

HP Server Automation

Enterprise Edition

Software Version: 10.0

Integration Guide

Document Release Date: June 13, 2013

Software Release Date: June 2013



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2001-2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Support

Visit the HP Software Support Online website at:

<http://www.hp.com/go/hpsoftwaresupport>

This website provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online website:

http://h20230.www2.hp.com/sc/support_matrices.jsp

You can also download the *HP Server Automation Support and Compatibility Matrix* for this release from the HP Software Support Online Product Manuals website:

<http://h20230.www2.hp.com/selfsolve/manuals>

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details. See Documentation Change Notes for a list of any revisions.

Product Editions

There are two editions of HP Server Automation:

- HP Server Automation (SA) is the Enterprise Edition of Server Automation. For information about Server Automation, see the SA Release Notes and the SA User Guide: Server Automation.
- HP Server Automation Virtual Appliance (SAVA) is the Standard Edition of Server Automation. For more information about what SAVA includes, see the SAVA Release Notes and the SAVA at a Glance Guide.

Documentation Change Notes

The following table indicates changes made to this document since the last released edition.

Date	Changes
June 13, 2012	Original release of this document with SA 10.0.

Contents

1	SA-DMA Integration	9
	Prerequisites to Run DMA Flows	9
	Connecting to DMA	9
	Installing DMA Agents	10
	Identifying Managed Server Candidates	11
	Installing DMA Agents On Your System	11
	Activating the DMA Agent	13
	Troubleshooting the DMA Agent Installation	15
	Linux Installation	15
	Testing Your DMA Configuration	15
2	SA-NA Integration	17
	SA-NA Integration Overview	17
	SA-NA Integration Features	18
	How NA Data is Collected	19
	NA Topology Data Gathering Diagnostic	19
	NA Duplex Data Gathering Diagnostic	19
	NA Database/SA Database	19
	Authentication	19
	Prerequisites	19
	Time Requirements	20
	NA Integration Port Requirements	20
	SA-NA Integration Configuration Tasks	20
	SA Client Communication with NA	20
	Edit the jboss_wrapper.conf File	21
	SA Configuration Changes	22
	Configuring NA for Integration	23
	SA Gateway Requirements	23
	User Permissions	23
	NA Authentication Configuration	23
	Configuring SA-NA Integration with CiscoWorks NCM	25
	Gather Topology Data	26
	Troubleshooting Tips	26
	Resetting the NA Host in the SA Client	26
	Using SA-NA Integration	27
	Connections Between Network Devices and Servers	27
	Data Link Connections	27
	Physical Connections	28
	Network Device Information in SA	28

Viewing Network Interfaces	29
Viewing Network Ports	29
Network Device Information in NA	30
Viewing a Network Device	30
Viewing Event History	31
Duplex Mismatch	31
Viewing Duplex Mismatches in the Dashboard	32
Viewing Duplex Mismatches by Server	32
Viewing Duplex Mismatches by Network Device	32
Network Reports	33
Connections by Network Device	33
Connections by Server	33
Network Diagrams	33
Launching Service Automation Visualizer (SAV)	33
Launching NA Diagramming	33
NA and the SA Global Shell	34
Launching OGFS	34
Remote Terminal (rosh)	34
Inferred Physical Connections	35
Device Groups and NA	35
Associating a NA Device Group	35
3 SA-OO Integration – Running Flows	37
What’s New for SA-OO Integration	37
Support for OO 10.0	37
Edit Flow Integration Settings Window	38
Displaying Real-Time Information	38
Administrators: Setting Up Flows	38
Prerequisites	38
Prerequisites for Using OO	38
Environment	38
Importing the OO SDK Client Certificate	39
Permissions	40
Editing the Flow Integration Settings	40
Replacing OO Connector File Functionality	42
SA-OO Integration Flows	43
Verifying Your Changes and Settings	45
Flow Edits and Flow Status	45
Users: Running Flows	45
Choosing a Flow to Run	45
Adding or Deleting Servers	47
Choosing Flow Input, Runtime Option, Scheduling Option, and Notification Parameters	47
Troubleshooting	49
SA-OO Connection Error	49
Flow Run Error	49
4 SA-OO Integration – Job Blocking and Approving	51
Blocking Jobs	51

What are Blocked Jobs?	51
Scenario 1.	51
Scenario 2.	51
Scenario 3.	52
What SA Job Types Can be Blocked?	52
sRequired Permissions	53
How Do I Block and Unblock Jobs?	54
How Do I Designate Job Types to Block?	54
How Do I Disable Job Blocking?	55
How Do I View Blocked-Job Information?	55
Checking OO Connection Information in the SA Flow Integrations Panel	55
Checking Blocked-Job Status in the Job Log	56
Configuring or Editing a Flow Setting	56
Approving and Deleting Blocked Jobs	57
Java Methods for Handling Blocked Jobs	57
Job-Status Values	58
5 SA-uCMDB Connector	61
The SA-uCMDB Integration	61
Highlighted Features	61
uCMDB Browser	61
Installing and Configuring the SA-uCMDB Connector	62
Customizing SA Data Sent to the uCMDB Server	63
<i>The Mapping File</i>	<i>63</i>
Customizing the Mapping File	63
Editing the Mapping File	64
Support for SA Custom Attributes	68
<i>How to Transfer SA Custom Attributes to uCMDB</i>	<i>68</i>
<i>Filter Support for Queries</i>	<i>68</i>
Extended Out-Of-The-Box Mappings	69
Additional Out-of-the-Box Mappings	69
Customized Data Conversion Function	69
Sample Conversion File – MyConvertVirtualizationType.Java	71
Managing the SA-uCMDB Connector	72
Stopping and Disabling the SA-uCMDB Connector	72
The stop Command	73
The disable Command	73
Enabling and Starting the SA-uCMDB Connector	73
The enable Command	74
Displaying the Status of the SA-uCMDB Connector	75
SA-uCMDB Data Relationship and Transfer	76
CI Relationships Maintained	76
Example: uCMDB Showing an SA Managed Server	76
SA Data Transferred to uCMDB	77
Frequency of Data Transfer to uCMDB	78
Accessing the uCMDB Browser from the SA Client	79
The uCMDB Browser Window	79

Configuring the uCMDB Browser	79
Support for uCMDB Server Versions 9.05 and 10.01	80
Global uCMDB IDs	80
Configurable Files Archived During Upgrade	81
Troubleshooting Tips	82
Running the SA-uCMDB Connector on a Second Core	82
On-Demand Synchronization	83
Viewing Log Files	83
SA-uCMDB Connector Daemon	83
EXAMPLE – SA-uCMDB Connector Mapping File	83

1 SA-DMA Integration

This chapter discusses the use of HP Database and Middleware Automation (DMA) flows with HP Server Automation's Application Deployment Manager.

To follow the procedures in this chapter, you must be familiar with DMA flows, the DMA interface, and the Application Deployment Manager interface.

The chapter includes the following topics:

- [Prerequisites to Run DMA Flows](#) on page 9
- [Connecting to DMA](#) on page 9
- [Installing DMA Agents](#) on page 10
- [Testing Your DMA Configuration](#) on page 15

For more information on DMA flows or the Application Deployment Manager, see the *Database and Middleware Automation User Guide* and the *Application Deployment Manager User Guide*.

Prerequisites to Run DMA Flows

This section describes the major steps required to run DMA flows.

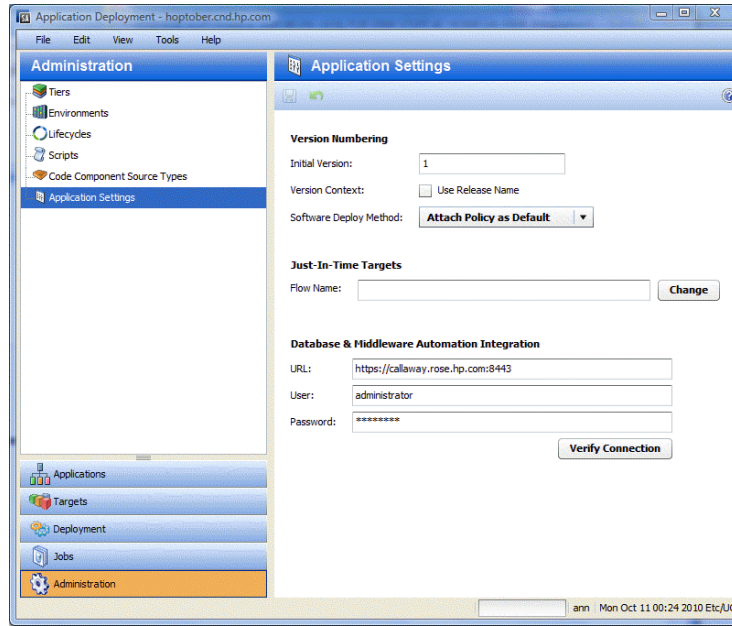
- Install and configure a DMA server. Steps for this process are documented in the DMA Installation Guide.
- Configure Application Deployment Manager to communicate with DMA – see [Connecting to DMA](#) on page 9 and the Application Settings section in the *Application Deployment Manager User Guide*.
- Install DMA agents on the managed servers where the DMA flows will be run – see the *DMA Installation Guide*.
- Create an application that includes your DMA workflow or deployment – see Creating DMA Flow Components in the 9.02 *Application Deployment Manager User Guide*.
- Deploy your application using Application Deployment Manager – see the *Application Deployment Manager User Guide*.

Connecting to DMA

To create a connection between DMA and Application Deployment Manager:

- 1 As an Application Deployment Manager administrator, open Application Deployment Manager from within SA (choose Tools ► Application Deployment).
- 2 In Application Deployment Manager, select the Administration tab.
- 3 Choose Application Settings.

Figure 1 Application Settings Section



- 4 In the Application Settings section, enter the following information:
 - URL: URL of the server where DMA is installed.
 - User name: User name that has DMA administrative privileges.
 - Password: Password corresponding to the user name.
- 5 Click **Verify Connection** to test your Application Deployment Manager/DMA connection.

A connection status message is displayed.

Installing DMA Agents

There are three major steps involved in installing DMA agents:

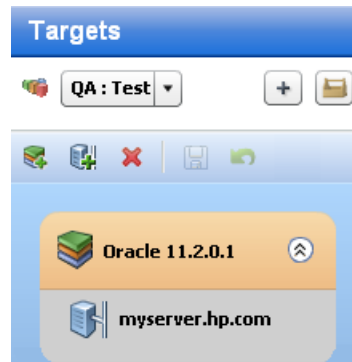
- Identify the managed-server candidates where you should install the agents – see [Identifying Managed Server Candidates](#) on page 11.
- Confirm that the DMA agent can be installed on your system and follow the correct steps to install the agent – see [Installing DMA Agents On Your System](#) on page 11.
- Activate the DMA agent – see [Activating the DMA Agent](#) on page 13.

Identifying Managed Server Candidates

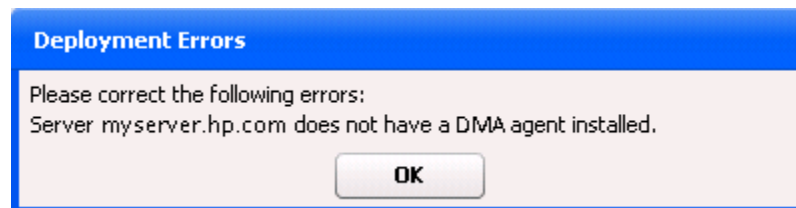
You can use Application Deployment Manager targets to help you decide on which managed servers you should install the DMA agents.

If you deploy an application that runs DMA flows to a target, all managed servers that the target references *must* have a DMA agent installed. For example, as the following figure shows, if you were to deploy an application to the target QA: Test, which references the managed server myserver.hp.com, you must install the DMA agent on the myserver.hp.com server.

Figure 2 Target Server



Note: At deployment time, if a referenced managed server does not have a DMA agent installed, Application Deployment Manager will issue the following warning:



Installing DMA Agents On Your System

DMA agents are supported on the following platforms:

Table 1 Platforms that Support the DMA Agent

Platform	Version
AIX	5.1 pSeries 5.3 pSeries 6.1 pSeries
HP-UX	11.23 pa-risc 11.23 Itanium2 11.31 pa-risc 11.31 Itanium2
Linux - RedHat EL 4	i386, x86_64

Table 1 Platforms that Support the DMA Agent (cont'd)

Platform	Version
Linux - RedHat EL 5	i386 x86_64
Solaris 9	Sparc
Solaris 10	Sparc x86
Windows 2003 Server	x86 x86_64
Windows 2008 Server	x86 x86_64

See the *DMA Installation Guide* for details on installing agents on individual platforms.

Activating the DMA Agent

This section explains how to activate the DMA agent.

Note: For information about bulk agent activation, contact your HP support representative.

After you install DMA agents on the managed servers you chose in [Identifying Managed Server Candidates](#) on page 11, you must activate the agents using the DMA interface.

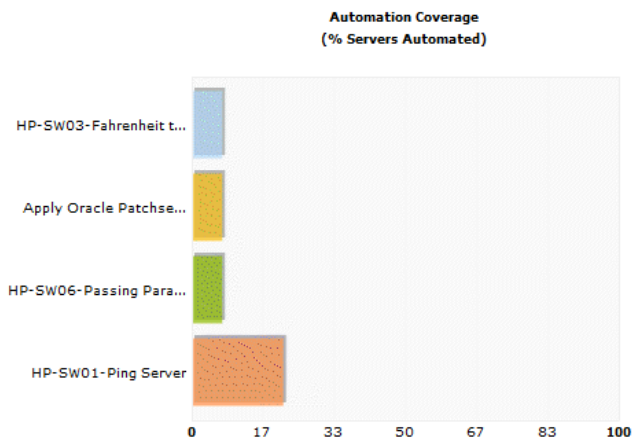
To activate the agent:

- 1 Log in to the DMA Nerve Center.

Figure 3 DMA Dashboard

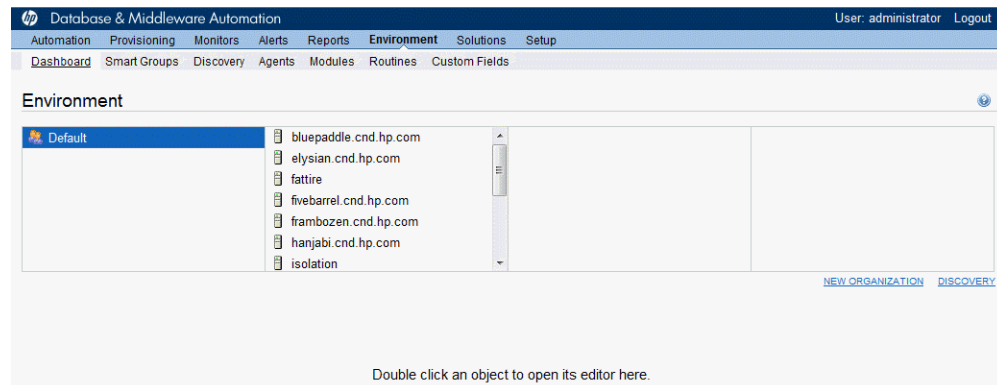


Dashboard



- 2 In the navigation bar, click **Environment**.

