

How to exclude vulnerabilities in SanerNow VM tool

SanerNow VM tool will detect and identify all the vulnerabilities that exist in an account. You can see all the detected vulnerabilities displayed on the *All Vulnerabilities* page. However, there might be scenarios in which you want VM tool to exclude vulnerabilities from certain devices or groups.

VM tool allows you to exclude vulnerabilities. And you can do this namely at – Account, Group(s), and Device(s) level.

Follow the below mentioned steps on how to exclude vulnerabilities at Account, Group(s), and Device(s) levels.

Step 1: On the VM Dashboard, click on *All Vulnerabilities* which is located at the top right hand side of the page.

The screenshot displays the SanerNow VM tool interface. At the top, the 'All Vulnerabilities' link is highlighted in the top right corner. The main content area shows a 'Vulnerability Statistics' section with a pie chart indicating the distribution of vulnerabilities by severity: Critical (36.7%), High (50.8%), Medium, and Low. Below this, there is a table of 'Vulnerable Devices' with columns for Host Name, Operating System, Group, Risks Count, Severity Distribution, Assets, Last Scanned, and Status. The table lists several devices, including 'qa-secpod-ubuntu-18-04-x86_64', 'win-10-1757ghef0', and various Android devices. Below the device table, there is a section for 'Vulnerabilities' with a table listing various CVEs and their details, including ID, Title, Severity, Assets, Hosts, Detection Date, Release Date, and Fix status.

Step 2: You will be directed to the *All Vulnerabilities* page. Here, you can view all the vulnerabilities found by VM tool.

sanernow Managing Test_Account

Mon Feb 27 12:54:20 AM

SecPod

All Vulnerabilities Manage Detection

Vulnerabilities Source: All Groups Family: All selected (4) Severity: All selected (4) Quick Action search... CSV 25

ID	Title	Severity	Assets	Hosts	Detection Date	Release Date	Fix	
USN-3914-2	USN-3914-2 ntf5-3g update	10	2	1	2023-02-24	-		<input type="checkbox"/>
USN-4037-1	USN-4037-1 policykit-desktop-privileges update	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-4360-2	USN-4360-2 json-c regression	10	1	1	2023-02-24	-		<input type="checkbox"/>
CVE-2011-3086	Use-after-free vulnerability in Google Chrome and Apple iTunes via vectors involving a STYLE element	10	1	1	2023-02-22	2012-05-15		<input type="checkbox"/>
CVE-2021-38503	The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypas...	10	3	2	2023-02-24	2021-12-10		<input type="checkbox"/>
USN-4436-2	USN-4436-2 libsvg regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
CVE-2010-1119	WebKit removeChild() Remote Code Execution Vulnerability	10	2	1	2023-02-22	2010-03-25		<input type="checkbox"/>
CVE-2023-23599	Malicious command could be hidden in devtools output on Windows in Mozilla Firefox, ESR and Thu...	10	1	1	2023-02-09	-		<input type="checkbox"/>
CVE-2010-1763	Apple iTunes WebKit Unspecified Vulnerability	10	1	1	2023-02-22	2010-06-18		<input type="checkbox"/>
USN-5122-1	USN-5122-1 apport vulnerability	10	3	1	2023-02-24	-		<input type="checkbox"/>
CVE-2012-5112	Use-after-free vulnerability in the SVG implementation in WebKit in Google Chrome and Apple iTunes	10	1	1	2023-02-22	2012-10-11		<input type="checkbox"/>
USN-4024-1	USN-4024-1 evince update	10	3	1	2023-02-24	-		<input type="checkbox"/>
USN-3866-2	USN-3866-2 ghostscript regression	10	2	1	2023-02-24	-		<input type="checkbox"/>
USN-5606-2	USN-5606-2 poppler regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
USN-4134-2	USN-4134-2 ibus regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
USN-4171-6	USN-4171-6 apport regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
CVE-2019-6235	Memory corruption vulnerability in AppleKeyStore in Apple iTunes - CVE-2019-6235	10	1	1	2023-02-22	2019-05-31		<input type="checkbox"/>
USN-5473-1	USN-5473-1 ca-certificates update	10	1	1	2023-02-24	-		<input type="checkbox"/>
CVE-2021-4140	Iframe sandbox bypass with XSLT - CVE-2021-4140	10	3	2	2023-02-24	2022-02-08		<input type="checkbox"/>

