



Issue:

Configuring Command Center with Enterprise, Branch Pro and Nano Appliances

Resolution:

Command Center is an application on the Enterprise and Branch Pro NETSHIELD appliance used to manage remote appliances from a central location without having to open multiple browser sessions.

A common network environment has a main location with an Enterprise or Branch Pro appliance running Command Center and Nano appliances at remote locations such as a bank with a main branch and multiple remote locations.

In an environment with multiple Enterprise or branch Pro appliances decide on one appliance to run Command Center. Do not run Command Center on multiple Enterprise or Branch Pro appliances as it will cause issues with replication and the trust state of assets.

Trust state should be managed on the local appliance in the Manage Assets page or from the Enterprise appliance running Command Center by opening the managed appliance Manage Assets page.

Create a group on the Command Center appliance and add all of the appliances into the group including itself. Enable replication, if desired, from the Command Center appliance and all assets will be replicated between appliances.



Asynchronous Connection Settings

Maximum Connections: <input type="text" value="20"/>	<i>This setting will only allow 20 asynchronous connections simultaneously</i>
Milliseconds Added to Refresh Period per Appliance: <input type="text" value="1500"/>	<i>Based on 3 appliance your refresh period for this setting is 4.5 seconds</i>
Milliseconds Buffer Added to Refresh Period: <input type="text" value="50000"/>	<i>This setting adds 50 seconds for a total refresh period of 54.5 seconds</i>
Milliseconds to Wait for a Connection: <input type="text" value="6000"/>	<i>If all connections are in use this setting will wait 6 seconds before attempting another connection</i>
Background Polling Interval: <input type="text" value="5 Minutes"/>	<i>This setting will poll client appliances every minutes.</i>
Asset Replication Frequency: <input type="text" value="Every 1 Hour"/>	<i>This setting will replicate assets amongst branches every hour(s).</i>

Using the Filter Panel in the Manage Assets screen will show replicated assets.

Replicated assets do not count against the license count of an appliance.

Asset Actions:

Panel Actions:

Filter:

Asset Status	Trust Status	Override	Detected	Operating Systems	Manufacturer
Active	Trusted	<blank>	Yes	Allied Telesis AT-8000S;	^ Apple ^
Known Missing	Untrusted	Never Block	No	Dell PowerConnect 2824, 3448, 5316M, or 5324;	Asustek Computer
Replicated	Blocked	Always Block		Linksys SFE2000P, SRW2024, SRW2048, or SRW224G4; or TP-LINK TL-SL3428 switch	Belkin International
Imported					Brother Industries
					Cisco Systems
					^ D-Link International ^



If the message “Content was blocked because it was not signed by a valid security certificate.” Is seen while attempting to access a managed appliance, open a web browser. This can be done from the appliance menu in Command Center.

Remote Operations

Mouse Over Status Icons For More Information. [Click Here For Status Icon Legend.](#)

Device Status	Threat Potential	CVE Audit Status	Group Name
			bc test
			Device IP
			netshield 192.168.4.137

- [Click Here To Manage Remote Assets](#)
- [Click Here To Manage Remote Audits](#)
- [Click Here For Remote Audit Results](#)
- [Click Here For Remote One Click Audit Wizard](#)
- [Appliance Console - Opens In New Window](#)**
- [Click Here To View Network Alerts](#)
- [Click Here To View System Alerts](#)

Add an exception for the appliance to allow the browser to access the appliance.

Your connection is not secure

The owner of 192.168.4.188 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

[Go Back](#) [Advanced](#)

192.168.4.188 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[Add Exception...](#)