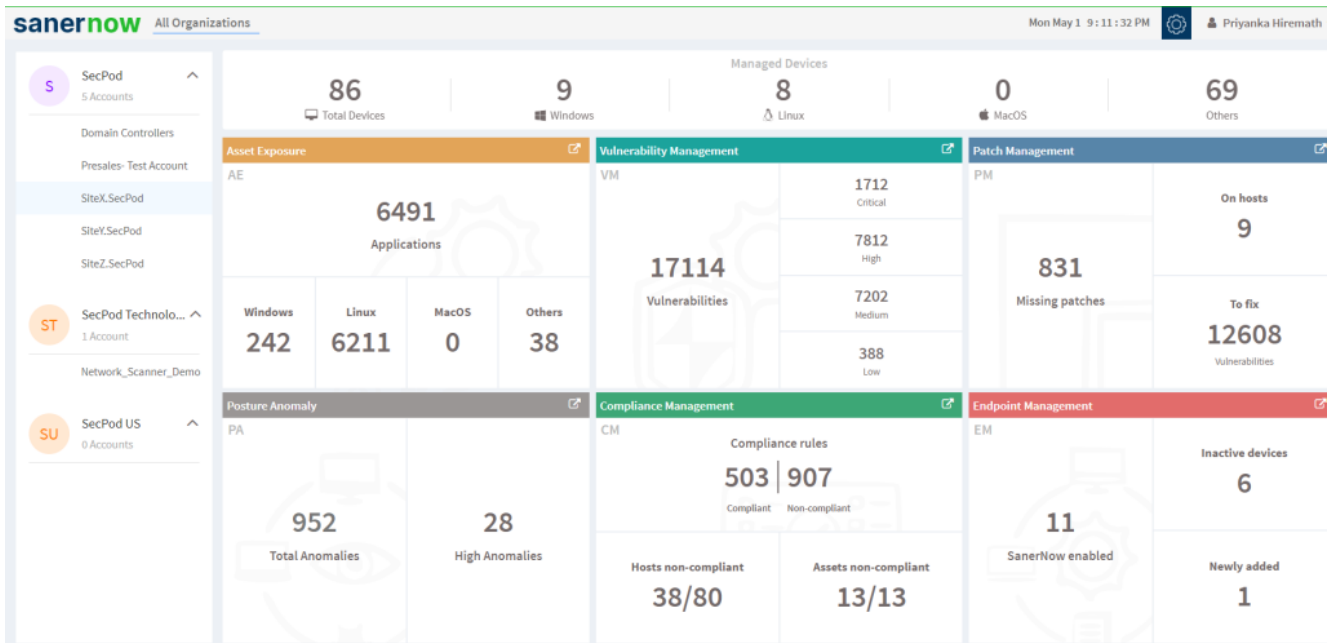
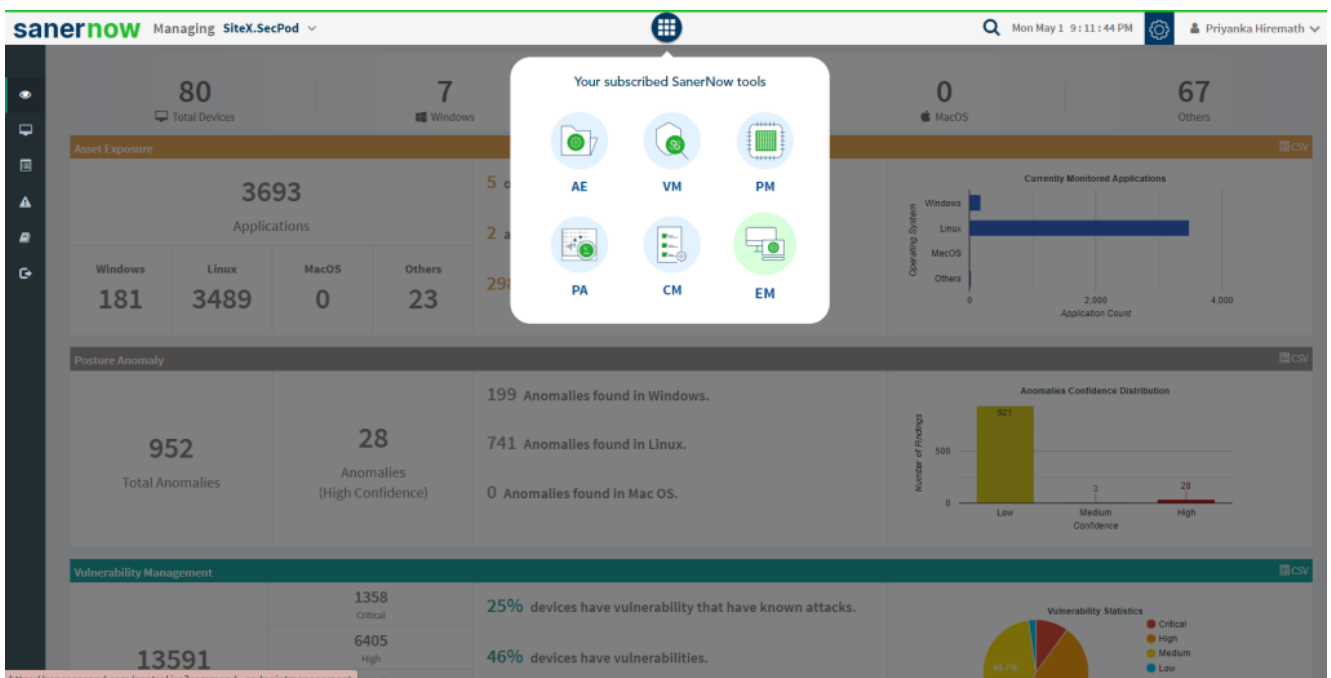


