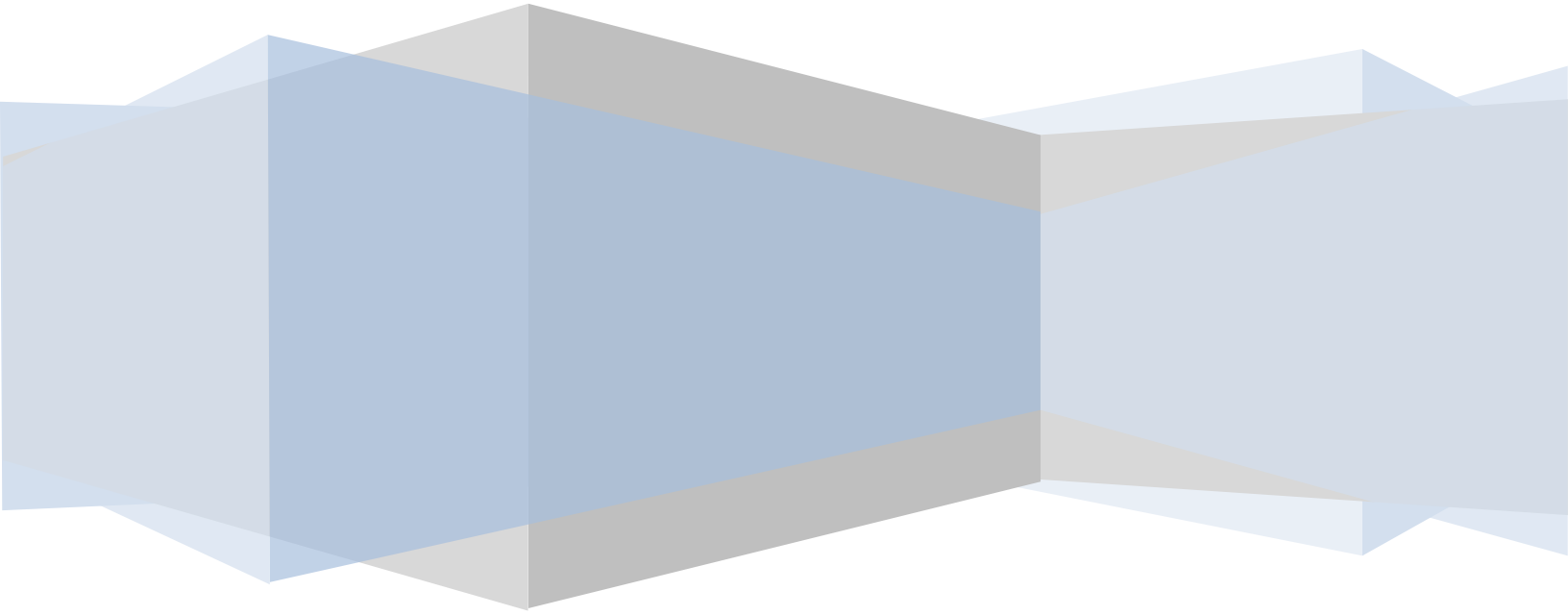
Cisco Systems

# Cisco Process Orchestrator 3.3 Hardening Guide

**Tuan Tran**



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

# Contents

**INTRODUCTION** ..... **2**

**WINDOWS SECURITY HARDENING POLICY** ..... **2**

**MICROSOFT SQL SERVER HARDENING BEST PRACTICE** ..... **2**

**HARDENING AN ORACLE DATABASE** ..... **3**

**PORTS USED BY PROCESS ORCHESTRATOR SERVER** ..... **3**

**CHANGING ORCHESTRATOR DEFAULT PORTS** ..... **5**

PROCESS ORCHESTRATOR CONSOLE PORT ..... 5
NORTHBOUND WEB SERVICE PORTS ..... 6
REST WEB SERVICE PORTS ..... 7

**PORTS USED BY ORCHESTRATOR ADAPTERS** ..... **7**

SNMP ..... 7
OTHER PORTS ..... 10

# Cisco Process Orchestrator Hardening Guide

## Introduction

This document contains information to help you secure your Cisco Process Orchestrator installation by adjusting at various levels of your infrastructure. This guide discusses on the various points of vulnerability in the Process Orchestrator, from your Windows® servers to the applications, resources used, and explains the best practices that can be employed to make your installation more secure.

