PCI Monitor OrionSW ADD ONE LINUX Server Procedure

Process Effective Date:	4/18/2016
Last Review/Change Date:	4/18/2016
Accompanying Attachments (Yes or No):	None
Functional Area(s):	MTS Monitoring Group
Critical Dependencies:	None
Author(s):	James Dougherty, Technical Writer
MTS Technical Owner:	
Approver(s):	
PCI Standard(s):	None
Review Cycle:	Annual – by June 1, in line with our yearly requirement for PCI re-certification *Not necessary for *Implementation* documents
Concept Title:	OrionSW ADD ONE LINUX Server

Purpose

The purpose of this procedure is to instruct on how to add a specific device(s) such as switch, router, Linux server ESXI device into the Orion monitoring tool for the purpose of statistical health reporting and monitoring on devices hardware utilization.

Scope

The process scope outlines the monitoring of this subject/device to be able to monitor the CPU, ram and disk utilization and provide alerting / reporting on specific threshold settings if necessary to prevent performance/hardware health issues in the PCI environment.

Definitions

Networking Details

Data Flow Diagrams

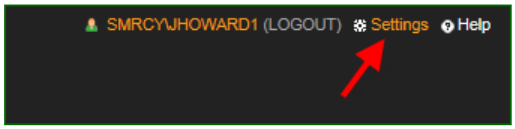
PCI Network solarwinds Environment Poller Design Diagram