Step 3: Click on the checkboxes displayed towards the right side of the vulnerabilities that you want to exclude. And then click on the *Quick Action* button.

sanernow Managing TestBug

Fri Feb 24 9:56:22 PM

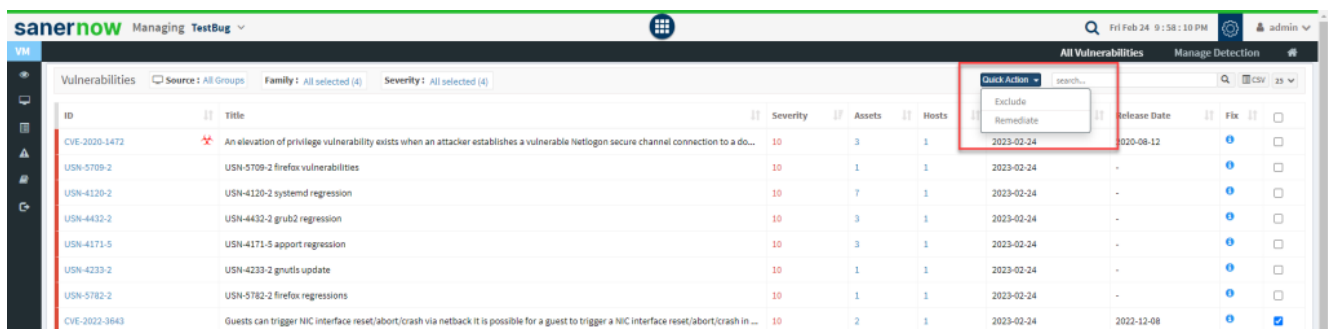
admin

All Vulnerabilities Manage Detection

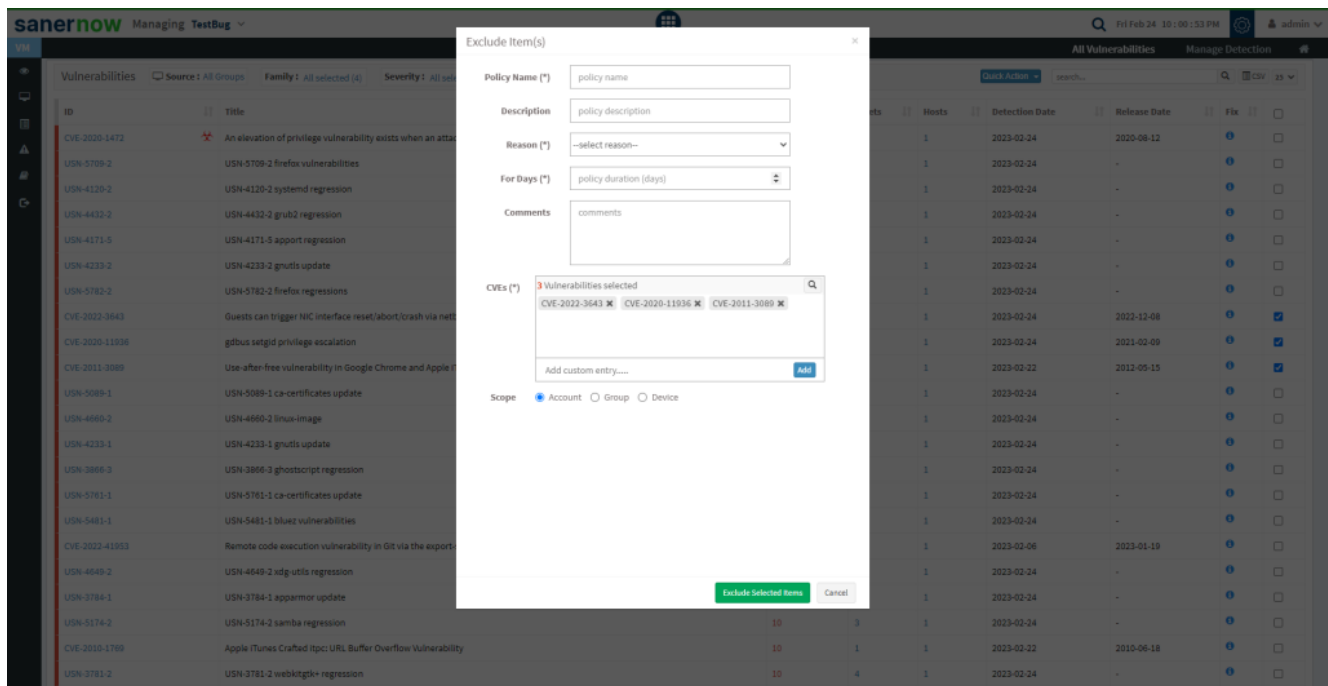
Vulnerabilities Source: All Groups Family: All selected (4) Severity: All selected (4) Quick Action search... CSV 25

