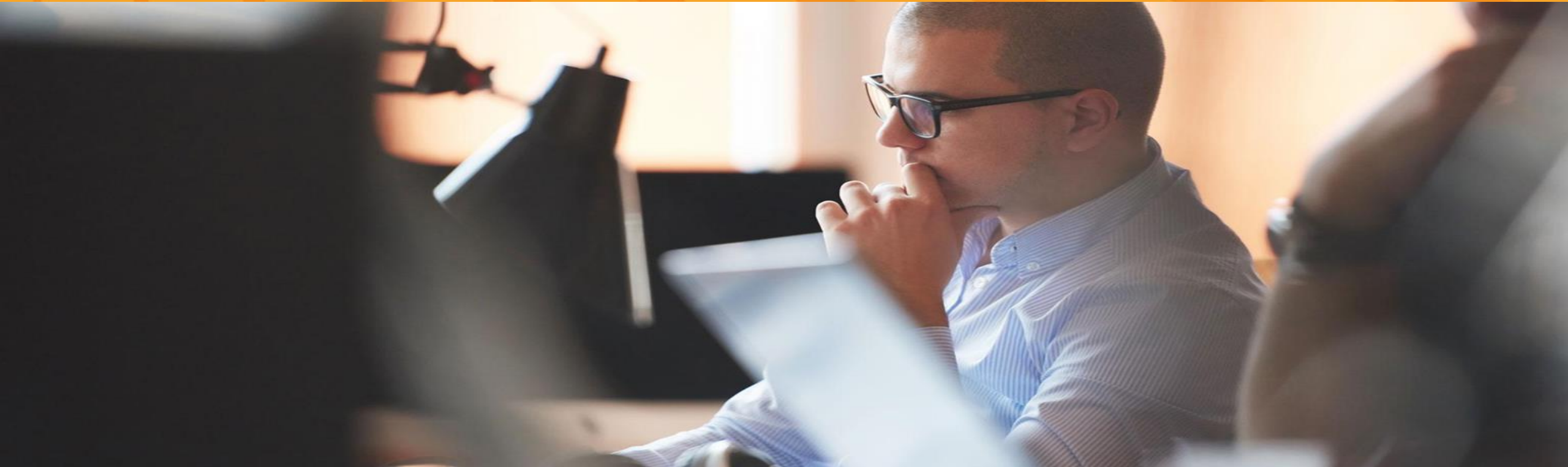




# ServiceNow – ITOM - Midserver



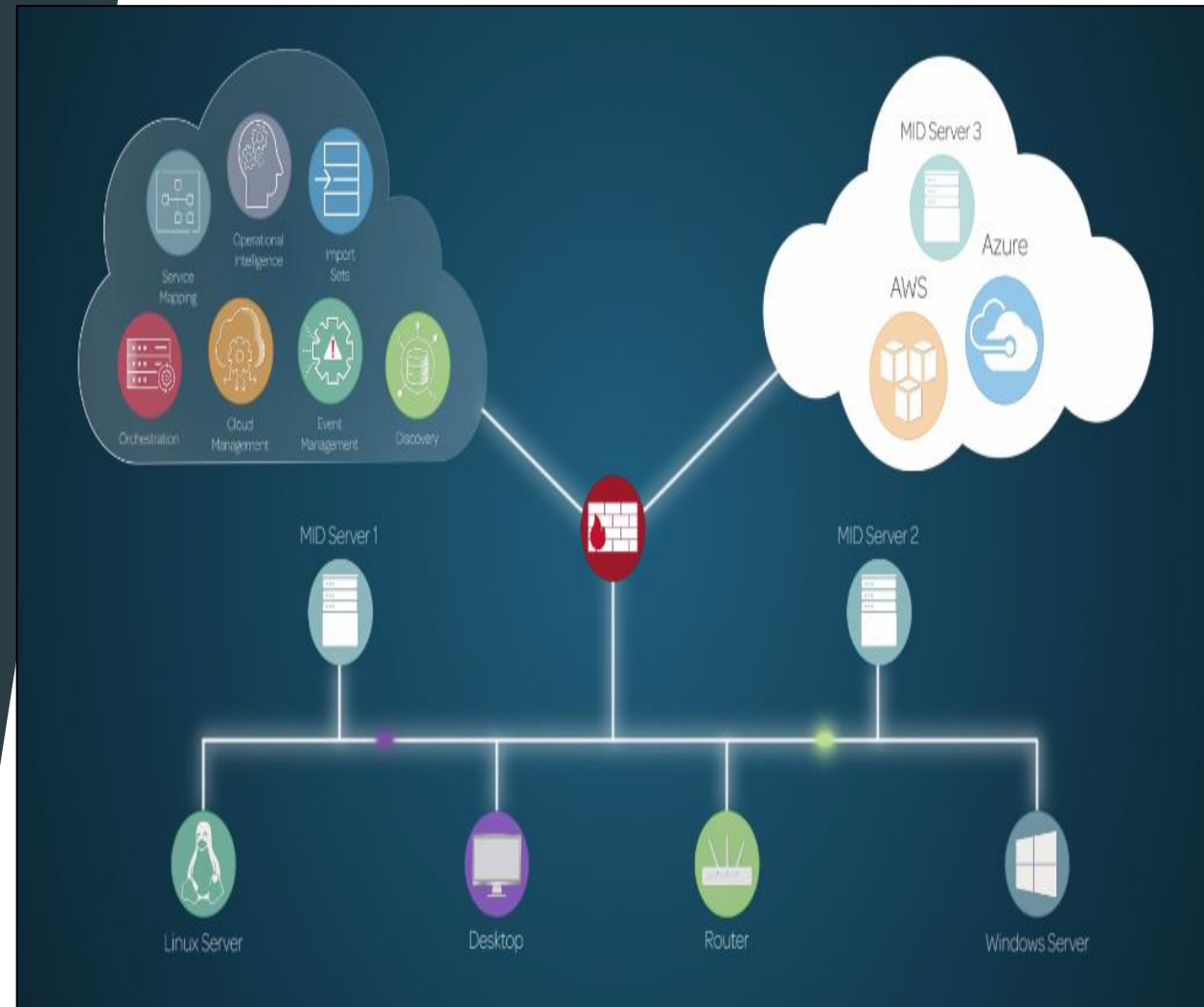
# ITOM - Midserver

- ▶ 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



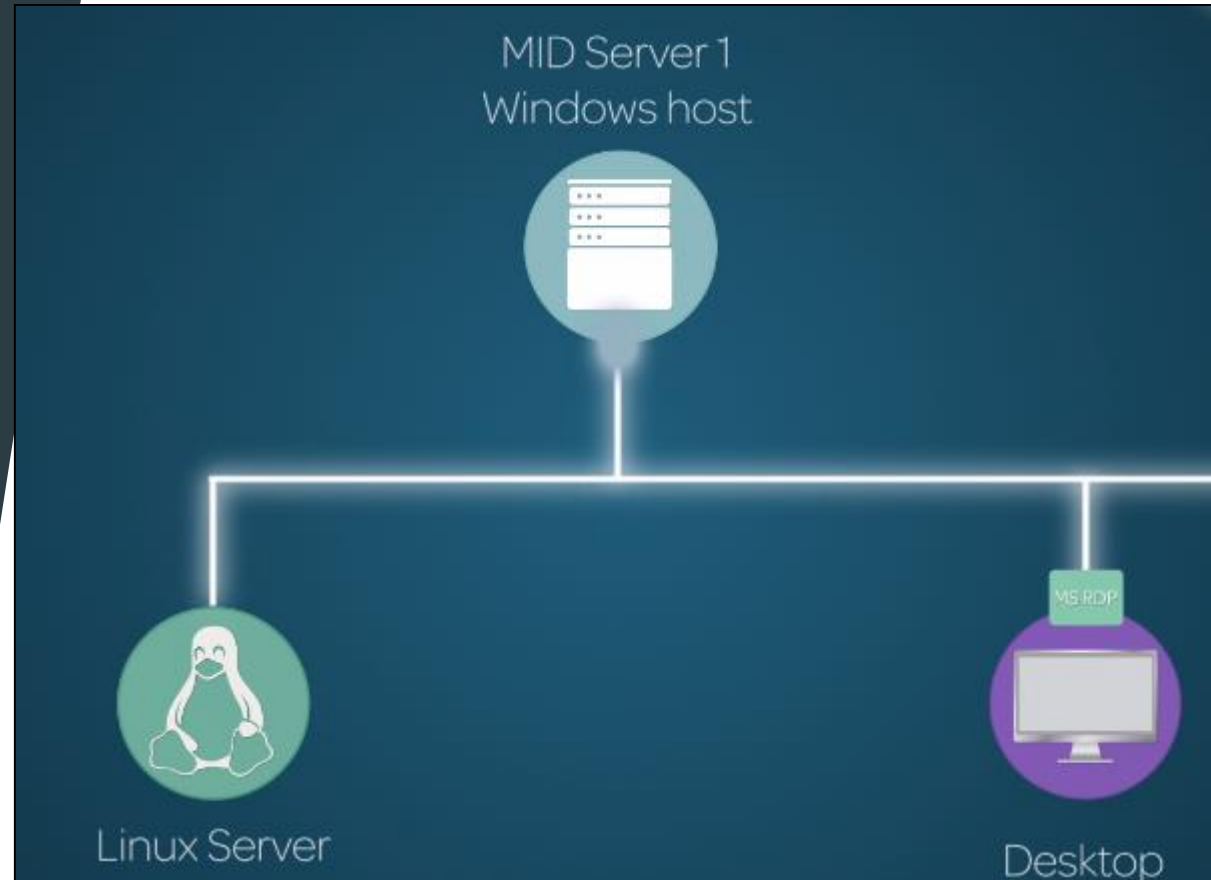
# ITOM - Midserver

- ▶ 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

The screenshot shows the ServiceNow IT Operations Management Guided Setup interface. The top navigation bar includes the ServiceNow logo, 'Service Management', a 'Global' dropdown, and a user profile for 'System Administrator'. The left sidebar contains a search bar with 'ITOM' entered, and a list of items: 'Guided Setup' and 'ITOM Guided Setup'. The main content area is titled 'IT Operations Management Guided Setup' and shows a progress bar at 43% Complete. Below the progress bar is a 'Getting started' section with a 'Continue' button. The 'Welcome to IT Operations Management' section contains a paragraph about moving from a reactive response team to a proactive business partner. Below this are three steps: 'Get going!' (Get up and running with ServiceWatch quick and easily), 'Learn' (Learn common configuration tasks within ServiceWatch), and 'Be empowered' (Empower you to make additional configuration changes at a later time). At the bottom, there is a recommendation for new customers to run the setup in their production instance and clone it to sub-production instances, and a note for existing customers to learn more about using 'Update Sets' and 'Exporting Data'.

service**now** Service Management

Global System Administrator

ITOM

43% Complete

Guided Setup

ITOM Guided Setup

## IT Operations Management Guided Setup

### Getting started

[Continue](#)

## Welcome to IT Operations Management

Move IT operations from a reactive response team to a proactive business partner with ServiceNow® IT Operations Management. Gain visibility into your end-to-end business services by understanding the relationship with the underlying IT resources. Guided Setup will walk you through the core configuration activities involved in setting up the applications that are part of the ITOM suite. Click the Continue button in the upper-right corner when you are ready to begin realizing value.

#### Get going!

Get up and running with ServiceWatch quick and easily

#### Learn

Learn common configuration tasks within ServiceWatch

#### Be empowered


Empower you to make additional configuration changes at a later time

We recommend new customers run IT Operations Management Guided Setup in their production instance and clone the production instance over sub-production instances after going live.

If you are an existing customer or want to run IT Operations Management Guided Setup in a sub-production instance, learn more about using [Update Sets](#) and [Exporting Data](#) in our product documentation before starting.