Note: Complying with these hardening guidelines does not guarantee the elimination of all security threats. However, by implementing these guidelines, you can achieve a higher-level of security and help manage unforeseen risks.

## Windows Security Hardening Policy

This section describes the recommended hardening guidelines that are required to harden Windows system using Microsoft Windows to run the Process Orchestrator, and to make additional changes to harden its configuration. If your system has additional hardening steps, changes are required for the Process Orchestrator to work.
For hardening Windows Server 2008 R2 and 2012, the Best Practices Analyzer (BPA) server management tool, is installed by default on all editions of Windows Server 2008 R2 and Windows Server 2012, except the Server Core installation option, can be used.
The BPA server management tool helps administrator to reduce best practice violations by scanning one or more roles that are installed on your Windows Server and reports best practice violations to the administrator.
For additional information on recommended Windows OS hardening guidelines, see Microsoft Security Compliance Manager.

## Microsoft SQL Server Hardening Best Practice

Applications that are not included with Windows Server 2008 R2 have a separate BPA for optimizing and hardening applications. These BPAs run on the Microsoft Baseline Configuration Analyzer (MBCA) application that maintains optimal system configuration by analyzing configurations of a system against a predefined set of best practices.

- To download MBCA v2.0, click http://www.microsoft.com/download/en/details.aspx?id=16475.

The Microsoft SQL Server 2008 R2 BPA is a diagnostic tool that gathers information about a server and a Microsoft SQL Server 2008 or 2008 R2 instance installed on that server, and recommends solution for the potential problems.

- To download the SQL Server 2008 R2 Best Practices Analyzer, click http://www.microsoft.com/download/en/details.aspx?id=15289.
- To download the SQL Server 2012 Best Practices Analyzer, click http://www.microsoft.com/en-us/download/details.aspx?id=29302.
- Currently Microsoft has not published a tool for SQL Server 2014 or 2016
- To submit a feedback to the Microsoft Connect, *see* *https://connect.microsoft.com/SQLServer/Feedback*" (*https://social.technet.microsoft.com/Forums/windows/en-US/23151f36-2486-484c-b736-51495888078e/sql-server-2014-missing-best-practices-analyzer?forum=sqlsecurity*)

# Hardening an Oracle Database

For information on hardening an Oracle 11g or 12c database, *see* Oracle Database Hardening Guide.

# Ports Used by Process Orchestrator Server[1]

Process Orchestrator utilizes various TCP ports to facilitate communication between the server and its different clients. You can view the Default Port assignment details in the **Table 1**.

**Table 1 - Default Port Assignments**

| Default Port | Use |
|---|---|
| **61525** | Orchestrator Console |
| **61526** | Secure Northbound Web Service |
| **61527** | Non-secure Northbound Web Service |
| **51526** | Secure REST Northbound Web Service |
| **51527** | Non-secure REST Northbound Web Service |
| **61600** | OpenStack Adapter |
| **162** | SNMP Adapter |

[1] Refer to the Cisco Process Orchestrator Port and Services section of the Installation Guide for additional information.

You can view the ports that are in use by given Orchestrator server through the Orchestrator Console.

To view the port details, follow these steps:

1. **In the** Administration **view, select** Orchestrator Servers **as shown in the** Double-click the server and select the **Ports** tab.

   The port details appear as shown in the Figure 2.

2. Figure 1.
3. Double-click the server and select the **Ports** tab.

   The port details appear as shown in the Figure 2.

