

MTS - PCI - Monitoring
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 <i>Implementation</i> 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

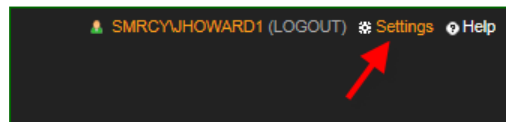


PCI Monitoring
solarwinds Envirom

Process / Procedure

Process / Procedures Steps

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



MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

2. Select Managed Nodes.

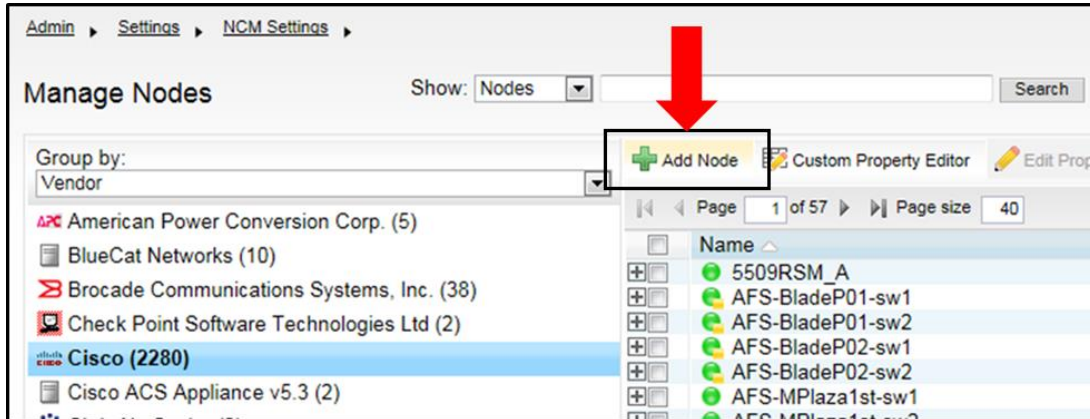
The screenshot shows the SolarWinds Orion web interface. At the top, there is a navigation bar with tabs for HOME, NETWORK, APPLICATIONS, WEB, CONFIGS, VOIP & NETWORK QUALITY, NETFLOW, and DEVICE TRACKER. Below the navigation bar, a yellow banner displays a message: "UDT Remote Event Log Jobs failed (2). > More Details Dismiss Message".

The main content area is titled "Main Settings & Administration" and is divided into several sections:

- Getting Started with Orion**: Discover your network and add the objects you want to monitor in Orion. Links include: > Discovery Central, > Network Sonar Discovery, > Add a Node, > Add a Transaction Monitor.
- Node & Group Management**: Manage, create, delete nodes, dependencies and groups. Edit node properties. A red arrow points to the **Manage Nodes** link. Other links include: > Manage Agents, > Manage World Map, > Manage Virtual Devices, > Manage Groups, > Manage Pollers, > Manage Dependencies, > Manage Custom Properties, > Manage Hardware Sensors.
- Alerts & Reports**: Create new alert / report or edit existing definitions. Links include: > Manage Alerts, > Manage Reports, > Manage SMTP Servers, > Configure Default Send Email Action.
- Product Specific Settings**: Global and product specific settings such as session timeout, page refresh, site logo, chart settings etc. Links include: > NTA Settings, > VoIP & Quality Settings, > Web Console Settings, > Agent Settings, > WPM Settings, > Virtualization Settings, > NCM Settings, > UDT Settings, > SAM Settings, > QoE Settings.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

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.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

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:

SNMP Port:

Allow 64 bit counters

SNMPv3 Credentials

SNMPv3 Username:

SNMPv3 Context:

SNMPv3 Authentication

Method: ← **SHA1**

Password: Password is a key

SNMPv3 Privacy / Encryption

Method: ← **DES / AES128/AES192/AES256**

Password: Password is a key

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.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

Credential Set Library

Name: Save

Saved Credential Sets Delete

Read / Write SNMPv3 Credentials

SNMPv3 Username:

SNMPv3 Context:

SNMPv3 Authentication

Method:

Password: Password is a key

SNMPv3 Privacy / Encryption

Method:

Password: Password is a key

Credential Set Library

Name: Save

Saved Credential Sets Delete

Test

Windows Servers: WMI and ICMP
Recommended agentless polling method for Windows servers.