# 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



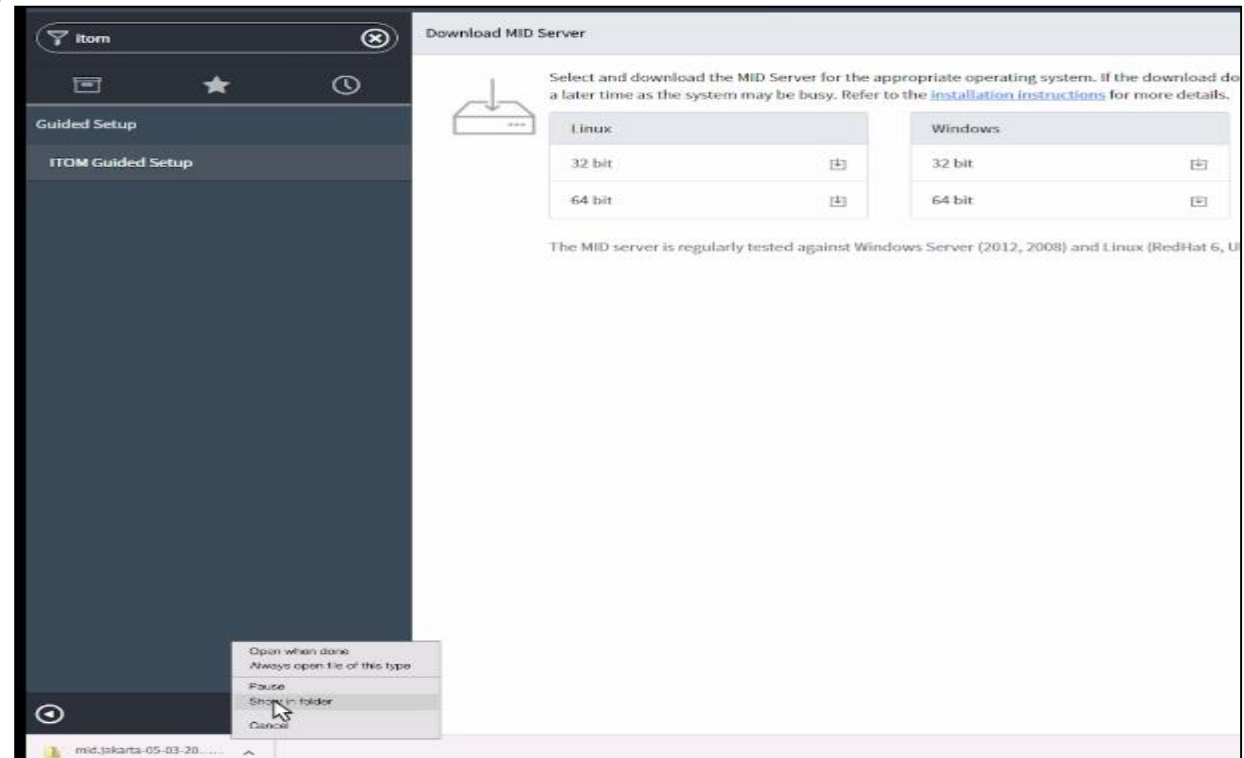
### Create MID Server User

User name

Password

Confirm password

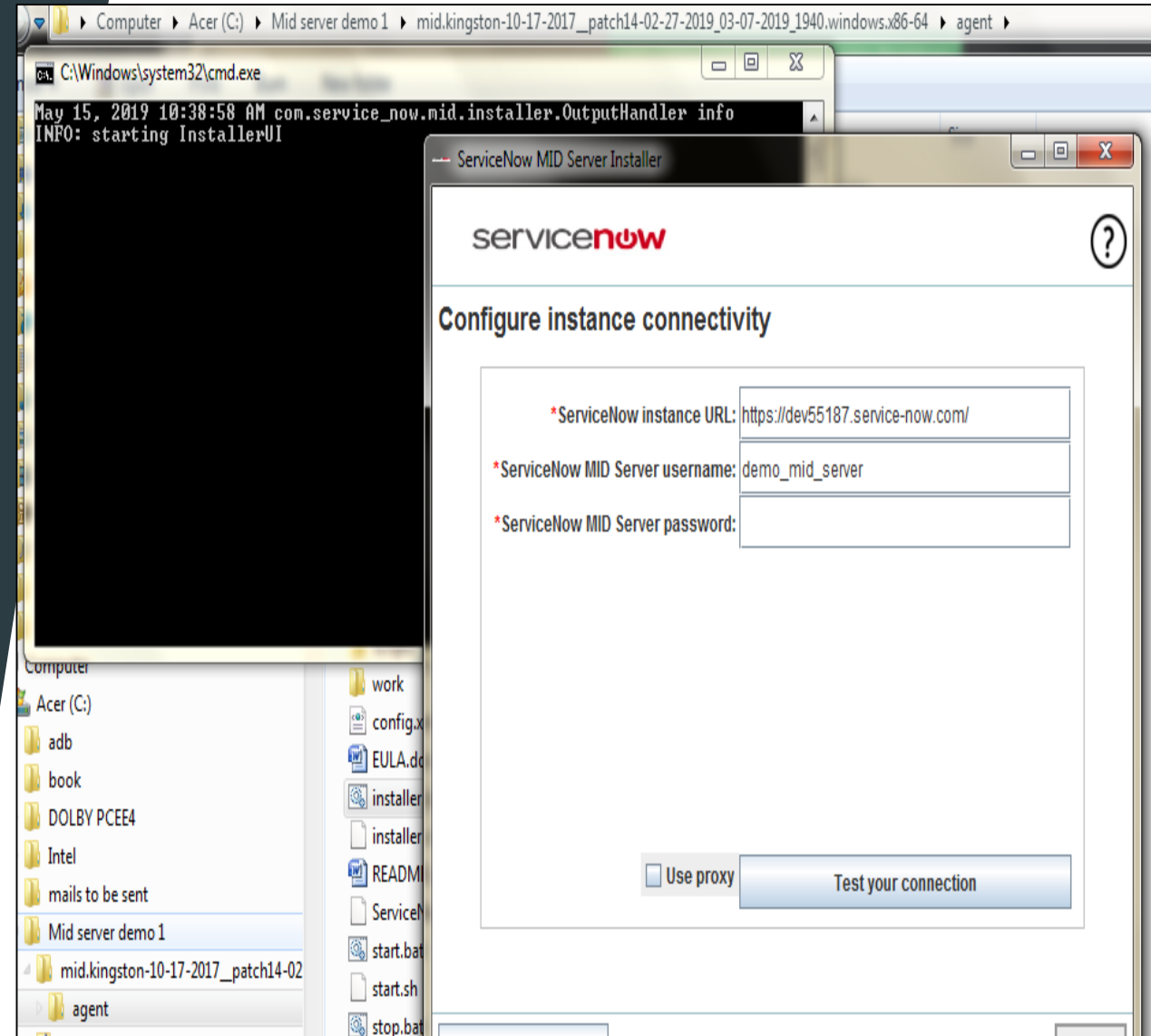
### Existing MID Server Users





# 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.

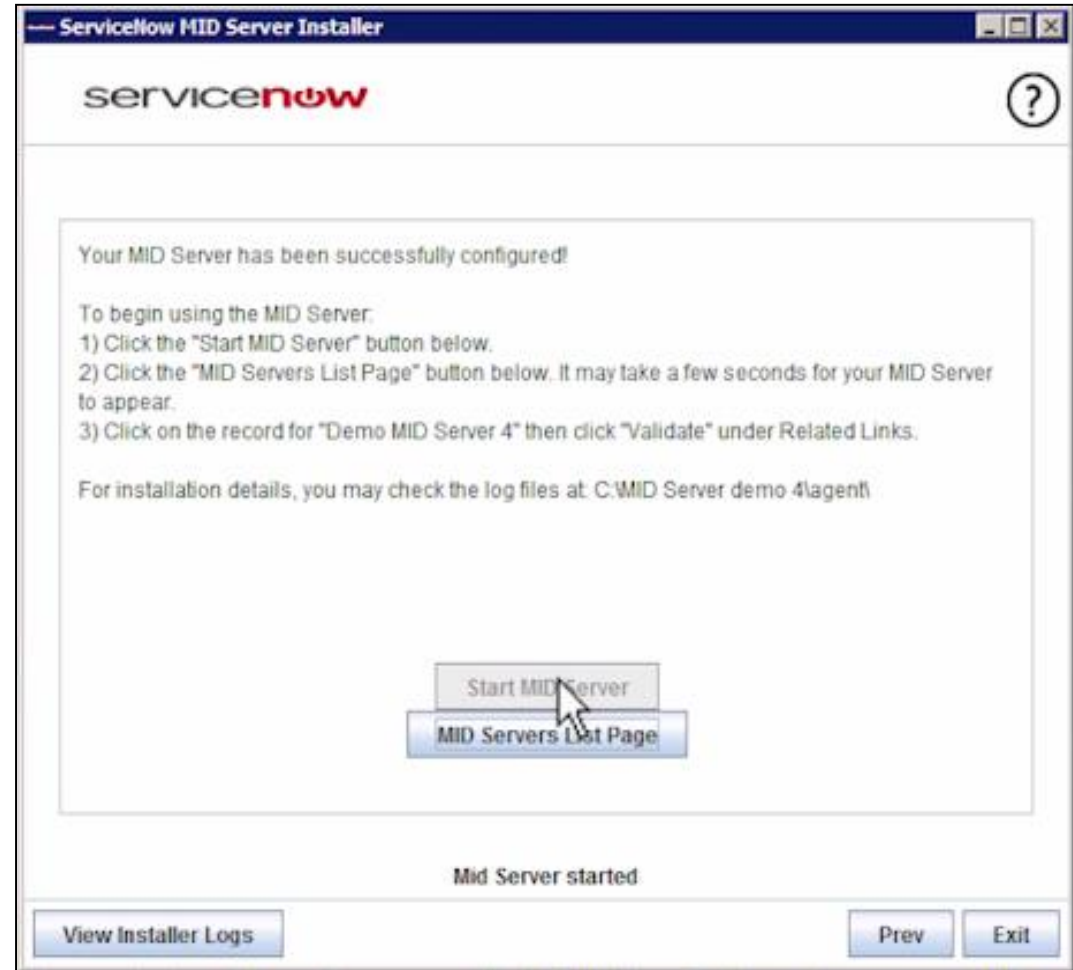
The screenshot shows the 'Configure MID name parameters' window of the ServiceNow MID Server Installer. The window has a title bar 'ServiceNow MID Server Installer' and the ServiceNow logo. A help icon (?) is in the top right. The main area contains three input fields: '\*MID Server name:' with the value 'Demo MID Server', 'MID service wrapper name:' with the value 'snc\_mid\_Demo MID Server', and 'MID service wrapper display name:' with the value 'ServiceNow MID Server\_Demo MID Server'. At the bottom, there are three buttons: 'View Installer Logs', 'Prev', and 'Next'.

The screenshot shows the 'Configuration summary' window of the ServiceNow MID Server Installer. The window has a title bar 'ServiceNow MID Server Installer' and the ServiceNow logo. A help icon (?) is in the top right. The main area displays a 'Configuration summary:' section with the following details: Instance URL: https://nowsupportv3.service-now.com/, Instance username: demo\_mid\_server, Instance password: \*\*\*\*\* (masked), Use proxy: false, MID Server name: Demo MID Server 4, MID service wrapper name: snc\_mid\_Demo MID Server 4, and MID service wrapper display name: ServiceNow MID Server\_Demo MID Server 4. At the bottom, there is a message 'Save the configuration by clicking "Next".' and three buttons: 'View Installer Logs', 'Prev', and 'Next'.



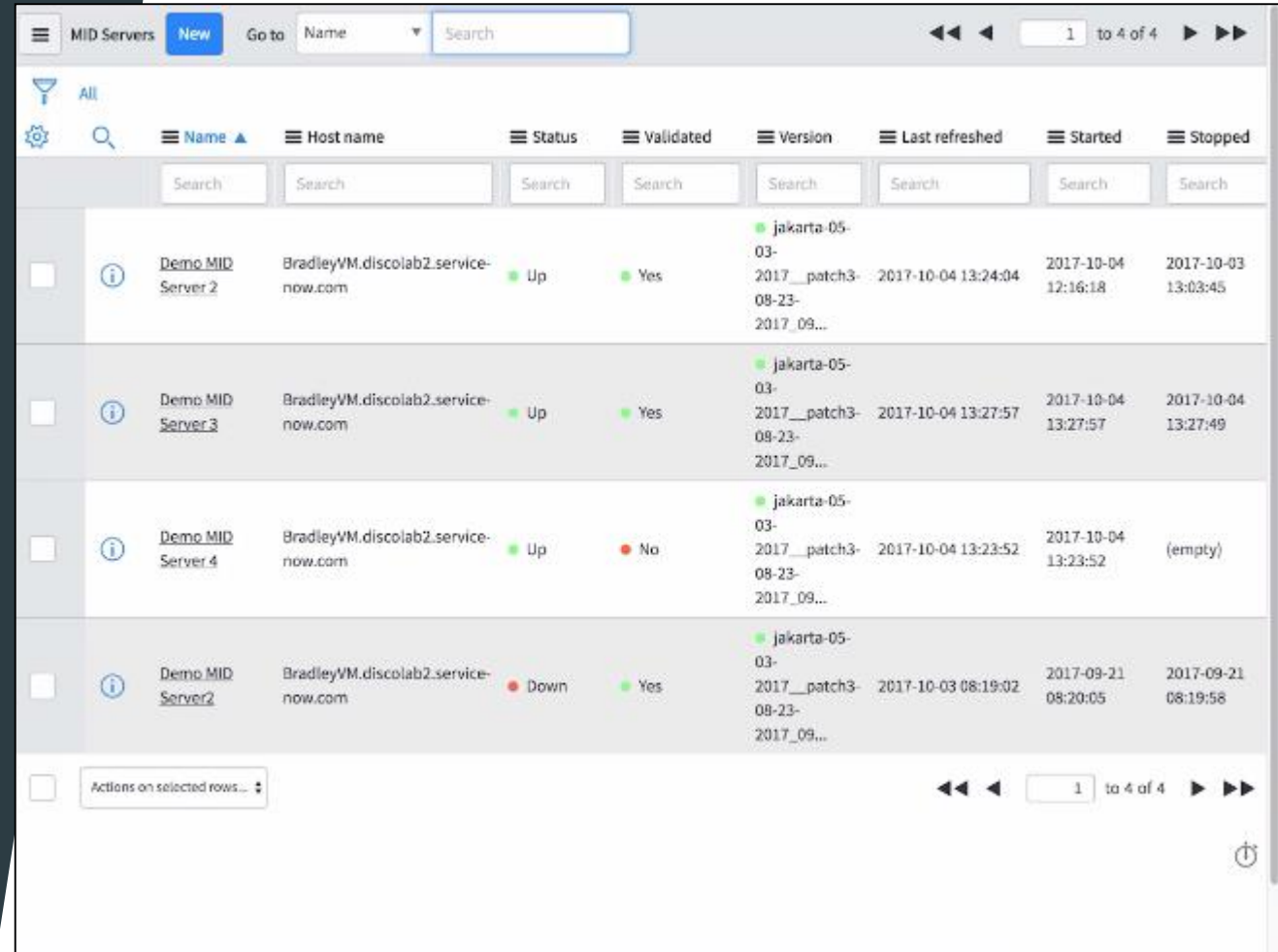
# ITOM - Midserver

- ▶ 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 feature 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.



The screenshot displays the 'MID Servers' management interface. At the top, there is a 'New' button and a 'Go to' search bar. Below this is a table with columns for Name, Host name, Status, Validated, Version, Last refreshed, Started, and Stopped. The table contains four rows of midserver data. The first three rows show midservers with status 'Up' and 'Validated' as 'Yes'. The fourth row shows a midserver with status 'Down' and 'Validated' as 'Yes'. The interface also includes a 'Search' bar for each column and a 'Actions on selected rows...' dropdown at the bottom.

	Name	Host name	Status	Validated	Version	Last refreshed	Started	Stopped
<input type="checkbox"/>	<a href="#">Demo MID Server 2</a>	BradleyVM.discolab2.service-now.com	Up	Yes	jakarta-05-2017__patch3-08-23-2017_09...	2017-10-04 13:24:04	2017-10-04 12:16:18	2017-10-03 13:03:45
<input type="checkbox"/>	<a href="#">Demo MID Server 3</a>	BradleyVM.discolab2.service-now.com	Up	Yes	jakarta-05-2017__patch3-08-23-2017_09...	2017-10-04 13:27:57	2017-10-04 13:27:57	2017-10-04 13:27:49
<input type="checkbox"/>	<a href="#">Demo MID Server 4</a>	BradleyVM.discolab2.service-now.com	Up	No	jakarta-05-2017__patch3-08-23-2017_09...	2017-10-04 13:23:52	2017-10-04 13:23:52	(empty)
<input type="checkbox"/>	<a href="#">Demo MID Server 2</a>	BradleyVM.discolab2.service-now.com	Down	Yes	jakarta-05-2017__patch3-08-23-2017_09...	2017-10-03 08:19:02	2017-09-21 08:20:05	2017-09-21 08:19:58

# 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

parameters and capabilities here. Read about [configuring the MID Server](#) or find assistance with [MID Server troubleshooting](#).

Name	Demo MID Server 4	Host name	BradleyVM.discolab2.service-now.co
Status	Up	IP address	10.11.128.146
Validated	No	Router	10.11.128.1
Version	jakarta-05-03-2017__patch3-08-23-2	Network	10.11.128.0/22
Last refreshed	2017-10-04 13:23:52	Host OS	Windows
Started	2017-10-04 13:23:52	Windows domain	DISCOLAB2
Stopped			
Logged in user	demo_mid_server		

[Update](#) [Delete](#)

Related Links

- [Validate](#)
- [Rekey](#)
- [Grab MID logs](#)
- [MID statistics](#)
- [Restart MID](#)
- [Upgrade MID](#)

**Set Initial Selection Criteria**

Selected MID Server(s) are now being validated.  
Approve setting the initial [selection criteria](#) for each MID Server.

Allow ALL applications ☒

Allow ALL capabilities ☐

Allow ALL IP ranges ☐

Note that any previous criteria will be overwritten.

[Cancel](#) [OK](#)




# ITOM - Midserver

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

<

≡

MID Server  
Demo MID Server 4



Update

Delete

↑

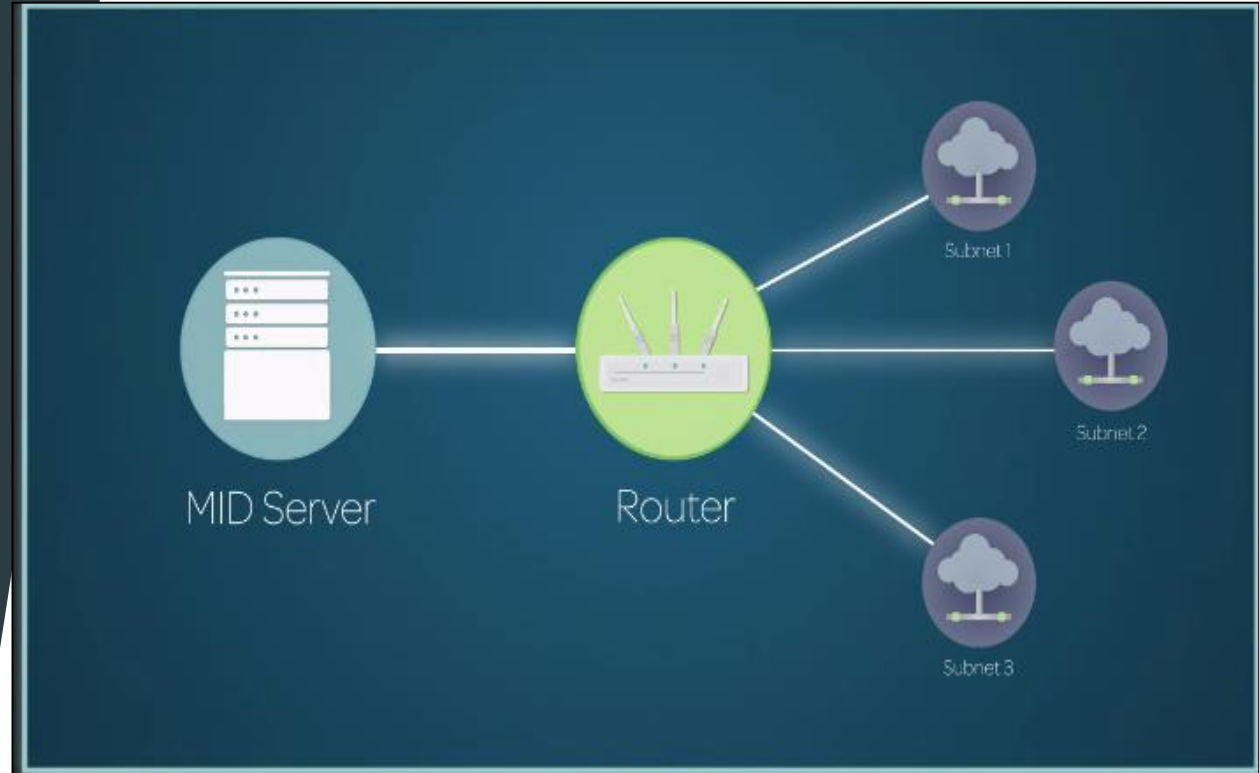
✓ MID server being validated

The MID Server facilitates communication between the ServiceNow platform and external applications, data sources, and services. Add MID Server configuration parameters and capabilities here. Read about [configuring the MID Server](#) or find assistance with [MID Server troubleshooting](#).

Name	Demo MID Server 4	Host name	BradleyVM.discolab2.service-now.co
Status	Up	IP address	10.11.128.146
Validated	Yes	Router	10.11.128.1
Version	jakarta-05-03-2017_patch3-08-23-2	Network	10.11.128.0/22
Last refreshed	2017-10-04 13:28:58	Host OS	Windows
Started	2017-10-04 13:28:58	Windows domain	DISCOLAB2
Stopped	2017-10-04 13:28:49		
Logged in user	demo_mid_server		

# 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.
- ▶ In order to discover subnets MID server needs SNMP (Simple Network Management Protocol) credentials to log on to network devices. Ensure it has required permissions as mentioned in MID server product documentation



## Add SNMP Credentials [Skip](#) [Add Notes](#)

Last visited just now by System Administrator

[Mark as Complete](#)

[Configure](#)

[Optional] If you want to automatically populate the selected MID Server's IP Ranges in the next step, you will need SNMP credentials to access the routers on your network.