Figure 4 Environment Tab



- 3 To the right of the Environment window, click New Organization to create the new ADM organization.

Figure 5 Create New Organization

New organization

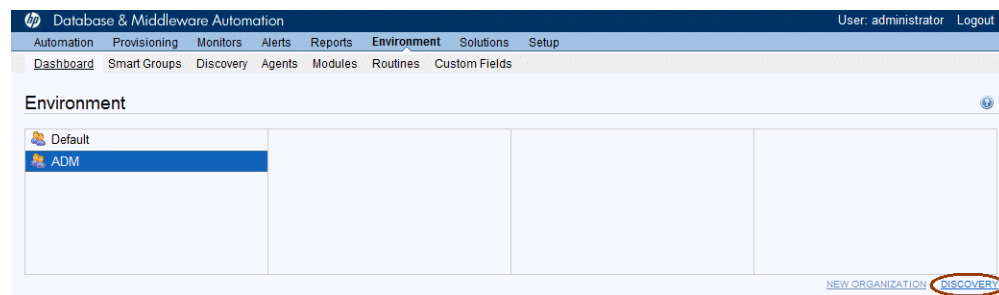
Properties Custom Fields Policies Roles

General

Name: ADM

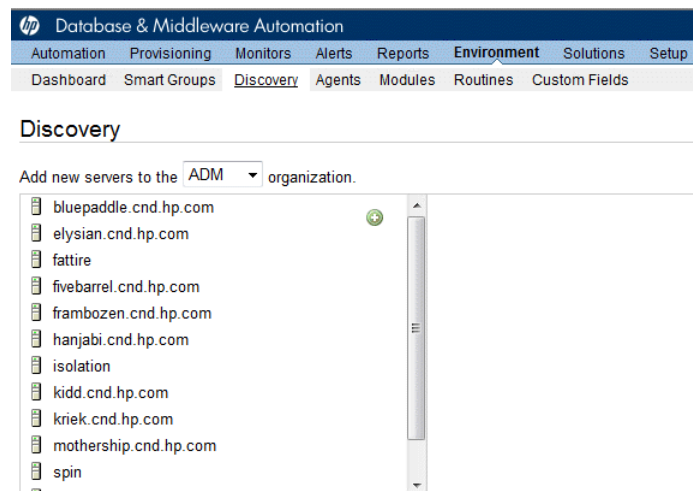
- 4 In the New organization window, enter ADM in the Name field and click **Save**.
If the information was saved correctly, an Organization Saved Correctly message and the ADM environment icon are displayed.


Figure 6 ADM Environment Icon



- 5 To the left of the Environment window, click **Discovery**.

Figure 7 Discovery Window



- 6 In the Discovery window:
 - a Choose ADM from the organization menu.
 - b Select a server from the new servers list.
 - c Click the green plus icon  to add servers to the ADM organization.
- 7 Click **Save**.

Repeat the steps in this procedure for each managed server that requires a DMA agent.

Troubleshooting the DMA Agent Installation

Linux Installation

You might need to install additional RPM dependencies.

Note: If you are upgrading from a previous release of Stratavia Data Palette to DMA 1.0, you will need to delete your existing solution packs and re-install the equivalent HP DMA Solution Packs.

Testing Your DMA Configuration

After you complete the configuration described in this chapter, you will be able to use DMA flows in Application Deployment Manager. To verify that your DMA integration is working correctly, create an application that uses a DMA flow and deploy it using Application Deployment Manager. For more information, see the *Application Deployment Manager User Guide*.

2 SA-NA Integration

SA-NA Integration Overview

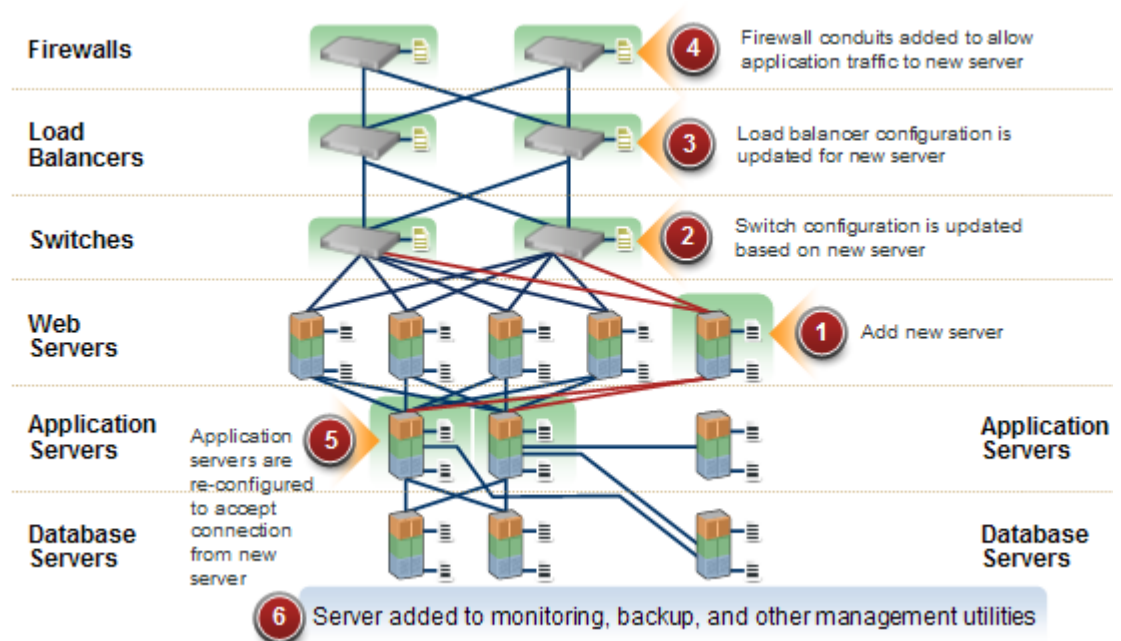
Implementing changes in an IT environment often requires a coordinated effort between network administrators, system administrators, and application architects who must manage an application environment that may consist of servers with different operating systems as well as network devices that can include firewalls, load balancers, switches, servers, Web applications, and so on.

For example, in some environments, you are required to make changes to network devices in front of an application, such as load balancers, firewalls, switches, and so on.

SA-NA Integration makes this process easier by enabling you to see how servers are connected to network devices and enables them to closely examine managed servers. With this information, you can determine how all devices are related and coordinate and implement required changes.

Figure 8 shows some of the coordinated tasks you can perform through SA-NA Integration.

Figure 8 Overview of Coordinating Tasks Using SA-NA Integration



This section contains information about how to configure NA Integration with SA. After integration is established, you can view device details, examine connections between network devices and servers, identify duplex mismatches, and view combined device history information. It also contains information about implementing changes across the environment and generating network reports.

To support an integrated approach to making changes in your environment, such as server reallocation, ensuring compliance across servers and network devices, and detecting and resolving duplex mismatches, SA-NA Integration provides the following interface points:

- HP Server Automation (SA)
- Network Automation (NA)
- SA Global Shell
- Service Automation Visualizer (SAV) (in SA)
- HP Reports (in SA)

SA-NA Integration Features

After SA-NA Integration is configured you can perform the following tasks:

- View summarized and detailed hardware information about SA Managed Servers and their attached network devices, and about their network connections (interfaces and ports).
- Use the SA Global File System (OGFS) to:
 - navigate between managed servers and connected network devices by tracing their associated physical connections
 - find network device configurations
 - run scripts across servers and network devices.
- Call NA scripts from SA scripts to automate operations across servers and network devices.
- Use features in SA and NA to create diagrams that illustrate the managed servers, network devices, and layer 2 (and inferred layer 1) connections in your environment.
- Use SA to identify, troubleshoot, and remediate configuration duplex mismatches between managed servers and network devices.
- Use SA to perform actions on SA Device Groups that can contain both servers and network devices.
- Use SA to review a combined server and network device event history log that records changes made to applications in your environment.
- Use SA to export combined event history logs to CSV and/or HTML files.
- Use NA to directly access additional network device details and event history.
- Use SA to run network reports that identify layer 2 and inferred layer 1 connections and configuration mismatches (duplex compliance).



References to *connections* in this document refer to *physical connections*, except where noted.

How NA Data is Collected

The SA-NA Integration feature uses the NA Topology Data Gathering and NA Duplex Data Gathering diagnostic tools to collect information about network devices.

NA Topology Data Gathering Diagnostic

The NA Topology Data Gathering diagnostic instructs NA to collect MAC addresses for all switches. MAC addresses are required to discover and add physical connections to the SA data model.

For example, when you add a server to a switch, that information is collected the next time the NA Topology Data Gathering diagnostic runs. You can also manually run the NA Topology Data Gathering diagnostic or the NA Duplex Data Gathering diagnostic for specific network devices. For more information about these diagnostics, see the *NA User Guide*.



For NA performance reasons, you should not run these diagnostics on multiple devices more frequently than once a week. If you are required to refresh the NA data more frequently, contact your support representative. These diagnostics can be run on single devices more frequently.

NA Duplex Data Gathering Diagnostic

For network devices, speed and duplex is gathered by the NA Duplex Data Gathering diagnostic, which runs after a device is initially added to NA and subsequently according to a schedule that you define.

To ensure that you have the latest speed and duplex information about network devices, SA recommends that you set up a recurring schedule that runs the diagnostic. For more information about this diagnostic and scheduling, see [Duplex Mismatch](#) on page 31 and the *NA User Guide*.

NA Database/SA Database

The NA and SA databases are not integrated – NA and SA each manage their own data.

Authentication

For SA/NA integrated functionality, authentication is handled by SA. For more information, see [NA Authentication Configuration](#) on page 23. NA-only functionality continues to be authenticated using NA credentials.

Prerequisites

The following prerequisites must be satisfied.

Time Requirements

The SA and NA core servers must be synchronized and have the same time and time zone settings.

NA Integration Port Requirements

Before you configure NA Integration, ensure that SA and NA can communicate with each other over the following ports:

- **Port 1032 (NA to SA)**

NA must be able to access port 1032 on the server that is running the SA Web Services Data Access Engine component (part of the Component Slice bundle). By default, the Web Services Data Access Engine listens on port 1032.

- **Port 8022 (Unix) / Port 22 (Windows) (SA to NA)**

For the Global File System (OGFS) feature to be able to display data about network devices, SA must have access to port 8022 (Unix-based NA Servers) or 22 (Windows-based NA Servers).

- **RMI Ports for NA API**

The NA API uses Java RMI to connect to the NA server. SA uses the NA API for the NA integration. RMI requires that the following ports be open:

- **Port 1099**

JNDI

- **Port 4444** (for NA versions 9.10 and earlier)

RMI Object

- **Port 4446** (for NA versions 9.20 and later)

RMI Object

- **Port 1098**

RMI Method

SA-NA Integration Configuration Tasks

The SA administrators must perform certain tasks on SA Core servers to enable SA-NA Integration.

Configuration includes changing certain configuration settings in both NA and SA, running diagnostics for NA topology data, and configuring certain user permissions.

SA Client Communication with NA

Ensure that the SA Client can communicate with NA. If the SA Client cannot communicate with the NA server, see [Resetting the NA Host in the SA Client](#) on page 26.

Edit the jboss_wrapper.conf File

Required only for NA versions prior to 7.6. Version 7.6 and later do not include these entries in jboss_wrapper.conf.

You should adjust the values for wrapper.java.additional.x where x > 8 is consecutive.

For example:

Change this:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal.
Interceptors.PIORB
wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se.
internal.corba.ORBSingleton
wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore. This is used to make SSL request.
wrapper.java.additional.9=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.10=-XX:MaxPermSize=80m
```

To this:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
#wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal
.Interceptors.PIORB
#wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se
.internal.corba.ORBSingleton
#wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore. This is used to make SSL request.
wrapper.java.additional.6=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.7=-XX:MaxPermSize=80m
```

SA Configuration Changes

Complete the following tasks to prepare SA for NA Integration:

- **Specify the NA Server Name**

If you did not specify an NA server name during the SA Core Installer Interview, you must specify the value for the `twist.nasdata.host=<hostname>` parameter in the `/etc/opt/opsware/twist/twist.conf` file.

Find the entry:

```
twist.nasdata.host=
```

add the hostname or IP address of your NA server.

For more information about modifying this file, see the *SA Administration Guide*.



If you have installed multiple Slice Component bundles, you must edit the `twist.conf` file on all slices. Then, you must restart all NA services and the Web Service Data Access Engine for each Slice component bundle.

- **Specify the NA Port (Windows-only) in SA**

If NA is running on a Windows server, you must change the port setting parameter from `nas.port=8022` to `nas.port=22` in the `/etc/opt/opsware/hub/hub.conf` file.

A default Windows server installation runs the proxy SSH/Telnet servers on port 22/23 rather than the Unix default of port 8022/8023.




After you make this configuration change, you must restart the server hosting the Slice Component bundle.

- **Enable the `spin.cronbot.check_duplex.enabled` Parameter**

The `spin.cronbot.check_duplex.enabled` system configuration parameter must be enabled for NA integration.

To enable this system configuration parameter, perform the following steps:

- a Select the **Administration** tab in the SA Client.
- b Select System Configuration in the navigation pane. This displays the SA components, facilities and realms that have system configuration parameters.
- c In the list of SA components, select Data Access Engine. This displays the system configuration parameters for this component.
- d Locate the parameter `spin.cronbot.check_duplex.enabled`.
- e In the Value column, select the new value button  and set the value to 1.
- f Select the Revert button to discard your changes or the Save button to save your changes.

For more information about system configurations, see the *SA Administration Guide*.

Configuring NA for Integration



To configure NA Integration with the current SA version, you must have a compatible version of Network Automation (NA) installed. For more information, see the *NA Support Matrix*.

The NA administrator should perform the following tasks on your NA server.

SA Gateway Requirements

NA must be configured to use the Master Gateway for the SA Core you are integrating with. For more information about specifying the SA Core Master Gateway in NA, see the *NA Satellite Guide*.

User Permissions

Access permissions for SA-NA Integration are based on two separate databases: a NA database and a SA database. NA uses its own database for authorization. SA uses a different security mechanism for authorization. However, for NA integration, all authentication (for both NA and SA) is processed by SA.