Windows Servers: Agent
Optional agent useful for monitoring Windows hosts in remote or distributed environments, such as the cloud. Administrator credentials are needed only for installing the agent. The agent does not need to be installed on the server already. [What is an agent?](#)

Polling Engine:

- If this network device/appliance has a firewall, it will need to be configured 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.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

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

Define Node
Specify the node you want to add by completing the fields below. Are you adding a large number of nodes? Try the [Network Discovery](#).

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 is a secure version of the SNMP protocol, adding authentication and encryption. SNMPv3 may require extra configuration on your network.
SNMP Port:
 Allow 64 bit counters

SNMPv3 Credentials
SNMPv3 Username:
SNMPv3 Context:

SNMPv3 Authentication
Method:
Password: Password is a key

SNMPv3 Privacy / Encryption
Method:
Password: Password is a key

Credential Set Library
Name:
Saved Credential Sets:

Read / Write SNMPv3 Credentials
SNMPv3 Username:
SNMPv3 Context:

SNMPv3 Authentication
Method:
Password: Password is a key

SNMPv3 Privacy / Encryption
Method:
Password: Password is a key

Credential Set Library
Name:
Saved Credential Sets:

✔ Test Successful!

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.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

7. Click the Submit button.

List Resources - Inxvmbpmrptp01

Select resources and statistics to monitor:

Select: All None All Volumes All Interfaces All Active Interfaces No Interface Statistics

- Routing
 - Routing table
- Status & Response Time
 - ICMP (Ping) - Fastest
 - SNMP
- CPU & Memory
- Topology: Layer 3
- Volume Utilization
 - Physical memory
 - Virtual memory
 - Memory buffers
 - Cached memory
 - Swap space
 - /
 - /dev/shm
 - /boot
 - /opt
 - /tmp
 - /var
 - /opt/tibco
 - /var/tibco
 - /var/log/apps
 - /home
- io
- eth0
- Asset Inventory

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

8. Select the Next button.

The screenshot shows the 'Add Node' wizard in OrionSW, specifically the 'Add Application Monitors' step for the node 'wdc-aoptfxp01.smrcey.com'. The wizard has four steps: 'DEFINE NODE', 'CHOOSE RESOURCES', 'ADD APPLICATION MONITORS', and 'CHANGE PROPERTIES'. The current step is 'ADD APPLICATION MONITORS'. The user is prompted to 'Select any applications that you would like to monitor.' There is a 'Show only:' dropdown menu set to 'Popular'. A list of applications is shown with checkboxes and edit icons: Active Directory 2003-2008 Services and Counters, Active Directory Services and Counters, Apache, Exchange Server 2000 and 2003, Internet Information Service (IIS) Services and Counters, Internet Information Services (IIS), and Windows Server 2003-2012 Services and Counters. To the right, a box indicates '0 Selected applications:'. Below the application list, there is a section for 'Set Credentials for selected templates:' with an unchecked checkbox for 'Inherit credentials from template' and a link 'What if my components use separate credentials?'. There are input fields for 'Choose Credential:' (set to '<New Credential>'), 'Credential Name:', 'User Name:', 'Password:', and 'Confirm Password:'. A 'Test' button is below these fields. A red box highlights the 'NEXT' button at the bottom right. A 'Credential Tips' box on the right provides instructions for setting credentials for various applications and operating systems.