**Figure 1 - Orchestrator Servers View**

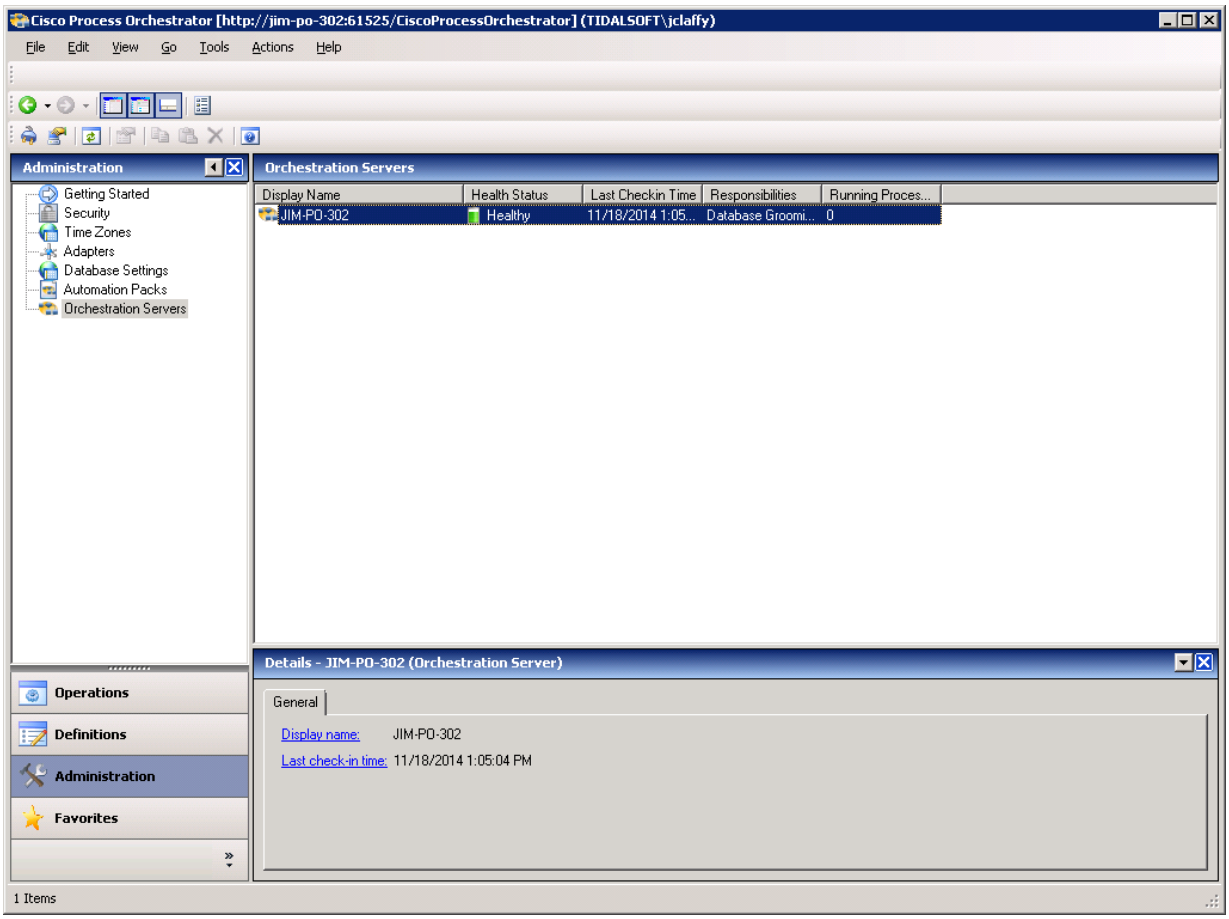
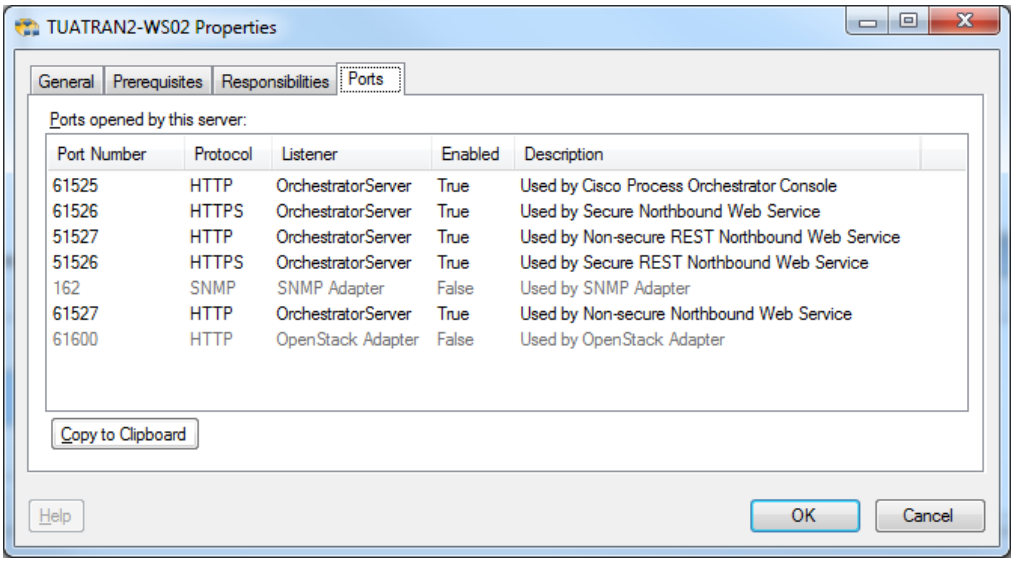