How to list all Administrator accounts on Windows systems?

1. Choose the organization and corresponding account to list all administrator accounts on Windows systems.



2. Select the **Endpoint Management** module



3. Click on **Checks** on the right top corner

The screenshot shows the SanerNow interface with the following data:

- Summary Metrics:**
 - Total Devices: 13
 - SanerNow enabled: 13
 - Active Devices: 7
 - Windows: 7
 - Linux: 6
 - MacOS: 0
- Newly Added Devices Table:**

Host Name	Group	Date
sp-nagraj-laptop	Windows-Test	2023-04-26 03:18:57 PM IST
- Not Scanned Devices Table:**

Host Name	Group	Date
ms1-home-device	Windows-Test	2023-04-26 04:57:19 PM IST
qa-debian-11-x64	grp-1.0	2023-04-19 12:34:28 PM IST
sp-mcentos1-x86-64	centos	2023-03-17 09:51:05 PM IST
sp-nagraj-laptop	Windows-Test	2023-04-29 03:24:26 PM IST
sp-nagraj-laptop.localdomain	ubuntu	2023-04-19 08:12:50 PM IST
- Devices Based on Groups:** A pie chart showing the distribution of devices across groups: Windows-Test (53.8%), grp-1.0 (23.1%), centos, and ubuntu.
- Devices Based on OS:** A bar chart showing the device count for various operating systems: Debian, Ubuntu, CentOS, Microsoft, Linux, and Mac OS.
- All Devices Table:**

Host Name	Operating System	Processor	Installed Memory (RAM)	System Type	Group	Primary Mac Address	Primary IP Address	Status
			No information available	No information available	centos	9E:4E:14-07-05-92	192.168.2.237	