ID	Title	Severity	Assets	Hosts	Detection Date	Release Date	Fix	
CVE-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a do...	10	3	1	2023-02-24	2020-08-12		<input type="checkbox"/>
USN-5709-2	USN-5709-2 firefox vulnerabilities	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-4120-2	USN-4120-2 systemd regression	10	7	1	2023-02-24	-		<input type="checkbox"/>
USN-4432-2	USN-4432-2 grub2 regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
USN-4171-5	USN-4171-5 apport regression	10	3	1	2023-02-24	-		<input type="checkbox"/>
USN-4233-2	USN-4233-2 gnutls update	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-5782-2	USN-5782-2 firefox regressions	10	1	1	2023-02-24	-		<input type="checkbox"/>
CVE-2022-3843	Guests can trigger NIC interface reset/abort/crash via netback it is possible for a guest to trigger a NIC interface reset/abort/crash in ...	10	2	1	2023-02-24	2022-12-08		<input checked="" type="checkbox"/>
CVE-2020-11936	gdbus setgid privilege escalation	10	3	1	2023-02-24	2021-02-09		<input checked="" type="checkbox"/>
CVE-2011-3089	Use-after-free vulnerability in Google Chrome and Apple iTunes via vectors involving tables	10	1	1	2023-02-22	2012-05-15		<input checked="" type="checkbox"/>
USN-5089-1	USN-5089-1 ca-certificates update	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-4660-2	USN-4660-2 linux-image	10	2	1	2023-02-24	-		<input type="checkbox"/>
USN-4233-1	USN-4233-1 gnutls update	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-3866-3	USN-3866-3 ghostscript regression	10	2	1	2023-02-24	-		<input type="checkbox"/>
USN-5761-1	USN-5761-1 ca-certificates update	10	1	1	2023-02-24	-		<input type="checkbox"/>
USN-5481-1	USN-5481-1 bluez vulnerabilities	10	2	1	2023-02-24	-		<input type="checkbox"/>
CVE-2022-41953	Remote code execution vulnerability in Git via the export-subst mechanism - CVE-2022-41953	10	1	1	2023-02-06	2023-01-19		<input type="checkbox"/>

Step 4: You will see two options when you click on the Quick Action button – 1. Exclude and 2. Remediate.



Step 5: Click on *Exclude* option. You will now be presented with a new pop-up screen.



Step 6: You need to fill in information in all the textboxes marked with an asterisk (*). Fill in the required info in the below text boxes.

- Policy Name – Provide a name for the policy you are creating.
- Reason – You need to select the reason you want to exclude the vulnerabilities. Select one of the reasons presented by the drop-down box. The following reasons are available for you to choose.
 - False Positive
 - Not Applicable
 - Risk Accepted
- For Days – Enter the number of days you want VM tool to exclude the vulnerabilities.