**Figure 2 - Orchestration Server Properties**




# Changing Orchestrator Default Ports

## *Process Orchestrator Console Port*

To change the Process Orchestrator Console Port, follow these steps:

1. Choose **Start > Control Panel > Administrative Tools > Services**.
   The **Services** dialog box displays.

2. Select **Cisco Process Orchestrator Server**, right-click the server, and choose **Stop**.

   Note: Ensure that the **Services** dialog box is kept open.

3. In the Cisco Process Orchestrator install directory, open the following configuration files and modify the port number to a non-default port number.
   The XML files open in the default application associated with the file. If the file does not open by default, then use *Notepad.exe* to open the file.

4. Follow the configuration file instructions as given in:

### Configuration File Instructions

- *Tidal.Automation.Server.exe.config*
  Navigate to the *ClientCommunicationPort* and change the value to a non-default port, such as *11111*. Document the port number elsewhere for later use.

- *Tidal.Automation.Console.Loader.exe.config*
  Navigate to the *Server URL* and change the port number to match the *ClientCommunicationPort number* variable in the *Tidal.Automation.Server.exe.config* file.

  Note: This file needs to be modified on the all machines where the Console is installed, including Remote Consoles.

- *Web.config*
  Located in the WebConsole folder this file needs to be modified so that the *WebServiceUris* property contains the same port number as the one configured in *Tidal.Automation.Server.exe.config*.

- *Tidal.Automation.WinForms.AutomationPackManagement.Wizard.Setup.exe.config*
  This file exists in the Console folder under the Cisco Process Orchestrator install directory. Modify the URL "http://localhost:%NewPortNumber%" in this file with the new port number.
- *Tidal.Automation.CLI.CorePSSnapin.dll.config*
  Modify the URL "http://localhost:%NewPortNumber%" in this file with the new port number.

5. Save and close each file after the port number is changed.

6. Return to the **Services** dialog box and restart the **Cisco Process Orchestrator Server** service.

## *Northbound Web Service Ports*

The Northbound Web Services (NBWS) offered by the Orchestrator server are available on both secure and unsecure ports as shown in **Table 1**.

Securing the NBWS ports are performed in two ways:

- Change the port assignments from their default value.
- Change the security certificate assigned to the secure NBWS port from the default certificate by the Orchestrator server.

For instructions on changing the ports used by the server to listen for connections to its Northbound Web Services, and for instructions on utilizing an alternate certificate for the secure NBWS port, *see* Cisco Process Orchestrator Northbound Web Services Guide.

### *REST Web Service Ports*

The REST Web Services offered by the Orchestrator server are available on both secure and unsecure ports **Table 1**.

Securing the REST ports are performed in two ways:

- Change the port assignments form there default value.
- Change the security certificate assigned to the secure REST port from the default certificate by the Orchestrator server.

For instructions on changing the ports used by the server, to listen for connections to its REST Web Services, and for instructions on utilizing an alternate certificate for the secure REST port, *see* Cisco Process Orchestrator REST Web Services Guide.

# Ports Used by Orchestrator Adapters

In addition to the ports used by the Orchestrator server, various adapters loaded by the server, either listen to additional ports or connect to ports on remote servers. In general, many adapters allow the user to specify port numbers when configuring targets such as, SNMP, Email, Service Catalog, VMware vSphere, JMX, and so on. These ports are accounted for configuring firewalls or other network security tools.

### *SNMP*

When functioning as an SNMP manager, the SNMP adapter listens to the traps on UDP port 162. The SNMP adapters *Trap listening port* are changed through the SNMP Adapter configuration as shown in the Figure 3.