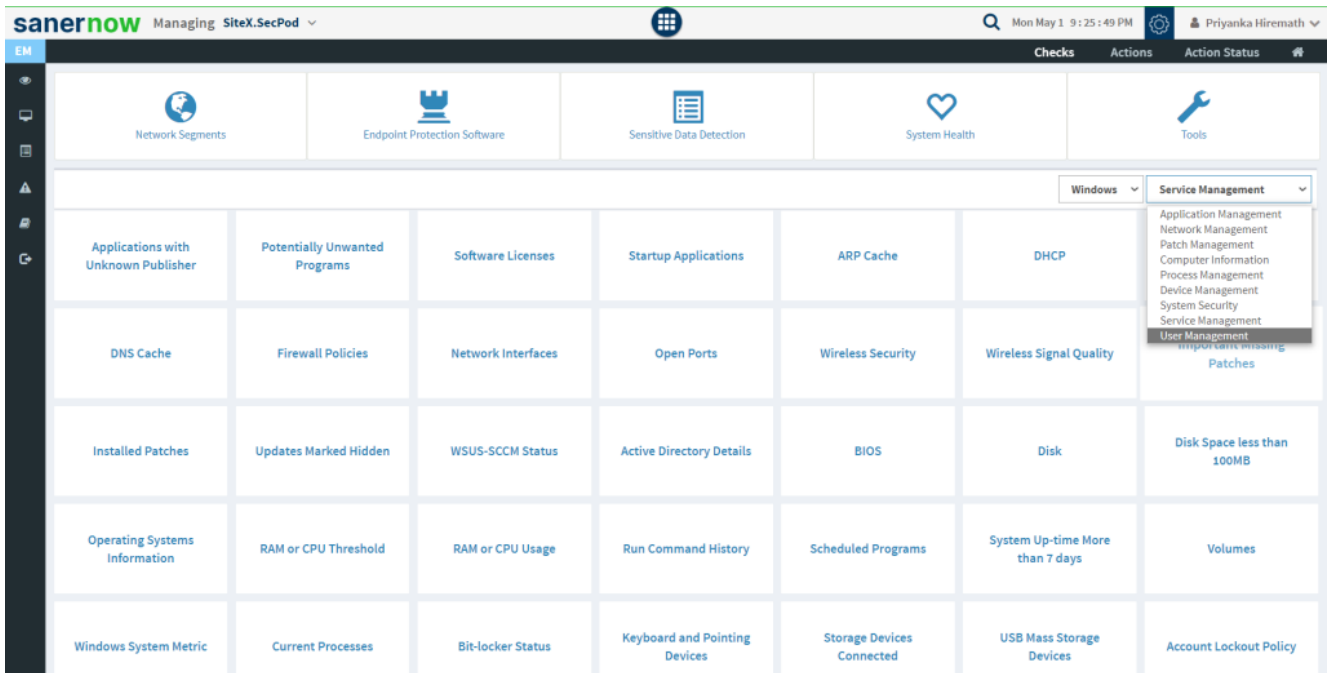
4. From the drop-down menu, select **Windows** and **User Management**

The screenshot shows the SanerNow interface with a grid of system checks. A dropdown menu is open over the 'DHC' check, showing the following options:

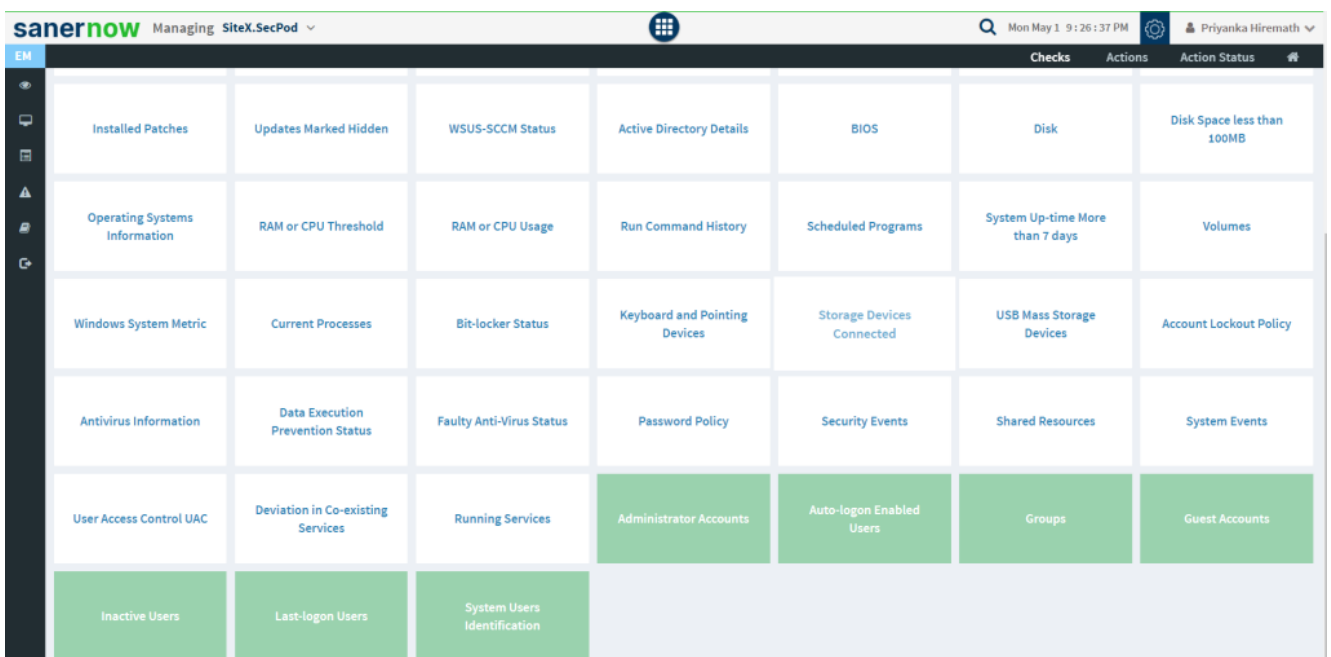
- Windows
- Linux
- Mac
- Common

The grid of checks includes:

- Applications with Unknown Publisher
- Potentially Unwanted Programs
- Software Licenses
- Startup Applications
- ARP Cache
- DHC
- DNS
- DNS Cache
- Firewall Policies
- Network Interfaces
- Open Ports
- Wireless Security
- Wireless Signal Quality
- Important Missing Patches
- Installed Patches
- Updates Marked Hidden
- WSUS-SCCM Status
- Active Directory Details
- BIOS
- Disk
- Disk Space less than 100MB
- Operating Systems Information
- RAM or CPU Threshold
- RAM or CPU Usage
- Run Command History
- Scheduled Programs
- System Up-time More than 7 days
- Volumes
- Windows System Metric
- Current Processes
- Bit-locker Status
- Keyboard and Pointing Devices
- Storage Devices Connected
- USB Mass Storage Devices
- Account Lockout Policy