When NA is configured to use SA authentication, NA tries to authenticate against SA first. If NA fails to authenticate against SA, it falls back to the NA database. If there is an account in the NA database, the fallback is only allowed if that user is configured to allow fallback authentication. See the *NA User Guide* for more information on NA authentication.

When a new user is authenticated through SA, an account is created in NA. The account is placed in the Default User Group that was specified when SA authentication was enabled in the Administrative Settings in NA. This user group, which is configurable, controls the default permissions that the system administrator has assigned to SA users.



You must have the required set of permissions to view servers and network devices. To obtain these permissions, contact your SA administrator, or for more information, see the *SA Administration Guide*.

NA Authentication Configuration

To set up SA-NA Integration, you must configure NA to use SA Authentication. Before beginning this configuration, you must have this information (see [Figure 10](#)):

- **Twist Server:** the IP address or Hostname of the server hosting the Web Services Data Access Engine (*twist*: part of the Slice Component bundle which is typically installed on the SA Core host but can be installed on a different host).
- **Twist Port Number:** The port number that the Web Services Data Access Engine listens on.
- **Twist Username:** The Web Services Data Access Engine user name.
- **Twist Password:** The Web Services Data Access Engine user's password.
- **OCC Server:** The IP address or hostname of the server hosting the Command Center (OCC).
- **Default User Group:** The default user group for new SA users.

To change the authentication settings in NA, perform the following tasks:

- 1 Log in to NA.
- 2 Select **Admin ► Administrative Settings ► User Authentication** to display the Administrative Settings — User Authentication page.
- 3 In the External Authentication Type section, use the radio button to select HP Server Automation software & TACACS+ (if used) as shown in [Figure 9](#).

Figure 9 External Authentication Type in NA

The screenshot shows the 'User Authentication' configuration page. At the top, there are tabs for Configuration Mgmt, Device Access, Server, Workflow, User Interface, Telnet/SSH, Reporting, **User Authentication**, Server Monitoring, and 3rd Party Integrations. Below the tabs is a 'Save' button. The page is divided into two main sections: 'User Password Security' and 'External Authentication Type'. The 'User Password Security' section includes fields for 'Minimum User Password Length' (set to 1), 'User Password Must Contain Upper and Lower Case' (checked), 'Additional User Password Restriction' (set to 'No additional restrictions'), and 'Maximum Consecutive Login Failures' (set to 0). The 'External Authentication Type' section has a list of radio buttons: 'None (Local Auth)', 'HP Server Automation Software', 'HP Server Automation Software & TACACS+' (selected and circled in red), 'TACACS+', 'RADIUS', 'SecurID', and 'LDAP'. A note on the right states: 'Choose the type of external authentication you would like to use. If you choose TACACS+, RADIUS or HP Server Automation Software, it can be configured in the section below. SecurID has no additional external authentication options.' Below the radio buttons, a note says: '(After saving the settings, go to [LDAP Setup](#) page for more options)'.

- 4 Scroll down and complete all fields in the HP Server Automation software Authentication section shown in [Figure 10](#).

NA uses the Web Services Data Access Engine (`twist`) Username and Password when it gathers layer 2 data. NA gathers server interface information by MAC address using the Twist user's permissions. The Twist user must have read access to server information.

Figure 10 HP Server Automation Software Authentication

The screenshot shows the 'HP Server Automation Software Authentication' configuration page. It contains several fields with labels and descriptions: 'Twist Server' (twistc43.dev.example.com), 'Twist Port Number' (1032), 'Twist Username' (defuser), 'Twist Password' (password field), 'OCC Server' (occ.c43.dev.example.ocm), and 'Default User Group' (Limited Access User). Each field has a description of its purpose.

- 5 Click **Save** to save your configuration changes.

See the *NA User Guide* for more information on NA configuration.

Configuring SA-NA Integration with CiscoWorks NCM

If you are deploying SA with CiscoWorks NCM 1.2, you must make certain configuration changes. Some CiscoWorks NCM deployments (where CiscoWorks LMS is co-resident with NCM) use non-standard ports that affect integration with SA.

To determine which changes you will need to make, perform the following tasks:

Phase 1: Edit `tomcat4-service.xml`:

- 1 Log in to your NCM server.

- 2 Open the XML file:

```
<NCM_install_dir>/server/ext/jboss/server/default/deploy/  
tomcat4-service.xml.
```

- 3 Search for the string 'scheme=https'.

- 4 Check the preceding entry which should be

```
port = "port_no".
```

If the `port_no` value is 443, then go to Phase 4; otherwise, note the specified port and continue to Phase 2.

Phase 2: Assign the port number:

- 1 Log in to the SA Client.

- 2 In the SA Client, from the **Tools** menu, select **Options**.

- 3 In the Set Options window, select **Network Automation**.

- 4 In the Host field, append `:<port>` to the hostname, where `<port>` is the port number found in Phase 1, **step 4**, for example:

```
mycore.opsware.com:443
```

Click Save.

The following warning will appear: "General.Host: must be a valid host string." Ignore this warning. Close the Set Options window.

(Phase 2 must be performed for every user of the SA Client.)

Phase 3: Edit Primary Data Access Engine files:

- 1 Log in to the SA Core Server where the Primary Data Access Engine is installed (part of the Infrastructure Component bundle).

- 2 Open the `/opt/opsware/twist/twist.sh` file and change this line:

```
https://$NASHOST/tcdocs/truecontrol-client.jar
```

to read (assuming that 443 was the port you noted in Phase 1, **step 4**):

```
https://${NASHOST}:443/tcdocs/truecontrol-client.jar
```

- 3 Restart the server hosting the Web Services Data Access Engine (part of the Component Slice bundle):

```
/etc/init.d/opsware-sas restart twist
```

(You will need to perform Phase 3 for each Web Services Data Access Engine server installation.)

Phase 4: Assign the SSH port:

- 1 Log in to NCM.
- 2 Select **Admin ► Administrative Settings ► Telnet/SSH** to display the Administrative Settings - Telnet/SSH page.
- 3 In the SSH Server section, locate the SSH Server Port.
- 4 If the port is 8022, then you are finished; otherwise, note the port being used and continue to Phase 4, **step 5**.
- 5 Log in to the SA Core Server where the Global File System (OGFS) is installed (part of the Slice Component bundle).
- 6 Open the `/etc/opt/opsware/hub/hub.conf` file and change the value for `nas.port` to the port you found in Phase 4, **step 4**. For example:

```
nas.port=9022
```

Gather Topology Data

After SA-NA Integration tasks are completed, you must run the NA Topology Data Gathering and NA Duplex Data Gathering diagnostics. For instructions about running these utilities, see the *NA User Guide*.

Troubleshooting Tips

To test whether SA is communicating with NA, check the following conditions:

- You can log in to NA with your SA credentials. This verifies that NA can communicate with SA.
- The SA credentials specified in the NA Administrative Settings under External Authentication Type are set to SA. This ensures that NA can look up server MAC addresses.
- The NA Topology Gathering Diagnostic has run successfully. To verify this condition, search for tasks and check their results. This ensures that NA has gathered MAC addresses and tried to look them up in SA.

Resetting the NA Host in the SA Client

Some SA-NA Integration features require that the SA Client (Java) opens the NA Web interface (directly from SA) so that you can access additional details about certain NA events. If your administrator has completed the setup tasks in the *SA Planning and Installation Guide*, but the SA Client is unable to communicate directly with the server running the NA host (server) Web interface, you might need to change the NA option in the SA Client. For example, if a firewall is preventing the SA Client from reaching the NA host, you need to specify the name of a server that is acting as a proxy for the NA host. This will override the default setting. This task must be performed on every desktop running a SA Client that cannot communicate with the NA host.

To reset the NA host in the SA Client, perform the following steps:

- 1 From the **Tools** menu in the SA Client window, select **Options**.
- 2 In the Views pane, select HP Network Automation.
- 3 In the Host field, enter the name of a server that is acting as a proxy for the NA host, such as m208, which is the proxy for the m208.example.com NA host.
- 4 (Optional) Click **Restore Default** to restore the previously saved NA host name.
- 5 (Optional) Click **Test** to open the NA login window.
- 6 Click **Save**.

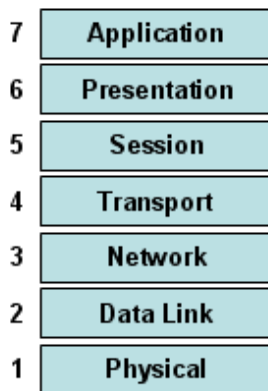
Using SA-NA Integration

After you have successfully configured SA-NA Integration, the following capabilities are available.

Connections Between Network Devices and Servers

The SA-NA Integration features are based on layer 2 connections and inferred layer 1 connections. See [Figure 11](#) for definitions of the OSI Model layers.

Figure 11 OSI Seven Layer Model



Data Link Connections

The SA-NA Integration feature includes functionality that detects data link (layer 2) connections and reports on physical (layer 1) and data link connections. These data link connections include switches that are directly connected to a managed server and switches that are indirectly connected through other switches. These connections are discovered by correlating the MAC addresses reported by the device with the known MAC addresses for servers and switches.

Physical Connections

The physical connections are inferred from the data link connections. See [Inferred Physical Connections](#) on page 35. Physical connections represent direct connections (cables) between server and switches.

In the SA Client, you can see physical connections in the Server Explorer, the Network Device Explorer and in detailed layout diagrams in Service Automation Visualizer (SAV). In the NA diagramming feature, you can see physical, data link or network (layer 3) connections.

Network Device Information in SA

In addition to basic hardware details about managed servers and network devices, the SA-NA Integration feature also reports the following information about network interfaces and network ports:

- On the server side, network interfaces have the following properties:
 - MAC address
 - subnet mask
 - interface type
 - IP address
 - DHCP setting
 - connected switch port
 - speed
 - duplex (excluding Windows).
- On the network device side, network ports have the following properties:
 - port name
 - speed
 - duplex settings
 - devices connected
 - interface type.



For most devices, auto-negotiation works best when both sides of the connection (server and network device) are set to auto-negotiate mode. For example, a duplex policy could specify that a port should be set to full, half, or auto, and not to full (auto). A full (auto) duplex setting indicates that the port was set to auto-negotiate and it negotiated to full duplex.

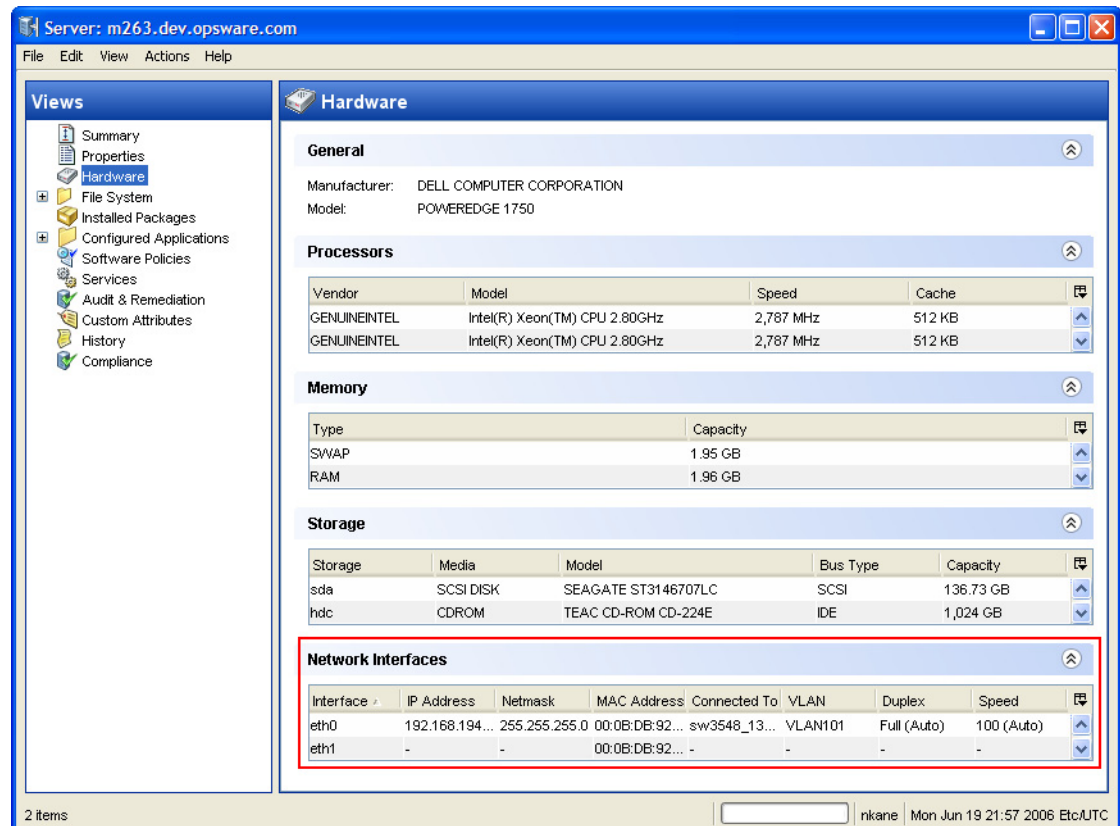
The following tasks describe how you can access detailed hardware information for servers and network devices directly in SA. See [Network Device Information in NA](#) on page 30 for instructions on how to access hardware information about network devices directly in NA.

Viewing Network Interfaces

To view hardware information about a server, including network interfaces, perform the following steps:

- 1 Log in to the SA Client.
- 2 From the Navigation pane, select **Devices** ► **All Managed Servers**.
- 3 From the View drop-down list, select Hardware.
- 4 Double-click on a server in the Content pane to display hardware details in the Server Explorer. See [Figure 12](#).