Admin > Node Management >

Add Node

DEFINE NODE > CHOOSE RESOURCES > **ADD APPLICATION MONITORS** > CHANGE PROPERTIES >

Add Application monitors on wdc-aoptfxp01.smrcey.com
Select any applications that you would like to monitor.

Show only:
Popular [v] An application may appear in more than 1 group.

- Active Directory 2003-2008 Services and Counters [edit]
- Active Directory Services and Counters [edit]
- Apache [edit]
- Exchange Server 2000 and 2003 [edit]
- Internet Information Service (IIS) Services and Counters [edit]
- Internet Information Services (IIS) [edit]
- Windows Server 2003-2012 Services and Counters [edit]

0 Selected applications:

Set Credentials for selected templates:

Inherit credentials from template
[What if my components use separate credentials?](#)

Choose Credential: <New Credential> [v]

Credential Name: [text box]

User Name: [text box]

Password: [text box]

Confirm Password: [text box]

If you continue, the password will be sent in clear text! It is recommended that you use HTTPS or configure credentials locally on the SAM server.

Test

BACK **NEXT** CANCEL

Credential Tips

- Credentials allow Orion SAM component monitors to retrieve information from password protected applications and systems.
- For Windows domain accounts, specify the username in the DOMAIN\username format.
- For nodes polling via an agent, choose *Inherit credentials from node* to use the Local System account.
- Database credentials may differ from Windows credentials. Ask your database administrator if you are not sure.
- Linux scripts component monitors require a credential for an SSH-enabled account.
- Windows script component monitors require a credential with rights to the Orion SAM server itself.
- WMI-based components require a credential with Administrator rights on the target server.
- > [What if my components use separate credentials?](#)

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

9. Select Next.

The screenshot shows the 'Add Node' wizard interface. The breadcrumb trail at the top is: DEFINE NODE > CHOOSE RESOURCES > ADD APPLICATION MONITORS > **ADD POLLERS** > ADD UDT PORTS > CHANGE PROPERTIES. The main heading is 'Add UnDP Pollers to Inxvmbpmrtp01.smrcy.com' with the instruction 'Select universal device pollers to add to node'. A list of poller types is displayed, each with a checkbox: APC PDU, BGP4, CheckPoint, Cisco ASA VPN, Cisco Call Manager, Cisco Call Manager Gateways, Cisco Contact Center, Cisco Eigrp, Cisco Firewall, Cisco Nexus, Default Group, Eaton UPS, Example, Exide UPS, F5, F5 CPU, F5 Hardware, F5 Memory, F5-BigIP, Geist, HP BladeChassis, IronPort, MGE, Netapp, NetApp Health, NetApp Volume Usage, SmartUPS, TemPager, and TemPager Sensors. At the bottom right, there are three buttons: 'BACK', 'NEXT' (highlighted with a red box), and 'CANCEL'.

10. Select Next.

The screenshot shows the 'Add Node' wizard interface at the 'ADD UDT PORTS' step. The breadcrumb trail is: DEFINE NODE > CHOOSE RESOURCES > ADD APPLICATION MONITORS > ADD POLLERS > **ADD UDT PORTS** > CHANGE PROPERTIES. The main heading is 'Add Ports on Inxvmbpmrtp01.smrcy.com'. There is a single checkbox labeled 'Scan device for ports' which is currently unchecked. At the bottom right, there are three buttons: 'BACK', 'NEXT' (highlighted with a red box), and 'CANCEL'.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

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.

The screenshot shows the 'Add Node' configuration page in OrionSW. The 'Polling Method' section has three radio buttons: 'External Node: No Status', 'Status Only: ICMP', and 'Windows Servers: WMI and ICMP'. The 'Windows Servers: WMI and ICMP' option is selected. Below this, there are fields for 'Choose credential', 'Credential name', 'User name', 'Password', and 'Confirm password'. At the bottom, there are fields for 'Node Status Polling' (120 seconds), 'Collect Statistics Every' (10 minutes), and 'Poll for Topology Data Every' (30 minutes).