PCI Monitoring solarwinds Enviroment

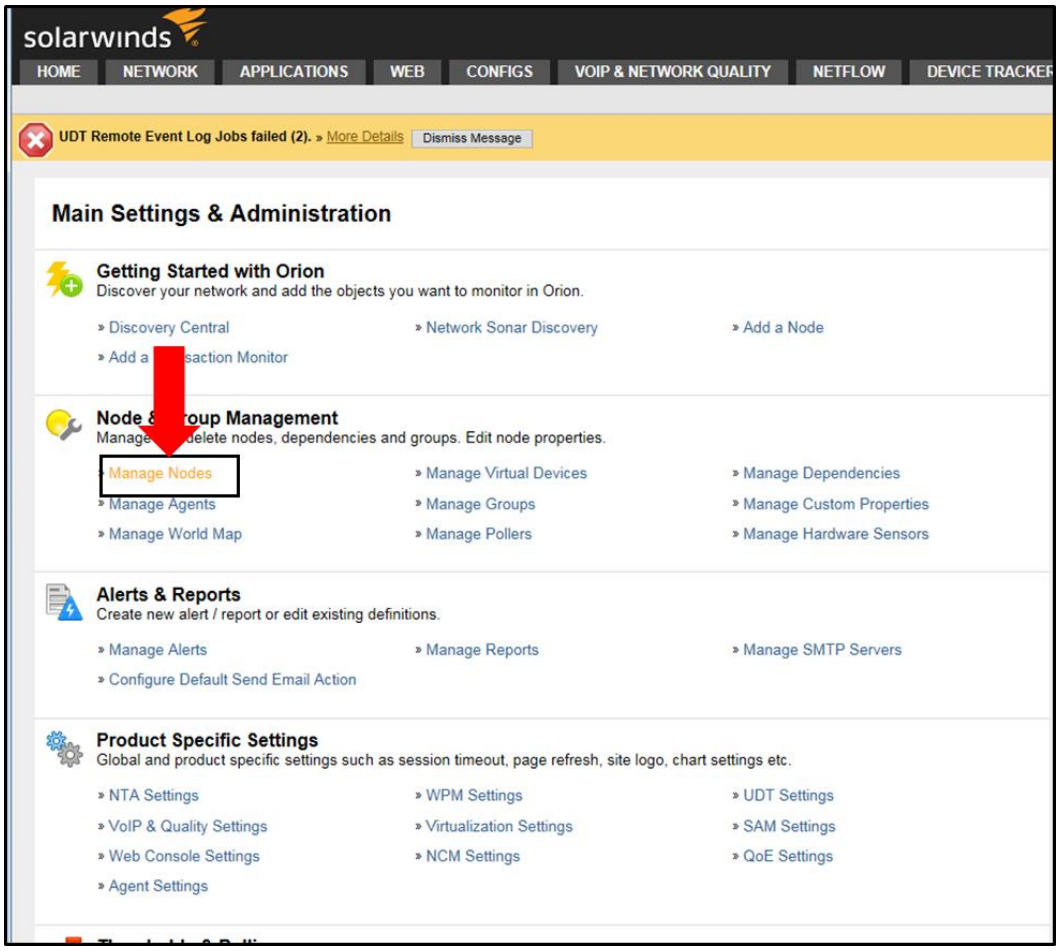
Process / Procedure

Process / Procedures Steps

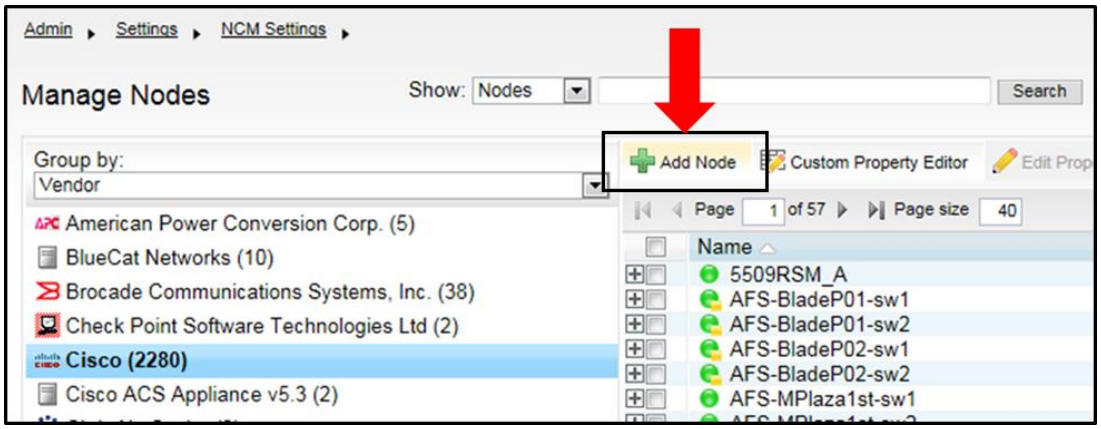
1. Select the Orion Settings link to access the Discovery ONE Window sever manually.



2. Select Managed Nodes.



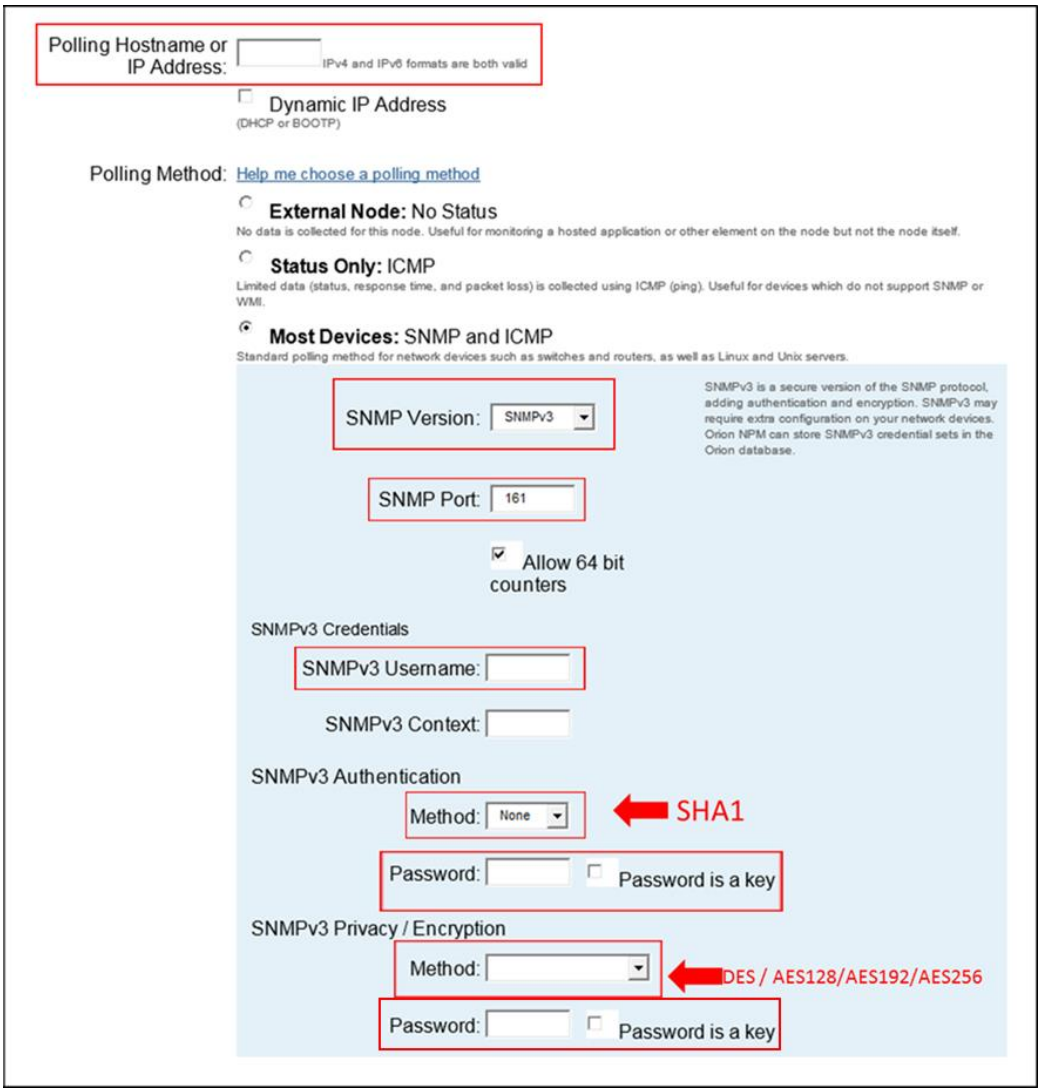
3. Click the Add Node button.