Figure 12 Hardware View in the Server Explorer

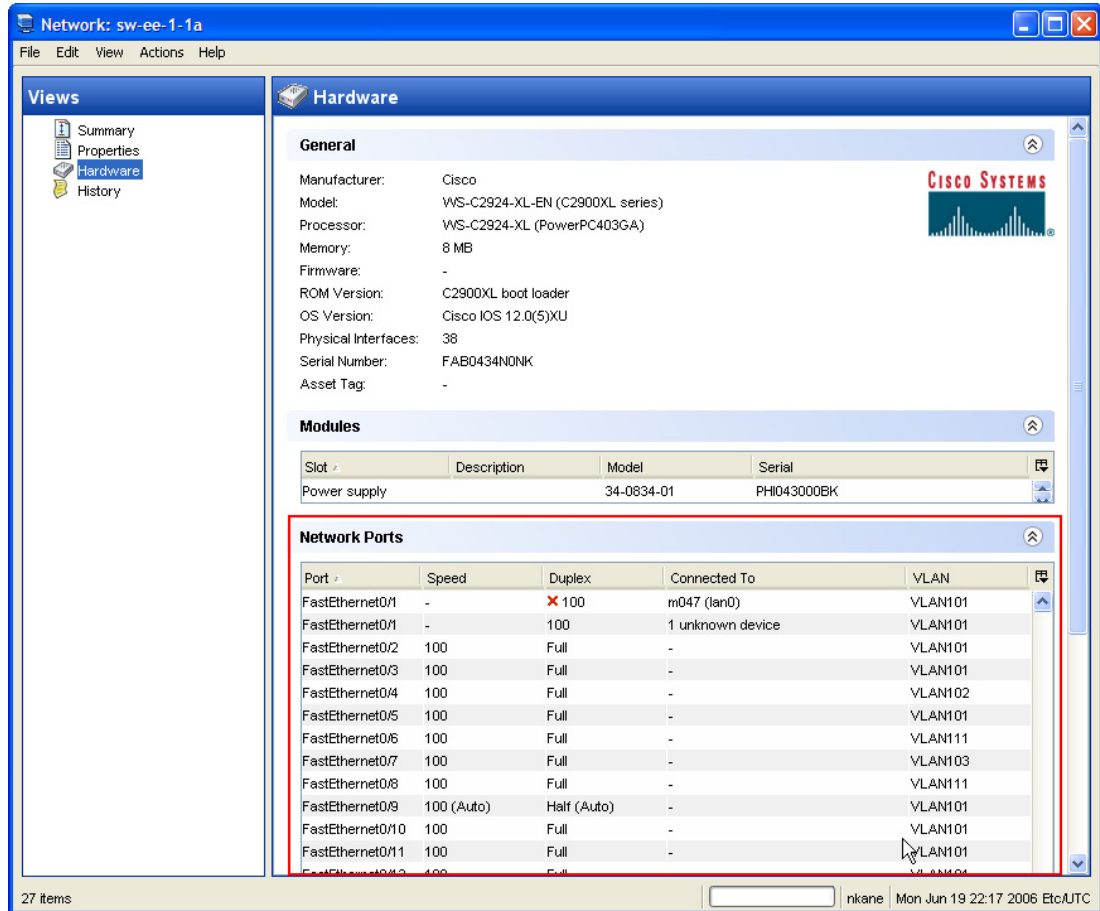


Viewing Network Ports

To view hardware information about a network device, including network ports, perform the following steps:

- 1 Log in to the SA Client.
- 2 From the Navigation pane, select **Devices** ► **Device Groups** ► **Public** and then select a device group.
- 3 Double-click on a network device in the Content pane to display the Network Device Explorer.
- 4 In the Views pane, select Hardware to display information about the selected network device. See [Figure 13](#).

Figure 13 Hardware View in the Network Device Explorer



Network Device Information in NA

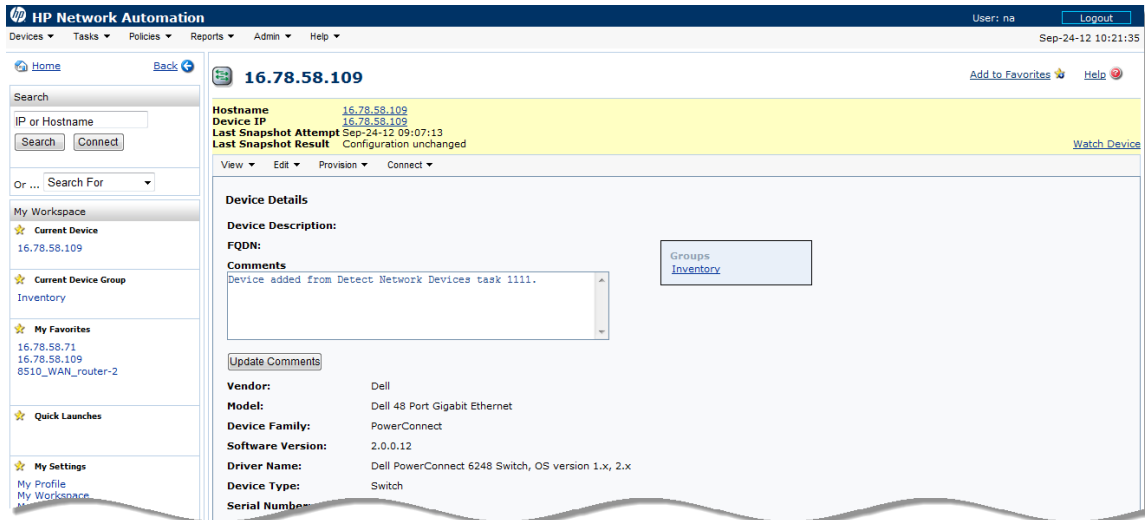
To help you with troubleshooting tasks that involve network devices in your environment, you can examine additional network device details and network device event history by logging directly in to NA. The SA-NA Integration feature provides a login option to access detailed information about network devices and their event history as recorded in NA.

Viewing a Network Device

To view detailed information about a network device:

- 1 From the Navigation pane, select **Devices** ► **Device Group** ► **Public**.
- 2 In the Content pane, select a network device.

Figure 14 Network Device Details in NA



Viewing Event History

In the Event Details window, click on the Device link to view additional information, such as timestamps for when the device was added, the last snapshot and the last configuration change.

Figure 15 Event Details for a Network Device in NA



Duplex Mismatch

The SA-NA Integration feature provides automatic detection of duplex mismatches. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.

For servers' network interfaces, speed and duplex information is gathered during every hardware registration, which occurs every 24 hours.

Due to the lack of a device independent method of determining duplex for servers running a Windows operating system, the Server Agent for Windows does not report duplex settings out-of-the-box. A custom script can be added to the Server Agent to collect and report the speed and duplex setting for a certain network interface. For instructions on how to create and integrate the script with the Agent, contact your support representative.

Speed and duplex information for servers is *not* updated when you select **View ► Refresh** or press F5 in the SA Client. This data gets updated when the NA Duplex Data Gathering diagnostic runs. See [NA Duplex Data Gathering Diagnostic](#) on page 19.

For network devices, speed and duplex is gathered by the NA Duplex Data Gathering diagnostic, which runs according to a schedule that you define. To ensure that you have the latest speed and duplex information about network devices, it is recommended that you set up a recurring schedule that runs the diagnostic. See the *NA User Guide*.

If the network interface information (speed and duplex) for a server does not match the network port information (speed and duplex) for a connected network device, the device is considered to be non-compliant.

In the SA-NA Integration feature, you can see duplex mismatches identified at a top level by using the Dashboard. You can also see duplex mismatches identified by server and network device by using the Server Explorer and Network Device Explorer, respectively.


Viewing Duplex Mismatches in the Dashboard

See the *SA User Guide: Audit and Compliance* for information about duplex compliance levels and how they are displayed in the Dashboard.

Viewing Duplex Mismatches by Server

To view duplex mismatches using the Server Explorer, perform the following steps:


- 1 From the Navigation pane, select **Devices ► All Managed Servers**.
- 2 In the Content pane, select a server.
- 3 Double-click on the server to display the Server Explorer.
- 4 In the Views pane, select Hardware.
- 5 In the Network Interfaces section, review the Duplex column for detected mismatches.

Mismatches are identified by an  icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column.

Viewing Duplex Mismatches by Network Device

To view duplex mismatches using the Network Device Explorer, perform the following steps:

- 1 From the Navigation pane, select **Devices ► Device Groups ► Public**.
- 2 In the Content pane, select a network device.
- 3 Double-click on the network device to display the Network Device Explorer.
- 4 In the Views pane, select Hardware.
- 5 In the Network Ports section, review the Duplex column for detected mismatches.

Mismatches are identified by an  icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column. See [Figure 12](#).

Network Reports

To help troubleshoot problems that involve physical connections and duplex compliance, you can run and examine network reports. By using the Reports feature in the SA Client, you can produce the following network reports that identify layer 1 connections between managed servers and network devices in your environment:

Connections by Network Device

This report lists all physical connections to a selected network device.

Connections by Server

This report lists all physical connections to a selected managed server.



See the *SA Reports Guide* for information about how to run, export, and print these reports.

Network Diagrams

You can use Service Automation Visualizer (SAV) functions in SA and the Diagramming feature in NA to create detailed diagrams that illustrate managed servers, network devices, and layer 2 and layer 1 connections in your environment. You can also export these network diagrams to .gif, .jpg, and .svg files, annotate, and use them in other applications.

See the *SA User Guide: Service Automation Visualizer (SAV)* and the *NA User Guide* for more information about SAV and the Diagramming tool.

Launching Service Automation Visualizer (SAV)

To access SAV, perform the following steps:

- 1 From the Navigation pane, select **Devices ► All Managed Servers**.
- 2 In the Content pane, select one or more servers.
- 3 From the **Tools** menu, select **Service Automation Visualizer (SAV)** and then select one of the following options:
 - Select **New** to open the SAV window.
 - Select **Open** to open a previously saved topology.
- 4 To create and export topology diagrams, see the procedures for using Service Automation Visualizer (SAV) in the *SA User Guide: Service Automation Visualizer (SAV)*.

Launching NA Diagramming

See the *NA User Guide* for instructions on launching and using the NA Diagramming feature.

NA and the SA Global Shell

You can use the SA Global File System (OGFS) to navigate between servers and connected network devices by tracing their physical connections in the `/opsw/Servers/@` and `/opsw/Network/@` directories in the OGFS.

You can also run three types of NA scripts in the OGFS:

- Command
- Advanced
- Diagnostic

These scripts correspond to the three directories in the OGFS under `/opsw/Scripts/Network`. See “Network Directories” in the *SA User Guide: Server Automation*.

You can also write Bourne shell and Python scripts that can perform the following tasks when run in the OGFS:

- Find servers and network devices.
- Find all servers that are connected to a specified switch.
- Find servers with a duplex mismatch.
- Display the network interfaces of a specified server.
- Get the IP addresses of all devices.
- Compare two files to identify changes in a network device's configuration.
- Change device details, such as the `snmp-location`.

Launching OGFS

To access the OGFS in the Global Shell feature, perform the following steps:

- 1 From the **Tools** menu, select **Global Shell** to launch a terminal window. See “Opening a Global Shell Session” in the *SA User Guide: Server Automation* for more details about using OGFS.
- 2 To navigate between servers and connected network devices, use the guidelines described in “SA Global Shell” and “OGFS Directories” in the *SA User Guide: Server Automation*.

Remote Terminal (rosh)

The `rosh` utility enables you to log in to devices (servers and network devices) and run native commands. You invoke `rosh` from within a Global Shell session. You can run `rosh` and enter native commands interactively, or you can specify the native commands as an option of `rosh`. For example, you can log in to a switch with `rosh` and run the `show vlan` command to view all VLAN details.

See “Remote Terminal” and “Logging on to a Managed Server With `rosh`” in the *SA User Guide: Server Automation* for more information about using the `rosh` utility.

Inferred Physical Connections

The SA-NA Integration feature also includes functionality that detects and reports on inferred physical (layer 1) connections. These connections are inferred from data (such as MAC addresses that are seen by switches), captured, and then added to the SA data model.

These physical connections (inferred layer 1 data) are based on heuristics. In the OSI model, each layer is an abstraction designed to hide the layer below. Therefore, the layer 2 data gathered from devices cannot generate 100% accurate layer 1 data. In particular, layer 1 data may be incorrect if any of the following conditions exist:

- The device does not return the port number where MAC addresses are seen.
- There was no traffic between the devices within a few minutes of when NA gathered the topology data (where MAC addresses are seen).
- There is an unmanaged device between two managed devices.
- There is a hub between two managed devices.

In the SA Client, you can see inferred layer 1 connections by navigating network device directories in Global Shell .

Device Groups and NA

A device group helps you categorize your devices (servers and network devices) in ways that make sense for your organization. For example, you can group devices by customer, facility, usage, application, and so on, and then perform actions on all of the devices in the group.

In SA, a device group can contain managed servers *and* network devices, or *only* managed servers. In NA, a device group contains only network devices. You create and edit network device groups only in NA. See the *NA User Guide* for more information about using the `rosh` utility.

To monitor an application that is running on multiple servers and relies on multiple network devices in your environment, HP recommends that you model it as a device group that contains all servers and network devices the application runs on. This enables you to troubleshoot the application by using SA.

Associating a NA Device Group

When you associate a public device group in SA with a device group in NA, you will be able to monitor information about all servers and network devices that you are interested in. You associate device groups by using identical group names.

Associated device groups have the following requirements:

- The SA device group is public.
- The SA device group is static.
- The names of the associated NA and SA device groups are identical.

To associate device groups in SA and NA, perform the following steps:

- 1 From the Navigation pane, select **Devices ► Device Groups ► Public**.
- 2 In the Content pane, select a device group.

- 3 Right-click on the device group and then select Open to display the Device Group Explorer.
- 4 From the View drop-down list, select Properties.
- 5 Check the “Associate with a NA device group of the same name” check box to enable this functionality.
- 6 From the **File** menu, select **Save**.

3 SA-OO Integration – Running Flows

This chapter describes how system integrators and flow managers can use Server Automation (SA) to set up and run flows using SA. It also describes how users can run flows. Flows are operations that perform some of the most common automated tasks.

SA-Operations Orchestration (OO) integration allows flow authors to build OO flows that are integrated with SA and users to run flows from SA. See OO documentation for more information about flows.

You must be familiar with SA, OO, and OO flows to implement the procedures described in this chapter.

The chapter includes the following topics:

- [What's New for SA-OO Integration](#) on page 37
- [Administrators: Setting Up Flows](#) on page 38
- [Users: Running Flows](#) on page 45

To check for recent updates, to verify that you are using the most recent edition of a document, or to check the release notes for the most up-to-date information, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

What's New for SA-OO Integration

This section describes what is new in SA-OO integration for this version.

Support for OO 10.0

For the SA-OO Integration, SA 10.0 or later supports HP Operation Orchestration 10.0 and 9.0.

- OO 9.0 support is enabled by OO-SA 9.00.08 content
- OO 10.0 support enabled by OO-SA 10.00.01 content

NOTE: Version support and compatibility information is subject to change. For complete and up-to-date support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online web site:

http://support.openview.hp.com/sc/support_matrices.jsp

You can also download the HP Server Automation Support and Compatibility Matrix for this release from the HP Software Support Online Product Manuals web site:

<http://support.openview.hp.com/selfsolve/manuals>

Edit Flow Integration Settings Window

This window, its sub-window, and its panels have two new functions: displaying real-time flow information and replacing the OO Connector Configuration file functionality.

Displaying Real-Time Information

The Flow Integrations panel displays real-time information for an OO user whose credentials are used to run flows from SA, to verify that SA and OO can communicate with one another, and to verify that a user is a valid OO user. Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

For more information on this panel, see [Editing the Flow Integration Settings](#) on page 40.

Administrators: Setting Up Flows

This section describes how system and flow administrators can set up OO flows in SA.