The screenshot shows the 'Custom Properties' form in OrionSW. The form contains several fields: 'AssetTag', 'City', 'Comments' (with value 'Request 1343515'), 'Decom_Date', 'Decom_Request', 'Department', 'InServiceDate' (with value '3/26/2015'), 'Mercy_Location' (dropdown menu with value 'WDC'), 'PONumber', 'PurchaseDate', and 'PurchasePrice'.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

12. Select OK, ADD NODE.

Web Browse Template

Active Directory Domain Controller Poll to monitor Active Directory users logged in to your network

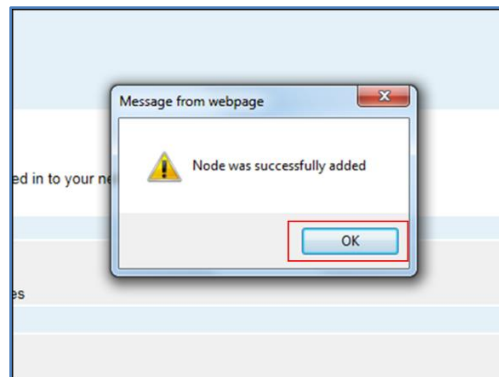
Alerting Thresholds [Manage Orion General Thresholds](#)

Category	Warning	Critical	Capacity Trending	Override Orion General Thresholds
CPU Load	greater than or equal to 80 %	greater than or equal to 90 %	Calculate exhaustion using average daily values	<input type="checkbox"/>
Memory Usage	greater than or equal to 90 %	greater than or equal to 95 %	Calculate exhaustion using average daily values	<input type="checkbox"/>
Response Time	greater than or equal to 500 ms	greater than or equal to 1000 ms		<input type="checkbox"/>
Percent Packet Loss	greater than or equal to 30 %	greater than or equal to 50 %		<input type="checkbox"/>

Manage node(s) with NCM

BACK **OK, ADD NODE** CANCEL

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.

Admin > Settings > NCM Settings >

Manage Nodes

Show: Nodes 10.9.166.252 Search

Group by: Vendor

Actions: Add Node, Custom Property Editor, **Edit Properties**, List Resources, Unmanage, Remanage, Assign Pollers, More Actions, Delete

Name	Polling IP Address	Status
wdc-aoptfxp01	10.9.166.252	Node status is Up

15. Highlight and delete “.smrcy.com”.

MTS - PCI - Monitoring PCI Monitor OrionSW ADD ONE LINUX Server Procedure

Edit Properties

Edit Properties of the following selected nodes:

- Inxvmbpmrtp01.smrty.com

Name:

Polling IP Address:

IPv4 and IPv6 formats are both valid

Dynamic IP Address (DHCP or BOOTP)

View type used for displaying details about this node

View Type

16. Scroll down and select Submit.

Alerting Thresholds

CPU Load	<input type="checkbox"/> Override Orion General Thresholds
Warning:	greater than or equal to 80 %
Critical:	greater than or equal to 90 %
Capacity Trending	Calculate exhaustion using average daily values
Memory Usage	<input type="checkbox"/> Override Orion General Thresholds
Warning:	greater than or equal to 90 %
Critical:	greater than or equal to 95 %
Capacity Trending	Calculate exhaustion using average daily values
Response Time	<input type="checkbox"/> Override Orion General Thresholds
Warning:	greater than or equal to 500 ms
Critical:	greater than or equal to 1000 ms
Percent Packet Loss	<input type="checkbox"/> Override Orion General Thresholds
Warning:	greater than or equal to 30 %
Critical:	greater than or equal to 50 %

Manage node(s) with NCM

MTS - PCI - Monitoring

PCI Monitor OrionSW ADD ONE LINUX Server Procedure

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

MTS - PCI - Monitoring
PCI Monitor OrionSW ADD ONE LINUX
Server Procedure

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