How to check status of DEP in Windows systems?

1. Login to SanerNow and choose the **Organization** and corresponding **Account** to check the status of DEP in Windows systems.

sanernow Managing	SiteX.SecF	Pod ^		•		Q Thu May 25 12:1	4 : 28 PM 🙆 🎍 Priyanka Hiremath 🗸
EM	*					Checks	Actions Action Status 👫
 Total Devices 9 	S	SecPod 3 Accounts	^	Active Devices	₩indows 4	∆ Linux 5	⊯ MacOS O
•		SiteX.SecPod			1		
Newly Added Devices		SiteY.SecPod		Q CSV 7 Days 🗸	Not Scanned Devices		Q, IDay ∽
Host Name		SiteZ.SecPod			Host Name 🥼	Group 👫	Date 11
No data available					ms-win-test3	Production group	2023-05-23 11:18:30 PM IST
G	ST	SecPod Technologies	\sim		qa-debian-11-x64	grp-1.0	2023-04-19 12:34:28 PM IST
	1 Account	1 Account			sp-nagraj-laptop.	ubuntu	2023-05-09 05:01:50 PM IST
		SecPod US	~		sp-td-win10	Windows-Test	2023-05-10 07:54:05 PM IST
	SU	0 Accounts			sp-ubuntu-ms1	ubuntu	2023-05-24 10:00:40 AM IST
Devices Based on Groups				■ CSV	Devices Based on OS		I≣ csv
					Device Count		
44.4%				р	2		
	22.2%				1		
					0	nt cento	licros
					Dep. Upu	Center	
All Devices					Se	earch for host name, group, MAG	Cor IP Address Q ECSV T Filter 15 V

2. Select the Endpoint Management module

🖵 Total Devices	SanerNow ena	bled	ubscribed San	erNow tools		∆ Linux		d MacOS
9	9					5		0
Newly Added Devices		AE	VM	РМ				Q CSV 1 Day
Host Name	Group				J.L.	Group	1 Date	
No data available						Production group	2023-05-23 11:18:30	0 PM IST
						grp-1.0	2023-04-19 12:34:28	8 PM IST
		PA	СМ	EM		ubuntu	2023-05-09 05:01:50	0 PM IST
				sp-td-win10		Windows-Test	2023-05-10 07:54:05	5 PM IST
						ubuntu	2023-05-24 10:00:40	0 AM IST
Devices Based on Groups			≣ csv	Devices Based on OS]
Devices Based on Groups		Distriction	CSV .					[
Devices Based on Groups	22.2%	ubuntu grp-1.0	CSV .	Devices Based on OS				
Devices Based on Groups	22.7%		CSV (Devices Based on OS				
	22 7%	 grp-1.0 Windows-Test 	E csv	Devices Based on OS		P		

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

sar EM	Nernow Managing	SiteX.SecPod ~		•	Q	Thu May 25 12:14 Checks	: 58 PM	
•	Network Segments	Endpoint	2 Protection Software	Sensitive Data Detection	System He		Actions	Action Status #
∎						Wind	lows ~	Application Management 🛛 🗸
<i>₽</i> G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHCP		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 M days	ore than 7	Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Storage	e Devices	Account Lockout Policy

4. From the drop-down menu, select **Windows** and **System Security**

sa	nernow Managing	SiteX.SecPod ~			Q	Thu May 25 12:	15:12 PM {	👌 🛔 Priyanka Hiremath 🗸
EM						Checks	Actions	Action Status 🛛 🔗
•	Network Segments	Endpoint	Protection Software	Sensitive Data Detection	System He	alth		Tools
∃							indows ~	Application Management 🗸 🗸
<i>∎</i> G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	Lir Ma	indows nux ac ommon	DNS
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Sign	al Quality	Important Missing Patches
	Installed Patches	Updates Marked Hidden	WSUS-SCCM Status	Active Directory Details	BIOS	Disk	c	Disk Space less than 100MB
	Operating Systems Information	RAM or CPU Threshold	RAM or CPU Usage	Run Command History	Scheduled Programs	System Up-time days		Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Store	age Devices	Account Lockout Policy