Prerequisites

This section describes the prerequisites that must be fulfilled to set up and run flows in the SA Client.

Prerequisites for Using OO

This section describes the environment and the permissions required for using OO.



NOTE: SA Integration can only be performed with one version of OO.

Environment

To use OO with SA to set up and run flows, your environment must meet the following requirements:

- SA version 10.0
- HP Operations Orchestration (OO) version 7.5X, 7.6X, 9.X and 10.0
- OO installation server networked to SA core server
- Valid OO SDK Client Certificate to communicate with OO



NOTE: SA version 10.0 ships with OO SDK Client Certificate for OO 7.51.

Importing the OO SDK Client Certificate

This section describes how to import the required OO SDK Client Certificate. You must import the certificate before you can run OO flows from SA.



NOTE: If your architecture includes a master core and one or more secondary cores, follow the steps in this section for the master core and for each of the secondary cores. Similarly, if your SA computer has a sliced-core installation with one or more slices, repeat the steps for each slice.

To import the SDK:

- 1 Stop the Web Services Data Access Engine (Twist):

```
/etc/init.d/opsware-sas stop twist
```

- 2 Transfer the OO Central Certificate to SA:

(When you are prompted for a password for the next steps, use: `changeit`)

- a Export the OO Central Certificate:

The procedure of exporting the OO client certificate depends on the OO version to which you are connected:

OO Version	Instructions
OO 7.5x, 7.6x, 9.0	Open a terminal on the SA core, and execute: <pre>/opt/opsware/jdk1.6/jre/bin/keytool -exportcert -alias oocert2007 -file /tmp/oocentral.crt -keystore /var/opt/opsware/twist/oocert</pre>
OO 9.0X (OO 9.02.0002 or later)	Open a terminal on the SA core, and execute: <pre>/opt/opsware/jdk1.6/jre/bin/keytool -exportcert -alias oocert2011 -file /tmp/oocentral.crt -keystore /var/opt/opsware/twist/oocert</pre>
OO 10.0	For this version of OO the procedure to export the certificate may differ, depending on the OS version you have on your OO server. For more details please consult the OO documentation. NOTE: The certificate export command must be run on the OO server. As of SA 10.0, the client certificate is not bundled with SA.

Example command for exporting the certificate from an OO 10.0 instance installed on a Windows server:

```
<OO_INSTALL_DIR>\java\win64\bin\keytool.exe -exportcert -alias tomcat  
-file C:\oocentral.crt -keystore  
<OO_INSTALL_DIR>\central\var\security\key.store
```

Next, make sure you copy the `C:\oocentral.crt` file to the SA core, under `/tmp/oocentral.crt`.

- b Import the OO Central Certificate to the SA Java Runtime Environment (JRE) Keystore:

```
/opt/opsware/jdk1.6/jre/bin/keytool -importcert -alias oocert -file /
tmp/oocentral.crt -keystore /opt/opsware/jdk1.6/jre/lib/security/
cacerts
```



The example above uses the alias: oocert. However, any alias can be used when importing the certificate, as long as it is not already used in that keystore.

c Make sure that no errors occurred when the commands were executed.

3 Check that the OO Central Certificate was imported successfully:

```
/opt/opsware/jdk1.6/jre/bin/keytool -list -alias pas -keystore /opt/
opsware/jdk1.6/jre/lib/security/cacerts
```

Example output:

```
pas, Feb 3, 2010, trustedCertEntry,
Certificate fingerprint (MD5):
DF:DD:22:1B:A2:1E:A9:9C:1C:AF:8F:E0:14:1F:B5:E0
```

4 Start the Web Services Data Access Engine (Twist):

```
/etc/init.d/opsware-sas start twist
```

Permissions

In order to be able to use the SA-OO integration the users must be granted the following permissions:

Table 2 Checking User Permissions

Permission	Description	Check in the SA Client
AdministerFlowIntegrations	Configure the OO integration settings	Select Administration in the navigation panel. If the Flow Integrations option appears in the list of choices in the navigation tree, the permission has been granted.
RunFlowOption (for users who want to run flows)	Run OO flows	Select Devices in the navigation panel. Select Servers ► All Managed Servers . Right-click a server name and choose Run. If the Flow... option is visible, the permission has been granted.

Editing the Flow Integration Settings

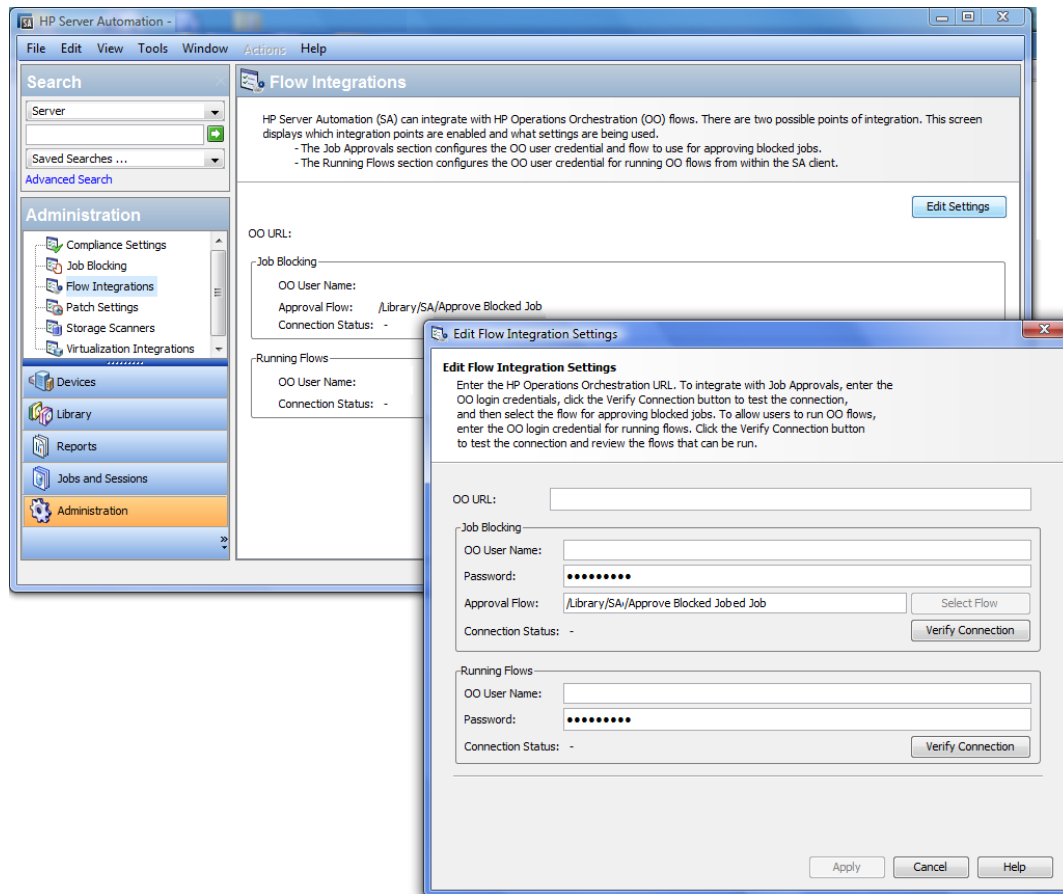
The Flow Integrations Settings in SA enable you to configure the integration between HP Server Automation and HP Operations Orchestration.

To configure or edit the Flow Integration Settings:

1 In the SA Client navigation panel, select **Administration ► Flow Integrations**.

- 2 In the Flow Integrations panel, click **Edit Settings** to display the Edit Flow Integration Settings window.

Figure 16 Edit Flow Integration Settings Window



The Flow Integrations panel displays real-time information for the following users:

- a For Job Blocking: OO user who has permission to run the Approval Flow.
- b For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

- 3 For running a flow, enter or change the following information:

- OO URL - the location of the OO server in the following format:

`<protocol>://<hostname or host IP address>:<port number>/`

Examples:

`https://10.255.166.110:8443/`
`https://10.255.166.110:8443/PAS/`

- OO user name and password ()

See [Table 3](#) for more information.

For information about blocking jobs and the blocking job section of this window, see the SA-OO - Blocking Jobs chapter.



A hyphen designates an unconfigured status, a red check mark designates an invalid status, and a green check mark designates a valid status. Both valid and invalid statuses are displayed with their latest verification timestamp.

4 Click Verify Connection to check the validity of the credentials you entered.

If the connection status is valid, a check mark appears.

5 Click Apply to save the flow-integration settings changes.



The Apply button is disabled if no data exists in the Edit Flow Integration Settings panel, if the data in the fields is incorrect, or if a check mark does not appear next to the connection status.

Replacing OO Connector File Functionality

If you are upgrading from SA versions prior to SA 9.0 and you want to use flow inputs, you must replace the inputs from the former OO Connector Configuration file into the corresponding Edit Flow Integration Settings window fields. See [Table 3](#) for mapping information for the connection settings. See [Editing the Flow Integration Settings](#) on page 40 for more information on the interface.

Table 3 Mapping Configuration File Inputs to Integration Window Fields

OO Connector Configuration Inputs	Description	Edit Flow Integration Settings Field
iconclude.enabled	An integer, either: 1 - enable the connector 0 - disable the connector Default: 0	Connector Status from Job Blocking (in the Running Flows field)
iconclude.host	OO server host name or IP address Default: None (required)	OO URL Use the following syntax: <protocol>://<hostname or host IP address>:<port number>/
iconclude.port	Port of the OO listener Default: 8443	OO URL Use the following syntax: <protocol>://<hostname or host IP address>:<port number>/
iconclude.protocol	Protocol (http or https) for connecting to the OO server Default: https	OO URL Use the following syntax: <protocol>://<hostname or host IP address>:<port number>/

Table 3 Mapping Configuration File Inputs to Integration Window Fields

OO Connector Configuration Inputs	Description	Edit Flow Integration Settings Field
<code>iconclude.flow.approve</code>	Path to the flow that will be run (the flow is located in the OO library) Default: None (required)	Approval Flow
<code>iconclude.user</code>	OO user name Default: None (required)	OO User Name
<code>inconclude.password</code>	OO user's clear text password Do not include this property in a production environment Default: None (required)	Password

SA-OO Integration Flows

This section lists flow inputs. Flow authors can define the input name, input type, and template in OO. After these inputs are defined and flows are run, SA automatically populates their values into the OO-SA Library `SACoreInputs` table - you do not have to input these values manually.

For these inputs:

- If the input has a text, encrypted field, or free form list field, and OO provides a default value, the field will be filled with the default value. If there is no default value, then, if you followed the guidelines in [Table 4](#), SA will fill the text field with one of the known inputs, which you can modify.
- If the input has a single-select list field or multi-select list field, OO provides the values - you cannot modify these values.

For more information on defining flow inputs, see the OO documentation.

Table 4 Flow Inputs

Flow Inputs	Related to	Automatically Assigned Values (by SA)
<code>coreHost</code> and <code>coreIPAddress</code>	SA Core	Host and IP address of the SA core associated with the SA user who is logged in to the SA Client
<code>coreUsername</code> or <code>coreUser</code>	SA Core	User name associated with the SA user who is logged in to the SA Client
<code>corePassword</code>	SA Core	Password associated with the SA user who is logged in to the SA Client The contents of the field are encrypted.
<code>coreVersion</code>	SA Core	Current SA core version SA provides these values

Table 4 Flow Inputs (cont'd)

Flow Inputs	Related to	Automatically Assigned Values (by SA)
saServerIdentifier	SA Managed Server	<p>Selected server identifiers:</p> <p>You can set two possible values (in OO):</p> <ul style="list-style-type: none"> • Not Assigned (for one value) • List of Values (for multiple values) - Define the input as a <code>freeFormList</code> type in OO.
saServerScriptName	SA Managed Server	<p>Name of the server script that is available in the SA core for that particular server's operating system</p> <p>Automatically assigned values: None</p> <p>Instead, the SA Client provides a widget that enables users to select a server script (excluding the OGFS script).</p>
saServerName/ hostName	SA Managed Server	<p>DNS name of the selected server</p> <p>This value is filled in only if one server is selected.</p> <p>You can set two possible values (in OO):</p> <ul style="list-style-type: none"> • Not Assigned (for one value) • List of Values (for multiple values) <p>Define the input as a <code>freeFormList</code> type in OO.</p>
platformName	SA Managed Server	<p>Operating system name of the selected server</p> <p>This value is filled in only if one server is selected.</p>
customerName	SA Managed Server	<p>Customer name of the selected server selected</p> <p>This value is filled in only if one server is selected.</p>
facilityName	SA Managed Server	<p>Name of the facility where the selected server is located</p> <p>This value is filled in only if one server is selected.</p>
saJobId	OO	<p>Job ID of the SA job that was used to run the OO flow (tracked in OO using the reports feature)</p> <p>This input is not displayed.</p>

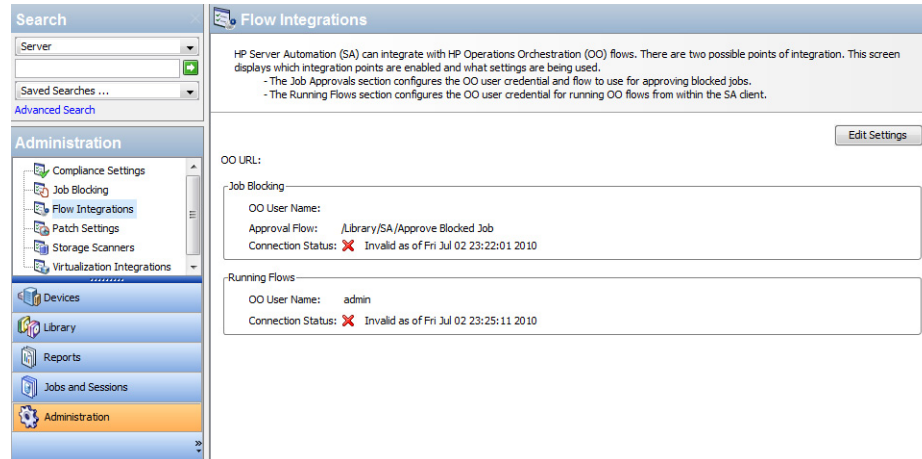
Verifying Your Changes and Settings

This section describes how to verify that your changes or settings have been applied.

Flow Edits and Flow Status

- 1 Log on to the SA Client.
- 2 In the navigation panel, select Administration.
- 3 In the navigation tree, select Flow Integrations.

Figure 17 Flow Integrations Panel



The Flow Integrations panel displays real-time information for the following users:

- a For Job Blocking: OO user who has permission to run the Approval Flow.
- b For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

When the flow or job-blocking action is complete, a check mark appears next to the status.

Users: Running Flows

This section describes how users can run flows, choose servers, and choose flow inputs.