**Figure 3 – Adapters**

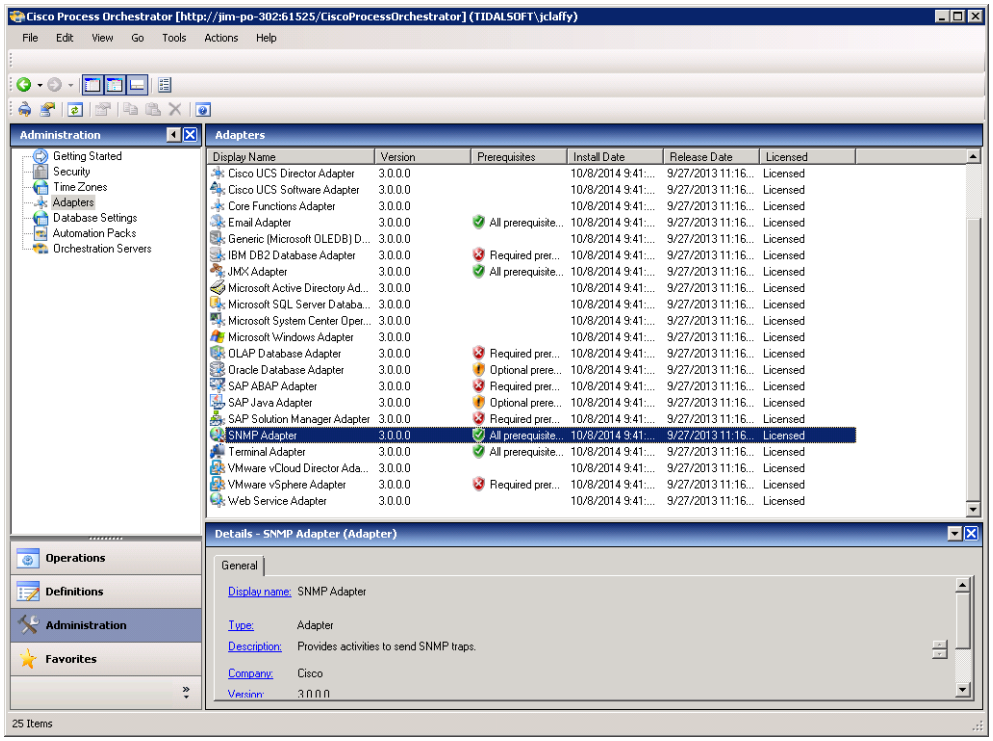
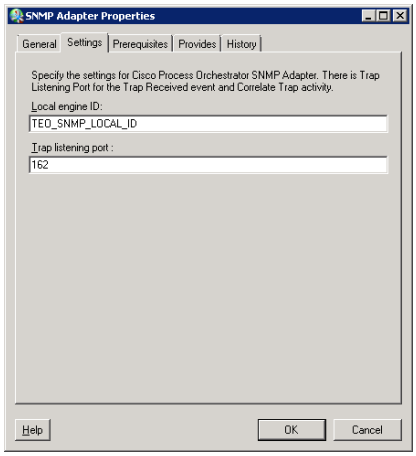



**Figure 4 - SNMP Adapter Configuration**




When functioning as an SNMP agent, the SNMP adapter sends traps to an SNMP manager on the port 162 by default. The port assignments can be changed through the SNMP target configuration as shown in the Figure 5.