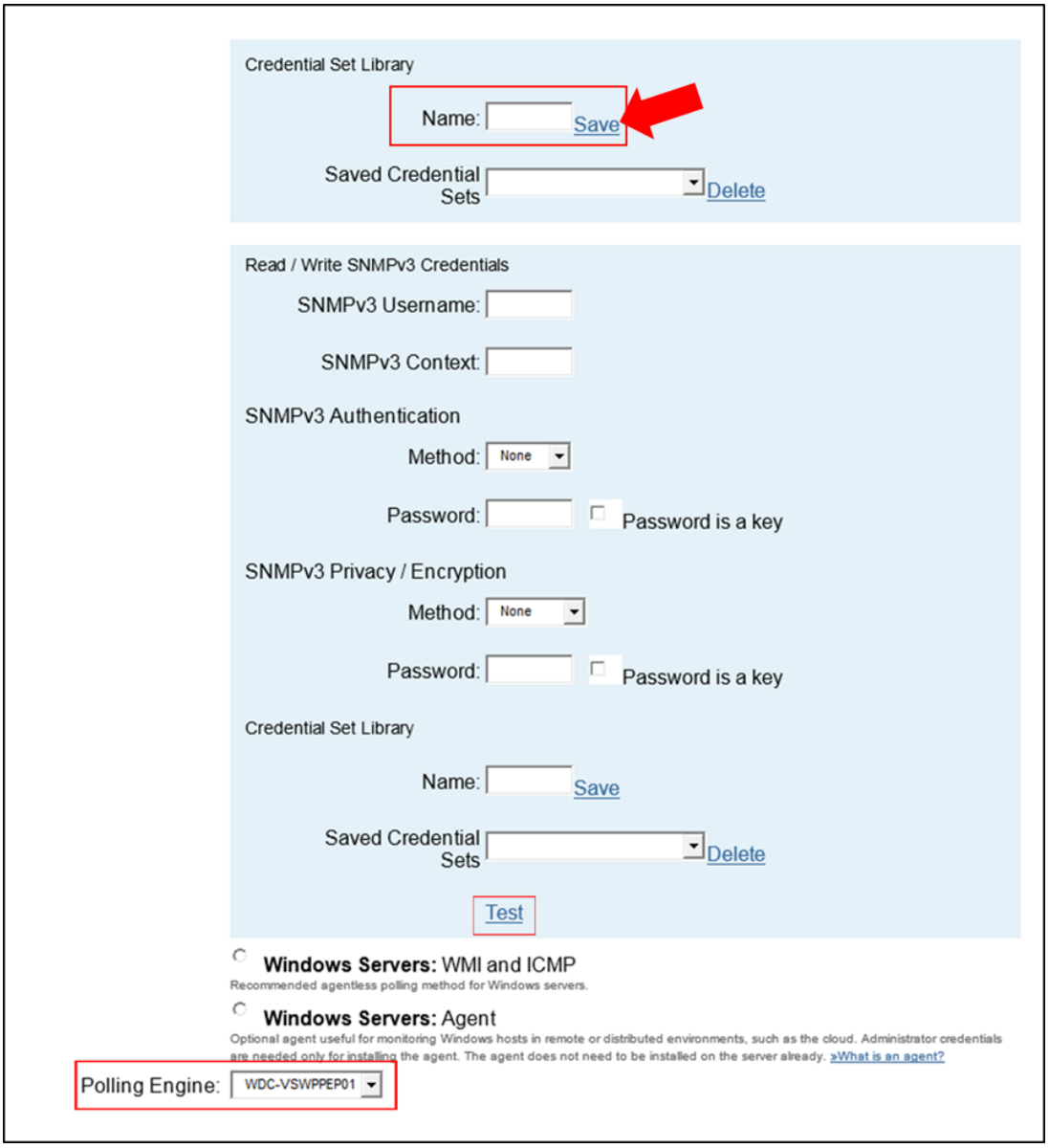


4. Setting SNMPv3 authentication and privacy

- SNMPv3 Authentication and Privacy setting configurations depend upon the manufacture of the network device/appliance type documentation and authority access.
  - a) Input Polling Name or IP Address of the device to monitor for SNMPv3
  - b) Select SNMPv3 and ensure that the network device/appliance uses port 161. Otherwise, change the port to the required port of the device.
  - c) Enter in the SNMPv3 username, this is created on the network device/appliance
  - d) Choose method of Authentication SHA1 and or add password and or click the check box for Password is a key if key is required by the device.
  - e) Choose Privacy Encryption method of DES / AES128/AES192/AES256:

    This also depends on what the network device/appliance supports.
  - f) Add the password and or click the “Password is a key” check box.
  - g) Give the credential set a name and click save.
    - It is possible for the user to reuse the credential set for these same devices by selecting the “saved set” from the Saved Credential Sets library.
  - h) Choose the correct Polling Engine that will provide the monitor and then click Test to ensure the configuration test result is successful. If successful, click Next.