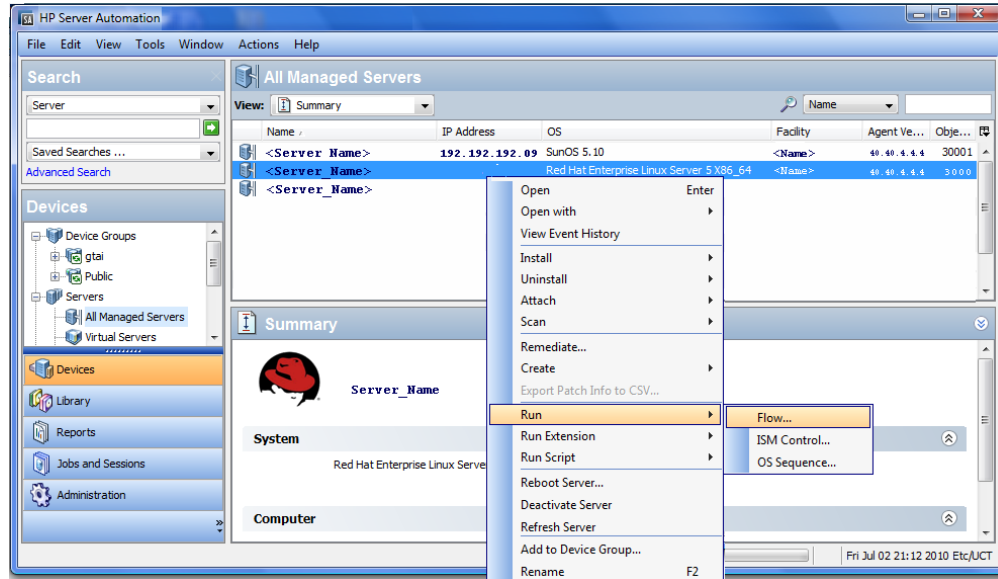
Users must have the Run Flow permission to run flows in SA.

Choosing a Flow to Run

To choose a flow to run:

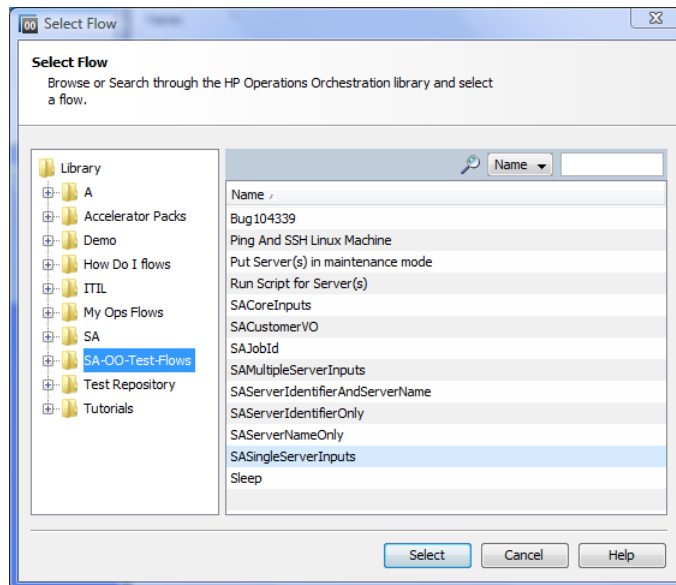
- 1 In the SA Client navigation panel, select Devices.
- 2 In the top panel, select **Servers ► All Managed Servers**.
You must select a server before you can select a flow.
- 3 Right-click a server name.

Figure 18 Run Flow Option



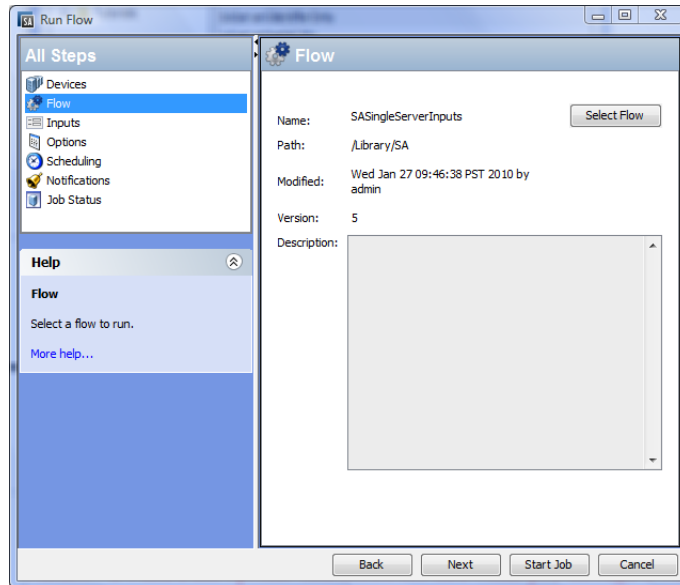
- 4 Select **Run** ► **Flow...** to display the Select Flow OO window.

Figure 19 Select Flow Window



- 5 In the Select Flow window, select a flow category from the library tree to display its component flows.
- 6 In the name list, select a flow and click Select to display flow details in the Run Flow window.

Figure 20 Run Flow Window



You can choose flow input, runtime option, scheduling option, and notification parameters. See [Choosing Flow Input, Runtime Option, Scheduling Option, and Notification Parameters](#) on page 47.

Adding or Deleting Servers

To add or delete servers:

- 1 First, follow the steps in [Choosing a Flow to Run](#) on page 45.
- 2 In the All Steps navigation panel of the Run Flow Window, select Devices.
- 3 Right-click a server icon and choose Add or Delete, or click the plus or minus sign.

The Select Servers and Device Groups window is displayed.

- 4 Click Select to add a server to the list of servers.

The Run Flow window displays the new server in the Devices panel, or shows that the removed server is absent.

Choosing Flow Input, Runtime Option, Scheduling Option, and Notification Parameters

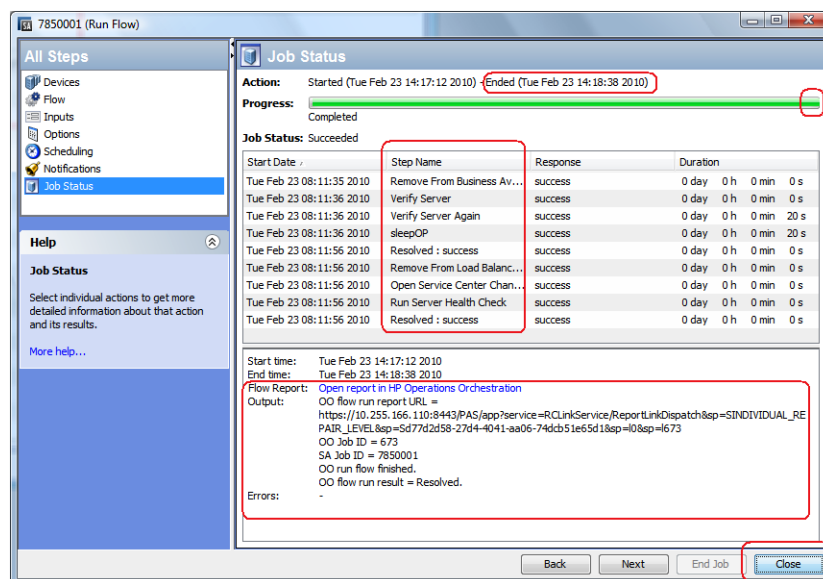
You can enter values for flow inputs, runtime options, scheduling, and notifications. Some parameters will be automatically filled in already.

- 1 Follow the steps in [Choosing a Flow to Run](#) on page 45, then:
- 2 In the All Steps panel of the Run Flow Window, select each of the categories in turn (Inputs, Options, Scheduling, and Notification) to enter values for their parameters, as the rest of this procedure explains. Alternatively, you can choose Next from each panel to view the categories.
- 3 To enter values for flow inputs, select Inputs in the All Steps panel and enter values for the inputs that the panel displays. For example:
 - a saServerScriptName or click Select Script to display a list of scripts.
 - b saServerName
 - c saServerIdentifier

See Table 4 for more information on inputs.

- 4 To enter values for runtime options, select Options from the All Steps panel, and enter a value for the job timeout. This is the number of minutes that the server will run a job before it times out. The default value is: 180 minutes and the timeout value is between 1 and 1440 minutes.
- 5 To select scheduling options, select Scheduling in the All Steps panel and enter values for:
 - a Schedule frequency
 - b Time and Duration
- 6 To enter notification information, click Notifications in the All Steps panel and add values for:
 - a Recipient email address
 - b Notifier (click Add Notifier)
 - c Ticket identification number (there are no conventions for the identification number - you can choose any number)
- 7 Click Start Job to start the job, or click Cancel to erase the choices you made in this session.
- 8 Click Job Status to view the status of the SA job. (optional)

Figure 21 SA Job Status



The Job Status window does *not* display the flow run status, but rather the status of the SA job that starts and monitors the flow in OO.

When the SA job is complete, this window displays the status of each step in the flow (in the Response field) and a URL that points to more detailed flow-related information on OO.

It is possible that SA job monitoring succeeded even if at least one step failed. The OO API does not provide a call that precisely determines success or failure of the entire OO flow. Therefore, you cannot determine the success or failure of your OO flow from the SA Job Status screen or from the information provided at the URL.

Troubleshooting

SA-OO Connection Error

If SA cannot connect to OO, administrators can:

- Check that the settings in the Edit Flow Integration Settings window fields are correct. (See [Editing the Flow Integration Settings](#) on page 40.)
- Examine the following log file for error messages on the Command Engine server:

```
/var/log/opsware/waybot/waybot.err
```

The error messages do not appear in the SA Client.

- Check that the OO URL, user name, and password are correct.
- Make sure the specified OO user has correct permissions to run the flow.

To check a flow status, see the Flow Integration Panel. For more information on this panel, see [Editing the Flow Integration Settings](#) on page 40.

If you are a user and you see this error, check with your administrator.

Flow Run Error

This section describes errors you might encounter when you run a flow as a user.

Incorrect Inputs

When you try to run a flow, you might receive one of the following error:

- SA will not pass the selected Device(s) to this flow.
- SA-OO Integration Configuration Error: Flow Integration Settings are incorrect. Please verify that the flow Integration URL, username, and password are correct.

Typically, these errors are displayed when one or more of the following occurred:

- You (as a user) selected the wrong flow to run.
- The OO server is not responding. Ask your administrator for help.
- The inputs an administrator entered in the Edit Flow Integration Settings window are incorrect. Ask your administrator to check the information in the Edit Flow Integrations Settings window. See [Editing the Flow Integration Settings](#) on page 40 for more information.
- The flow author must modify the flow definition to use the naming conventions.

Inputs Not Defined or Server Only Accepts One Device

When you try to run a flow, you might receive the following error:

SA will not pass the selected Device(s) to this flow. Either the flow does not have the required ServerIdentifier input defined or the input only accepts a single device.

If you receive this error, ask your administrator to check the ServerIdentifier input.

4 SA-OO Integration – Job Blocking and Approving

Software Automation (SA) jobs are major processes, such as installing patches or checking compliance, that you run in the SA Client.

This chapter describes how system integrators and software developers can block SA jobs in SA, and approve or cancel jobs in SA using flows that call the SA API.

For more information on SA jobs, see the *SA Application Deployment User Guide*.

You must be familiar with SA, Operations Orchestration (OO), SA jobs, and OO flows to block and unblock jobs.

The chapter includes the following topics:

- [Blocking Jobs](#) on page 51
- [Approving and Deleting Blocked Jobs](#) on page 57

For more information about jobs, see the *SA Application Deployment User Guide*. For more information on working with OO, see the OO documentation.

To check for recent updates, to verify that you are using the most recent edition of a document, or to check the release notes for the most up-to-date information, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

Blocking Jobs

This section describes several scenarios for blocking jobs, the types of jobs that can be blocked, the permissions needed to block jobs, how to block a job, how to disable job blocking, and how to view information related to a blocked job.

What are Blocked Jobs?

Some SA jobs might need to be reviewed and approved before they are executed. This section contains three sample scenarios of jobs that are candidates for job blocking.

Scenario 1

A job's approval should be postponed until the job can be run in the early morning hours if running it requires a system reboot. If the job were to run during regular business hours, it would disrupt normal work processes.

Scenario 2

Some jobs require further review before they can be run. For example, if a job updates a particular software application on a server, a Change Advisory Board (CAB) might need to review the proposed upgrade to make sure it does not conflict with other applications running in the environment. The board would determine if the job should run and when.

Scenario 3

In many IT environments, certain operations must be assigned tickets, assessed, and approved before they can be executed or cancelled. These jobs need to be blocked so the ticket can be created in the ticketing system, evaluated, and resolved.

What SA Job Types Can be Blocked?

The following table describes the SA job types.

Table 5 Blockable SA Job Types

Job Type	Function
Clone Virtual Machine	Clones a virtual machine on a VMware server
Create Snapshot	Creates a snapshot that captures the configuration of a managed server at a particular point in time
Create Virtual Machine (Hyper-V)	Provisions a virtual machine and installs an operating system on a Hyper-V virtual machine
Create Virtual Machine (VMWare)	Provisions a virtual machine and installs an operating system on a VMware ESX server
Create Virtual Zone	Provisions a Solaris virtual machine (non-global zone) on a global zone (Hypervisor)
Delete Virtual Machine	Deletes a virtual machine
Install Patch	Installs any patch on a managed server
Install Software	Installs any software on a managed server
Modify Virtual Machine	Modifies the properties of a VMware virtual machine
Modify Virtual Machine (Hyper-V)	Modifies the properties of a Hyper-V virtual machine
Modify Virtual Zone	Modifies the properties of a Solaris virtual machine
Push Configurations	Modifies configuration files on a managed server
Reboot Servers	Reboots servers
Remediate Audit Results	Remediates servers based on the findings of an audit operation
Remediate Policies	Remediates servers based on a software policy or a patch policy
Remediate Snapshot Results	Remediates servers based on a snapshot. A snapshot captures the configuration of a managed server at a particular point in time
Remove Virtual Machine	Removes a virtual machine from a VMware ESX server (Hypervisor)
Remove Virtual Zone	Removes a Solaris virtual machine (non-global zone) from a global zone (Hypervisor)

Table 5 Blockable SA Job Types (cont'd)

Job Type	Function
Restore Configurations	Restores a previous version of configuration files on a server Every time you push configurations to a server, the previous configuration are saved and can be restored.
Run Audit	Runs audits
Run Custom Extension	Runs custom extensions
Run ISM Control	Runs an ISM (Intelligent Software Module) control An ISM is an installable software package created with the ISM Development Kit (IDK). An ISM can contain control scripts that perform day-to-day, application-specific tasks, such as starting software servers.
Run OGFS Script	Runs an OGFS (Global File System) script on a server The OGFS scripts allows you to execute scripts in the Global Shell from the SA Client.
Run OS Build Plan	Runs OS builds plans
Run OS Sequence	Provisions a server and installs an operating system using an OS sequence An OS sequence defines what to install on an unprovisioned server, including OS build information from the OS installation profile, software and patch policies, and remediation settings.
Run Program Extension	Runs a custom feature added to SA HP can extend the functionality of SA by creating custom extensions to provide for specific customer needs.
Run Server Script	Runs a script on a server
Uninstall Patch	Uninstalls a patch on a server
Uninstall Software	Uninstalls software on a server

Required Permissions

The following permissions are required:

- *Edit or Cancel Any Job* (allows you to edit or cancel jobs if you launch a flow)
- *View All Jobs* (allows you to view jobs if you launch a flow)
- *Manage Job Blocking* (allows you to block and unblock jobs)
- *Administer Flow Integration* (allows you to configure the SA-OO integration connection settings to OO and specify the Approval Flow)

How Do I Block and Unblock Jobs?