- (You can exclude the vulnerability for minimum 1 day and a maximum for 999 days.)
- CVEs – Here, you will see all the vulnerabilities you selected to be excluded. At the same time, you can manually add vulnerabilities to be excluded using the *Add* button.

CVEs (*)

3 Vulnerabilities selected

CVE-2022-3643 ✕ CVE-2020-11936 ✕ CVE-2011-3089 ✕

Add custom entry.....

Add

- Scope – You need to select the scope. You can choose between Account, Group, and Device.

Scope ☒ Account ☐ Group ☐ Device

- Account – When you select Account, the selected vulnerabilities will be excluded from all the devices that are part of the account till the date specified by you.
- Group – When you select Group, the selected vulnerabilities will be excluded for all the devices that belong to the selected Group(s) till the date specified by you. (You can select multiple groups)

Scope ☐ Account ☒ Group ☐ Device

☒

Test_Group

☐

general purpose

☒

Lab_Infra

☐

ubuntu

Exclude Selected Items

Cancel

- Device - You can select one or more devices belonging to various groups to exclude the selected vulnerabilities till the time specified by you. You can select multiple devices belonging to various groups to exclude selected vulnerabilities from them.

Scope ☐ Account ☐ Group ☒ Device

☒

Test_Group

☒

Windows_Test_Machine

☐

general purpose

☐

Machine_6

☒

Test_Group2

☒

Machine_1

☒

Machine_3

☒

Machine_2

☐

Machine_4

☐

ubuntu

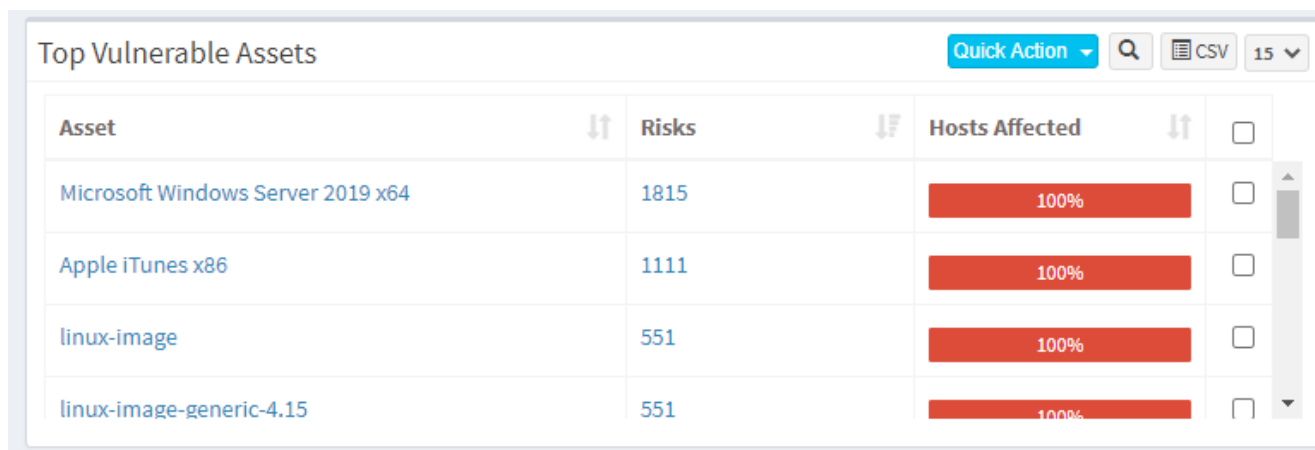
Exclude Selected Items

Cancel

Step 7: Once you have selected the *Scope*, click on *Exclude Selected Items* button. VM tool will exclude the selected vulnerabilities from applicable devices.