# ITOM - Midserver

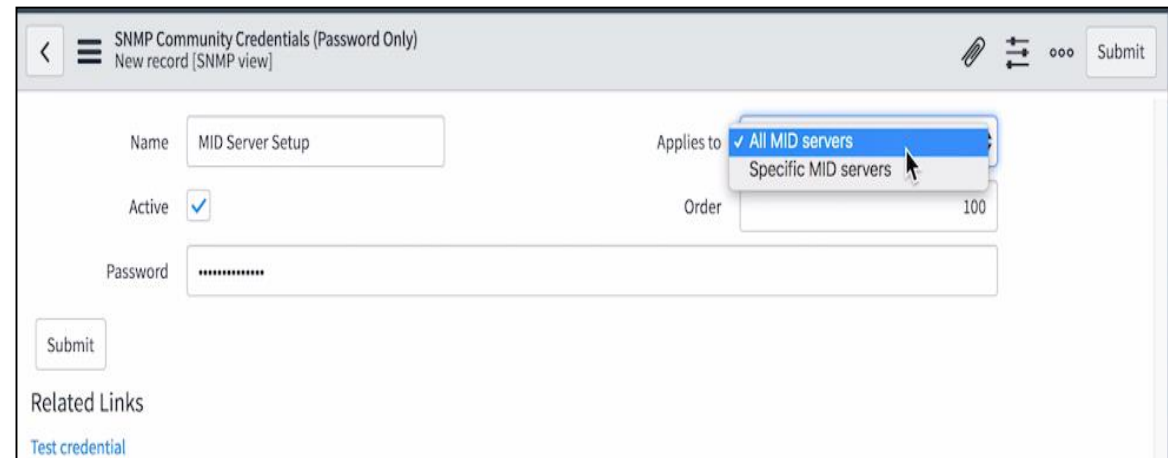
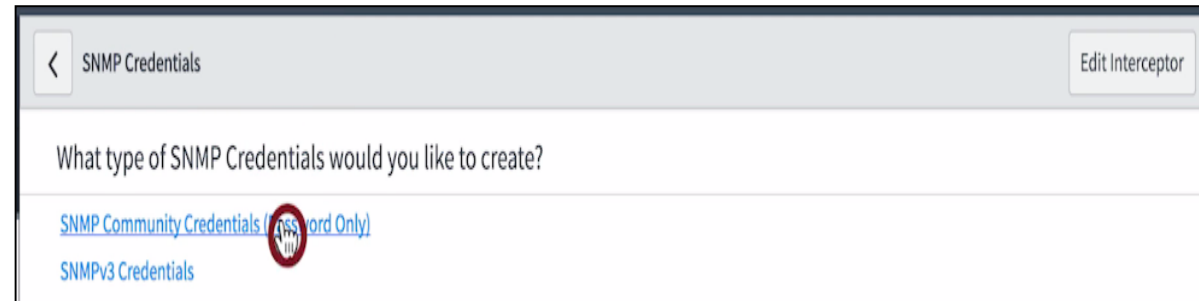
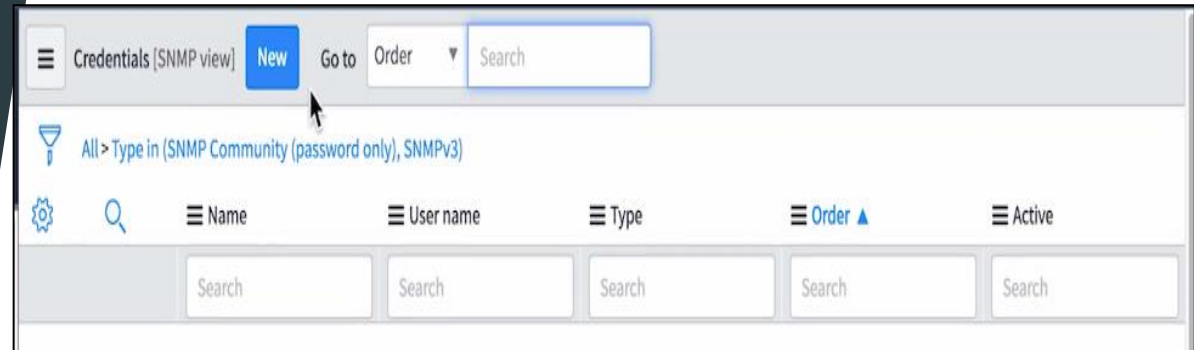
- ▶ Configure SNMP Credentials and click New Credentials and choose SNMP Community Credentials(password only) and give name for credentials

- ▶ Name : MID Server Setup

Password:\*\*\*\*

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.

Name	User name	Type	Order	Active
MID Server Setup		SNMP Community (password only)	100	true

**Auto-Assign MID Server IP Ranges** [Skip](#) [Add Notes](#) [Mark as Complete](#) [Configure](#)

Last visited 1m ago by System Administrator

[Optional] Use this feature to automatically populate the selected MID Server's IP Ranges, using the SNMP credentials added above. Otherwise, your MID Servers will either use the default 'All' IP Range that is applied optionally during Validation or any manually configured IP Ranges that are directly added to the MID Server form.

# 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

**MID Server range auto-assignment**

Please select the MID Servers you want to auto-assign ranges for. Only MID Servers that are 'Up' and 'validated' can be selected.

**Available**

- Demo MID Server 2
- Demo MID Server 3

**Selected**

- Demo MID Server 4

Buttons: Cancel, Confirm (highlighted with a red circle)

**Automation Status Set**  
STA0001002

This form shows the discovery processes that are executed to auto-assign MID Server IP Ranges for the MID Servers that were selected for auto-configuration.

Number: STA0001002  
State: Completed

Subnet discovery status: DIS0010208  
Range assignment status: DIS0010209

Subnet Discovery Status | Range Assignment Status

The status of the subnet discovery executed against the MID servers that were selected for auto-assignment. The Identified Subnets related list displays the subnet identified during this phase of the discovery.

Number	DIS0010208	State	Completed
Started	17	Discover	Subnet
Completed	17	Created	2017-10-03 20:54:37
Duration	8 Minutes	Updated	2017-10-03 21:02:53

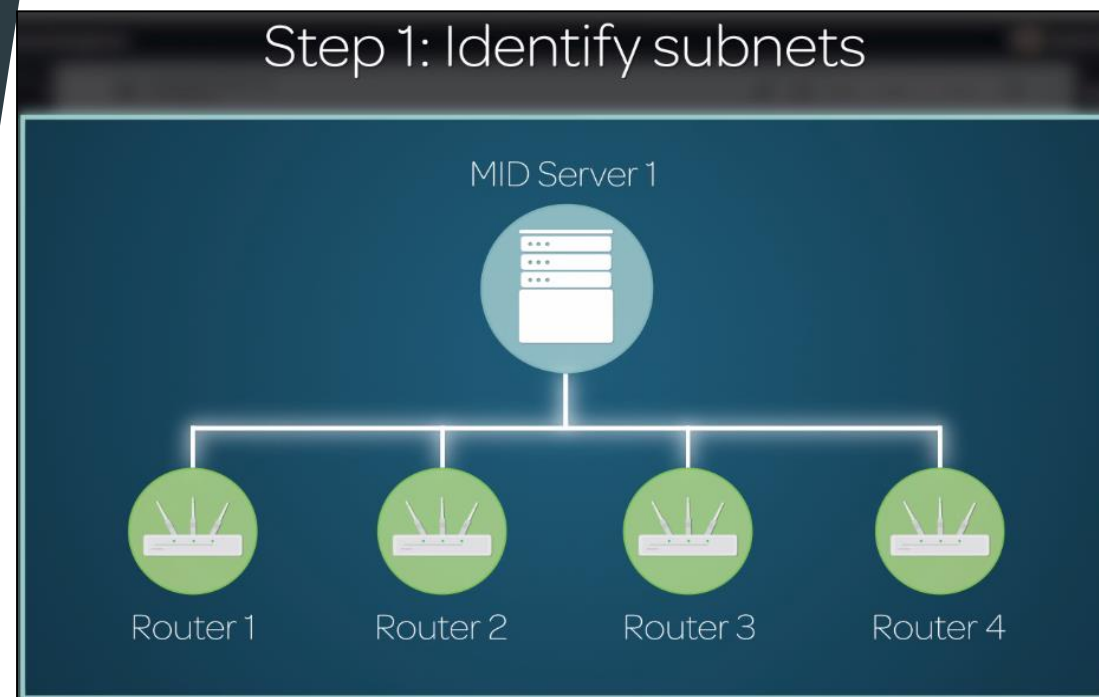
# ITOM - Midserver

- ▶ 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



Automation Status Set STA0001002

MID Servers Used (1) Subnet Router Queue (17) Subnet ECC Queue (34) Identified Subnets (24) Subnet Discovery Log (5) Autoconfig Queue (359)

Autoconfig ECC Queue (718) IP Range Assignments (29) Unreachable Subnets (330) IP Range Assignment Log (4)

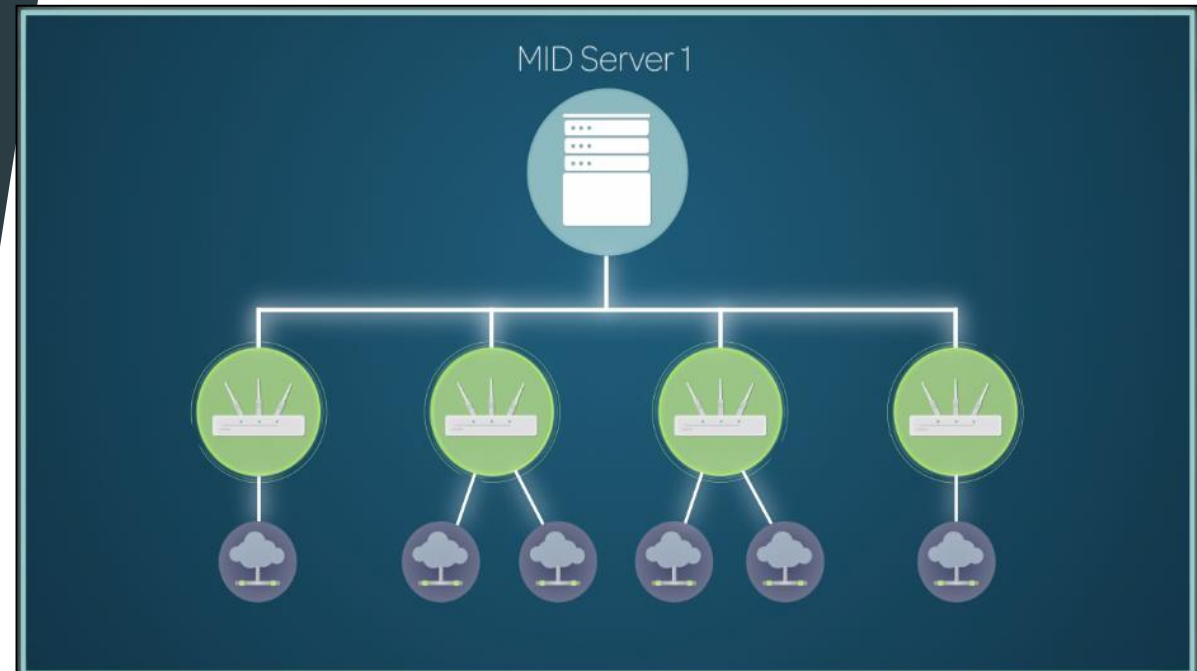
Subnet Router Queue Go to MID Server Search

Subnet Discovery Queues

	MID Server	Result	Router IP Address	State	Domain
<input type="checkbox"/>	Demo MID Server 4	success	10.22.26.6	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.28.13	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.26.4	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.28.6	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.26.7	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.26.13	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.17.15	processed	global
<input type="checkbox"/>	Demo MID Server 4	success	10.22.17.14	processed	global
<input type="checkbox"/>	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



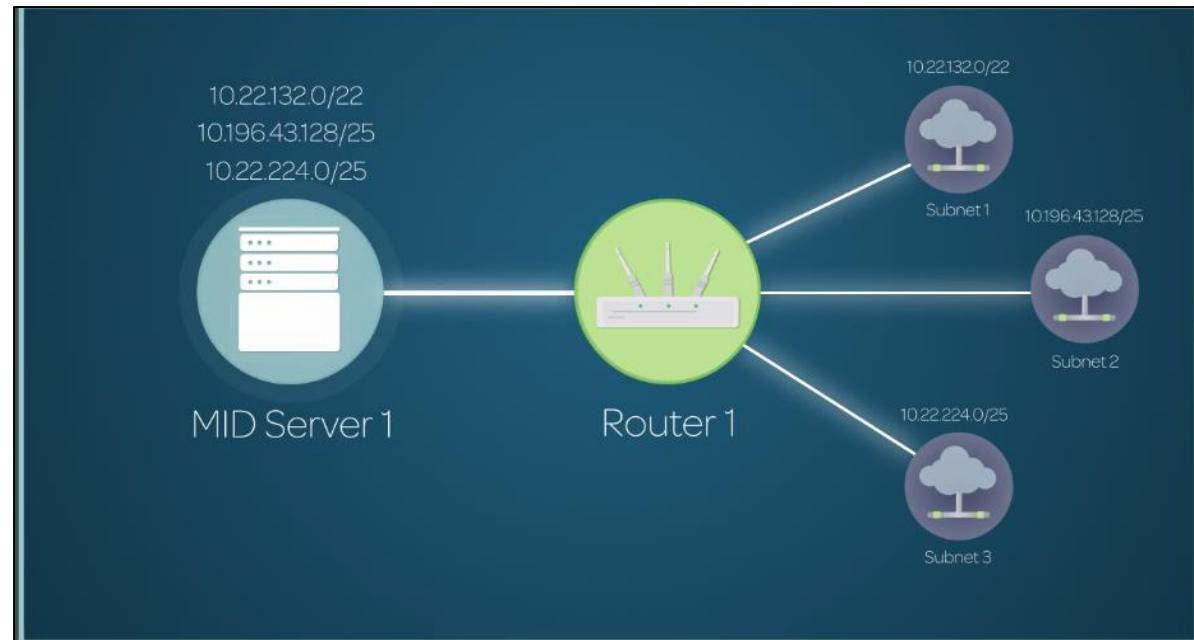
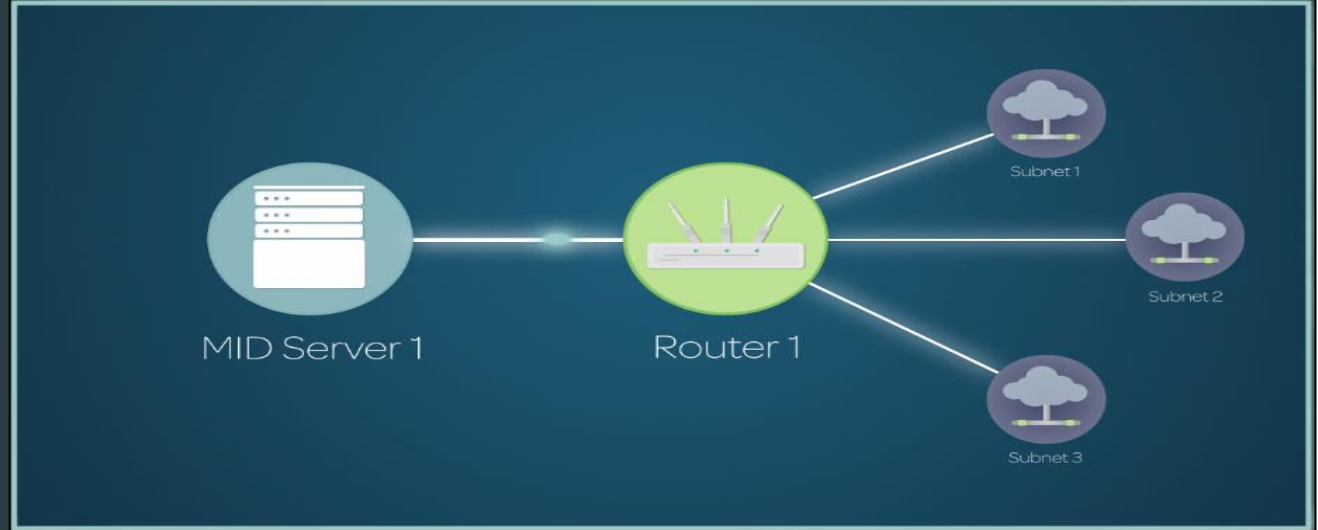
The screenshot shows the 'Identify Subnets' tab in the ITOM interface. The top navigation bar includes tabs for 'MID Servers Used (1)', 'Subnet Router Queue (17)', 'Subnet ECC Queue (34)', 'Identify Subnets (24)', 'Subnet Discovery Log (5)', and 'Autoconfig Queue (359)'. Below this, there are more tabs: 'Autoconfig ECC Queue (718)', 'IP Range Assignments (29)', 'Unreachable Subnets (330)', and 'IP Range Assignment Log (4)'. The main content area is titled 'Identified Subnets' and shows a list of subnets with their domains. The list is paginated, showing 1 to 20 of 24 items.