**Figure 5 - Target Configuration**

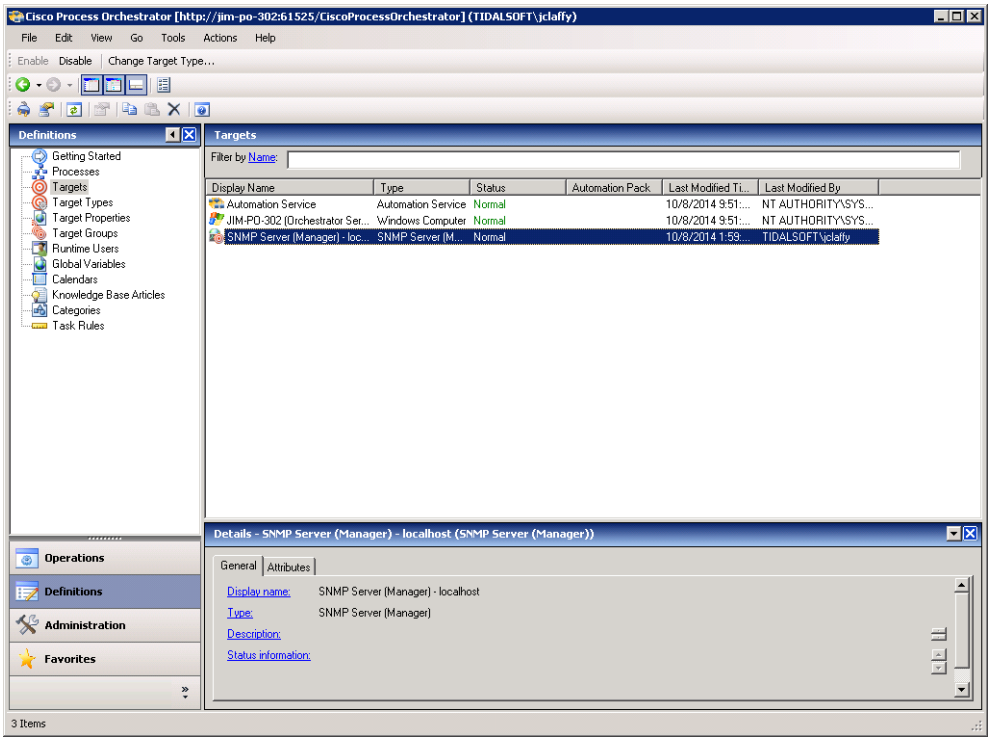
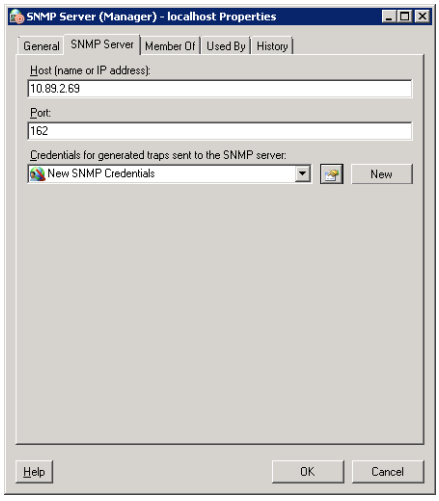
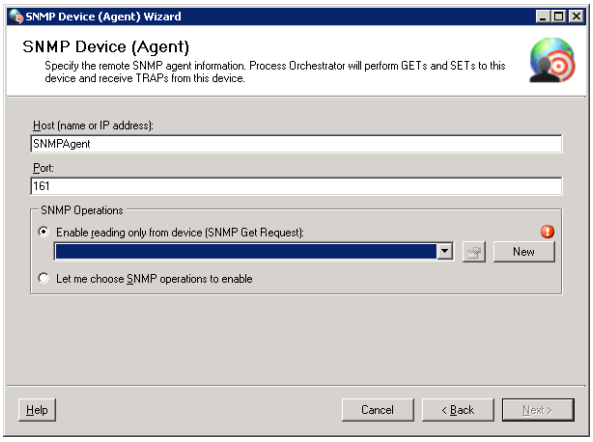



**Figure 6 - SNMP Manager Target Configuration**




When functioning as an SNMP manager, the adapter requests (get, getnext, and so on) to the UDP port 161 of the SNMP agent by default. The port assignments can be changed through the SNMP target configuration as shown in Figure 7.

**Figure 7 - SNMP Agent Target Configuration**




## *Other Ports*

The Windows adapter uses various protocols that depend on ports being opened on remote servers. The Windows adapter uses RPC calls to connect to remote machines. The ports required for RPC calls are controlled by the Operating System.

*"Remote Procedure Call (RPC) dynamic port allocation is used by server applications and remote administration applications such as Dynamic Host Configuration Protocol (DHCP) Manager, Windows Internet Name Service (WINS) Manager, and so on. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP, based on the implementation of the operating system used (see references below).*

*Customers using firewalls may want to control the ports RPC is using, so that their firewall routers are configured to forward only these Transmission Control Protocol (UDP and TCP) ports."*

For more information, see http://support.microsoft.com/kb/154596.

---



Cisco Process Orchestrator Hardening Guide