sar	nernow Managing	SiteX.SecPod 🗸		•	۵	Thu May 25 12:	15:15 PM	🚫 💧 Priyanka Hiremath 🗸
EM						Checks	Actions	Action Status 🛛 👫
•	Retwork Segments	End	Doint Protection Software	Sensitive Data Detection	System H	ealth		Tools
▲						w	∕indows ∽	Application Management 🗸 🗸
e G	Applications with Unknown Publisher	Potentially Unwante Programs	Software Licenses	Startup Applications	ARP Cache	DHCP		Application Management Network Management Patch Management Computer Information Process Management
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Sigr	nal Quality	Device Management System Security Service Management User Management
	Installed Patches	Updates Marked Hidd	n WSUS-SCCM Status	Active Directory Details	BIOS	Dis	k	Disk Space less than 100MB
	Operating Systems Information	RAM or CPU Threshol	I 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 Stor	rage Devices	Account Lockout Policy

5. Followed by scrolling down, the checks are highlighted in green. Select **Data Execution Prevention Status**

Iernow Managing	Siterisetrud *		•		Thu May 25 1:02:19 PM	Action Status
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 100ME
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
Antivirus Information	Data Execution Prevention Status	Faulty Anti-Virus Status	Password Policy	Security Events	Shared Resources	System Events
User Access Control UAC	Deviation in Co-existing Services	Running Services	Administrator Accounts	Auto-logon Enabled Users	Groups	Guest Accounts
Inactive Users	Last-logon Users	System Users Identification				

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.

Query run count	5	time(s)
Run query every	* ·	minute(s)
Schedule options		
How often	Immediate O Daily O Weekly O Mor	nthly 🔿 Date
Query Trigger Time Frame	HH ¥ MM ¥ AM ¥ - HH ¥ MM ¥ AM ¥	•
2		

• Set the time in minutes to run the query often.

ging SiteX,Se	Query Trigger Settings	(##)		C Thu May 25 12:16:34 PM X Actions
int Lockout Pc caccount lock	Query run count Run query every Schedule options	5	<pre>time(s) time(s) minute(s)</pre>	*
	How often Query Trigger Time Frame		O Weekly ○ Monthly ○ Date	ich -
		100		Update Close

• In Schedule options pane, set the **Query Trigger Time Frame**.

	Query Trigger Settings			× Actions
Account Lockout Po Theck account lock	Query run count	5	↑ time(s)	2
neck account lock	Run query every	7	<pre>minute(s)</pre>	
	Schedule options			
	How often		ly Weekly O Monthly O Date ad Weeks • weeks on Selected Days • days	
	Query Trigger Time Frame	HH 🖌 MM 🎽 AM 🖌	- HH ¥ MM ¥ AM ¥	
				Update Close

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

Managing SiteX.	SecPod V		O Thu May 25	12:17:20 PM
	Select Groups/Devices			Actions
Antivirus Informatic Checks for Anti-Viru running.	 grp-1.0 Production group ubuntu Windows-Test sp-td-win10 sp-win-2019-server 		Type here to search	
			Update	se
		100%		

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

10. In the **Result Pane**, you can check the system_dep_ploicy, Hosts, and Device Names. You can fetch the results and download the CSV format of the result pane.

Name	Data Execution Prevention Status - W	federes			ş	4	7
Description	Data Daecution Prevention or DEP is a maniharing programs to make sore the Mix-Area external			14	Eler.	forget	Salamit
1000.0	a, priliry		Tests		Davis Names		
-			1		reads tool (up which	enal 2003 all parts while	
Option					and and the second	- Bullharkers.ts.argod	
			_				
Possible Ac	lons			Created Acti	lons		
Possible Ad			-	Created Act	kons		

11. You can take possible actions according to the results. Click on the Any action, you will be redirected to **Create Response page**. In **Created Actions**, you will find all the responses created for the following check.

aner	NOW Managing Si	teX.SecPod 🗸					Q	Mon May 1 9:32:38 PM Checks Actions	
	Application and Device Control	June Up	Software Deployment	D Process	Registry	Service	Network	System	File
2	Startup Programs	Security							

Now you know how to check for DEP status in Windows systems.