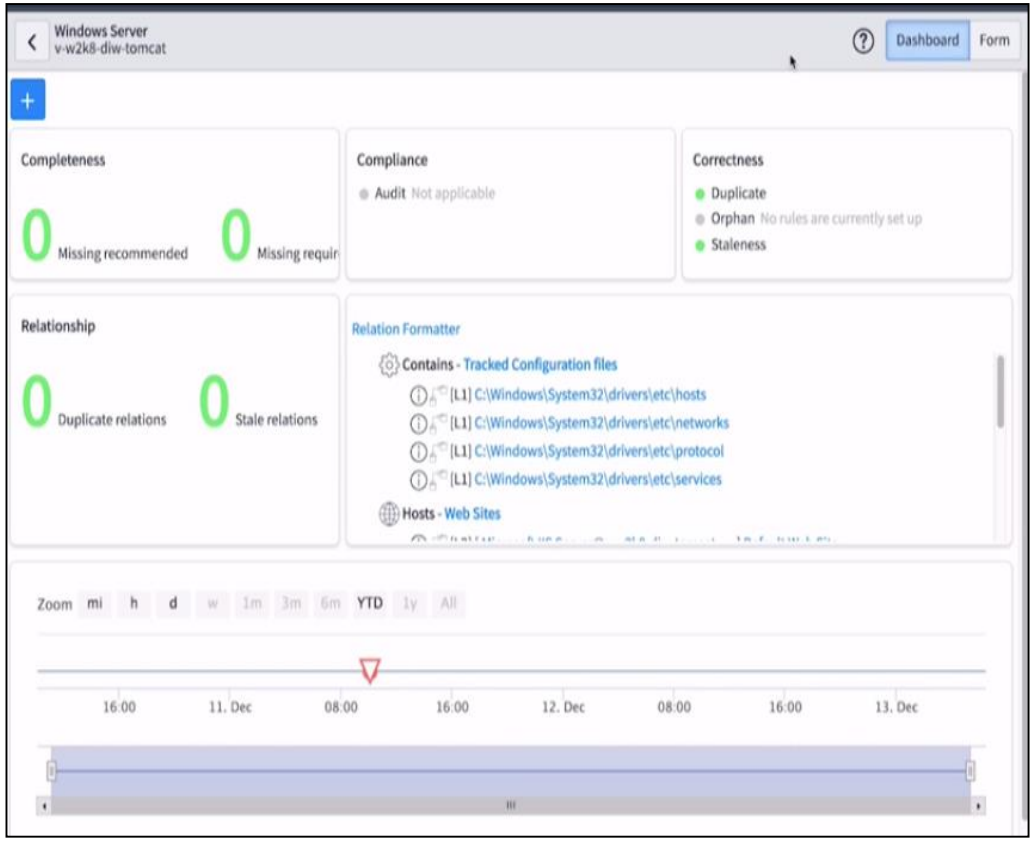
- In the Disovery Status we can see if new CI is updated in Devices found in the Related links



ITOM – Discovery with Service Mapping

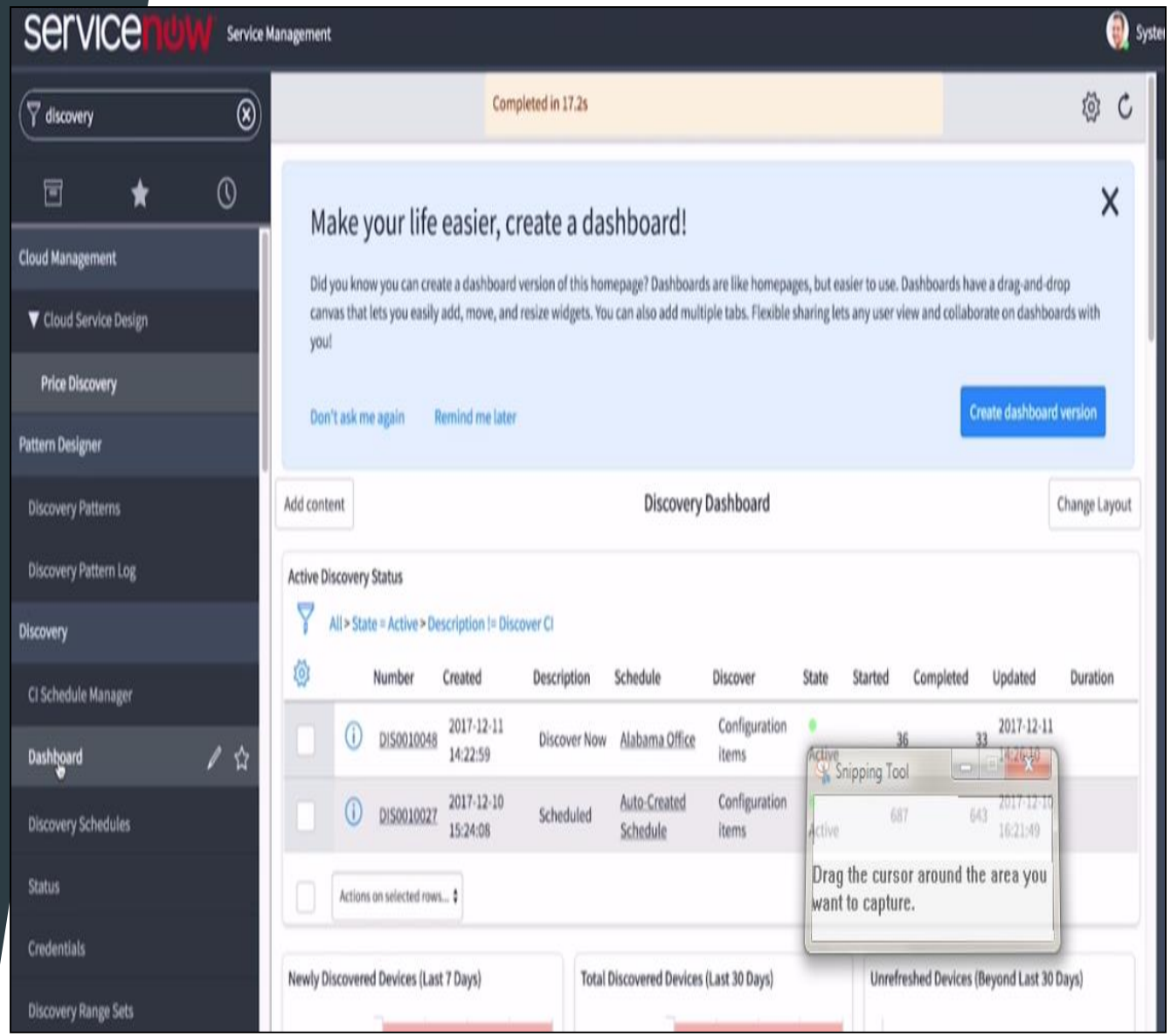
- For CI which are changed we can look at the timelines to see any changes in the list at the bottom





ITOM - Discovery

- We can also view Discovery→Dashboards to see status of discovery activities,
- This is Discovery of Cis with Service Mapping demonstration with handson Demo.



Thankyou