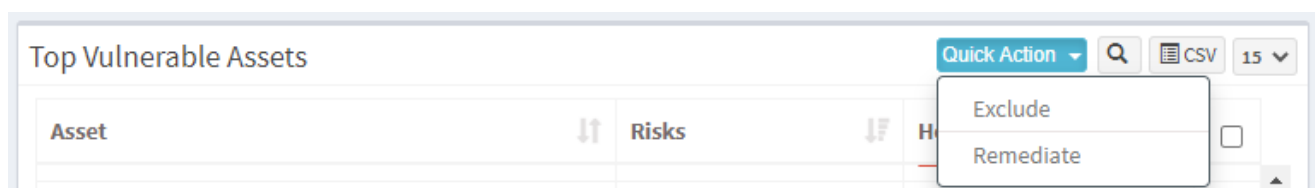
How to Exclude Assets in VM tool

Step 1: On the VM Dashboard, you can find the *Top Vulnerable Assets* section located at the bottom left corner of the page. All the top vulnerable assets found in the account are listed here.



Asset	Risks	Hosts Affected
Microsoft Windows Server 2019 x64	1815	100%
Apple iTunes x86	1111	100%
linux-image	551	100%
linux-image-generic-4.15	551	100%

Step 2: You will find the *Exclude* option when you click on the *Quick Action* button.



Step 3: You will see two options when you click on the *Quick Action* button – 1. *Exclude* and 2. *Remediate*. Click on *Exclude*. You will be presented with a new pop-up window.

Step 4: You need to fill in information in all the textboxes marked with an asterisk (*). Fill in the required info in the below text boxes.

- Policy Name – Provide a name for the policy you are creating.
- Reason – You need to select the reason you want to exclude the vulnerabilities. Select one of the reasons presented by the drop-down box. The following reasons are available for you to choose.
 - False Positive
 - Not Applicable
 - Risk Accepted

- For Days - Enter the number of days you want VM tool to exclude the vulnerabilities.(You can exclude the vulnerability for minimum 1 day and a maximum for 999 days.)
- Assets - Here, you will see all the assets you selected to be excluded. At the same time, you can manually add Assets to be excluded using the *Add* button.

Assets (*)

2 Assets selected

Microsoft Windows Server 2019 x64 ✕ Apple iTunes x86 ✕

Add custom entry.....

Add

- You need to select the scope. You can choose between Account, Group, and Device.

Scope ☒ Account ☐ Group ☐ Device

- Account - When you select Account, the selected vulnerabilities will be excluded from all the devices that are part of the account till the date specified by you.
- Group - When you select Group, the selected vulnerabilities will be excluded for all the devices that belong to the selected Group(s) till the date specified by you. (You can select multiple groups).

Scope ☐ Account ☒ Group ☐ Device

☒

Test_Group

☐

general purpose

☒

Lab_Infra

☐

ubuntu

Exclude Selected Items

Cancel

- Device - You can select one or more devices belonging to various groups to exclude the selected vulnerabilities till the time specified by you. You can select multiple devices belonging to various groups to exclude selected vulnerabilities from them.

