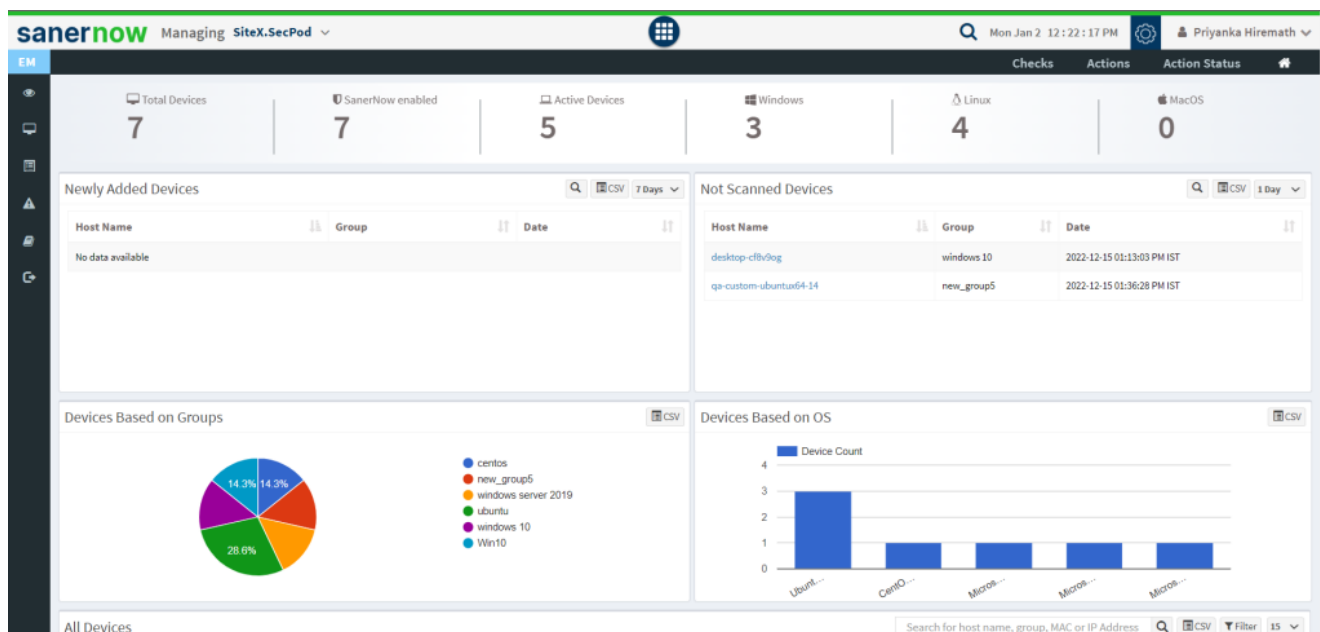


## How to collect all open ports in Windows systems?