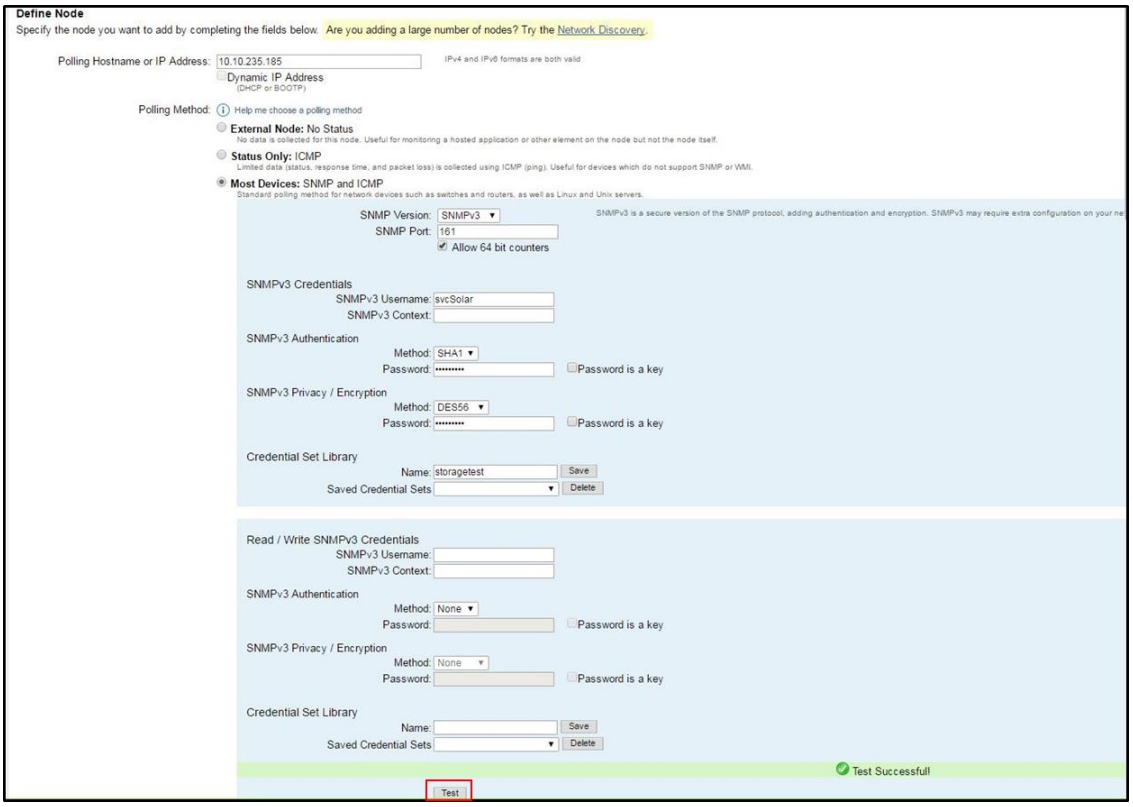

Polling Hostname or IP Address:
IPv4 and IPv6 formats are both valid
Dynamic IP Address
(DHCP or BOOTP)
Polling Method:
Help me choose a polling method
External Node: No Status
No data is collected for this node. Useful for monitoring a hosted application or other element on the node but not the node itself.
Status Only: ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful for devices which do not support SNMP or WMI.
Most Devices: SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as Linux and Unix servers.
SNMP Version: SNMPv3
SNMPv3 is a secure version of the SNMP protocol, adding authentication and encryption. SNMPv3 may require extra configuration on your network devices. Orion NPM can store SNMPv3 credential sets in the Orion database.
SNMP Port: 161
Allow 64 bit counters
SNMPv3 Credentials
SNMPv3 Username:
SNMPv3 Context:
SNMPv3 Authentication
Method: None
SHA1
Password:
Password is a key
SNMPv3 Privacy / Encryption
Method:
DES / AES128/AES192/AES256
Password:
Password is a key



- If this network device/appliance has a firewall, it will need to be configure to allow the selected Polling Engine request to be accepted.

NOTE: Remember the Authentication and Encryption settings are based from what the network device/appliance is capable of supporting. solarwinds/Orion is limited to the above settings in step 4 and 5.

5. Select the Test button. Verify test is successful then click next.



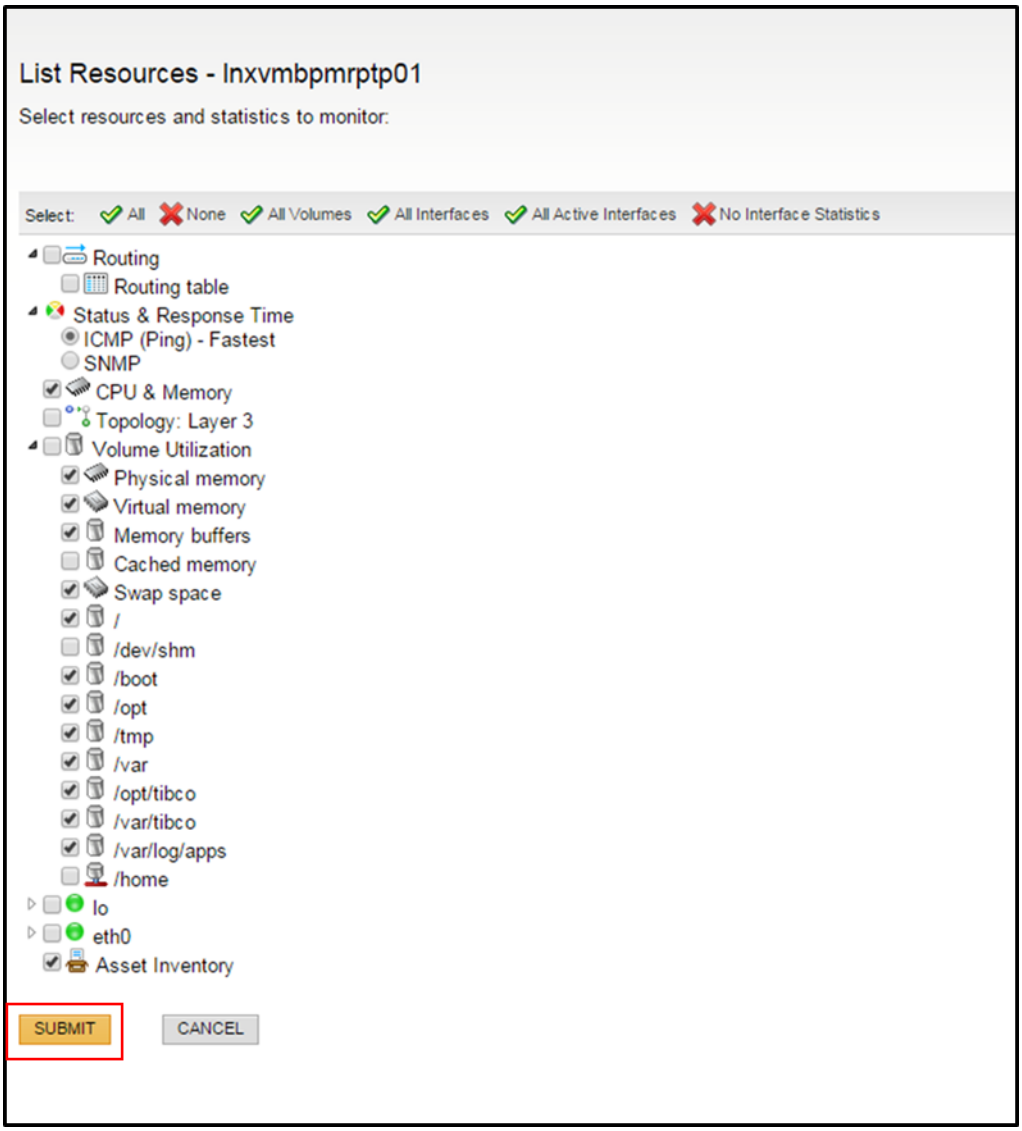
6. For virtual machines the configuration should be as follows:

NOTE:

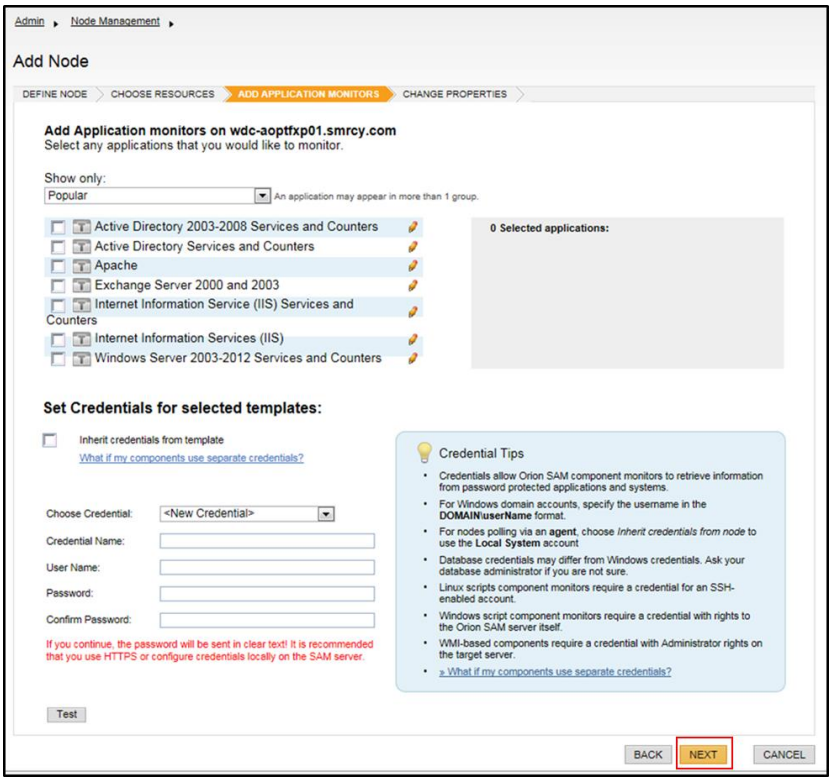
*** If the device being monitored are physical then the interfaces need to be considered.**

****The exception to this is the loopback [lo]. It should never be monitored.**

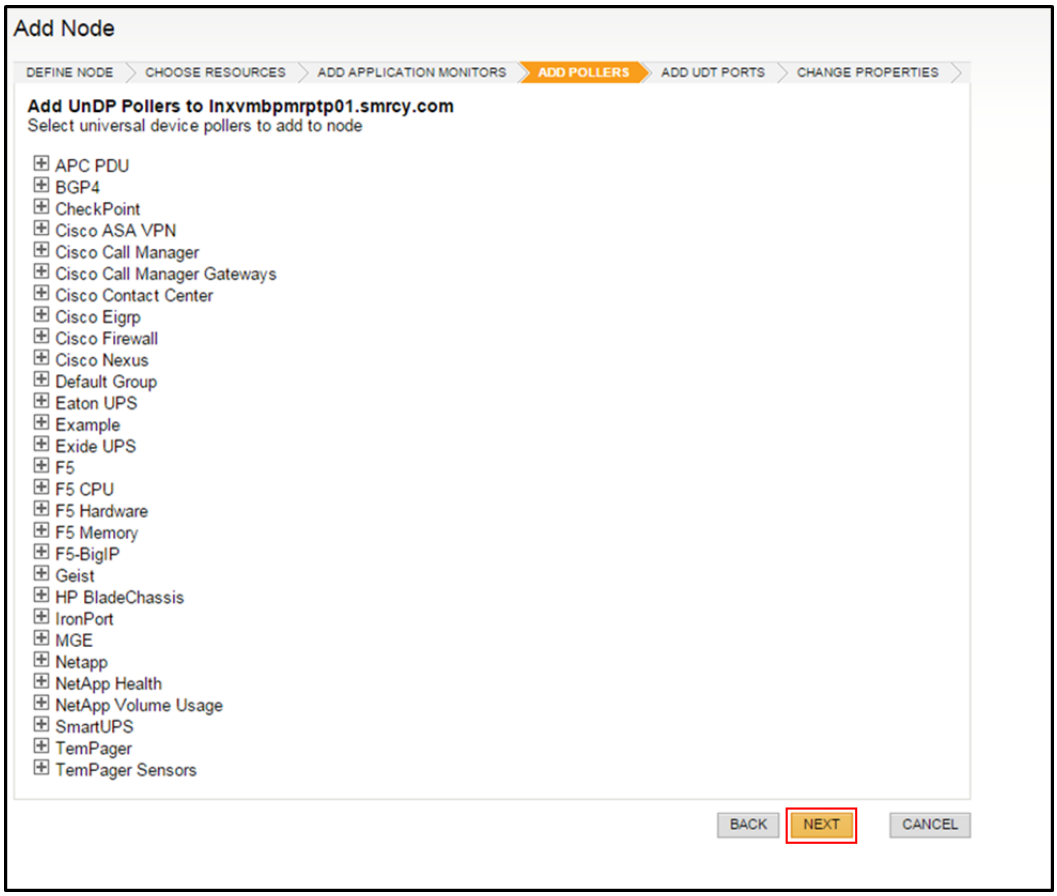
7. Click the Submit button.