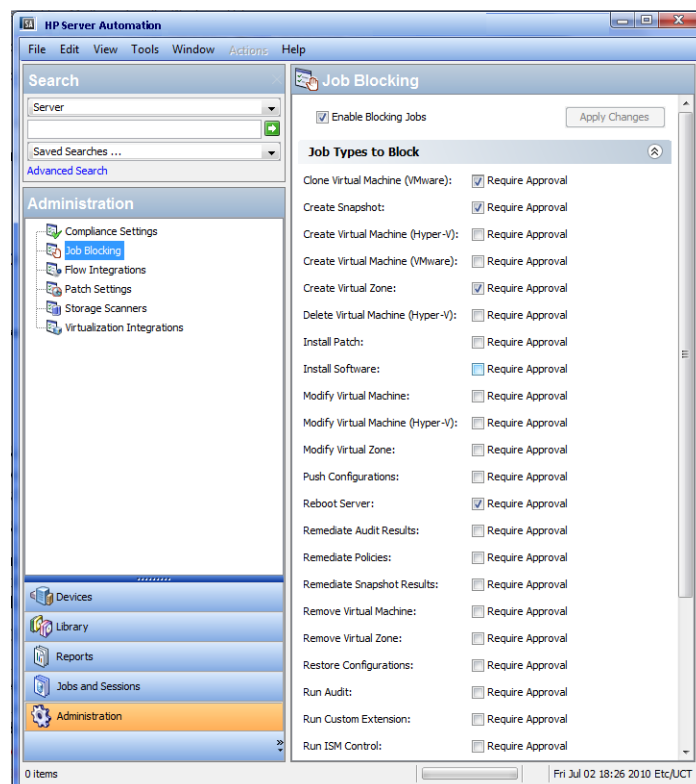
This section describes how to designate job types to block and how to disable job blocking.

How Do I Designate Job Types to Block?

To designate the type of jobs to block:

- 1 In the SA Client, select Administration in the navigation pane.
- 2 Select Job Blocking in the navigation tree. The list of job types is displayed in the right pane with a check box next to each type.

Figure 22 Blocking SA Job Types



See [Table 5](#) to see which types of jobs are available.

- 3 Select the check box: Enable Blocking Jobs.

This action sets up the potential to block all job types listed in the panel.

- 4 In the panel below the Enable Blocking Jobs check box, select the check box next to each job type you want to block. Jobs that correspond to the blocked job type will be unable to run until they receive the appropriate approval.

This action designates individual job types to block.

- 5 Click Apply Changes to block jobs belonging to the job types you selected.

Note: When you block jobs of a particular type, you block all future jobs that belong to that type until you deselect the Required Approval box for that job.

How Do I Disable Job Blocking?

To disable job blocking:

- 1 In the SA Client, select Administration in the navigation pane.
- 2 Select Job Blocking in the navigation pane.
- 3 Deselect the check box corresponding to the job that you no longer want to block.
This action disables job blocking for individual job types.
- 4 Above the list of job types, deselect the Enable Blocking Jobs check box. (See [Figure 22.](#))
This action disables job blocking for all job types.
- 5 Click Apply Changes.



When you deselect the Enable Blocking Jobs check box, the checks next to the job types designated for blocking remain checked for your convenience.

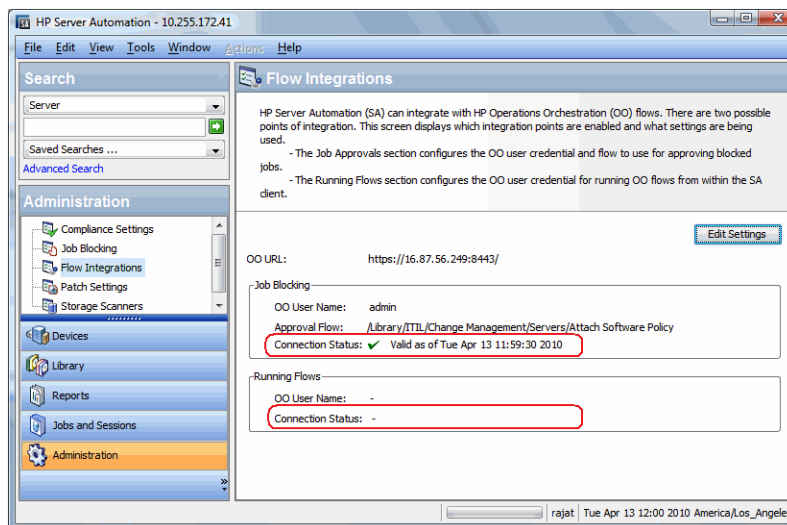
How Do I View Blocked-Job Information?

You can view OO connection information in the Flow Integrations panel and check job-status information in the job log.

Checking OO Connection Information in the SA Flow Integrations Panel

Choose **Administration** ► **Flow Integrations** to access the Flow Integrations Panel.

Figure 23 Flow Integrations Panel



The Flow Integrations panel displays real-time information for the following users:

- a For Job Blocking: OO user who has permission to run the Approval Flow
- b For Running Flows: OO user whose credentials are used to run flows from SA

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

A check mark appears next to the status if the connection to OO is active.

Checking Blocked-Job Status in the Job Log

If you know a job has been blocked and you want to see whether the job block has been lifted, check the job log (choose **Jobs and Sessions ► Job Logs ► Any Status**).

For a list of possible job status values and what they mean, see [Table 7](#).

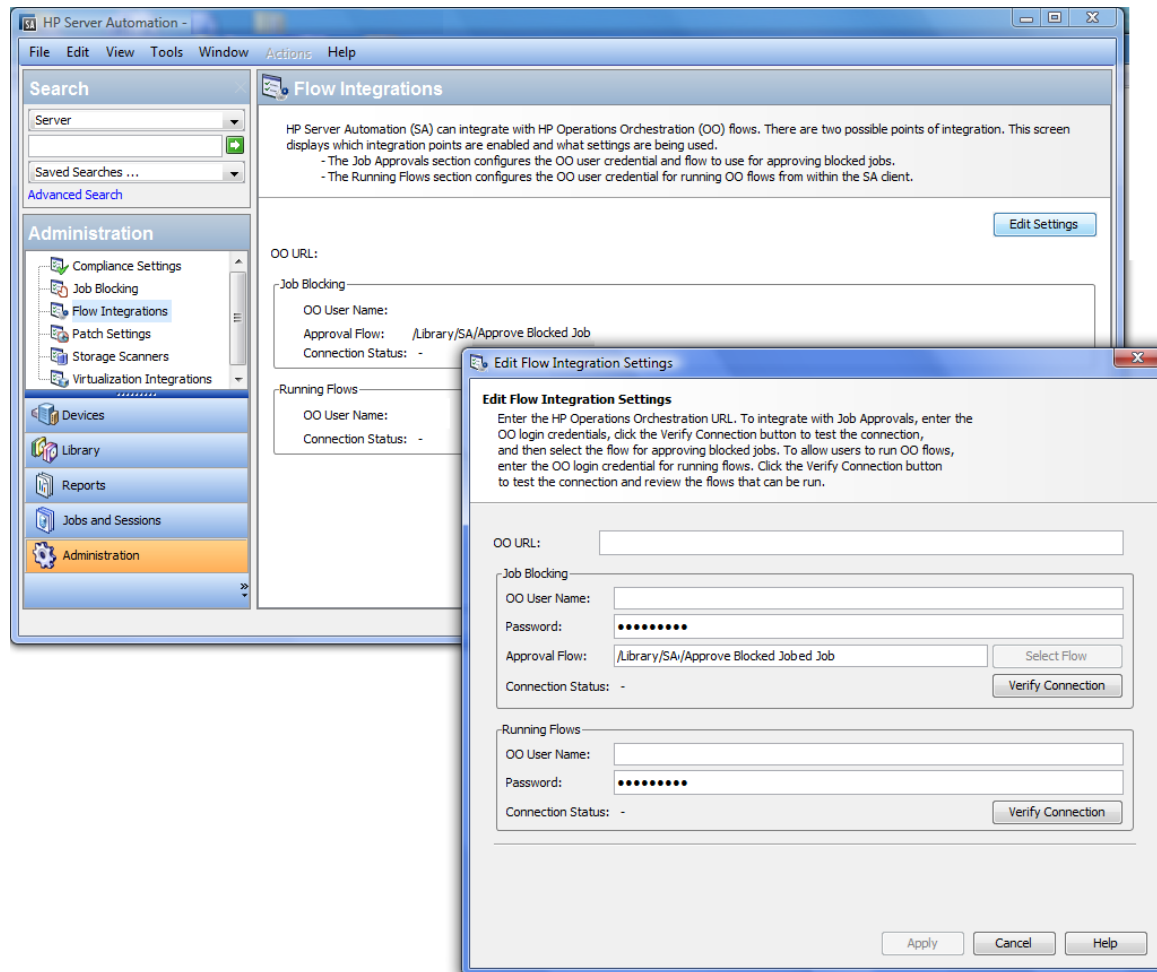
Configuring or Editing a Flow Setting

To edit or configure a flow setting, you must be logged in to OO and SA.

In the SA Client navigation panel:

- 1 Select **Administration ► Flow Integrations**.
- 2 In the Flow Integrations panel, click Edit Settings to display the Edit Flow Integration Settings window.

Figure 24 Edit Flow Integration Settings Window



The Flow Integrations panel displays real-time information for the following users:

- a For Job Blocking: OO user who has permission to run the Approval Flow.
- b For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

3 For running a flow, enter or change the following information:

- OO URL - the location of the OO server in the following format:

`<protocol>://<hostname or host IP address>:<port number>/`

Examples:

`https://10.255.166.110:8443/`

`https://10.255.166.110:8443/PAS/`

- Approval Flow - the location of the approval flow
- OO user name and password of the user who is authorized to communicate with OO

See [Table 3](#) for more information.



A hyphen designates an unconfigured status, a red check mark designates an invalid status, and a green check mark designates a valid status. Both valid and invalid statuses are displayed with their latest verification timestamp.

4 Click Verify Connection to check the validity of the credentials you entered.

If the connection status is valid, a check mark appears.

5 Click Apply to save the flow-integration settings changes.



The Apply button is disabled if no data exists in the Edit Flow Integration Settings panel, if the data in the fields is incorrect, or if a check mark does not appear next to the connection status.

Approving and Deleting Blocked Jobs

You can use the SA Application Programming Interface (SA API) to approve or delete jobs. This API is the only way to manage blocked jobs. You cannot approve a blocked job through the SA Client. For information about using the SA API, see the *SA Platform Developer Guide*.

For information on blocking jobs using OO, see the OO documentation.

Java Methods for Handling Blocked Jobs

The `JobService` Java interface in the SA API provides Java methods for handling blocked jobs. These methods are the callbacks into SA that enable job approval integration.



Users who invoke these methods must have the following required permissions:
Edit or Cancel Any Job and *View All Jobs*

The following table describes the SA JobService Java methods that you can use to handle blocked jobs.

Table 6 SA JobService Java Methods

Java Method	Method Description	SA CLI Method Examples
JobService. approveBlockedJob	Authorizes the job and unblocks it, allowing it to execute.	Within a Global Shell session: cd /opsw/api/com/opsware/job/ JobService/method./approveBlockedJob self:i=\$job_id
JobService. updateBlockedJob	Changes the value of the Ticket ID field (corresponding to the userTag parameter) and Reason field (corresponding to the blockReason parameter) of the blocked job in the Job Status window of the SA Client. Note: You cannot change these fields using the SA interface.	cd /opsw/api/com/opsware/job/ JobService/ method./updateBlockedJob self:i=\$job_id userTag=\$ticket_id \blockReason="This type of job requires approval of CMB."
JobService. cancelScheduledJob	Cancels a blocked job and prevents it from executing. Changes the status of the blocked job from <i>Awaiting Approval</i> to <i>Cancelled</i> .	(Note that the ID parameter is jobRef, not self) cd /opsw/api/com/opsware/job/ JobService/method./ cancelScheduledJob jobRef:i=\$job_id \reason="Job was scheduled to run outside of change window." A job that is currently running (job_status = "ACTIVE") cannot be canceled.
JobService. findJobRefs	Searches all existing jobs and returns the IDs of all blocked jobs or jobs in other states, such as jobs in progress, expired jobs, and scheduled jobs. Can view jobs launched by other users.	(Specify the job_status string in the filter, not the JobInfoVO.status integer.) cd /opsw/api/com/opsware/job/ JobService/method./findJobRefs:i filter='job:{job_status = "BLOCKED"}'

The job_id attribute is required when a flow must come back to SA and interact with the job. Job blocking requires this attribute to be sent from SA to OO.

Job-Status Values

This section describes the job-status values, which you can use in the job_status searchable attribute, as well as the corresponding integer values for the JobInfoVO.status, which you can examine if your client code has already retrieved the value object (VO).

Table 7 lists allowed job-status values.

In a Java client, you can compare `JobInfoVO.status` with field constants such as `STATUS_ACTIVE`, instead of using the integers listed in this table.

Table 7 Job-Status Values

Value of the job_status Searchable Attribute	Value of JobInfoVO.status	Job Status Displayed in the SA Client	Job Status Description
ABORTED	0	Command Engine Script Failure	Job has finished running. A Command Engine failure has been detected.
ACTIVE	1	In Progress	Job is currently running.
BLOCKED	11	Pending Approval	Job has been launched, but requires approval before it can run.
CANCELLED	2	N/A	Schedule has been deleted.
DELETED	3	Canceled	Job was scheduled but was later canceled.
EXPIRED	13	Expired	Current date is later than the job schedule's end date, so the job schedule is no longer in effect.
FAILURE	4	Completed with Errors	Job has finished running and an error has been detected.
PENDING	5	SCHEDULED	Job is scheduled to run once in the future.
RECURRING	12	RECURRING	Job is scheduled to run repeatedly in the future.
STALE	10	STALE	
SUCCESS	6	COMPLETED	Job has finished running successfully.
TAMPERED	9	TAMPERED	
UNKNOWN	7	Unknown	
WARNING	8	Completed With Warnings	Job has finished running and a warning has been detected.
ZOMBIE	14	Orphaned	

5 SA-uCMDB Connector

The SA-uCMDB Integration

This describes how to integrate HP Server Automation (SA) with the HP Universal Configuration Management Database (uCMDB) using the SA-uCMDB Connector. The SA-uCMDB Connector provides a single source for configuration data for asset compliance reporting.