Subnet	Domain
10.22.132.0/22	global
10.196.43.128/25	global
10.22.224.0/25	global
10.196.38.0/24	global
10.196.128.0/24	global
10.196.133.0/24	global
10.22.225.0/25	global
10.196.129.0/24	global

# 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.

## Step 2: Identify IP address ranges



# ITOM - Midserver

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

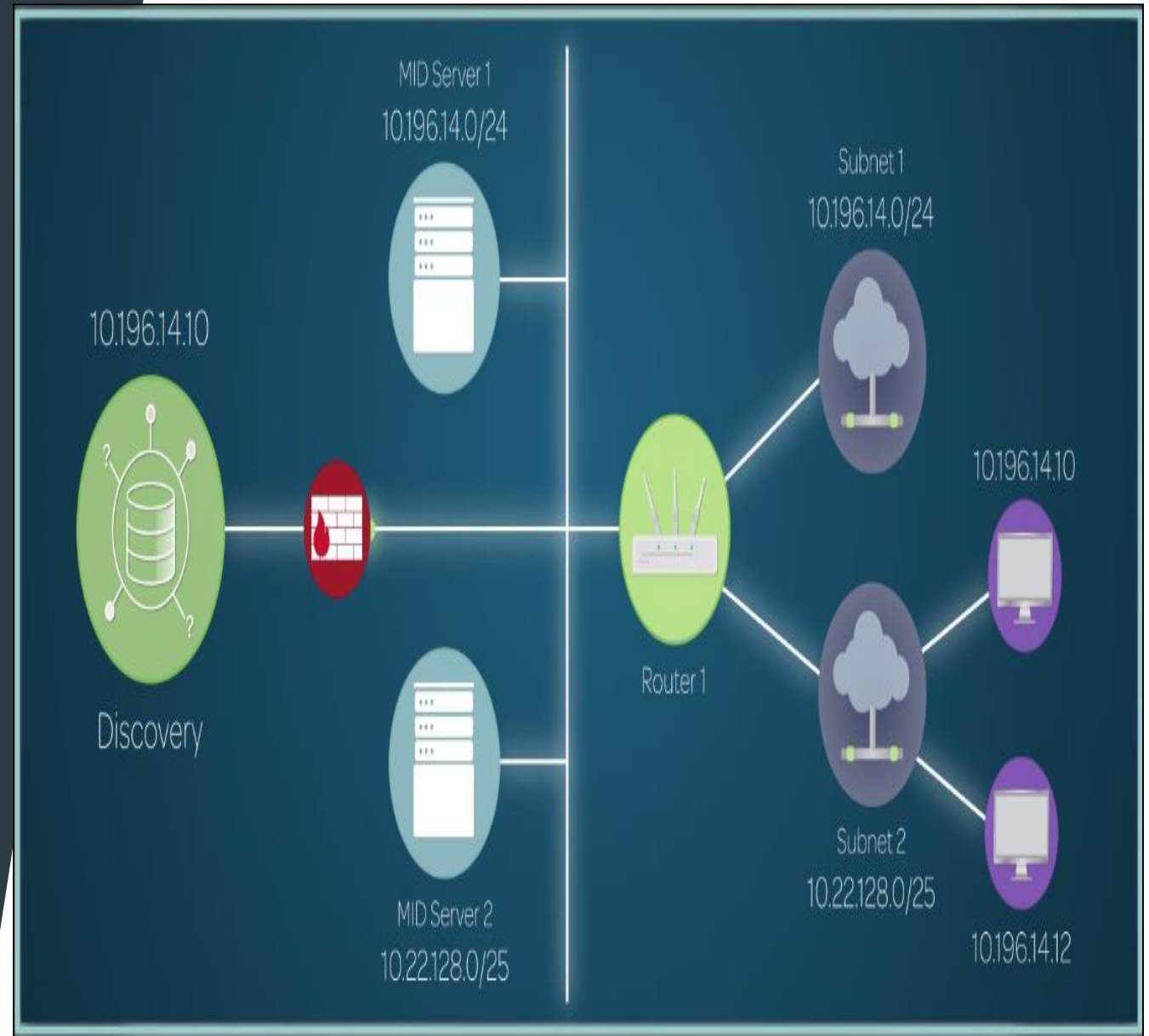
The screenshot displays the ITOM Midserver interface. At the top, there's a header bar with a navigation menu, the title 'Automation Status Set STA0001002', and action buttons like 'Update' and 'Delete'. Below the header, a series of tabs are visible: 'MID Servers Used (1)', 'Subnet Router Queue (17)', 'Subnet ECC Queue (34)', 'Identified Subnets (24)', 'Subnet Discovery Log (5)', 'Autoconfig Queue (359)', 'Autoconfig ECC Queue (718)', 'IP Range Assignments (29)', 'Unreachable Subnets (330)', and 'IP Range Assignment Log (4)'. The 'IP Range Assignments (29)' tab is selected and highlighted. Below the tabs, there's a sub-header for 'IP Range Assignments' with a 'Go to' dropdown set to 'IP Collection' and a search bar. The main content area shows a table titled 'MID Server Auto Configuration Queues'. The table has two columns: 'IP Collection' and 'MID Server'. It lists several IP ranges, each with an information icon (i) and a checkbox. The IP ranges are: 10.196.14.0/24, 10.22.128.0/25, 10.196.130.0/24, 10.255.20.0/24, 10.22.225.0/25, 10.196.43.0/25, 10.22.192.0/25, 10.12.251.0/24, and 10.196.129.0/24. All are assigned to 'Demo MID Server 4'. The table is paginated, showing '1 to 20 of 29' items.

IP Collection	MID Server
<input type="checkbox"/> <a href="#">10.196.14.0/24</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.22.128.0/25</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.196.130.0/24</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.255.20.0/24</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.22.225.0/25</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.196.43.0/25</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.22.192.0/25</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.12.251.0/24</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.196.129.0/24</a>	Demo MID Server 4
<input type="checkbox"/> <a href="#">10.355.16.0/24</a>	Demo MID Server 4



# 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 are 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.

The screenshot displays the ITOM Midserver configuration interface. On the left, a vertical progress bar shows 16% completion, with a green checkmark icon indicating the current step. The main area lists 5 tasks completed: Create MID User, Download & Install MID, Validate MID, Add SNMP Credentials, and Auto-Assign MID Server IP Ranges. The 'Auto-Assign MID Server IP Ranges' task is highlighted, showing options to 'Skip', 'Add Notes', 'Mark as Incomplete', and 'Configure'. Below this, a section titled 'Auto-Assign MID Server IP Ranges' provides optional instructions for populating IP ranges using SNMP credentials or manually configured ranges.

16% Complete

5 / 5 Tasks completed

- ✓ Create MID User
- ✓ Download & Install MID
- ✓ Validate MID
- ✓ Add SNMP Credentials
- ✓ Auto-Assign MID Server IP Ranges

**Add SNMP Credentials** [Skip](#) [Add Notes](#) [Mark as Incomplete](#) [Configure](#)

Completed just now by System Administrator

[Optional] If you want to automatically populate the selected MID Server's IP Ranges in the next step, you will need SNMP credentials to access the routers on your network.

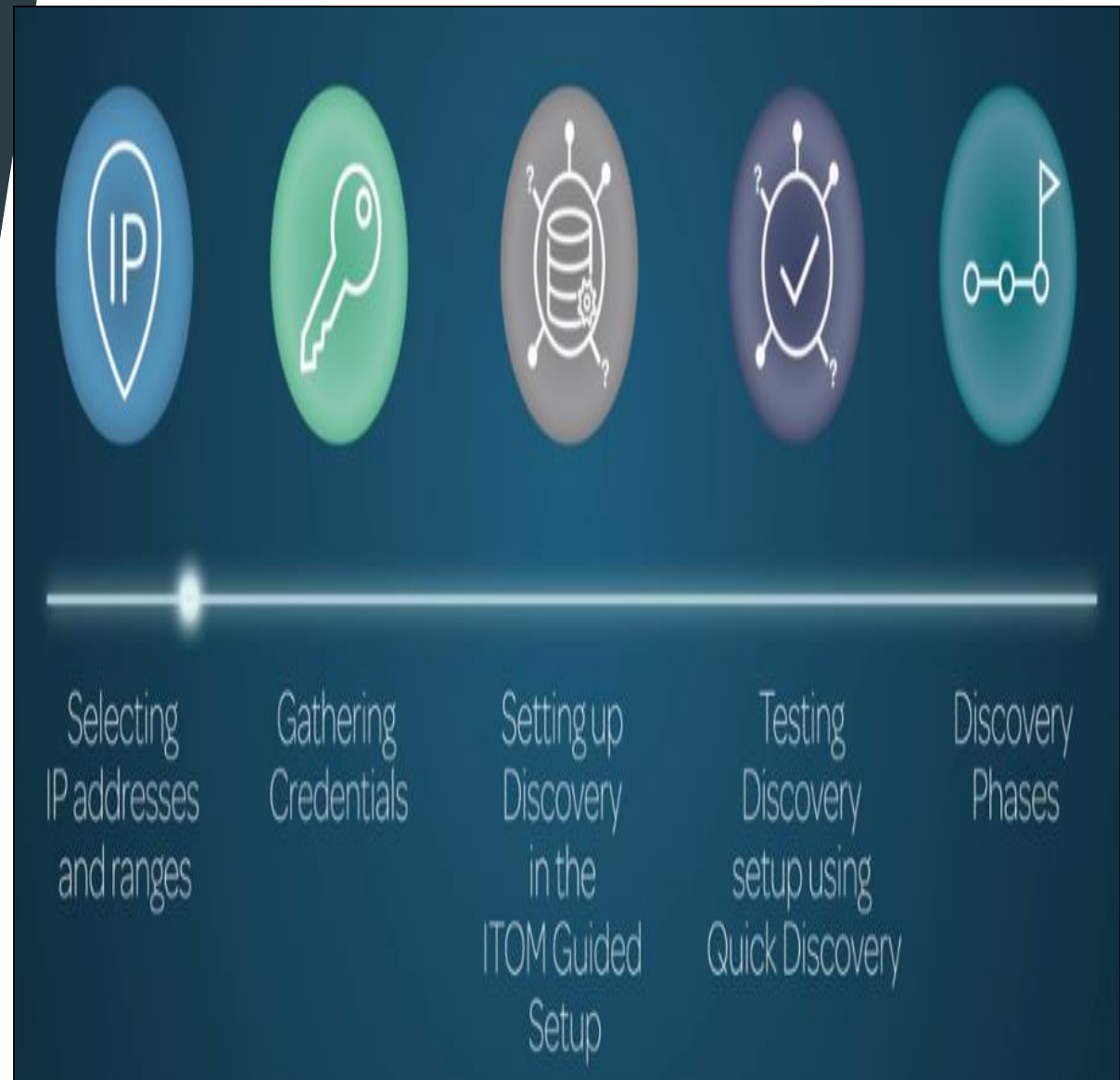
**Auto-Assign MID Server IP Ranges** [Skip](#) [Add Notes](#) [Mark as Incomplete](#) [Configure](#)

Completed just now by System Administrator

[Optional] Use this feature to automatically populate the selected MID Server's IP Ranges, using the SNMP credentials added above. Otherwise, your MID Servers will either use the default 'All' IP Range that is applied optionally during Validation or any manually configured IP Ranges that are directly added to the MID Server form.

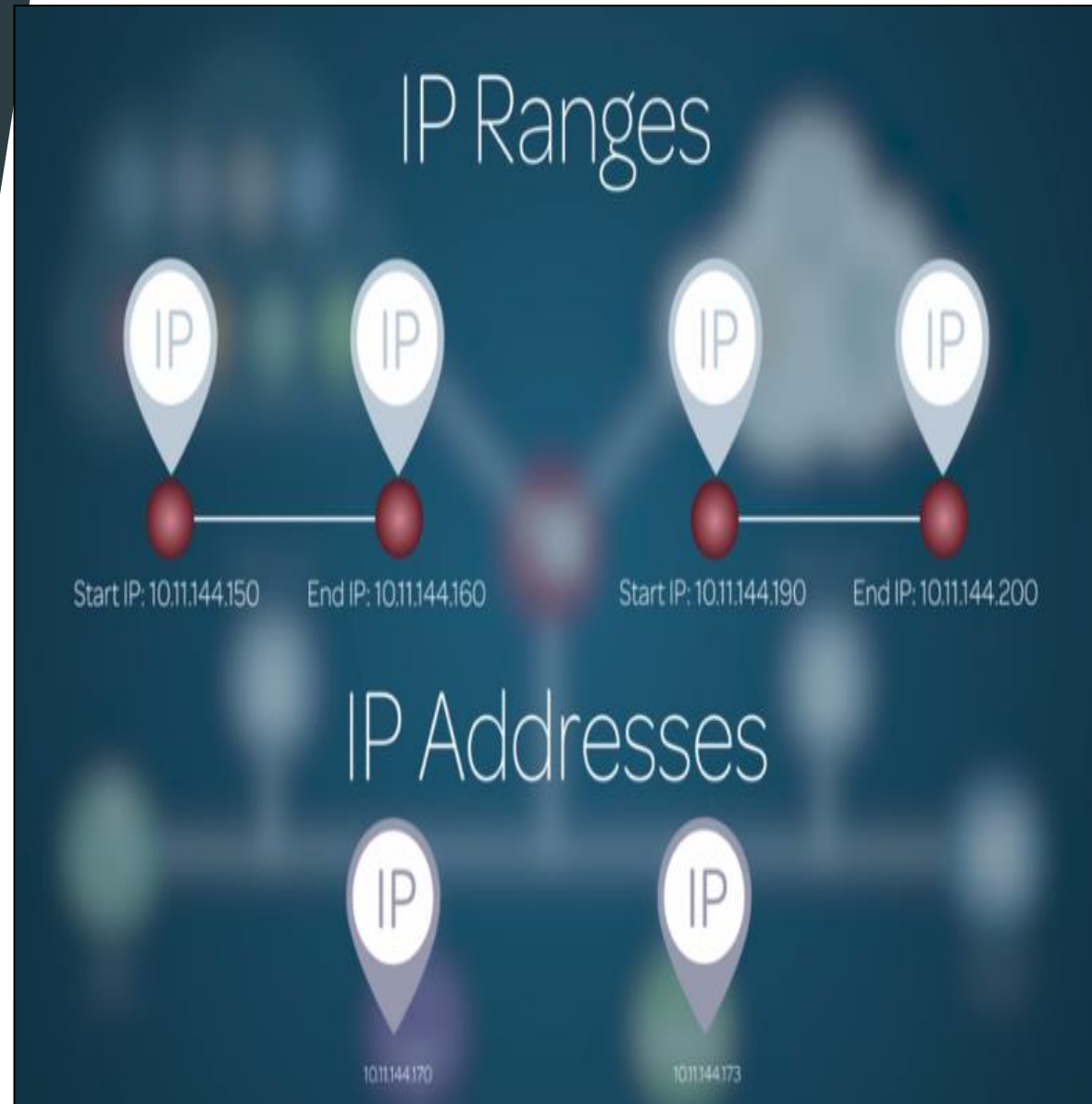
# ITOM - Discovery with Service Mapping

- ▶ 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 Addresses 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

The screenshot shows the 'Discovery Schedule' configuration page for 'Revature Office'. The page has a header with a back arrow, a menu icon, the title 'Discovery Schedule', the name 'Revature Office', and an 'Update' button. Below the header is a light blue instruction bar: 'Select a discovery type from the Discover list and configure its attributes to create a discovery schedule.' The main form contains several fields: 'Name' (text input with 'Revature Office'), 'Discover' (dropdown menu with 'Configuration items'), 'MID Server selection method' (dropdown menu with 'Auto-Select Mid Server'), 'Active' (checkbox, checked), 'Location' (text input with '800 K Street Northwest, Washington'), 'Max run time' (fields for Days, Hours, and Minutes, all set to 00), 'Run' (dropdown menu with 'Weekly'), 'Day(run\_dayofweek)' (dropdown menu with 'Monday'), and 'Time' (fields for Hours, Minutes, and Seconds, set to 22, 00, 00). At the bottom, there is an 'Advanced' section header.

The screenshot shows the 'Discovery IP Ranges' table for the 'Revature Office' schedule. The table has a header with a back arrow, a menu icon, the title 'Discovery Schedule', the name 'Revature Office', and buttons for 'Update' and 'Delete'. Below the header is a light blue instruction bar: 'Quick ranges Discover now'. The table has three tabs: 'Discovery IP Ranges (1)', 'Discovery Range Sets', and 'Discovery Status'. The 'Discovery IP Ranges (1)' tab is active. The table has a toolbar with a 'New' button, a 'Search' button, a search input field with 'for text', and a 'Search' button. The table has a filter icon and the text 'Schedule = Revature Office'. The table has a toolbar with a filter icon, a search icon, a menu icon, and the text 'Type', 'Summary', and 'Active'. The table has one row with the following data: 'IP Network', '10.0.0.0/24', and 'true'. The table has a toolbar with a filter icon, a search icon, a menu icon, and the text 'Actions on selected rows...'. The table has a toolbar with a filter icon, a search icon, a menu icon, and the text '1 to 1 of 1'.

	Type	Summary	Active
<input type="checkbox"/>	<a href="#">IP Network</a>	10.0.0.0/24	true

# ITOM - Discovery

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

The screenshot displays the 'Discovery IP Range' configuration window. The 'Name' field is set to 'IP Network'. The 'Application' is 'Global', and the 'Active' checkbox is checked. The 'Attributes' field is empty. The 'Network mask (or bits)' is set to '24', and the 'Network IP' is '10.0.0.0'. The 'Discovery range' is set to 'Private IP Addresses'. The 'Summary' is '10.0.0.0/24', the 'Domain' is 'global', the 'Type' is 'IP Network', and the 'Schedule' is 'Revature Office'. Below the main form are 'Update' and 'Delete' buttons. A section titled 'Discovery Range Item Excludes' contains a 'New' button, a search bar with 'for text' selected, and a search button. At the bottom, a filter bar shows 'Parent = IP Network' and a 'Summary' button.