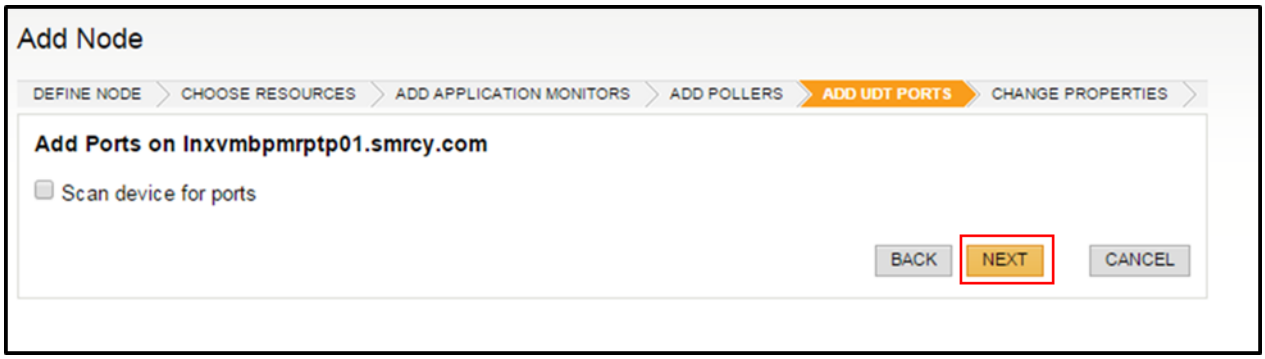
8. Select the Next button.



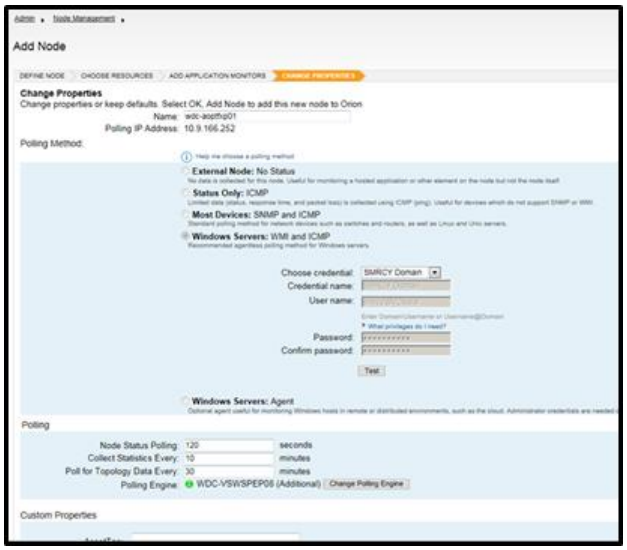
9. Select Next.

