How to check if Bit-locker protection is OFF in Windows systems?

1. Choose the organization and corresponding account to check if Bit-locker is OFF in Windows systems.

						Manas	ged Devices		
s	SecPod ^ 5 Accounts		86		9 Windows		8 5. Linux	0 MacOS	69 Others
	Domain Controllers	Asset Exposure	- Iotal Devices		C	Vulnerability Management	g cintx	-	otiers
	Presales- Test Account	Asset Exposure				Vunerability Management		Patch Management PM	
	SiteX.SecPod	7.66	64	91			1712 Critical		On hosts
	SiteY.SecPod SiteZ.SecPod		Applica			17114	7812 High	831	9
ST	SecPod Technolo 🔨	∧ Windows	Linux		Others 38	Vulnerabilities	7202 Medium	Missing patches	To fix 12608 Vulnerabilities
51	1 Account	242	6211				388		
	Network_Scanner_Demo	_			<i>с</i> а.		Low		
SU	SecPod US ^	Posture Anoma PA	ure Anomaly		ď	Compliance Management CM Compl	liance rules	Endpoint Management EM	Inactive devices
		952 2		8	503 Complian		11	6	
			nomalies		omalies	Hosts non-compliant	Assets non-compliant	SanerNow enabled	Newly added

2. Select the Endpoint Management module

	80		7		Your sub	oscribed SanerN	low tools	0		67
Asset Exposure	Total Devices		Windov 📲	vs	07			d MacOS		Others
	36 Applic			5 c 2 a	AE	VM	PM	Windows Linux	Currently Monitored Applic	ations
Windows 181	Linux 3489	MacOS O	Others 23	29	PA	CM	EM	O Others	2.000 Application Count	4.000
Posture Anomaly										
	952 28 Total Anomalies (High Confidence)		741 #	199 Anomalies found in Windows. 741 Anomalies found in Linux. 0 Anomalies found in Mac OS.			Anomalies Confidence Distribution			
Vulnerability Man	agement	13	58	254						_
13	591	cm 64	oical 05 gh		devices have v devices have v		at have known attacks.		Vulnerability Statistic	S Critical High Medium

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

						Checks	Actions Action S	tatus
⊊Total Devices 13		© SanerNow enabled	□ Active Devices	Windows 7		∆ Linux 6	t MacOS	
Newly Added Devices			Q CSV 7 Days	 Not Scanned Devices 			٩	CSV 1 Day
Host Name	II Group	11 Date		Host Name		Jà Group Jt	Date	
sp-nagraj-laptop	Windows-Test	2023-04-26 03:18:57 PM IST	т	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-mscentos1-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			III cs	Devices Based on OS				D
s	23.1%	ubuntu grp-1.0 centos Windows-Ti	est	4 Device C	Count			
All Devices				0	Ununt Cen	۵۰۰۰ میلاده. Search for host name, group,		T Filter 15
Host Name	Operating System	Processor	Installed Memory (RAM)	System Type	Group	Primary Mac Address	Primary IP Address	Status
These Platfing	operating system	Floceson	macaded memory (roAM)	-Ascent type	Group	r mary mac Address	Fillinary IF Address	Status

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

	nernow Managing s	iteX.SecPod 🗸		•		Q Mon May 1 9:12:0	4 PM 💮 🛔 Priyanka Hiremath 🗸 Actions Action Status 者	
■ ● ₽	Network Segments	Network Segments		Software Sensitive Data Detection		System Health		
A						Window		
₽ G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHC Commo		
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signal Quality	y 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	

anernow Managing	SiteX.SecPod ~			Q	Tue May 16 11:03:30 AM	💮 💄 Priyanka Hiremath
	1			l.	Checks Actions	Action Status 🛛 🖷
					Windows ~	Device Management
Applications with Unknown Publisher	Potentially Unwanted 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 Signal Quality	Device Management System Security Service Management User Management
Installed Patches	Updates Marked Hidden	WSUS-SCCM Status	Active Directory Details	BIOS	Disk	Disk Space less than 100
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

5. Followed by scrolling down, the checks are highlighted in green. Select **Bit-locker Status**.

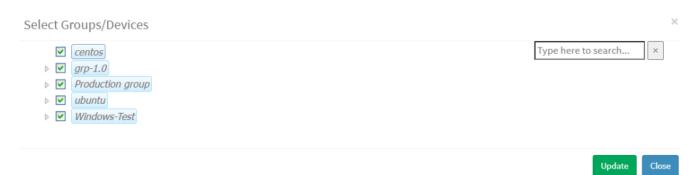
6. To schedule the query execution for the agent, click on **Trigger**. You need to fill up query trigger settings:

• Set the Query run count time in seconds.

Query Trigger Settings		>
Query run count	2 time(s)	2
Run query every	1 minute(s)	
Schedule options		
How often	🔿 Immediate 🔿 Daily 🛞 Weekly 🔿 Monthly 🔿 Date	
	Run Every Selected Weeks • weeks on Selected Days • days	
Query Trigger Time Frame	HH V MM V AM V - HH V MM V AM V	
	MM 00 01 02 03 04	Update Close
	04	
	06 Service Name	

• 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 see the Bit-locker status with Device_ID, Device_Letter, Status, Host, and Device Names. 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.

n and Device T Introl	J F uneUp S	Software Deployment	Q	ġ.				
			Process	Registry	Service	Network	System	File
Programs S	ecurity							
	Programs S							

Now you know how to check if Bit-locker protection is OFF in Windows systems.