NETSHIELD™ BLOCKING

ACCESSING THE NETSHIELD™

1. Access the **NETSHIELD™** using the IP address URL. (Example: https://192.168.4.27)
2. Enter the username and password

OVERVIEW

NETSHIELD™ Blocking works by blocking communication routes from **Untrusted or unknown Blocked assets** to protected assets on the network**.**

NOTE: 1. All blocked and protected assets, must reside on the same subnet as NetSHIELD™.

2. A full asset discovery should be run prior to enabling NetSHIELD™ Blocking. Assets within NetSHIELD™ Blocking Range will be blocked if they are unknown or untrusted.

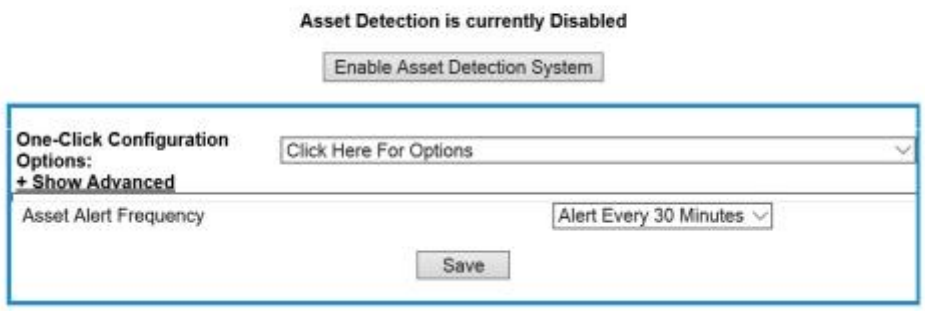
3. Packet Sniffing and NetSHIELD™ Block Ranges will be based on IP address(es) assigned to the appliance network interface cards. The appliance asset list will be used for the protect range. All IP addresses contained in the asset list, trusted and Untrusted, will be protected from assets blocked with NetSHIELD™ blocking.

ENABLING MANUAL NETSHIELD™ BLOCKING

If Asset Detection is currently disabled:

1. *Go to* **NAC Configuration→Asset Detection System.**

2. *Select* ***O*ption #1 "Detect Assets, Alert, Allow Manual Blocking with NETSHIELD™ Blocking",** from the **One-*Click* Configuration Options**.

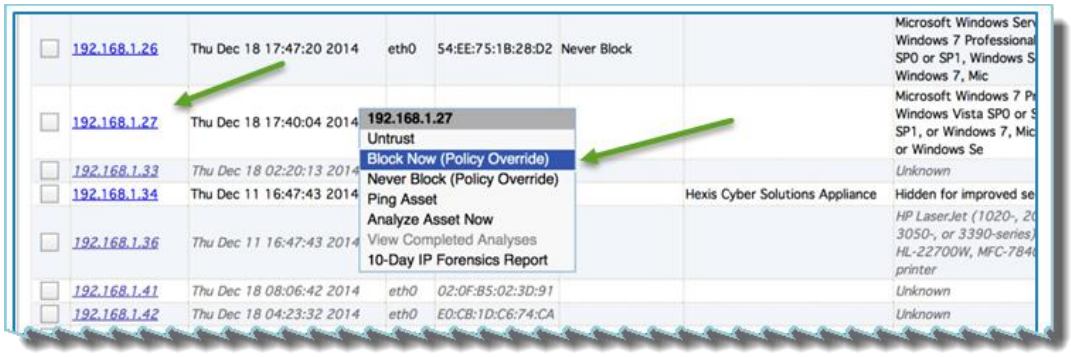


Click on **Show Advanced** to review the checked boxes.

3. *Click* on **Enable Asset Detection System**.

Manual Blocking of an asset:

1. *Go to* **Network Access Control→Manage Assets.**
2. *Click* the **right mouse button** over an asset listed in the grid.
3. *Choose* **Block Now** from the dropdown menu.



Block Now is only available with manual blocking.

The **Block Now** option can be applied to any asset whether it is untrusted, trusted, or never blocked. The value in the **Override column** changes to "**Always Block**".

If it is offline, the line will turn yellow indicating it is untrusted, but as soon as the asset accesses the network again, it will be blocked, and the line will turn red.

The **Block Now** menu item may only be applied to individual assets, not to multiples.

If you have multiple assets selected, Block Now is visible, but disabled.