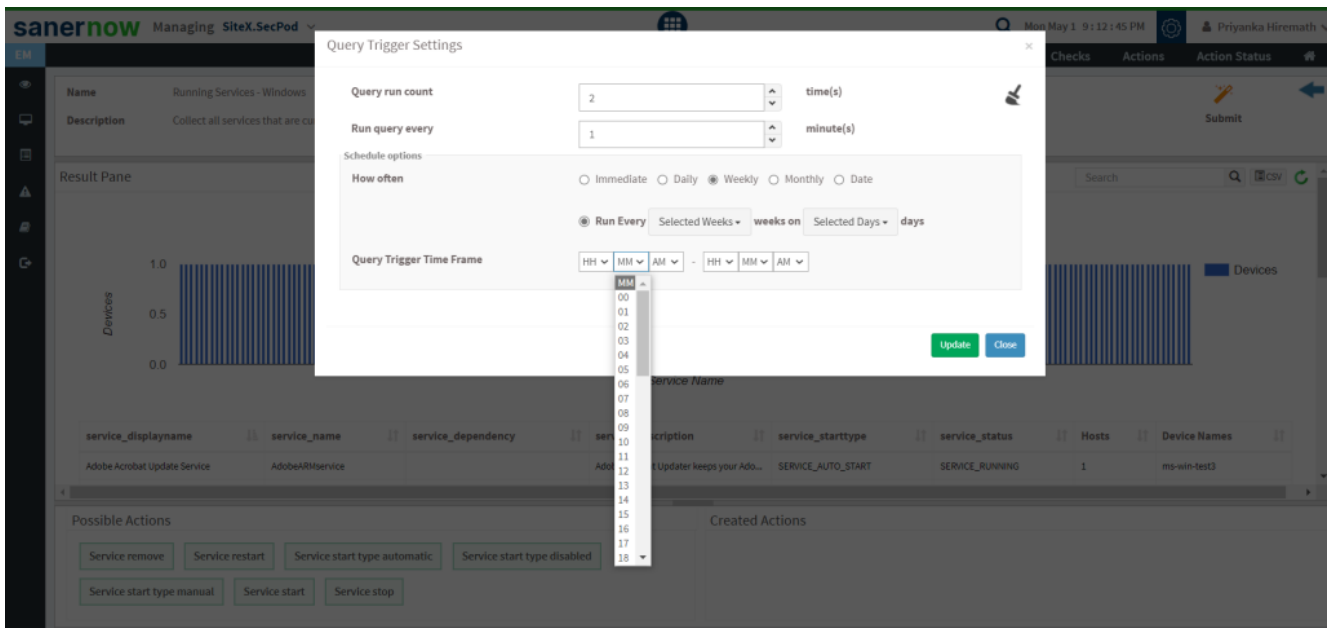


5. Followed by scrolling down, the checks are highlighted in green. Select **Administrator Accounts**



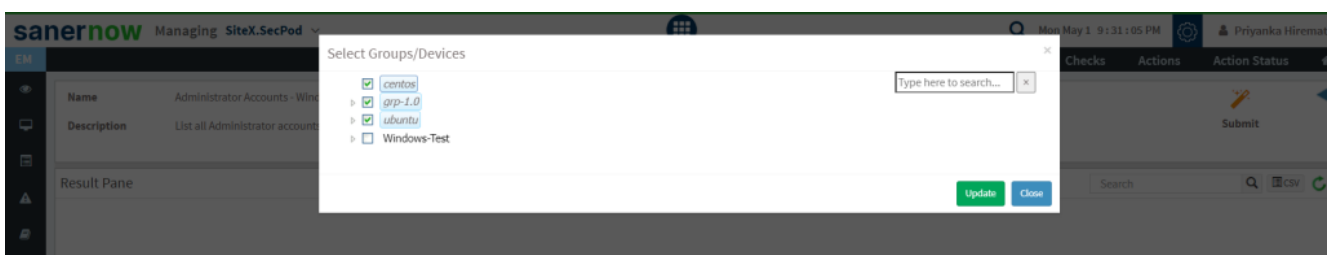
6. To schedule the query execution for the agent, click on **Trigger**. You need to fill up query trigger settings:

- Set the Query run count time in seconds.



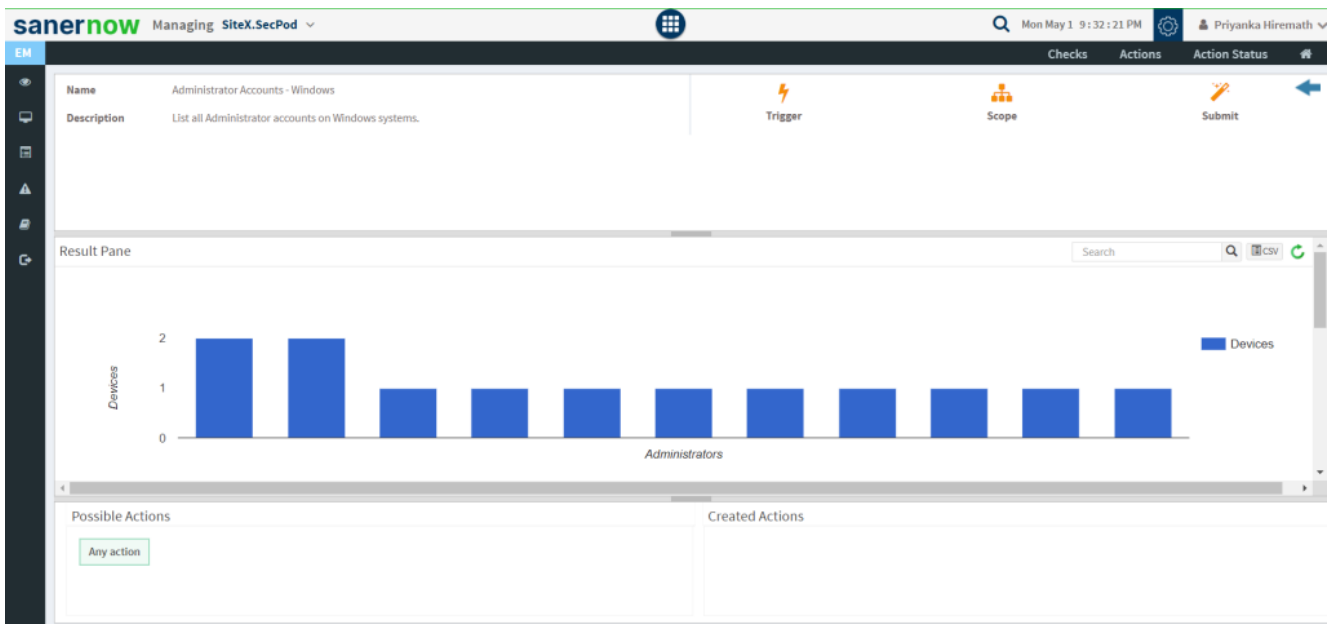
- Set the time in minutes to run the query often.
- In Schedule options pane, set the **Query Trigger Time Frame**.
- Click on **Update**.