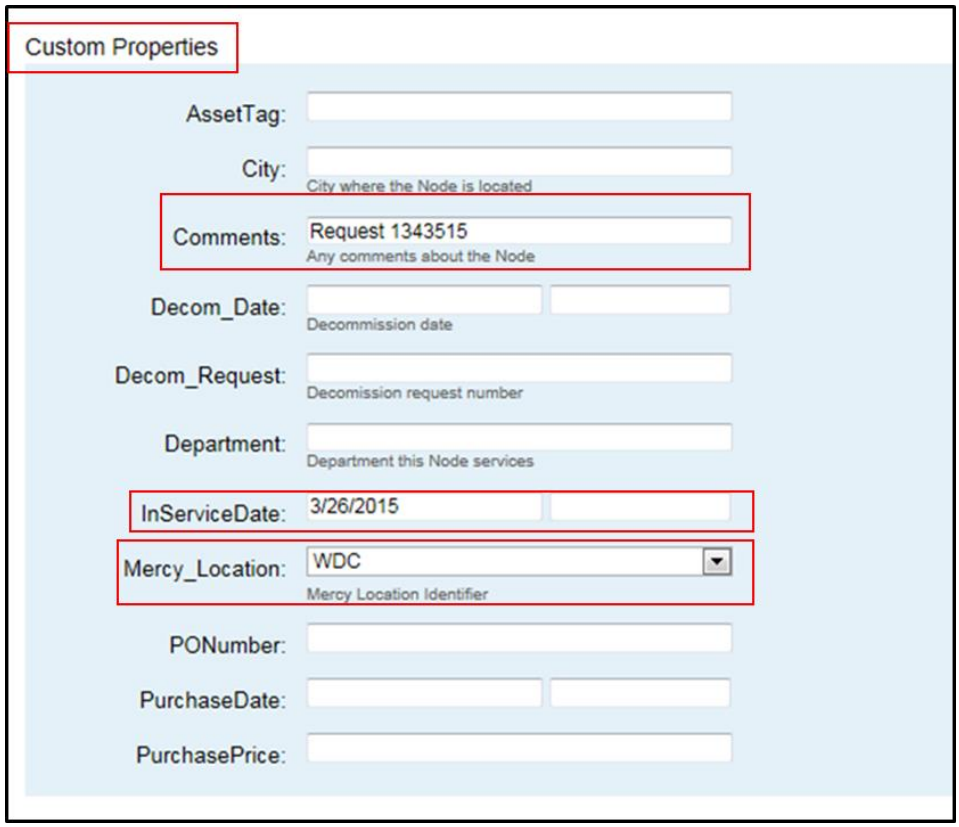


10. Select Next.

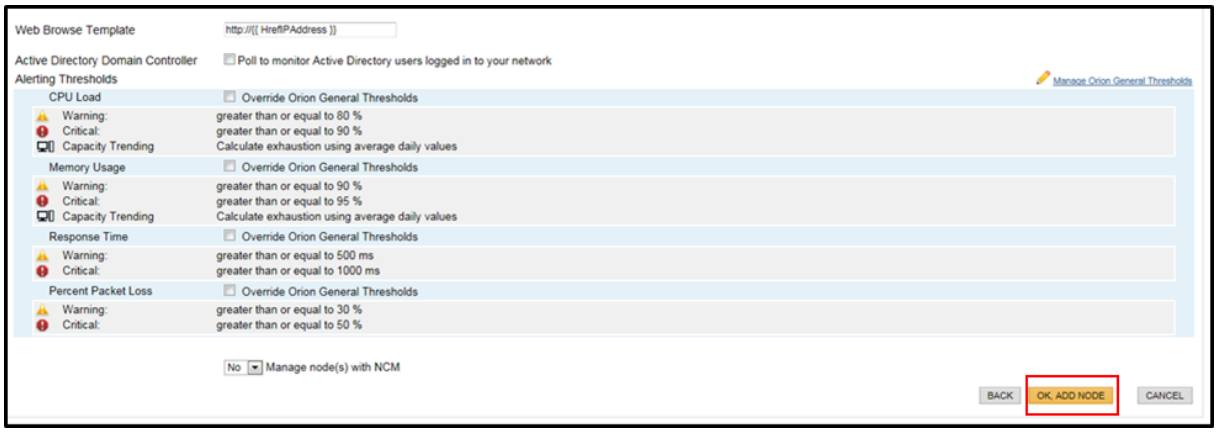


11. Fill in Custom Properties as follows: Comments: Paste Service Request Ticket Number; InserviceDate: Click the Day your inputting device; Mercy_Location: select Mercy Location of Device Installed in the dropdown.

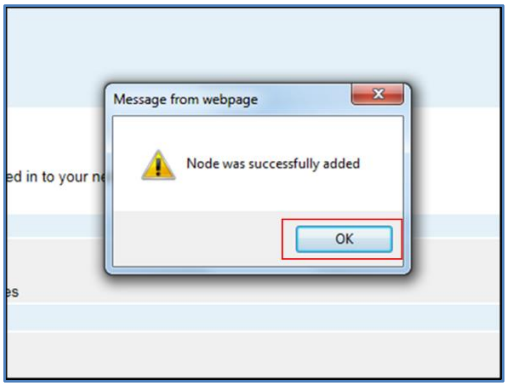




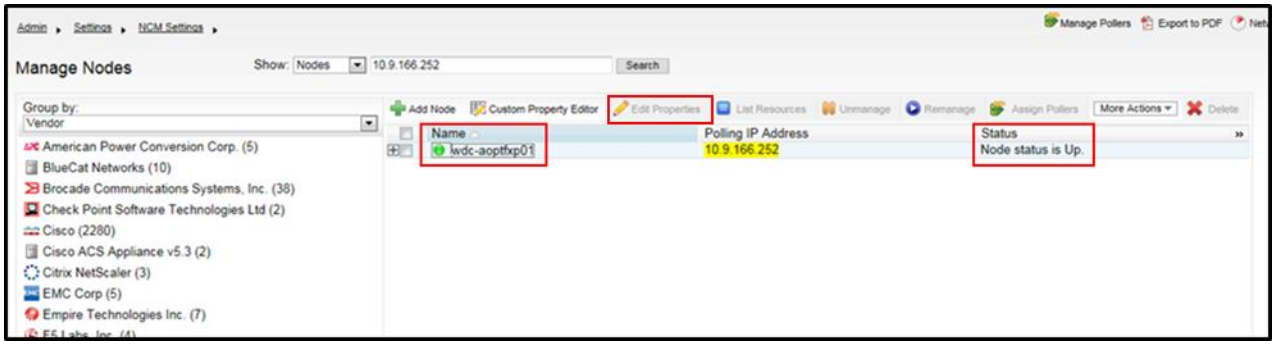
12. Select OK, ADD NODE.