AUTOMATIC NETSHIELD™ BLOCKING.

1. *Go to* **NAC Configuration→Asset Detection System.**
2. *Select* **option #2 from the One-*Click* Configuration options (Detect, Alert and Block with NETSHIELD™ Blocking).**
3. *Open* the **Show Advanced Settings** and examine the following options.

Block Range field

4. *Enter* the range of IP addresses that the ADS will attempt to block using NETSHIELD™ blocking if an asset is untrusted. By default the NETSHIELD™ will use the range of all networks identified.

To have a range of IP Addresses created for you,

5. *Click* **Auto-Fill Based On Appliance Address(es)**.

6. To *Enter* your own range, use a comma separated list of IP Address ranges (example: 192.1.1.1-100 or 192.1.1-3.1-100)

Protect Range field

7. *Enter* the range of IP addresses that the ADS will prevent a blocked asset from communicating with or,

8. *Click* the **Use Asset List For Protect Range** checkbox to protect all assets.

9. *Select* the **Enable NETSHIELD™ Check Alive** checkbox to cause the ADS to periodically determine if the blocked asset exists on the network. If the blocked asset no longer exists, the blocking will be stopped.

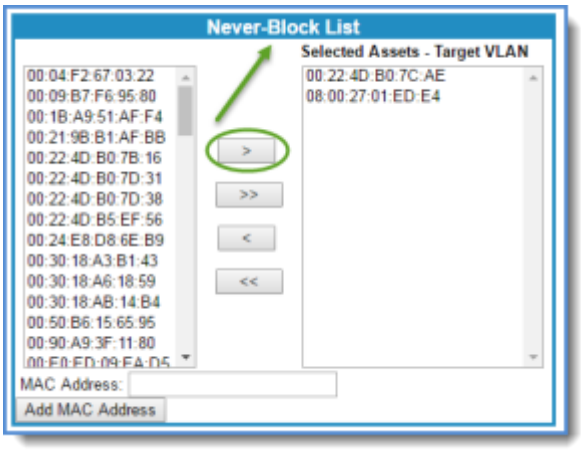
10. *Select the **Enable NETSHIELD™ UnBlocking Traffic checkbox** to cause the ADS to send traffic which will attempt to immediately allow network access to an asset which is being unblocked.*

11. *Click **Save** to save your settings.*

Excluding Assets From NETSHIELD™ Blocking,

The **Never-Block List** is used when automatic blocking has been enabled in the Asset Detection System.

Assets on the **Never-Block List** will never be untrusted or blocked.

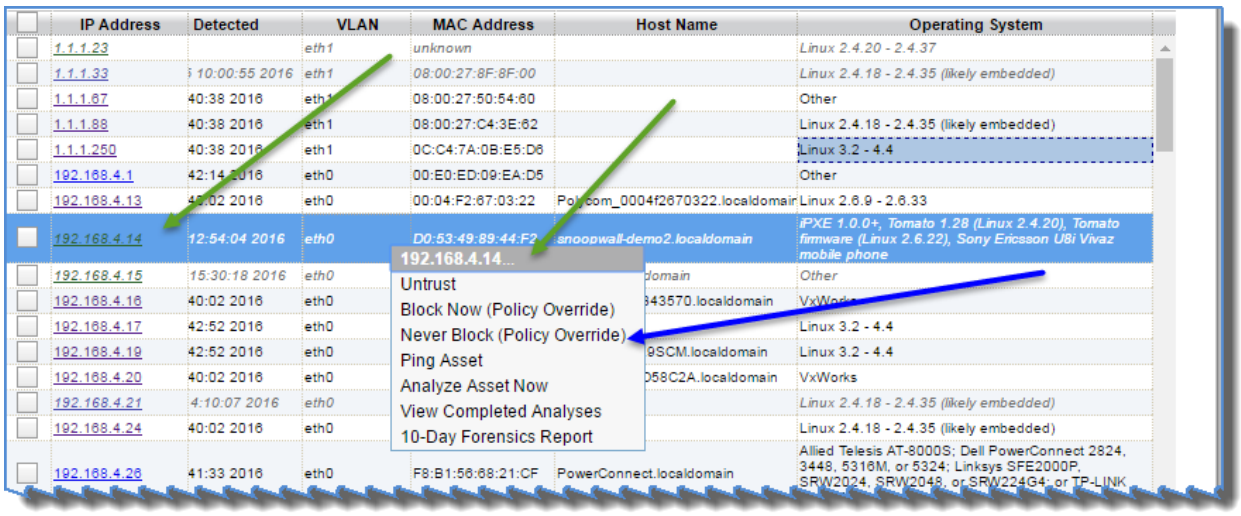


1. *Select* **Network Access Control→Never-Block List**. All assets included in the list on the right will never be blocked by NETSHIELD™ Blocking

You can **add** or **remove** assets to and from the list from by using the > and < arrows.