Discovery IP Range  
IP Network

Name: IP Network

Application: Global

Active: ☒

Attributes:

\* Network mask (or bits): 24

\* Network IP: 10.0.0.0

Discovery range: Private IP Addresses

Summary: 10.0.0.0/24

Domain: global

Type: IP Network

Schedule: Revature Office

Update Delete

Discovery Range Item Excludes

Discovery Range Item Excludes New Search for text Search

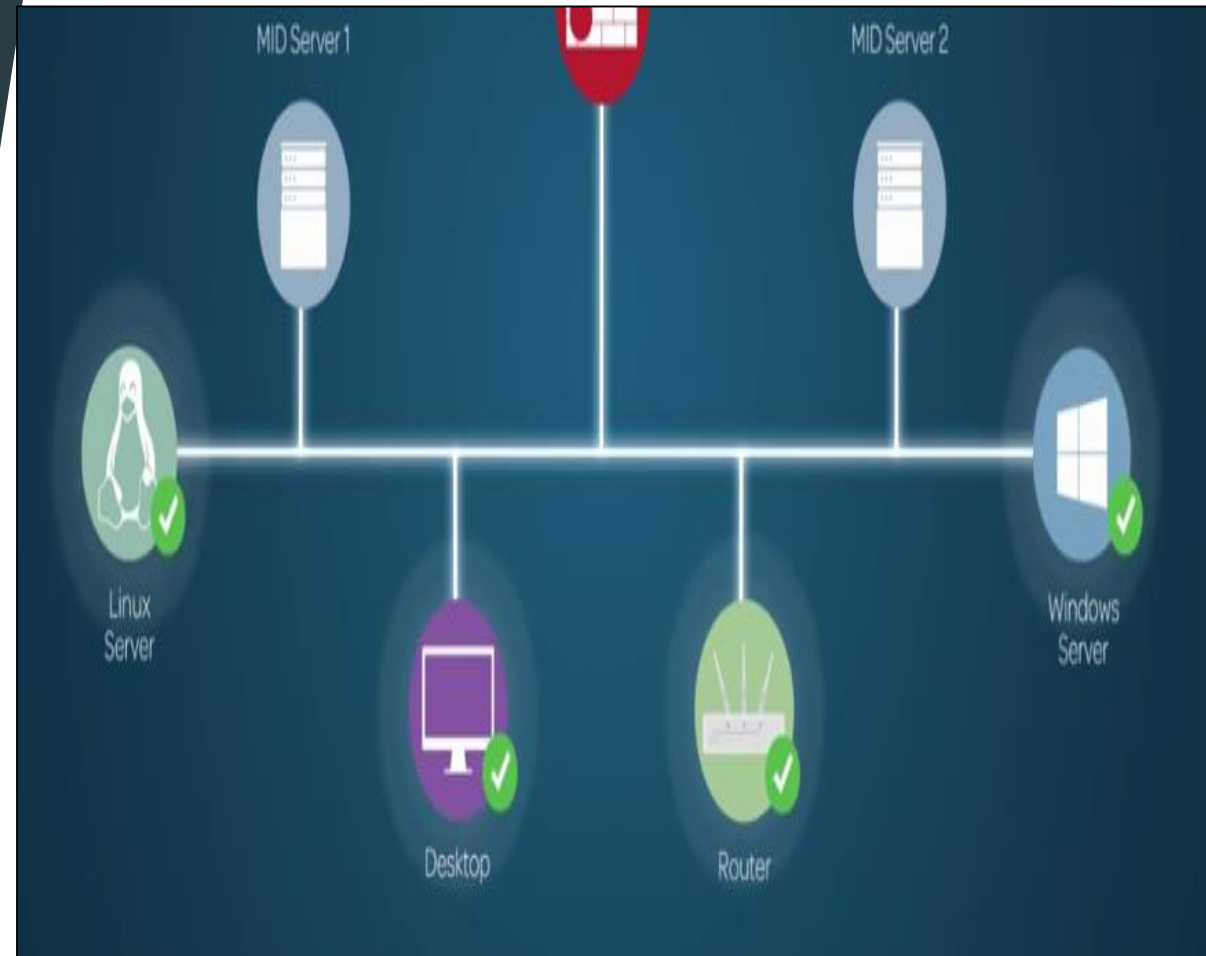
Parent = IP Network

Summary



# ITOM - Discovery

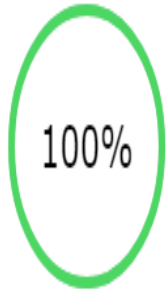
- ▶ Next step is to gather list of credentials for the devices on the network which you would want to discover including windows and unix computers.
- ▶ Midserver uses login credentials to query the devices otherwise it fails to discover them.



# ITOM - Discovery

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

[<](#) IT Operations Management Guided Setup > Discovery [Assign](#)



## Discovery

Discovery finds computers and other devices connected to an enterprise's network and populates the CMDB with such things as hardware attributes, software data, active business services, and the relationships between these configuration items. Complete the activities in this category to create the credentials Discovery needs to gain access to a computer or network device and to create the schedule that determines when Discovery runs and what MID Server it uses.

3 / 3 Tasks completed

✓ Select Discovery Targets

✓ Add Credentials

✓ Auto-Create Schedules

**Select Discovery Targets** [View Notes](#)

Completed 7d ago by System Administrator

Mark as Incomplete

Configure

Specify which devices and application types to include or exclude as Discovery populates the CMDB.

# 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.

The screenshot shows the 'Discovery Configuration Console' interface. At the top, a header bar contains a back arrow, the title 'Discovery Configuration Console', and a help icon. Below the header is a light blue informational box with text explaining how to populate the CMDB and a 'More Info' link. The main content area is divided into three sections: 'Devices', 'Applications', and 'Software Filter'. The 'Devices' section has a title bar with an info icon and lists four categories: 'Network Devices', 'Storage Devices', 'Unix Servers & Computers', and 'Windows Servers & Computers', each with a green toggle switch. The 'Applications' section also has a title bar with an info icon and lists three categories: 'Automation', 'Databases', and 'Web & Application Servers', each with a green toggle switch. The 'Software Filter' section has a title bar with an info icon and contains tabs for 'Unix' and 'Windows'. The 'Windows' tab is active, showing an 'Enabled' toggle switch and a 'Mode' selector with 'Include' and 'Exclude' buttons. Below this is a text input field labeled 'Enter a new key to filter on ...' and a green 'New Key' button.

Discovery Configuration Console

Populate the CMDB with the Discovery data you want to collect. You can specify which devices and application types to ignore and create a filter to include or exclude specific UNIX and Windows software. When you select a configuration item to exclude from the CMDB, the instance disables the related probe or classifier that scans that CI. This action does not deactivate the probe or classifier for general use across the system. [More Info](#)

**Devices**

- ▶ Network Devices
- ▶ Storage Devices
- ▶ Unix Servers & Computers
- ▶ Windows Servers & Computers

**Applications**

- Automation
- Databases
- Web & Application Servers

**Software Filter**

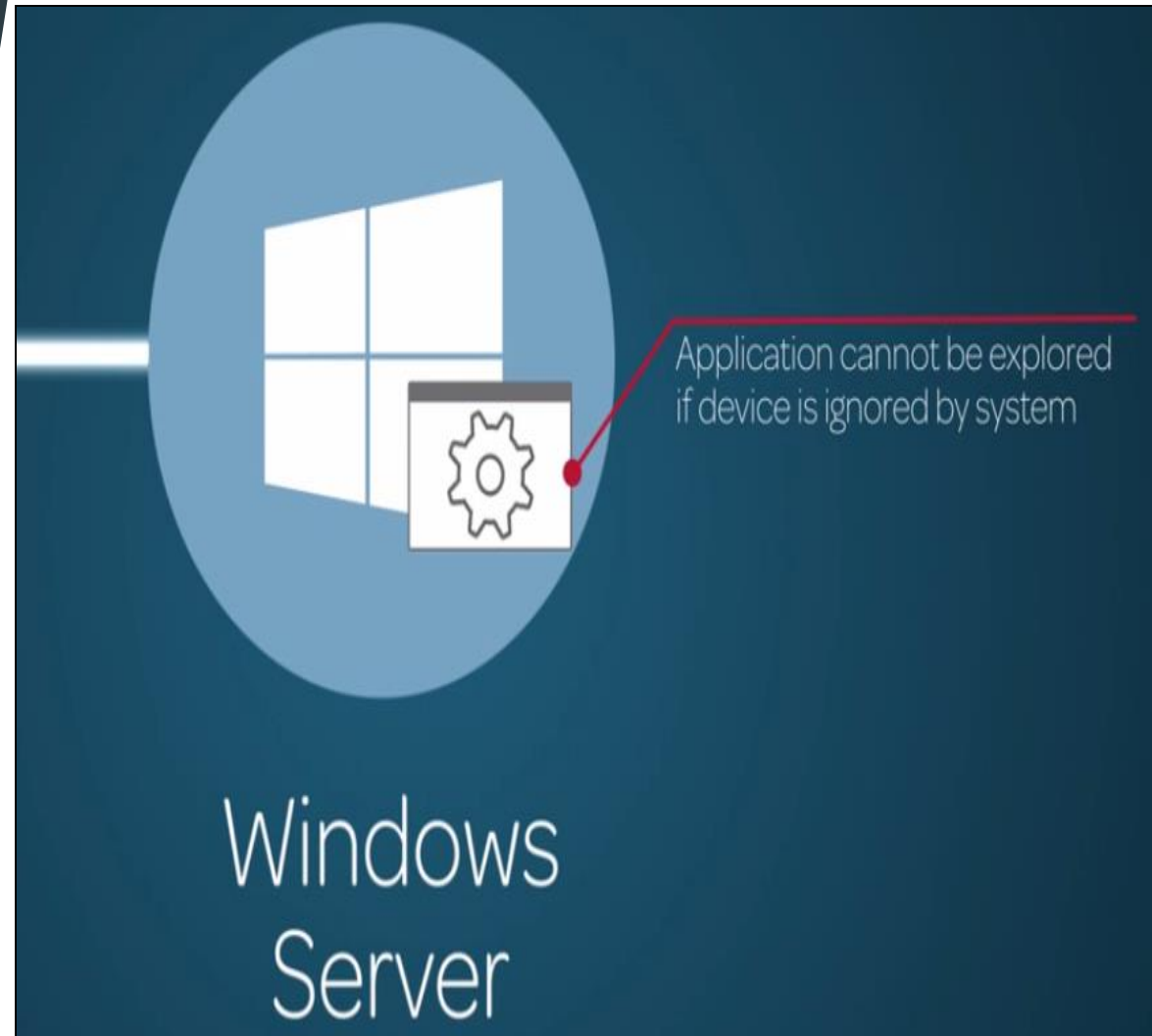
Unix Windows

Enabled: Mode: Include Exclude

Enter a new key to filter on ... New Key

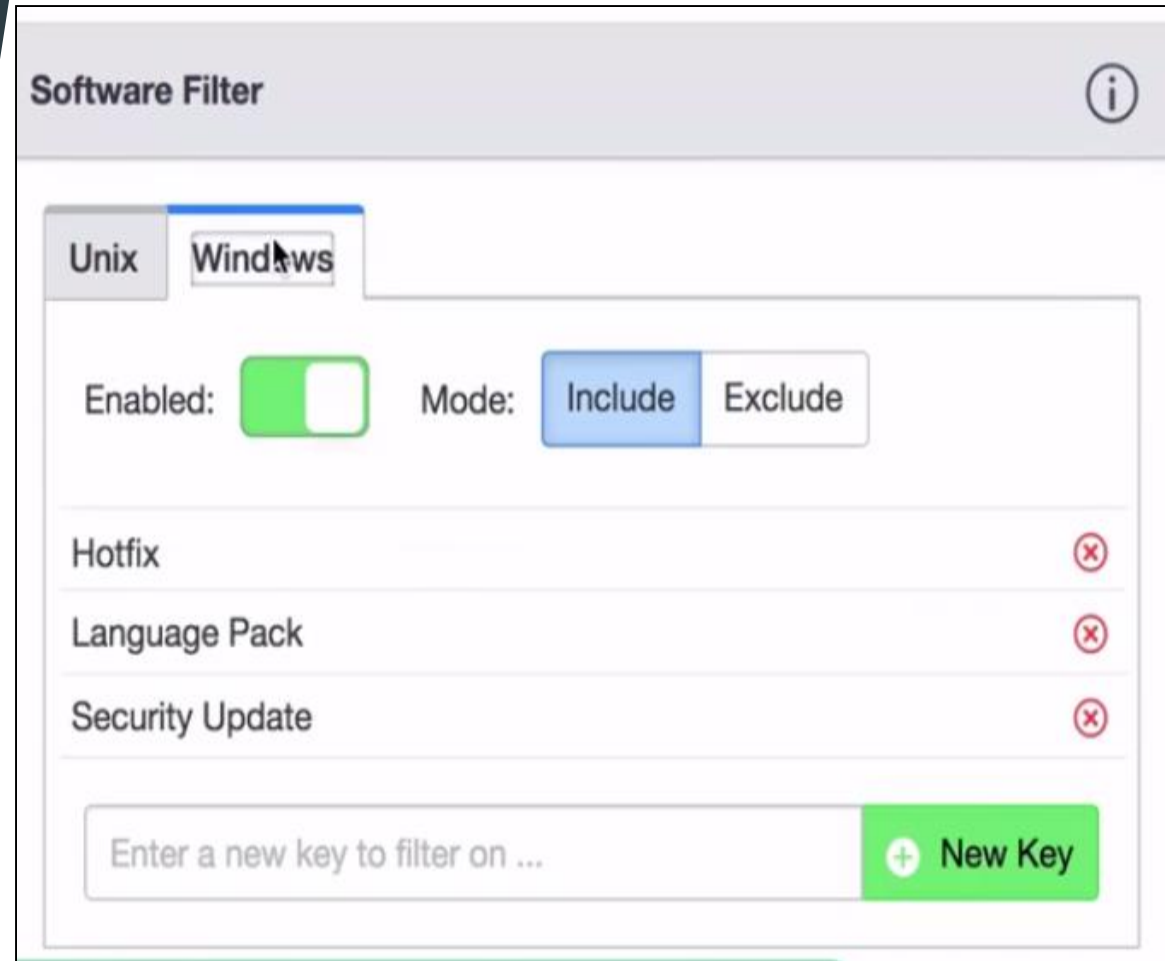
# ITOM - Discovery

- ▶ 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

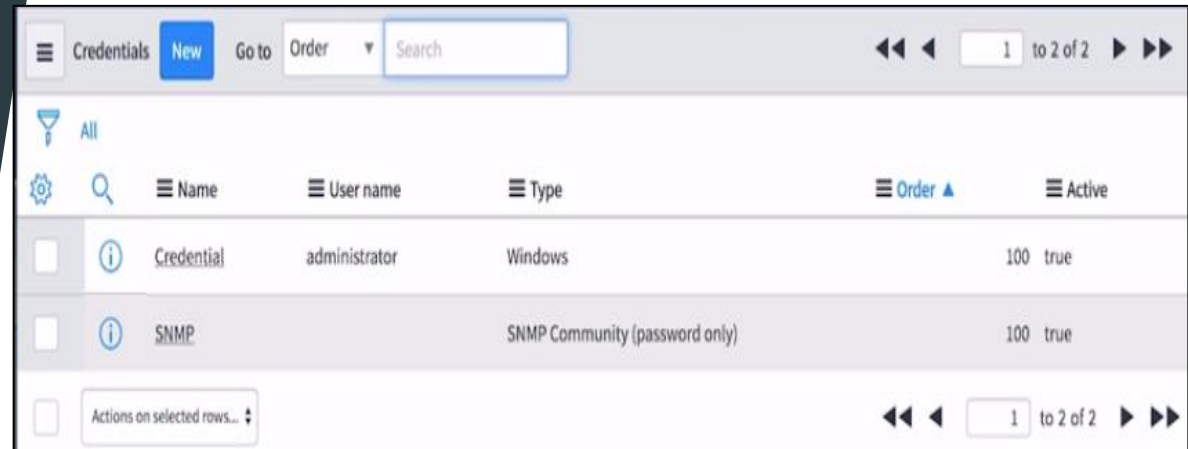
- ▶ Software filter allows you to filter the software's added to the CMDB using keywords.
- ▶ When the filter is disabled for the OS whole discovered softwares for that OS are not added to the CMDB conversely if the OS is enabled only softwares that includes or excludes with the specified keywords will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



The screenshot shows a 'Software Filter' window with a title bar and an information icon. It features two tabs: 'Unix' and 'Windows', with 'Windows' currently selected. Below the tabs, there is an 'Enabled' toggle switch that is turned on (green) and a 'Mode' section with 'Include' (selected) and 'Exclude' buttons. A list of keywords is displayed, each with a red 'X' icon to its right: 'Hotfix', 'Language Pack', and 'Security Update'. At the bottom, there is a text input field with the placeholder 'Enter a new key to filter on ...' and a green '+ New Key' button.