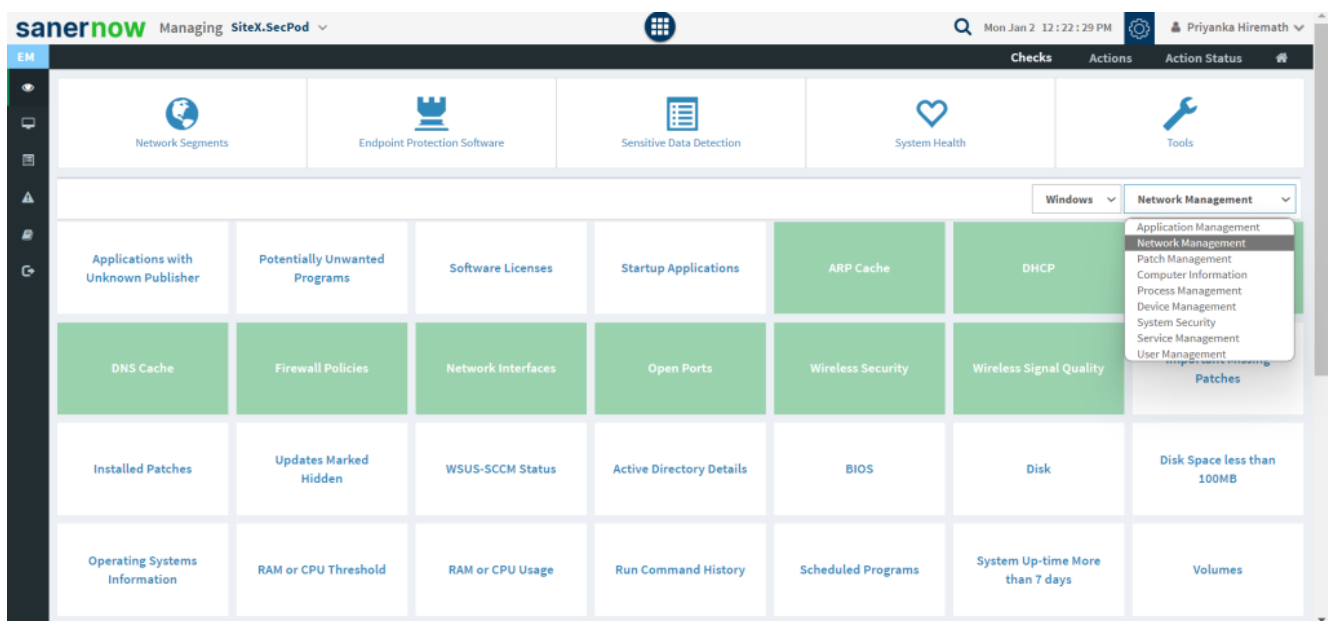
To collect all open ports in Windows systems, follow the steps below:

1. Go to **Endpoint Management** module in SanerNow.

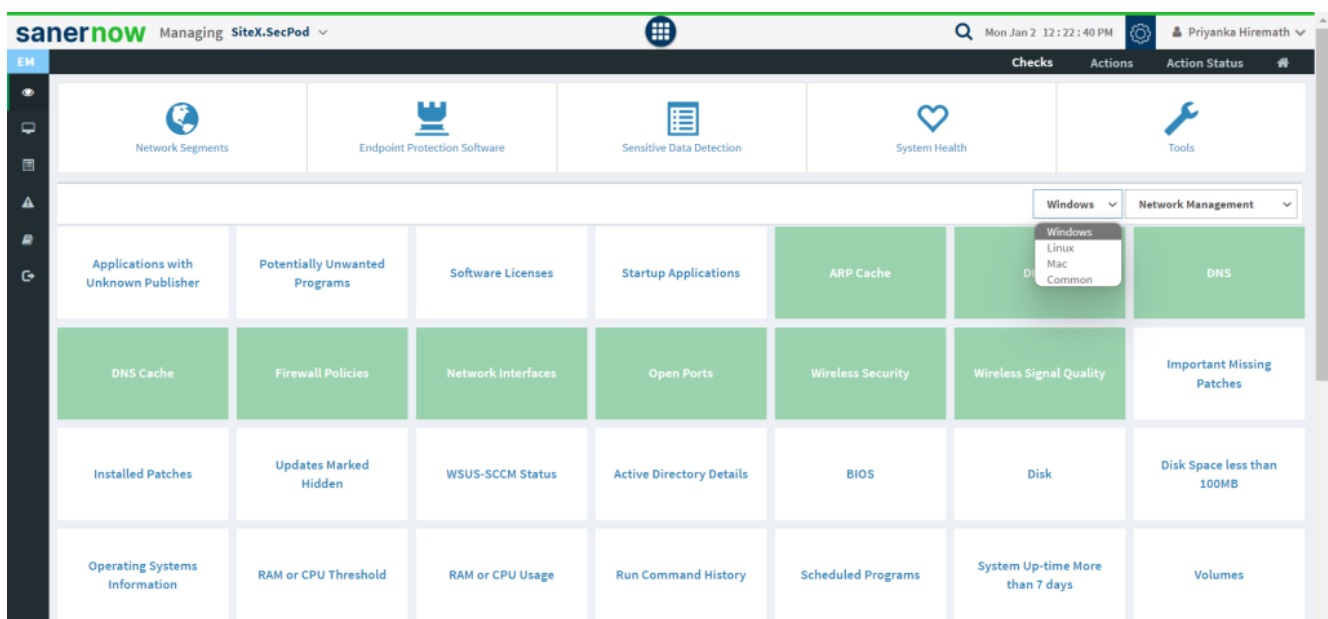


2. Click on **Checks**.

3. On the right-hand side, from the drop-down list select '**Network Management**'.



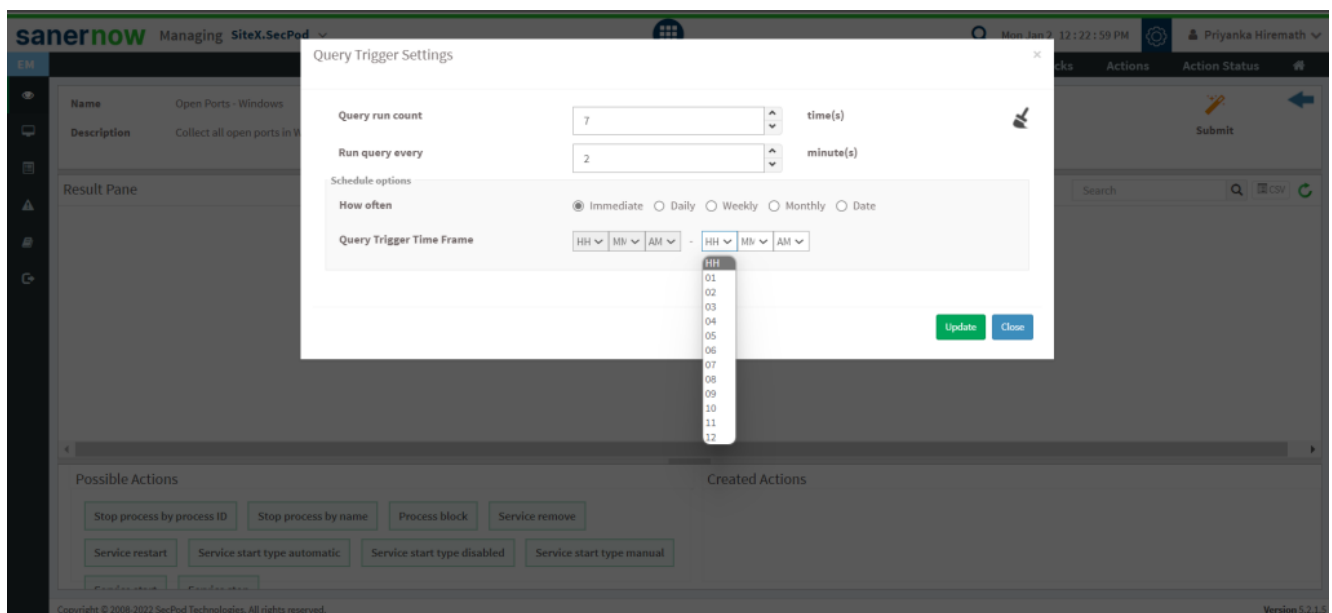
4. Select the operating system: **Windows**.