2. *Click* **Save** to save the list.

You can also add assets on the **Never-Block list** from the **Asset Manager.**



3. *Click* the **right** mouse button while hovering over any asset in the grid.

4. Select **Never Block** from the pulldown menu.

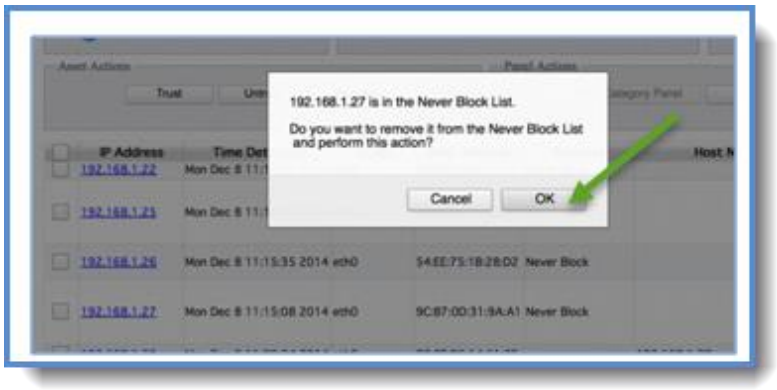
5. The Override column will now display the value **Never Block**.

6. Multiple assets may be selected as well, and the **Never-Block** menu will be applied to all of them.

When automatic blocking is running (**option #2**), these assets can be blocked by simply untrusting them.

Untrusting an asset will remove it from the **Never-Block List.**

You will receive a message that the asset is on the never block list, and asked to confirm that you want to untrust it.



If the asset is within the block range set in the **Asset Detection System**, it will be blocked automatically.

Viewing Assets Blocked With NETSHIELD™ Blocking

At any time, you may view a list of all assets currently being blocked by NetSHIELD™.

- *Select* **Network Access Control→NETSHIELD™ Blocking** from the left menu to go directly to the NetSHIELD™ Blocking screen.
- This displays assets currently blocked with NETSHIELD™ Blocking.

- *Click* **Unblock** to stop blocking the asset with NETSHIELD™ Blocking. Assets will also be marked as trusted when unblocked.

Blocked assets can also be viewed in the **Asset Manager** by *Select*ing *Blocked* from the **Trust Status** filter in the Filter Panel.

> **Note**: Marking an asset as Trusted simultaneously stops the asset from being blocked with NetSHIELD™

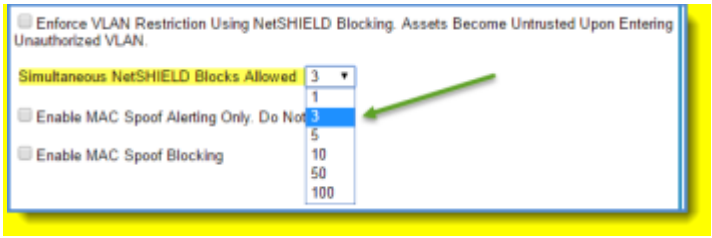
SIMULTANEOUS NETSHIELD™ BLOCKS RESTRICTION

NETSHIELD™ provides the ability to restrict the number of simultaneous NETSHIELD™ Blocks. This prevents overloading of the network traffic.