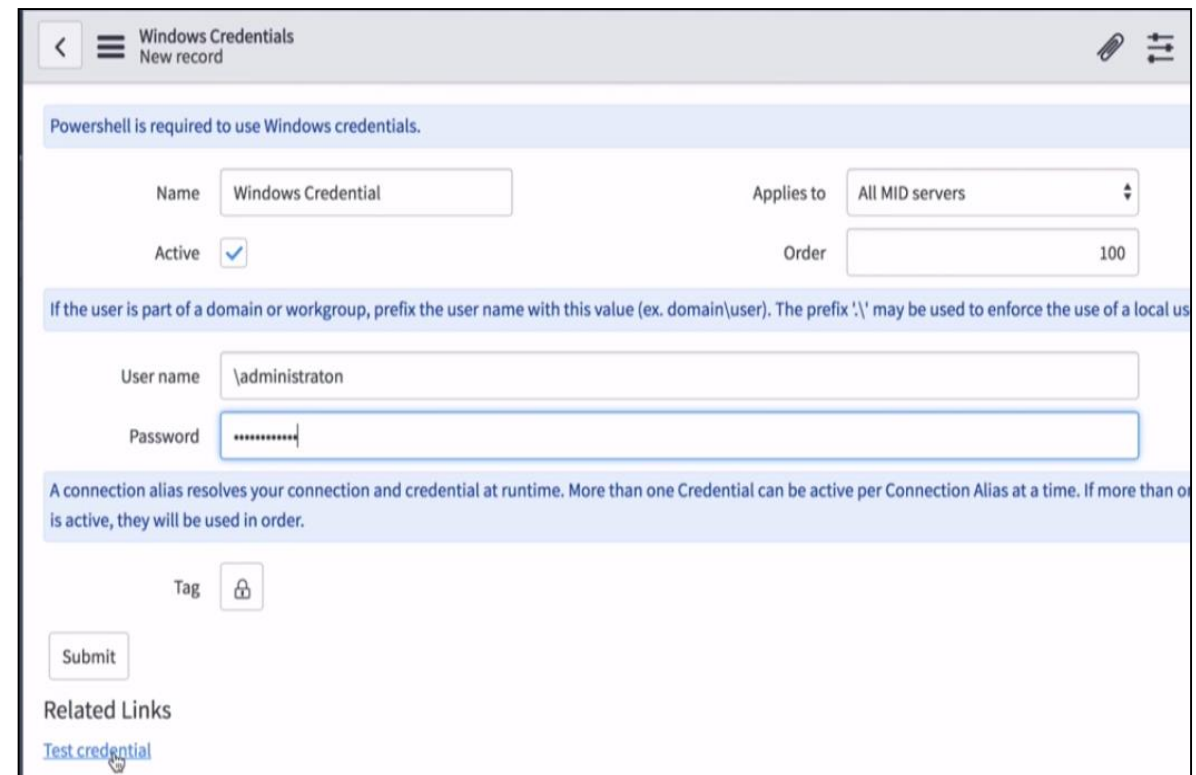
# ITOM - Discovery

- ▶ Mark the step as complete and return to Guided setup.
- ▶ Next step is to add credentials. In our example let's 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



The screenshot shows a web interface for managing credentials. At the top, there are tabs for 'Credentials', 'New', 'Go to', 'Order', and a search bar. Below the tabs, there is a table with columns: Name, User name, Type, Order, and Active. The table contains two entries: 'Credential' with user name 'administrator' and type 'Windows', and 'SNMP' with type 'SNMP Community (password only)'. Both have an order of 100 and are active.

	Name	User name	Type	Order	Active
<input type="checkbox"/>	<a href="#">Credential</a>	administrator	Windows	100	true
<input type="checkbox"/>	<a href="#">SNMP</a>		SNMP Community (password only)	100	true



The screenshot shows a form titled 'Windows Credentials' with a subtitle 'New record'. It includes a note: 'Powershell is required to use Windows credentials.' The form has fields for 'Name' (set to 'Windows Credential'), 'Applies to' (set to 'All MID servers'), 'Active' (checked), and 'Order' (set to 100). Below these, there is a note: 'If the user is part of a domain or workgroup, prefix the user name with this value (ex. domain\user). The prefix '\\' may be used to enforce the use of a local user.' The 'User name' field is set to '\\administraton' and the 'Password' field is masked with asterisks. At the bottom, there is a 'Tag' field with a lock icon, a 'Submit' button, and a 'Related Links' section with a link to 'Test credential'.

Windows Credentials  
New record

Powershell is required to use Windows credentials.

Name: Windows Credential Applies to: All MID servers  
Active: ☒ Order: 100

If the user is part of a domain or workgroup, prefix the user name with this value (ex. domain\user). The prefix '\\' may be used to enforce the use of a local user.

User name: \\administraton Password:

A connection alias resolves your connection and credential at runtime. More than one Credential can be active per Connection Alias at a time. If more than one is active, they will be used in order.

Tag:

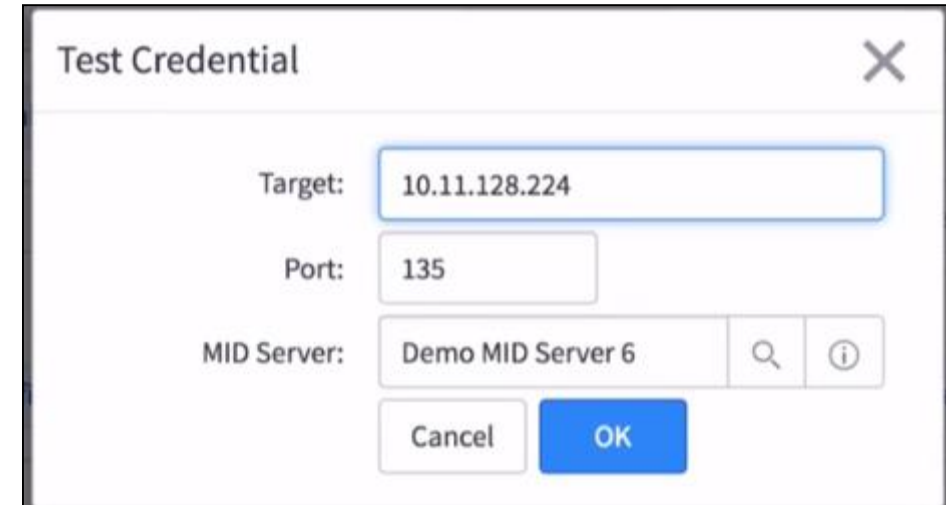
Submit

Related Links  
[Test credential](#)

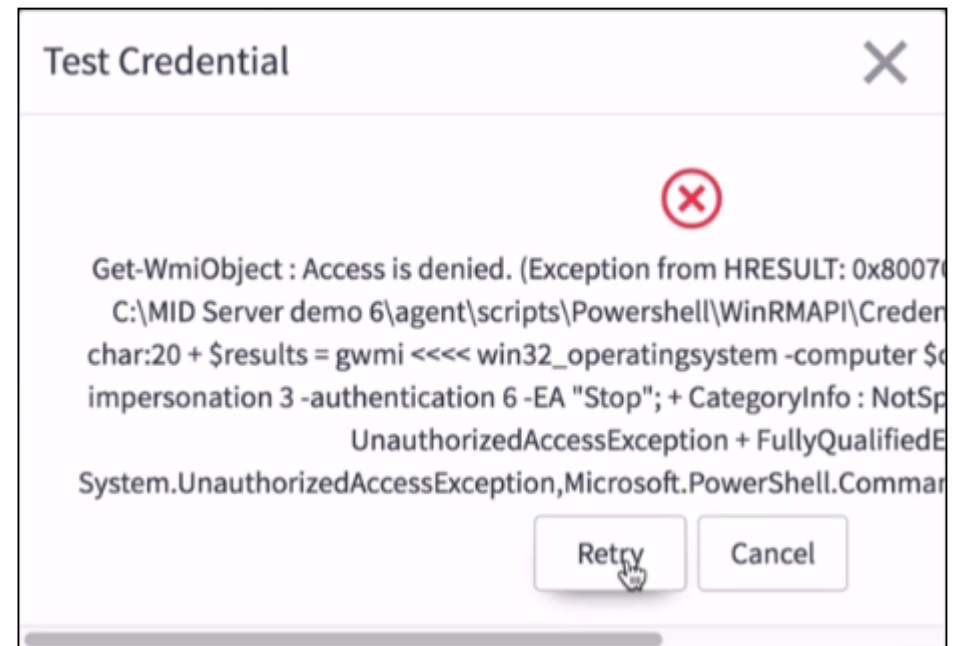


# ITOM - Discovery

- ▶ 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



A screenshot of a 'Test Credential' dialog box. It has a title bar with a close button (X). The dialog contains three input fields: 'Target:' with the value '10.11.128.224', 'Port:' with the value '135', and 'MID Server:' with the value 'Demo MID Server 6'. To the right of the 'MID Server' field are search and information icons. At the bottom are 'Cancel' and 'OK' buttons.



A screenshot of the 'Test Credential' dialog box showing an error. A red circle with a white 'X' is centered at the top. Below it, the error message reads: 'Get-WmiObject : Access is denied. (Exception from HRESULT: 0x80070005) C:\MID Server demo 6\agent\scripts\Powershell\WinRMAPI\Credent char:20 + \$results = gwmi <<<< win32\_operatingsystem -computer \$c impersonation 3 -authentication 6 -EA "Stop"; + CategoryInfo : NotSp UnauthorizedAccessException + FullyQualifiedE System.UnauthorizedAccessException,Microsoft.PowerShell.Command'. At the bottom are 'Retry' and 'Cancel' buttons, with a mouse cursor pointing at the 'Retry' button.

# ITOM - Discovery

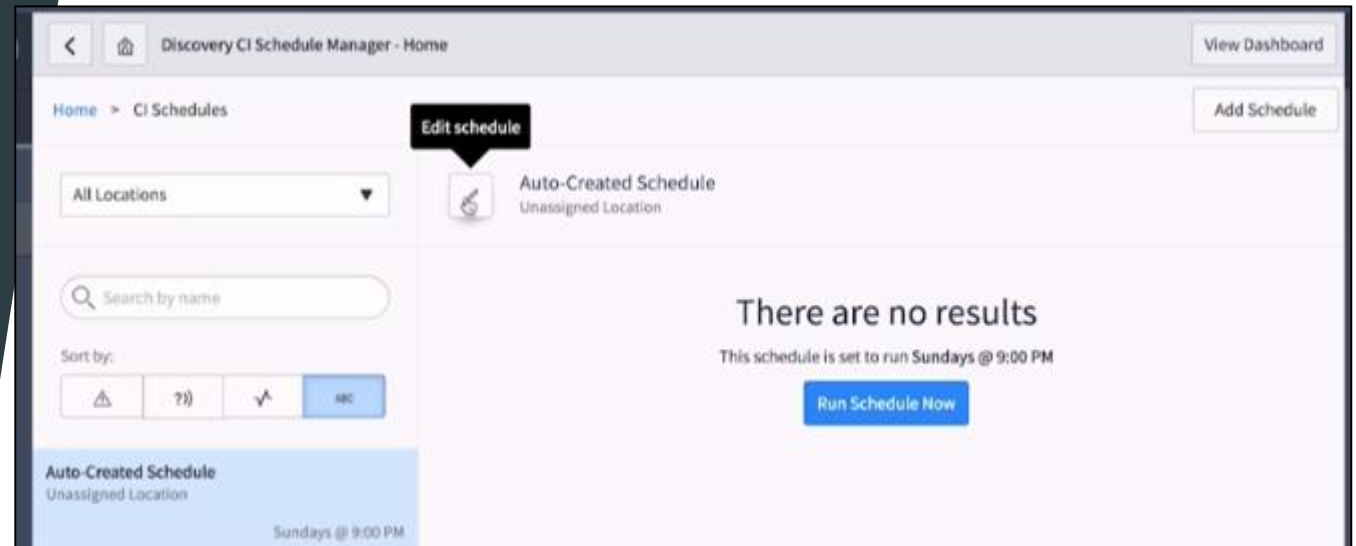
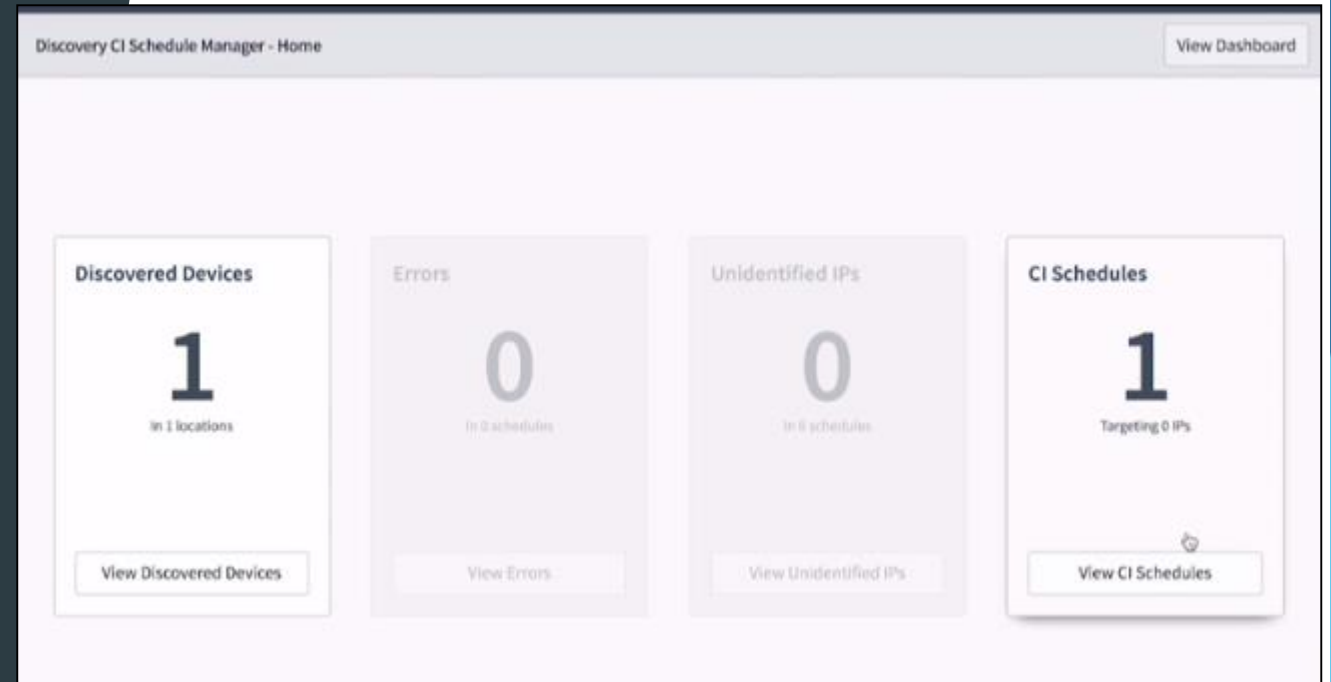
- ▶ Next step is to Auto create a schedule for discovery.
- ▶ Select the window you would want to run within and time options if its applicable.
- ▶ For demo lets create Window for weekly that runs Sunday at 9pm(SNOW uses 24 hr clock convention) relative to SNOW timezone settings.

After completing MID Server IP Range Auto-Assignment, determine when you want Discovery to run on the IP ranges that the MID Server(s) can reach. Discovery Window - select when you want discovery to run.

DISCOVERY WINDOW	FREQUENCY
Select Window Anytime ▼	Window Weekly ▼
	Day Sunday ▼
	Start time 21 ▼ : 00 ▼
<a href="#">Create Schedule</a>	

# 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.

The screenshot shows the 'Discovery Schedule' configuration page for an 'Auto-Created Schedule'. The page has a header with a back arrow, a menu icon, and the title 'Discovery Schedule Auto-Created Schedule'. On the right, there are 'Update' and 'Delete' buttons. The main content area has a light blue header with the instruction: 'Select a discovery type from the Discover list and configure its attributes to create a discovery schedule.'

The configuration fields are as follows:

- Name:** Auto-Created Schedule
- Discover:** Configuration Items
- MID Server selection method:** Auto-Select Mid Server
- Active:** ☒
- Location:** (empty field with a search icon)
- Max run time:** Days 7, Hours 00, 00, 00
- Run:** Weekly
- Day(run\_dayofweek):** Sunday
- Time:** Hours 21, 00, 00

Below these fields is an 'Advanced' section with a downward arrow. It contains:

- Include alive:** ☐
- Log state changes:** ☐
- Use SNMP version:** v1/v2c
- Shazzam batch size:** 5,000
- Shazzam cluster support:** ☒