5. The checks corresponding to network management for Windows are highlighted in green.

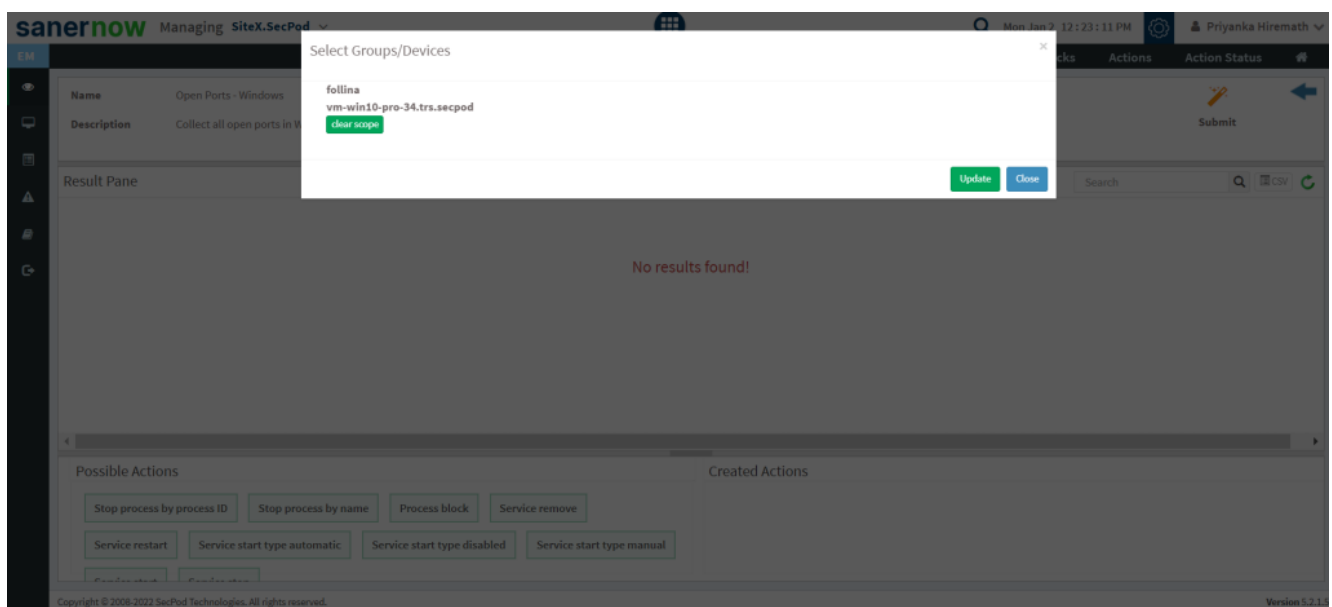
6. To schedule the query execution for the agent, click on **Trigger**. You need to fill up query trigger settings:

- Set the Query run count time in seconds.



- Set the time in minutes to run the query often.
- In Schedule options pane, set the **Query Trigger Time Frame**.
- Click on **Update**.

7. Click on the '**Scope**' to choose the scope of the query.



8. To send the query to agent, click on '**Submit**'.

9. In the **Result Pane**, you will be displayed with all open ports information on Windows systems.

10. You can take possible actions according to the results. Possible actions are specified at the bottom pane. Click on the desired action, you will be redirected to Create Response page. In Created Actions, you will find all the responses created for the following check.

The screenshot shows the 'Create Response' page in the SanerNow interface. The page has a header with the SanerNow logo, 'Managing SiteX.SecPod', and a user profile 'Priyanka Hiremath'. The main content area is titled 'Create Response'. It contains several form fields and a list of actions.

- Operating System Family\***: A dropdown menu with 'Windows' selected.
- Action\***: A dropdown menu with 'Process block' selected. A dropdown menu is open showing the following options: 'Process block', 'Start process', 'Stop process by process ID', 'Stop process by name', and 'Process unblock'.
- Response Name\***: A text input field containing 'name \*'.
- Response Description\***: A text input field containing 'Action for Open Ports - Windows'.
- Create Response**: A button to create the response.
- Clear Fields**: A button to clear the form fields.
- Enforce as a rule / Apply always.**: A checkbox.
- How often**: Radio buttons for 'Immediate' (selected), 'Daily', 'Weekly', 'Monthly', and 'Date'.
- Operating Systems**: A list of operating systems with checkboxes: 'centos', 'new\_group5', 'ubuntu', 'Win10', 'windows 10', and 'windows server 2019'.
- Processes**: A list of processes with checkboxes: 'ApplicationFrameHost.exe', 'ASMHost.exe', 'chrome.exe', 'cmd.exe', 'conhost.exe', 'coreFrameworkHost.exe', 'coreServiceShell.exe', 'ctfmon.exe', 'dillhost.exe', 'ds\_monitor.exe', 'dsa.exe', 'DSS.AdobeAuthoring.exe', 'DSS.AdobeInformation.exe', and 'DSS.OfficeConversion.exe'.

Now you know how to collect all open ports on Windows system.