The **default value** is **3.**

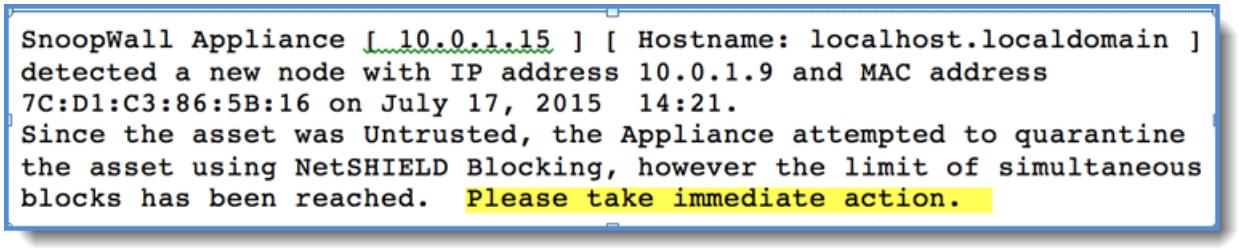
CONFIGURING SIMULTANEOUS BLOCKS

1. *Select* **NAC Configuration→Asset Detection System.**
2. *Click* **Show Advanced.**
3. *Select* a **Simultaneous NETSHIELD™ Blocks Allowed** Value using the pulldown arrow.



4. *Click* **Save**

In the event the simultaneous block limit is exceeded, the administrator will be alerted via email message such as this:

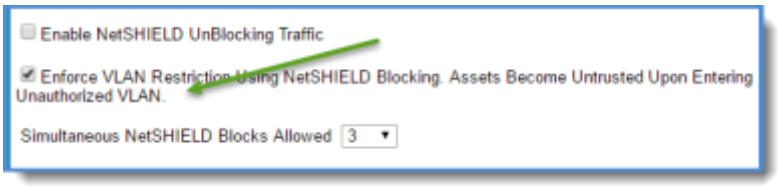


VLAN RESTRICTION USING NETSHIELD™ BLOCKING

NETSHIELD™ offers the ability to restrict assets to one or more target VLAN(s). In the event an asset attempts to access a VLAN that is not on the target list, a block event may occur based on NETSHIELD™ settings.

ENABLING VLAN RESTRICTION

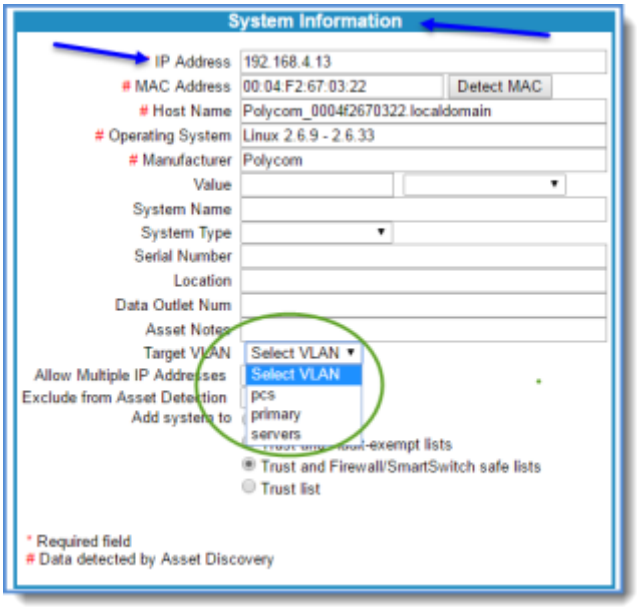
1. *Select* **NAC Configuration→Asset Detection System** from the menu.
2. From the **One-Click pulldown menu**,
3. *Select* **Option 1** from the pulldown menu.
4. *Click* on **Show Advanced**.
5. The **Asset Detection System** Menu opens
6. *Scroll* down the menu.
7. *Check* **Enforce VLAN Restriction** Using **NETSHIELD™ Blocking.**



8. *Click* **Save**

Configuring Asset Target VLAN List

1. *Select* **Network Access Control,**
2. *Select* Manage **Assets** from the menu.
3. *Click* the asset's **IP Address link.**
4. The **System Information** for that IP address opens.



5. *Select* **a Target VLAN from the pulldown menu.**
6. If **multiple VLANs** are to be assigned to an IP Address, use the Available VLANs screen.

The **Available VLANs** for this IP address are shown in the left column, Target VLAN(s)

7. *Click* on a **VLAN**, then *click* the **>** to move it to the right side, **Target VLANs** column.

8. *Repeat* this step for each additional VLAN required.

9. *To remove* a **VLAN**, select it then *click* the **<** arrow to return it to the right column.

10. *Click* **Update System.**

> **Note:** In the event VLAN Restriction is enabled and an asset is detected on an unauthorized VLAN, the administrator will be alerted via email and the asset will be set as untrusted. In the event the asset moves back into a target VLAN, the asset will be set as trusted.