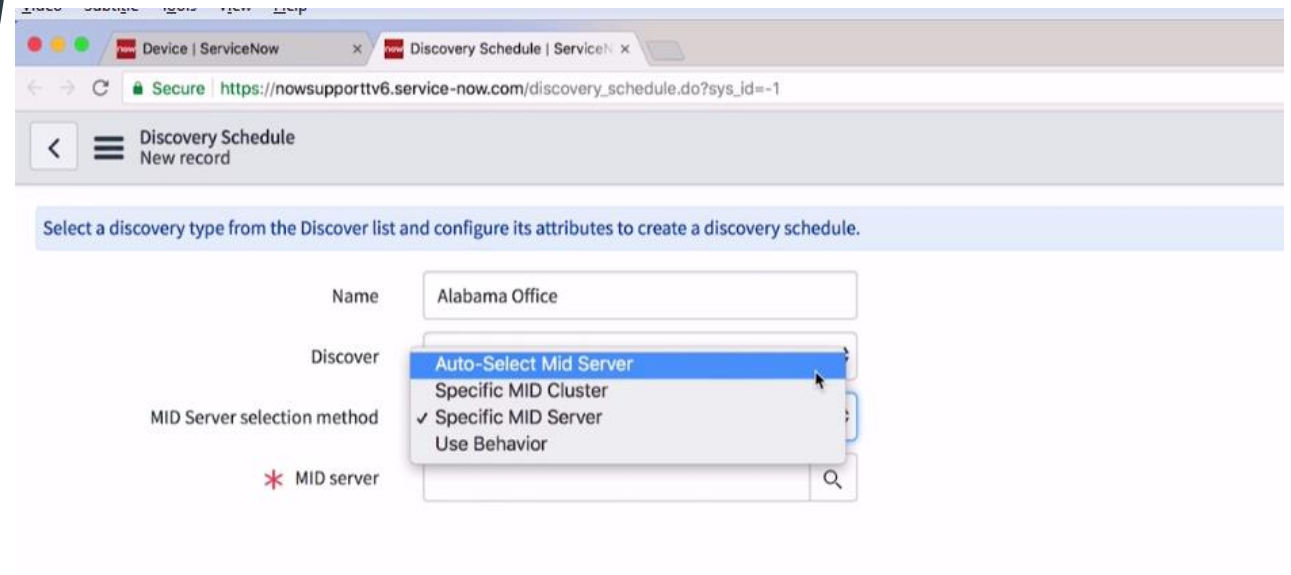
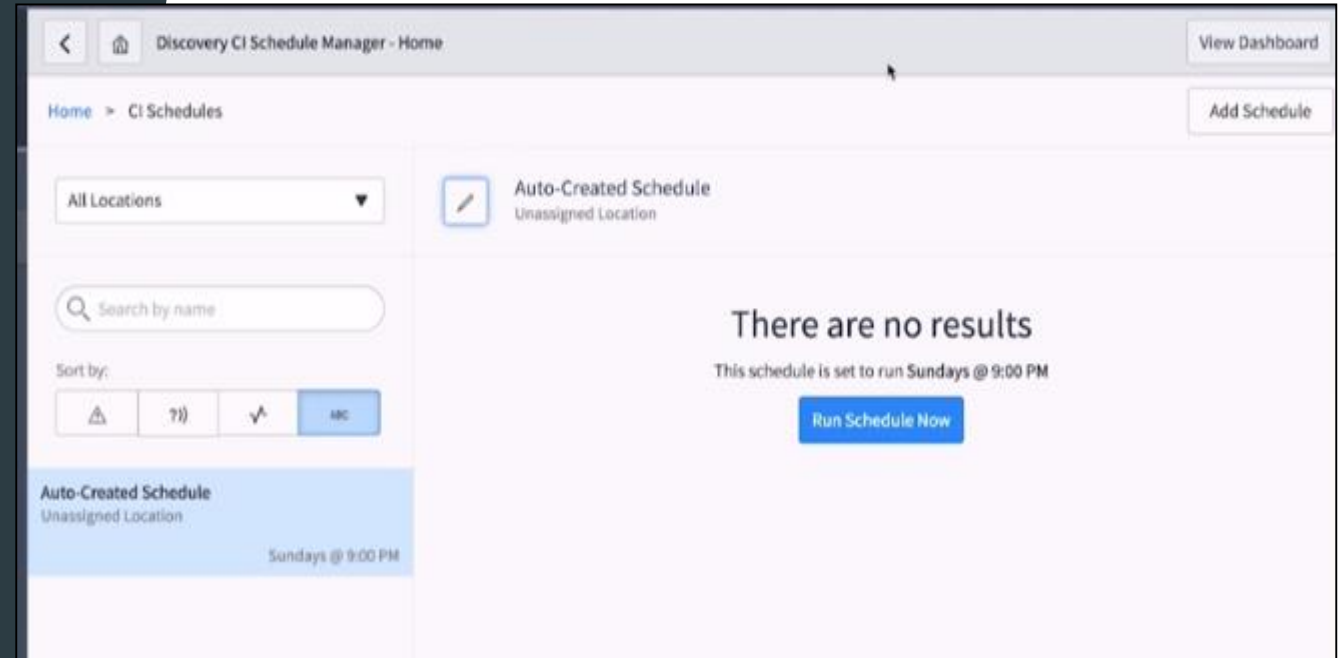
At the bottom left of the advanced section are 'Update' and 'Delete' buttons. Below the advanced section is a 'Related Links' section with two links: 'Quick ranges' and 'Discover now'.

The screenshot shows the 'Discovery IP Ranges' table. The table has a header with 'Discovery IP Ranges (77)', 'Discovery Range Sets', and 'Discovery Status'. Below the header is a search bar with the text 'Search for text' and a search icon. The table has three columns: 'Type', 'Summary', and 'Active'. The 'Type' column contains 'IP Network' for all rows. The 'Summary' column contains IP ranges. The 'Active' column contains 'true' for all rows. The table is sorted by 'Type' and 'Summary'.

Type	Summary	Active
IP Network	10.196.128.0/24	true
IP Network	10.196.129.0/24	true
IP Network	10.196.130.0/24	true
IP Network	10.196.131.0/24	true
IP Network	10.196.132.0/24	true
IP Network	10.196.133.0/24	true
IP Network	10.196.14.0/24	true
IP Network	10.196.31.192/26	true
IP Network	10.196.32.0/26	true
IP Network	10.196.32.192/26	true
IP Network	10.196.33.0/26	true

# 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

The screenshot shows a configuration window for a discovery task. At the top right, there are icons for a document, a list, and a 'Submit' button. The main configuration area includes the following fields:

- Active:** A checkbox that is checked.
- Location:** A text input field containing 'Alabama', with a search icon and an information icon to its right.
- Max run time:** A time selection field with 'Days' set to '00' and 'Hours' set to '00'.
- Run:** A dropdown menu set to 'Weekly'.
- Day(run\_dayofweek):** A dropdown menu set to 'Monday'.
- Time:** A time selection field with 'Hours' set to '22' (highlighted in yellow) and 'Minutes' set to '00'.

# 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

The screenshot shows the 'Advanced' configuration page in the ITOM interface. The 'Quick Ranges' dialog box is open, displaying the example IP ranges: 10.0.1.0/24, 10.0.2.1-10.0.2.15, 10.0.3.176, 10.0.3.222. The dialog box includes a text input field for entering IP ranges and buttons for 'Make Ranges' and 'Cancel'. The background page shows options for 'Include alive', 'Log state changes', and 'Use SNMP version' (v1/v2c).

This screenshot shows the 'Quick Ranges' dialog box with the IP range 10.0.1.0/24 entered in the text input field. The dialog box includes the same instructions and buttons as the previous screenshot.



# ITOM - Discovery

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

	Name	Run	Discover	Location	Active
<input type="checkbox"/>	Alabama Office	Weekly	Configuration Items	Alabama	true
<input type="checkbox"/>	Auto-Created Schedule	Weekly	Configuration Items		true

	Number	Created	Description	Schedule	Discover	State	Started	Completed	Upda
<input type="checkbox"/>	DIS0010048	2017-12-11 14:22:59	Discover Now	Alabama Office	Configuration Items	Starting	0	0	2017-12-14:22:59

# ITOM - Discovery

- ▶ We click the status of Discovery to watch the progress
- ▶ We can click refresh to check the updated status

The screenshot displays the 'Discovery Status' interface for DIS0010048. At the top, there are navigation icons and buttons for 'Update' and 'Delete'. The main section, titled 'From Schedule', contains configuration fields: 'Discover' (set to 'Configuration items'), 'Max run time' (set to '0'), 'Include alive' (checkbox), and 'Log state changes' (checkbox). Below these are 'Update' and 'Delete' buttons. A 'Related Links' section provides links for 'Refresh', 'Show Discovery timeline', and 'Cancel Discovery'. The bottom section, 'Discovery Log (1)', includes tabs for 'Discovery Log', 'Devices', and 'ECC Queue'. The 'Discovery Log' tab is active, showing a table with one entry. The table has columns for 'Created', 'Level', 'Short Message', 'ECC queue input', 'CI', 'Source', and 'Device'. The entry shows a timestamp of '2017-12-11 14:22:59', level 'Information', and message 'Discovery started'. Navigation controls for the log are visible at the bottom.

Discovery Status  
DIS0010048

From Schedule

Discover: Configuration items

Max run time: 0

Include alive: ☐

Log state changes: ☐

Update Delete

Related Links

[Refresh](#)  
[Show Discovery timeline](#)  
[Cancel Discovery](#)

Discovery Log (1) | Devices | ECC Queue

Discovery Log | New | Go to: Created | Search

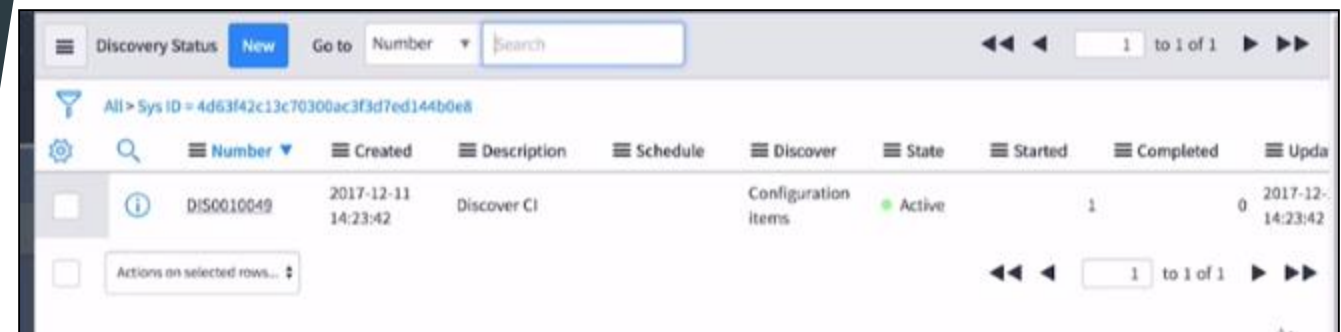
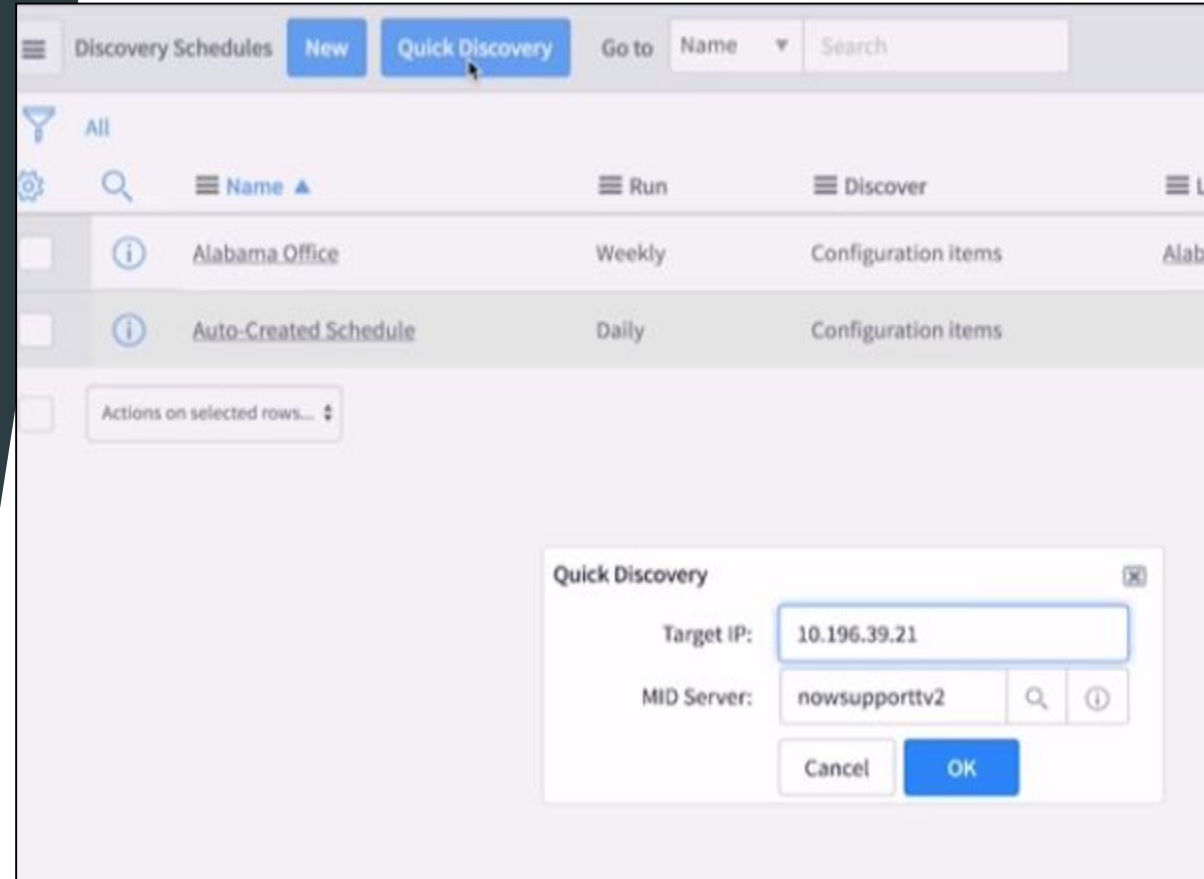
Discovery Log

	Created	Level	Short Message	ECC queue input	CI	Source	Device
<input type="checkbox"/>	2017-12-11 14:22:59	Information	Discovery started			Discovery	

Actions on selected rows...

# 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

<

Discovery Status  
DIS0010049



UpdateDelete

The Discovery Status contains the details of a Discovery that has been launched from a Discovery Schedule. The Status displays high level information about the results of a Discovery, including logs, probes, sensors, and the ECC queue. Read more about [the Discovery Status](#) or find assistance with [Discovery troubleshooting](#).

Number

DIS0010049

Description

Discover CI

Schedule

Q

State

Completed

⌵

Started

5

Completed

3

From Schedule

⌵

Discover

Configuration items

Max run time

00

00

00

Include alive

☐

Log state changes

☒

Update

Delete

Related Links

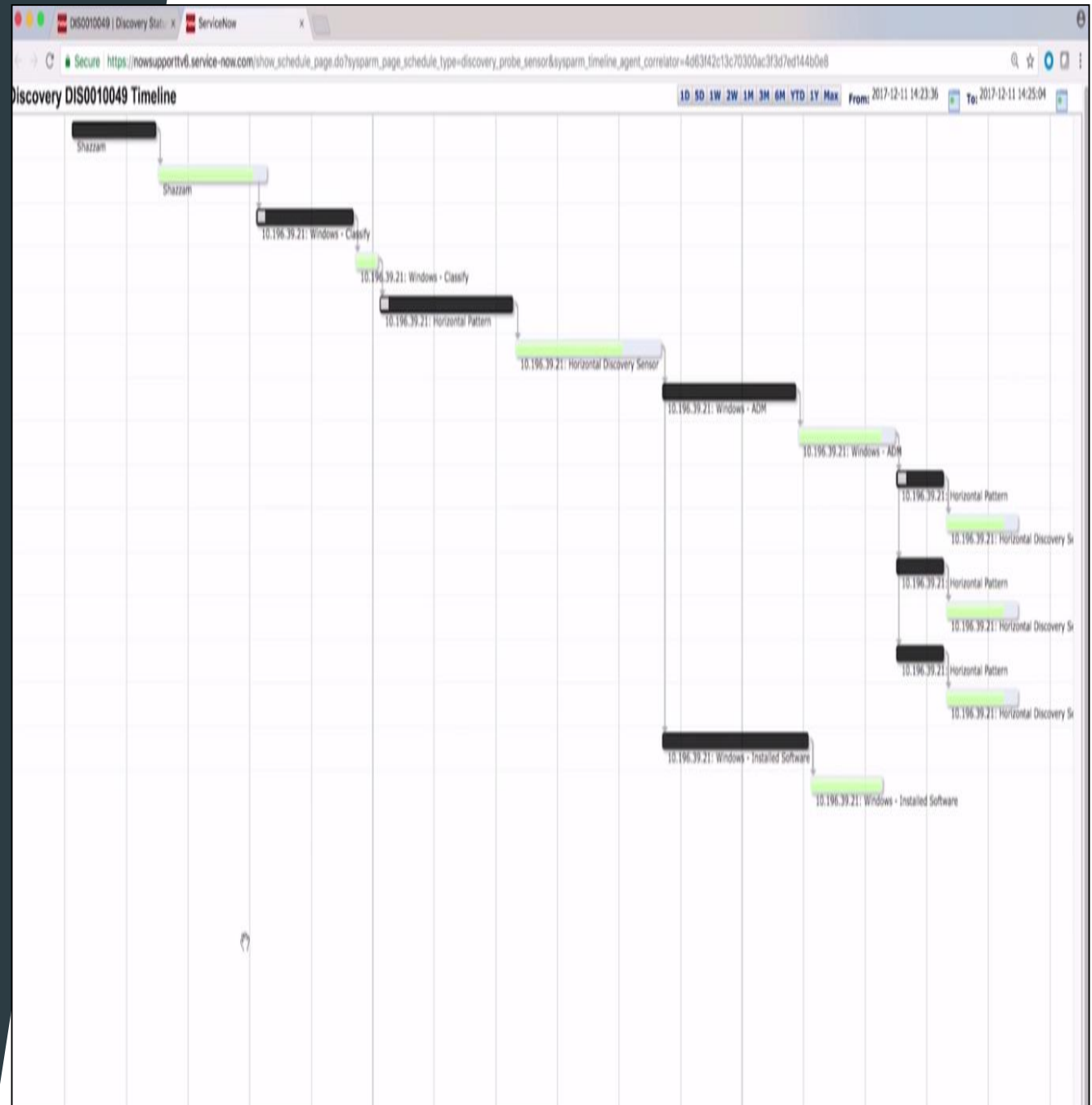
[Refresh](#)

[Show Discovery timeline](#)

[Cancel Discovery](#)

