Configuring Cisco Process Orchestrator

Configuring the Core Functions Adapter

The Core Functions Adapter provides the basic functionality in Process Orchestrator. Use the Core Functions Adapter Properties dialog box to configure default task settings, automation summary report

Configuring Return on Investment Settings

When you create a process, you have the option to enter the equivalent time it would take to run the process manually. This value is calculated against the hourly rate specified on this page to determine the return on investment for the process.

1. Choose **Administration > Adapters**, right-click **Core Functions Adapter** and choose **Properties**.
2. On the Core Functions Adapter Properties dialog box, click the **ROI** tab and specify the hourly rate (in dollars) that it would cost to execute a process manually, then click **OK**.

Configuring Task Expiration Settings

Use the Task Properties page to specify the default number of days used for the task expiration date. If a task is opened on its expiration date, an internal event is raised that can be used to trigger a process. Users will be able to modify the date manually on the appropriate task property page.

1. Choose **Administration > Adapters**, right-click **Core Functions Adapter** and choose **Properties**.
2. On the Core Functions Adapter Properties dialog box, click the **Task Properties** tab.
3. Under Task expiration days, modify the default task expiration date, then click **OK**.

Enabling Data Execution Prevention (DEP)

To secure your underlying hardware and operating system in Microsoft Windows 2008 R2 or later and Windows 2012, use the following Data Execution Prevention (DEP) features:

- Hardware-enforced DEP detects code that is running from these locations and raises an exception when execution occurs.
- Software-enforced DEP can help prevent malicious code from taking advantage of exception-handling mechanisms in Windows.

To enable DEP in Windows 2008 R2 or later and Windows 2012:

1. Choose **Start > All Programs > Control Panel > System**, then click **Advanced system settings**.
2. Choose **Performance > Settings**.

3. Click the **Data Execution Prevention** tab, then check **Turn on DEP for all programs and services except those I select**.
4. Choose the programs and services on which you do *not* want to run DEP, then click **OK**.

Hardening the Cisco Process Orchestrator Configuration

Hardening the Microsoft Windows Server operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required. For information about how to harden your Windows operating system and to make additional changes to Cisco Process Orchestrator to harden its configuration, see the *Cisco Process Orchestrator Hardening Guide*.

Configuring a High Availability Environment

Because there are a variety of load balancers and you might have your own that you want to use, this section does not describe how to set up or configure load balancers. Instead, it explains how to load balance different Cisco Process Orchestrator client connections using the generic load balancer, Microsoft Network Load Balancing Manager, as an example.

Microsoft Network Load Balancing Manager is a virtual load balancer that is not as feature-rich as what most customers probably use in production environments, but does demonstrate how Process Orchestrator clients work with a generic load balancer.

Setting Up a Load Balancer

To set up Microsoft Network Load Balancing Manager for Process Orchestrator requires at least three to five machines and three static IP addresses:

- One machine acts as the cluster host (with a static IP).
- Two machines act as Process Orchestrator servers and Web Consoles. Alternatively, the Web Console could be installed on a separate highly-available IIS (with a static IP).
- One machine hosts a High Availability database for Process Orchestrator (for testing purposes this could be the same machine as the cluster host).
- One machine performs client testing (for testing purposes this could also be the same as the cluster host).

In the example in the following sections, the cluster/load-balancer is not monitoring specific Process Orchestrator ports to verify that the application is healthy, but instead is tested using the Load Balancing Manager software (by stopping incoming connections to a specific host) or by shutting down the server or disabling network access on one of the Process Orchestrator servers to ensure that load-balancing is occurring. In production, the load balancer should be configured to monitor the health of the Process Orchestrator server, northbound web service, or IIS ports to determine if the server, northbound web service, or web console are running or down. The default ports are as follows:

- IIS ports: HTTP 2081, HTTPS 443
- SNMP 1: 61
- Console: 61525
- NBWS: 61526 HTTPS, 61527 HTTP
- REST: 51526 HTTPS, 51526 for HTTP

Configuring the Console Connection

To configure the Cisco Process Orchestrator console to connect through the load balancer:

1. Choose **Start > Cisco Process Orchestrator Console**, then in the Select Server dialog, enter the host name of the load balancer cluster.
2. To verify that the connection is being made through the load balancer, check the Cisco Process Orchestrator Console; the load balancer URL should appear in the title bar.
3. To ensure that load balancing is running successfully, perform *one* of the following actions on the load balancer:
   a. Select a specific host and Stop or Drainstop connections to that host.
   b. Disable the network interface or bring down the server that the Process Orchestrator is running on.

In a production environment, you should be monitoring the server port, and can test just by bringing it down.

Configuring the NBWS and REST Connections

Before You Begin

Configure the Cisco Process Orchestrator console to connect through the load balancer (see Configuring the Console Connection, page 45).

1. Choose **File > Environment Properties > Web Services**.
2. Enable the Web Services. By default, the ports for SOAP HTTPS is 61526 and for HTTP is 61527. And Rest uses 51526 for HTTPS and 51527 for HTTP.
3. Set up SSL on your Process Orchestrator servers.

You should not need to do any additional certificate setup or configuration on the load balancer itself.

4. Configure any Northbound connections to connect through the load balancer. For example, to connect to the Target Northbound Web Service using the default SOAP HTTPS port, connect to:

```
https://<load-balancer-name>:61526/WS/Target?wsdl
```

5. To ensure that load balancing is running successfully, perform *one* of the following actions on the load balancer:
   a. Select a specific host and Stop or Drainstop connections to that host.
   b. Disable the network interface or bring down the server that the Process Orchestrator is running on.

In a production environment, you should be monitoring specific NBWS ports, and can test just by bringing them down.

Configuring the Web Console Connection

Before You Begin

Configure the Cisco Process Orchestrator console to connect through the load balancer (see Configuring the Console Connection, page 45).

1. Choose **File > Environment Properties.**

2. Click the **General** tab and enter the required information, then click **Save**.

   a. In the Web Console location field, enter *one* of the following:

   – The load balancer URL. This is what gets set as the task URL for tasks and can be sent in emails as a URL location to the Web Console. This is also what is used to open and complete the task using the Web Console.

   – The IP address of the cluster in the Web Console location.

3. Copy the Web Console URL, which is now using load balancer URL in the environment properties dialog, into your browser and confirm that the Web Console is displayed properly.

4. On each server, confirm that IIS authentication for the `orchestratorwebconsole` web site and `OrchestratorWebConsole` application under it is set to only use basic authentication and ASP.NET Impersonation.

5. Using an ASCII text editor, edit the file `C:\Program Files\Cisco\Cisco Process Orchestrator\WebConsole\Web.config`:

   a. In the <system.web> section, verify `<authentication mode="Windows" />` and `<identity impersonate="true" />`.

   b. In the <appsettings> section, set `<add key="WebServiceUris" value="the load balancer's URL" />`.

6. To ensure that load balancing is running successfully, perform *one* of the following actions on the load balancer:

   a. Select a specific host and Stop or Drainstop connections to that host.

   b. Disable the network interface or bring down the server that the Process Orchestrator is running on.

In a production environment, you should be monitoring the IIS port and can test just by bringing it down.