Scope ☐ Account ☐ Group ☒ Device

☒

Test_Group

☒

Windows_Test_Machine

☐

general purpose

☐

Machine_6

☒

Test_Group2

☒

Machine_1

☒

Machine_3

☒

Machine_2

☐

Machine_4

☐

ubuntu

Exclude Selected Items

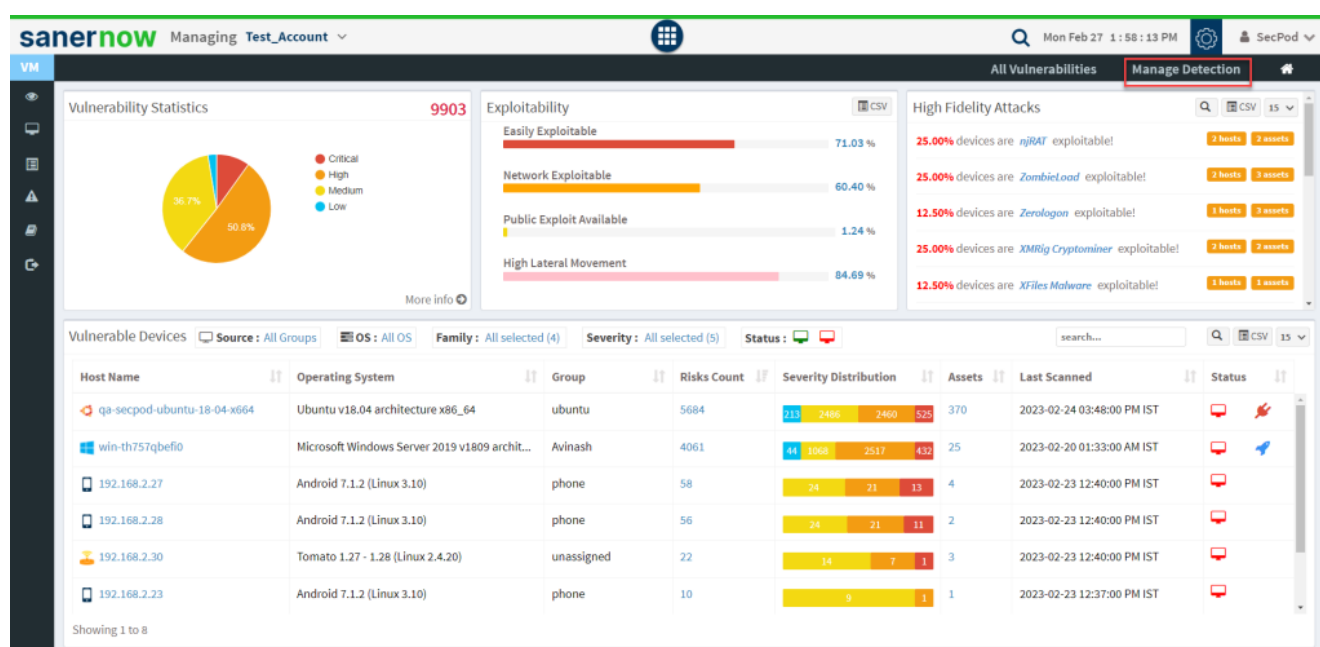
Cancel

Step 7: Once you have selected the *Scope*, click on *Exclude Selected Items* button. VM tool will create the Exclude policy and exclude the selected assets and all the vulnerabilities belonging to the asset from applicable devices.

Note: In VM tool, you can exclude vulnerabilities in various ways. For instance, you can exclude a vulnerability directly from the vulnerabilities table on the VM Dashboard. However, you must follow the steps mentioned above, irrespective of what page or section you use to exclude a vulnerability.

How to Enable/Disable, Edit and Delete an existing Exclude Policy in VM tool

Step 1: On the VM Dashboard, click on *Manage Detection* located at the top right corner of the page.



Step 2: You will be presented with a new screen. You can see all the Exclude Policy that exist in the account.

sanernow Managing Test_Account

Mon Feb 27 11:50:07 AM SecPod

All Vulnerabilities Manage Detection

Excluded Policies Scope: All Policies

Policy Name	Description	Scope	Exclude Item(s)	Policy Expiry	Reason	Action
Test_Policy_1	dsfsd	2 Groups	2	2023-02-24	False Positive	
Test_Policy_2	3 at account level	Account	4	2023-02-25	Not Applicable	
Test_Policy_3	nothing	Account	1	2023-02-13	Risk Accepted	
Test_Policy_4	CVE-2020-12389	1 Host	1	2023-03-02	False Positive	
Test_Policy_5	greg	3 Groups	1	2023-02-22	False Positive	
Test_Policy_6	one device	0 Host	2	2023-02-24	False Positive	
Test_Policy	Exclude	4 Hosts	3	2023-06-04	False Positive	
Test_Policy_7	as	Account	1	2023-02-11	Not Applicable	

The last column on this page - *Action* presents you with three buttons namely - a toggle button - Enable /Disable, Edit, and Delete buttons that can be used to control Exclude policies.

Button	Usage
	Using this button, you can enable the Exclude policy.
	Using this button, you can disable the Exclude policy.
	Using this button, you can edit the Exclude policy.
	Using this button, you can delete the Exclude policy.