# ITOM - Discovery

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



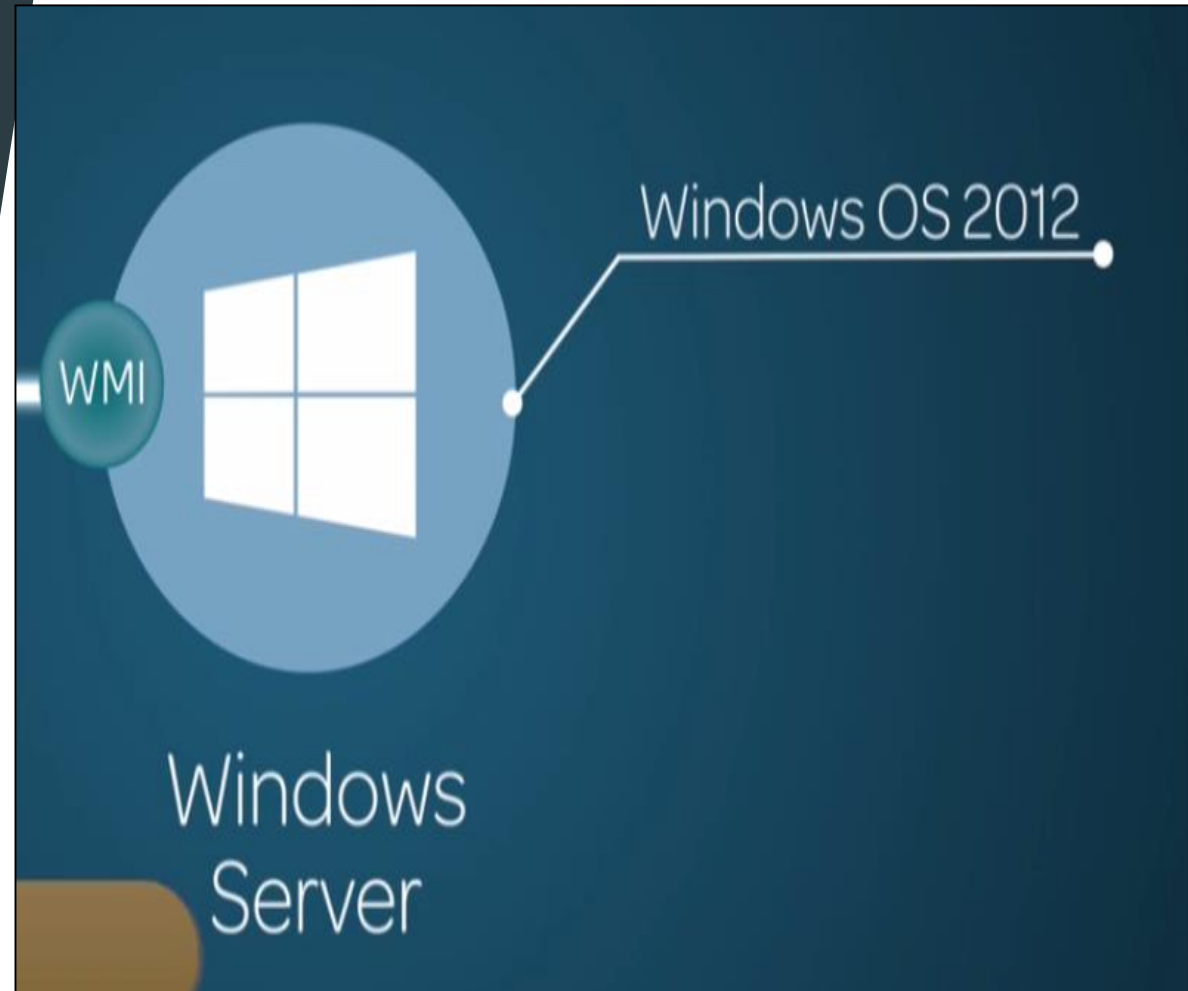
# ITOM - Discovery

- ▶ 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

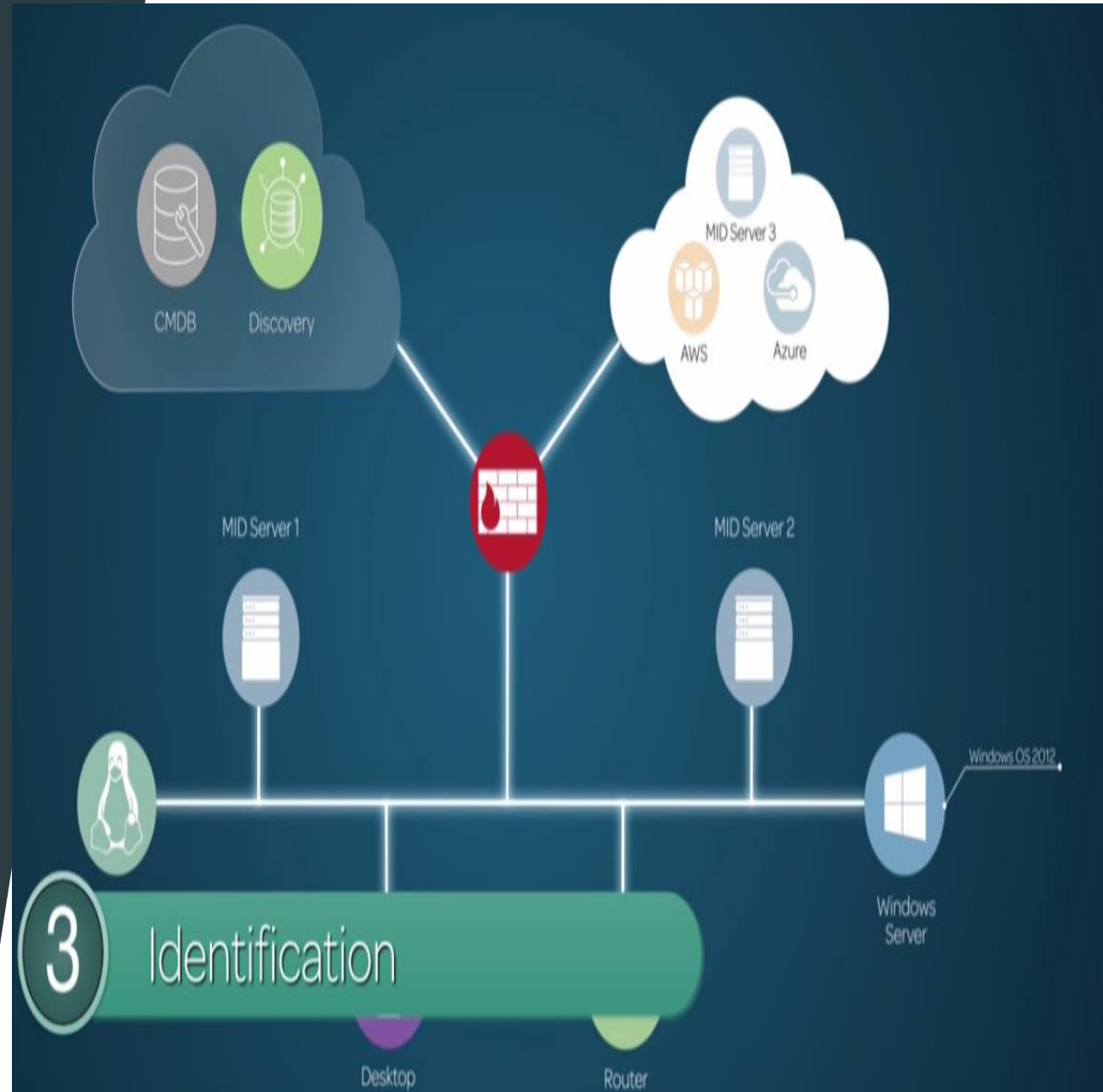
- ▶ In the second phase discovery Classification discovery continues to send probes to find type of device in each IP address
- ▶ In windows discovery example discovery sends WMI used for Windows device OS 2012 to determine which OS is running on that device





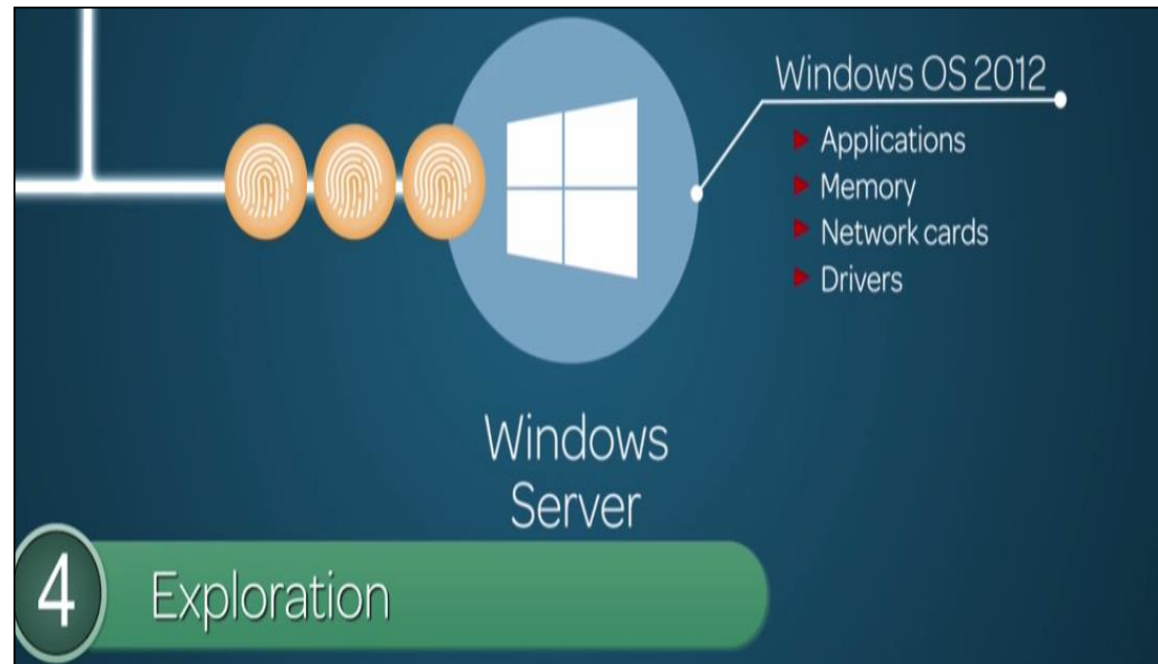
# ITOM - Discovery

- ▶ 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



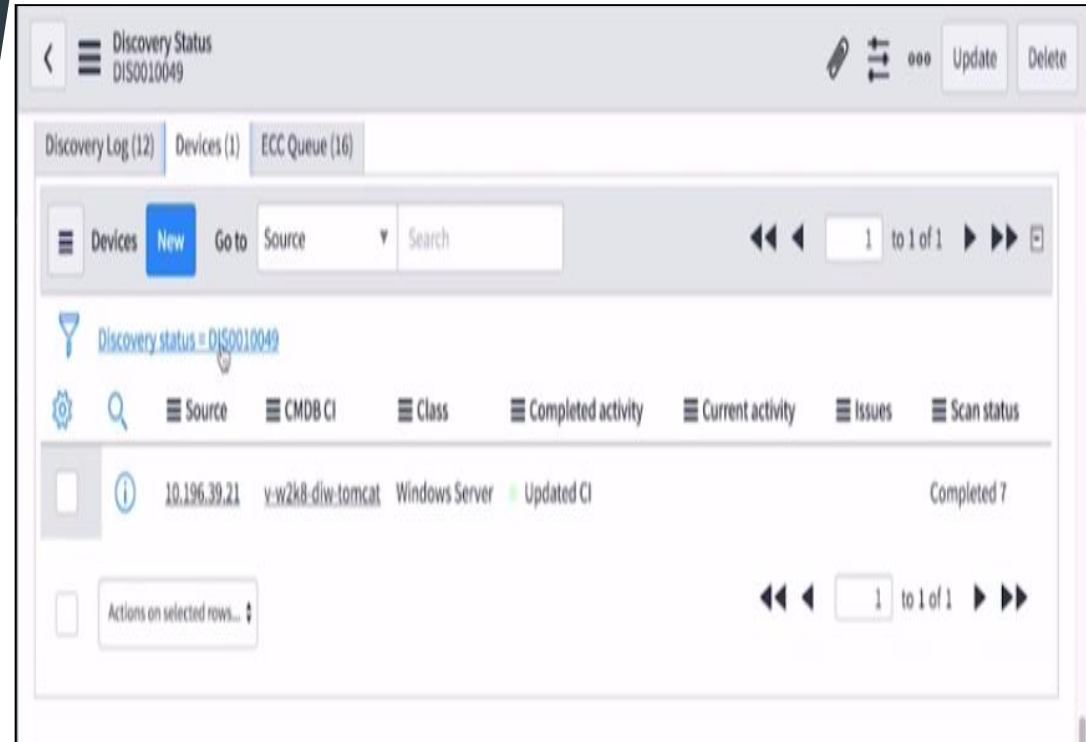
# ITOM - Discovery

- ▶ 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

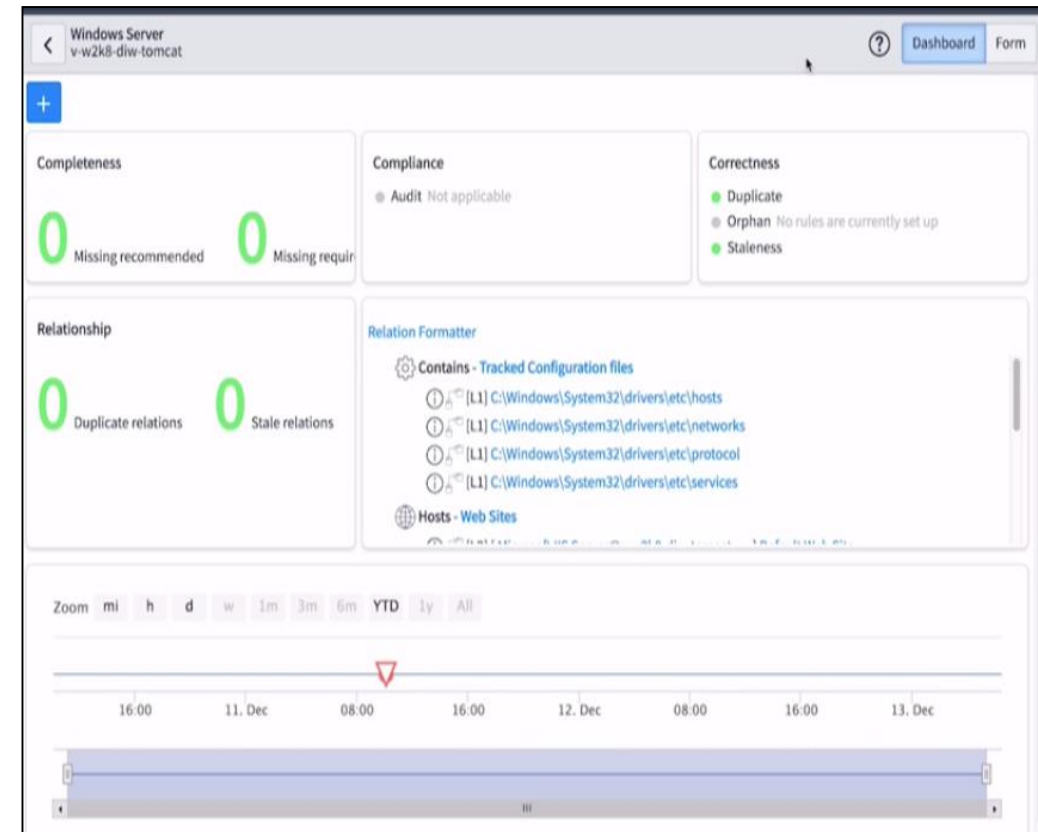
- ▶ In the Discovery Status we can see if new CI is updated in Devices found in the Related links



# 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

This screenshot shows the 'Form' view of an ITOM console for a specific asset. The header bar includes a back arrow, a hamburger menu, the asset name 'Windows Server v-w2k8-dlw-tomcat', and action buttons: 'Dashboard', 'Form' (selected), 'Update', and 'Delete'. The main form area contains several input fields: 'Name' (v-w2k8-dlw-tomcat), 'Company' (empty), 'Asset tag' (empty), 'Serial number' (VMware-42 00 06 38 4d cd ea 86-da c), 'Manufacturer' (VMware, Inc.), 'Model ID' (VMware, Inc. VMware Virtual PI), and 'Assigned to' (empty). Each field has a search icon and an information icon.



# 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.

The screenshot displays the ServiceNow Service Management interface. The left sidebar contains a navigation menu with items like Cloud Management, Cloud Service Design, Price Discovery, Pattern Designer, Discovery Patterns, Discovery Pattern Log, Discovery, CI Schedule Manager, Dashboard (highlighted), Discovery Schedules, Status, Credentials, and Discovery Range Sets. The main content area shows a 'Discovery Dashboard' with a 'Make your life easier, create a dashboard!' notification at the top. Below this, there's a section for 'Active Discovery Status' with a filter 'All > State = Active > Description != Discover CI'. A table lists discovery activities with columns: Number, Created, Description, Schedule, Discover, State, Started, Completed, Updated, and Duration. Two rows are visible: one for 'Discover Now' (Alabama Office) and one for 'Scheduled' (Auto-Created Schedule). A 'Snipping Tool' window is overlaid on the table, showing a capture area around the second row. At the bottom, there are three summary cards: 'Newly Discovered Devices (Last 7 Days)', 'Total Discovered Devices (Last 30 Days)', and 'Unrefreshed Devices (Beyond Last 30 Days)'.

Number	Created	Description	Schedule	Discover	State	Started	Completed	Updated	Duration
DIS0010048	2017-12-11 14:22:59	Discover Now	Alabama Office	Configuration items	Active	36	33	2017-12-11 14:26:50	
DIS0010027	2017-12-10 15:24:08	Scheduled	Auto-Created Schedule	Configuration items	Active	687	643	2017-12-10 16:21:49	

Thankyou