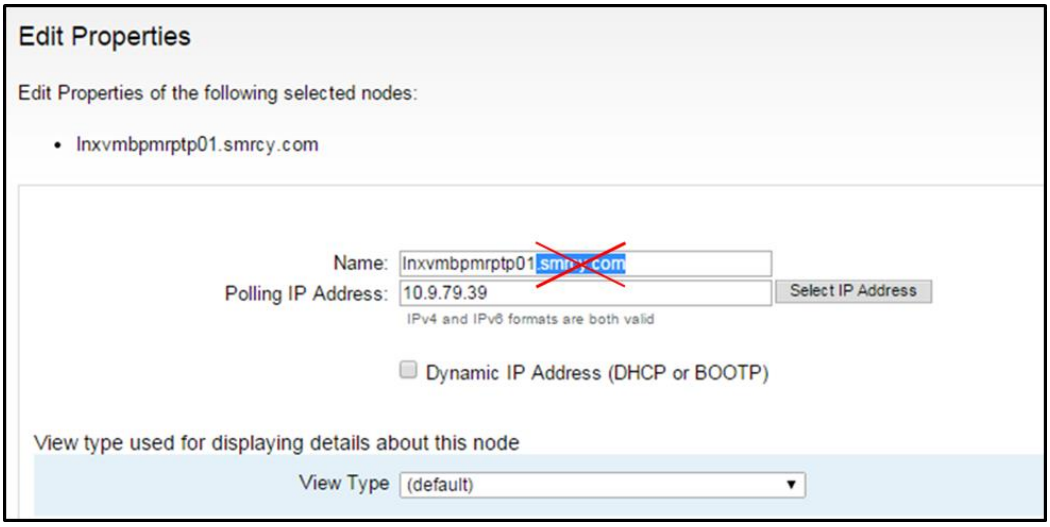
13. Click OK.



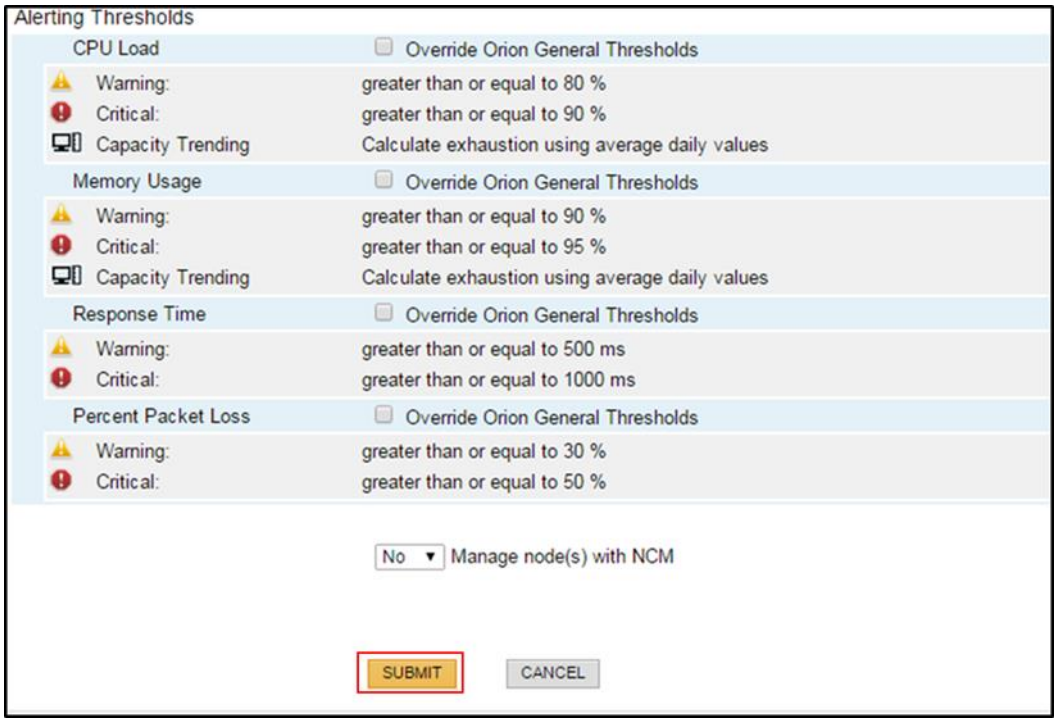
14. Confirm Status: Node status is Up. Confirm ".smrcy" is removed from the end of the name located in the Name field by selecting and clicking Edit Properties.



15. Highlight and delete ".smcry.com".



16. Scroll down and select Submit.



PCI Compliance

Organize or cross-reference material and PCI compliance notes by the 12 requirements outlined in the Payment Card Industry (PCI) Data Security Standards (PCI_DSS_v3-2). If possible, use sub-requirement details.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.**	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.**	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.**	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.**	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.**	Track and monitor all access to network resources and cardholder data.
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	**12.**	Maintain a policy that addresses information security for all personnel

Change History

Change / Review Date	Person Making Change	Change Detail

Approval

Approval of the procedure is needed from the Manager of the functional area to which the procedure applies. If the procedure applies to larger or multiple groups, teams, or departments, approval of procedure is needed from the Director, Executive Director, VP, or CIO as appropriate.

Lead System Administrator	6/7/2016
{insert name}	Date
{insert name}	Date
Director approval to send to QSA	Date