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

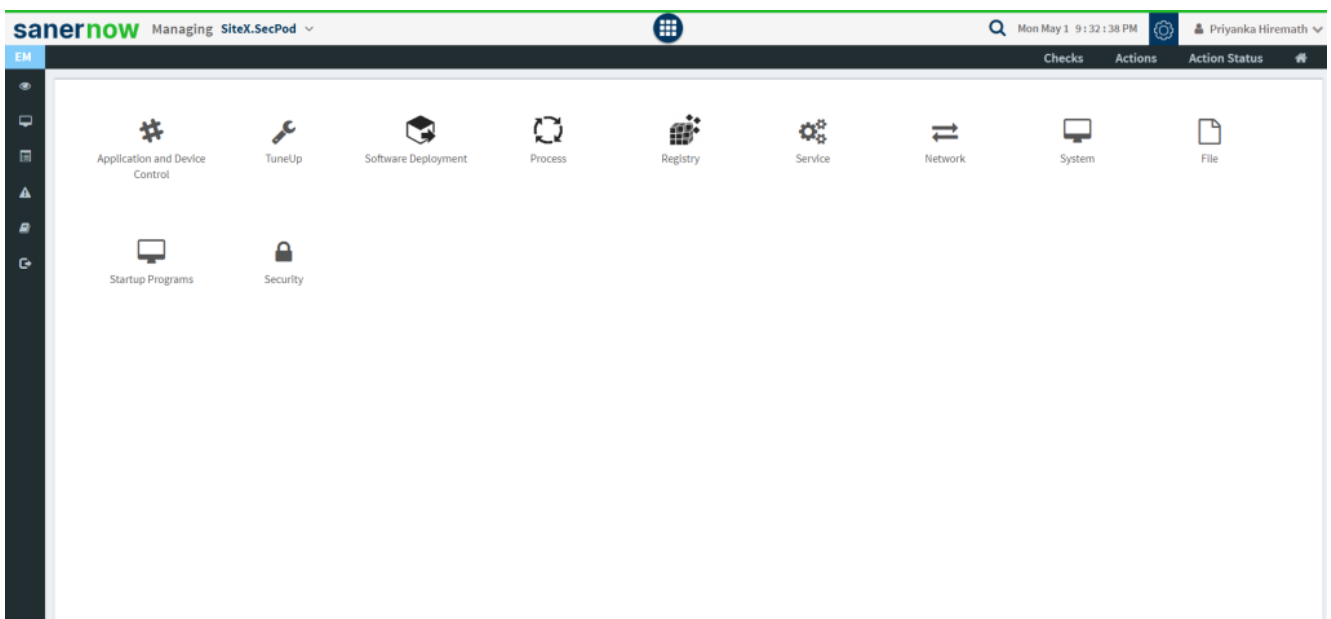


9. To send the query to agent, click on '**Submit**'.

10. In the **Result Pane**, you can view the list of all administrator accounts on Windows systems. You can also download the CSV format of the result pane.



11. 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.



Now you know how to list all administrator accounts on Windows systems.