HP SA stores a large amount of information about your servers and software in the SA database. The SA-uCMDB Connector copies some of this data to the HP uCMDB. Whenever the data in SA changes, the SA-uCMDB Connector automatically sends the updated data to the uCMDB Server.

The HP Universal CMDB is a configuration management database (CMDB) for enterprise IT organizations to document, store, and manage business service definitions and associated infrastructure relationships. The uCMDB provides a shared single version of truth to support business service management, IT service management, change management, and asset management initiatives. These initiatives help align IT efforts with business requirements and run IT operations more efficiently and effectively.

HP Server Automation provides life cycle management for enterprise servers and applications from discovery to provisioning, patching to configuration management and script execution to compliance assurance. HP Server Automation automates operations and processes across disparate IT teams and systems.

Highlighted Features

- Extended Out-Of-The-Box mappings
- Extensible ETL mapping and data normalizing capabilities
- Global uCMDB IDs
- On-demand Sync
- SSL Connectivity to the uCMDB Server and the uCMDB Browser
- Support for SA Custom Attributes
- Support for uCMDB server versions 9.05 and 10.01

uCMDB Browser

With the SA-uCMDB Connector, the SA Client provides the ability to launch the uCMDB Browser-Impact widget against an SA managed server.

For more information, see Support for uCMDB Browser integration in the SA Client.

Installing and Configuring the SA-uCMDB Connector

The SA-uCMDB Connector is installed when you install SA. No separate installation is required.

If you are upgrading to Server Automation 10.0, the uCMDB Server must already be upgraded to release 9.05, 10.01 or later.



The version compatibility information herein is correct at the time this document is released. However, cross-product version support can change over the lifecycle of a product version. For up-to-date support and compatibility information, see the HP Server Automation Support and Compatibility Matrix for the relevant product release.

To download the latest Cumulative Update Package:

- 1 The SA 10.0 SA-uCMDB Connector requires that you run with uCMDB 9.05 or uCMDB 10.01 or later.

- uCMDB 9.05 must include Cumulative Update Package 6 (CUP 6) or higher.
- uCMDB 10.01 includes Content Pack 12.
- Both are minimal requirements for using the SA-uCMDB Connector.

The latest CUP HP Software Patch is available on the SSO Portal at the following locations:

- Windows:

http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_uCMDB_00094

- Linux:

http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_uCMDB_00095

For version support information, see [Support for uCMDB Server Versions 9.05 and 10.01](#).

This site requires that you register for an HP Passport and sign in.

- 2 Run the **enable** command to configure the SA-uCMDB Connector with the new uCMDB server.



The syntax of the **enable** command varies depending on your environment. See [The enable Command](#) in this document for an explanation of the enable command syntax and options.

- 3 Enter the following command to start the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

- 4 Optionally check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

Customizing SA Data Sent to the uCMDB Server

The Mapping File

The SA-uCMDB Connector XML mapping file describes the data being transferred by the SA-uCMDB Connector and enables you to customize the data mappings.

The initial mapping.xml is generated when the connector first runs. After it is generated, you can find the new mapping file at:

```
/etc/opt/opsware/tell/metadata/mapping.xml
```

The mapping file allows you to control:

- the data type and attributes that populate uCMDB and
- the mappings between the optional SA custom attributes and the uCMDB Data Model Configuration Item (CI) attributes.



See [EXAMPLE – SA-uCMDB Connector Mapping File](#) for the complete original mapping file contents.

Customizing the Mapping File

In order to customize how data is mapped, you need to create and modify the **mapping_custom.xml** file, and then restart the Connector.



The **mapping_custom.xml** file is not used by default, so you need to restart the Connector to engage the customized mapping file.

To customize the uCMDB Connector mappings:

- 1 If the uCMDB Connector is running, you must stop and disable the Connector before editing the mapping file.



See [Stopping and Disabling the SA-uCMDB Connector](#) for instructions.

IMPORTANT: Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you edit the mapping file, you may encounter problems when you try to restart the Connector.

- 2 Create the custom mapping file:
 - a Go to: **/etc/opt/opsware/tell/metadata**
 - b Copy the **mapping.xml** file to the same folder and name the copy **mapping_custom.xml**.



The **mapping_custom.xml** file must be in the same specified folder as the **mapping.xml** file to function properly.

- 3 Edit the **/etc/opt/opsware/tell/metadata/mapping_custom.xml** as needed.



See [Editing the Mapping File](#) for details on how to edit the mapping file for different purposes.

4 Run the **enable** command to change the configurations of the SA-uCMDB Connector.



The syntax of the **enable** command varies depending on your environment. See [The enable Command](#) in this document for an explanation of the enable command syntax and options.

5 Run the **start** command to restart the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

6 Optionally check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

Editing the Mapping File

All customized mappings are defined in the **mapping_custom.xml** configuration file, so administrators can easily view and edit them. The XML mapping file can be modified to change the data being transferred by the SA-uCMDB connector. The mapping file also provides the ability to choose to omit specific CI and attributes. If the mapping_custom.xml does not exist, the connector by default will honor the out of box mapping.xml.

Permissions: In order to view or edit the **mapping_custom.xml** file, you must first log in to the SA Core as **root** in order to have read/write privileges.



This section describes your editing options within the customized mapping file. For instructions on the process for customizing the mapping file, including when you need to stop and start the connector in order to make the changes take effect, see [Customizing the Mapping File](#).

Illustration of Mapping File

Here is a snippet of the out-of-the-box mapping file:

```
<Model-Definition model-name='hosts'>
  <CI ucldb-ci-type-name='node' enable='true' base-class='node'
    <Attribute source='Node/Name' target-attr='name' enable='true' />
    <Attribute source='Node/Description' target-attr='description'
      enable='true' />
  </CI>
</Model-Definition>
```

where the highlighted text indicates editable fields.



See [EXAMPLE – SA-uCMDB Connector Mapping File](#) for complete out-of-the-box mapping file.

Each Model Definition tag in the mapping file defines a specific model name. In this example, this Model-Definition defines the 'hosts' model.

Each model can contain many Configuration Items (CIs). Each CI tag defines the composition of the CI. In this example, 'node' is the CI being defined.

For each attribute, **source** indicates the default attribute name in the source database.

- The **target-attr** field specifies the uCMDB attribute name that the source is mapping to.
- The **enable** field defines whether to map the attribute. The default value for **enable** is 'true'; which means the attribute will be loaded into the uCMDB. When you set **enable** to 'false', you are choosing not to map the attribute; which means the attribute will not be loaded to uCMDB.

XML Attribute Values

Table 8 shows the XML attribute values, indicating the editable and non-editable values:



WARNING: Do not change non-editable attribute values. It is crucial that the non-editable values, such as, source='Node/Name', remain unchanged. Changing these values can prevent the synchronization from running properly and can lead to errors.

Table 8 XML Attribute Values

XML Attribute Tag	Attributes	Sample Attribute Values and Notes	Editable?
Model-Definition	model-name	'hosts', 'sa', 'software', 'compliance', 'hypervisor', 'vmrelations', 'compliance_status'	NOT editable
	enable	'true' to enable this attribute; 'false' to disable	Editable
CI	ucmdb-ci-type-name	Specifies the uCMDB CI type. For example: 'node', 'ip_address'	Editable
	enable	'true' to enable this attribute; 'false' to disable	Editable

Table 8 XML Attribute Values (cont'd)

XML Attribute Tag	Attributes	Sample Attribute Values and Notes	Editable?
Attribute	source	Specifies the SA custom attribute name. For example: 'Node/Name', 'Node/Description', 'Node/BiosAssetTag', 'Node/BiosSerialNumber', 'Node/Facility', 'Node/VirtualizationTypeId' WARNING: Do not edit the Source value. Modifying the Source value will damage the mapping and may cause errors.	NOT editable
	target-attr	Specifies the uCMDB attribute name that the source is mapping to. For example: 'name', 'description' NOTE: target-attr value must be a unique name.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
	conversion-name	Only used for conversion functions. See Customized Data Conversion Function for details. For example: 'com.hp.tell.ConversionMethod\$com.hp.tell.MyConvertVirtualizationType'	Editable
Attribute-Custom	sa-custom-attribute-key-value	Specifies the SA custom attribute name. For example: 'HW_RACK', 'DEVICE_RACK' NOTE: See Support for SA Custom Attributes .	Editable
	target-attr	Specifies the uCMDB attribute name that the source is mapping to. For example: 'serial_number', 'facility' NOTE: target-attr value must be a unique name.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
CI-Filter	enable	'true' to enable this attribute; 'false' to disable. NOTE: See Filter Support for Queries for modifying CDATA block.	Editable

Table 8 XML Attribute Values (cont'd)

XML Attribute Tag	Attributes	Sample Attribute Values and Notes	Editable?
Relation	ucmdb-relation-type-name	Specifies uCMDB relationship between the CIs. For example: 'containment', 'aggregation'	Editable
	ucmdb-relation-from-ci-type-name	Specifies uCMDB relationship between the CIs of the 'from' CI. For example, if specifying a containment relationship from <i>node</i> to <i>ip_address</i> , the 'node' would be the 'from' CI in this relationship.	Editable
	ucmdb-relation-to-ci-type-name	Specifies uCMDB relationship between the CIs of the 'to' CI. For example, if specifying a containment relationship from <i>node</i> to <i>ip_address</i> , the 'ip-address' would be the 'to' CI in this relationship.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
	ucmdb-relation-id-link	'true' if the relationship contains an ID link. This 'true' value requires the 'from' CI to exist, 'false' if the relationship does not contain an ID link	Editable

Model Definitions

Table 9 shows model definitions. There are 7 models defined in the mapping file that define how data objects are represented in uCMDB. For example, the SA model would represent SA in uCMDB.

Table 9 Model Definitions

Model Definition model-name	Description
'sa'	generates installed_software.xml
'hosts'	generates node.xml
'software'	generates installed_software.xml
'compliance'	generates policy.xml
'hypervisor'	generates hypervisor.xml
'vmrelations'	generates hypervisor.Relationxml
'compliance_status'	generates policyResult.xml



These XML files are generated internally based on the mapping file and should not be edited directly. Editing the generated XML files directly is not supported. Any changes made to the generated files will be overwritten.

Support for SA Custom Attributes



IMPORTANT: All editing of mapping files must be done in the `mapping_custom.xml` file. Do not edit the out-of-the-box `mapping.xml` file. Editing the `mapping.xml` file directly can prevent the synchronization from running properly and can lead to errors.

How to Transfer SA Custom Attributes to uCmdb

Custom attributes can also be loaded to uCmdb.

In addition to the SA attributes that are synchronized with uCmdb, the mappings in the **mapping_custom.xml** file enable you to specify any SA Custom Attributes defined with an SA Device or inherited from SA Facilities.

Custom Attributes can be specified in the **mapping_custom.xml** file as follows:

The following example shows how a user could configure the mapping file to extract the custom attribute, *DEVICE_RACK*, and load it to the *my_location_rack* destination in uCmdb. The **enable** attribute is set to 'true,' showing that the user chose to load this attribute to uCmdb.

```
<CI ucmbd-ci-type-name='node' enable='true' base-class='node'>
  <Attribute-Custom sa-custom-attribute-key-value='DEVICE_RACK' target-
    attr='my_location_rack' enable='true' />
</CI>
```

where the highlighted text indicates editable fields.

Filter Support for Queries

The **mapping_custom.xml** file provides the capability to filter specific criteria.

To filter by specific criteria:

- Embed the filtering clause in the CDATA section under CI-Filter tag.
- Specify whether the filter is enabled by supplying the value for **enable** attribute ('true' to enable, 'false' to disable).



The CI-Filter specification is based on the SA database and requires knowledge of the SA schema. You can only supply one CI-Filter per CI type. If multiple filters are needed, you can specify a simple filter expression using AND and OR clauses.

Example of a single filter (out-of-the-box mapping in **mapping.xml** file):

```
<CI ucmbd-ci-type-name='node' enable='true' base-class='node'>
  <Attribute source='Node/Name' target-attr='name' enable='true' />
</CI>
```

```
<CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>
</CI>
```

In the above example, the filter selects SA devices with State: 'managed'. By default, the SA-uCMDB Connector only synchronizes Managed device objects.

Example of a filter which includes an AND clause (modified mapping in **mapping_custom.xml**):

```
<CI-Filter enable='true'><![CDATA[(DEVICES.DVC_MODEL = 'POWEREDGE 2950') and
(DEVICES.DVC_ID > 300000000)]]></CI-Filter>
```

In the above example, the filter selects SA devices with BOTH the Model, 'POWEREDGE 2950', and the ID greater than '300000000'.

Extended Out-Of-The-Box Mappings

The mapping file is provided to enable you to:

- Change names of attributes being populated in uCMDB
- Change how data is populated in uCMDB
- Specify which uCMDB CI type gets populated

Additional Out-of-the-Box Mappings

The **Facility** and **VirtualizationType** attributes are disabled by default in the out-of-the-box mapping file. However, they may be enabled, as shown below:

`ServerVO.getFacility()`

```
<Attribute source='Node/Facility' target-attr='facility' enable='true'/>
```

`ServerVO.getVirtualizationType()`

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='true'/>
```

Customized Data Conversion Function

If data to be populated in uCMDB needs to be tailored during synchronization, *custom conversion methods* can be written and provided to the SA-uCMDB Connector. The SA-uCMDB Connector can, then, apply these functions to transform the data from the SA syntax to the desired uCMDB syntax. For example, you can write custom conversion methods to convert lower case to upper case, or bytes to megabytes, and so on.

Customized conversion functions should be provided to the SA-uCMDB Connector via a jar file named **tell_conversions.jar**, and placed in **/etc/opt/opsware/tell/lib** prior to the connector startup. After you restart the connector, the custom conversion java class should extend the **ConversionMethod** class and import the **com.hp.tell.ConversionMethod** package.

To customize data conversion:

- 1 If the SA-uCMDB Connector is running, you must stop and disable the Connector before editing the mapping file.

- Run the **stop** command to stop the SA-uCmdb Connector:
`/etc/init.d/opsware-sas stop telldaemon`
- Run the disable command to disable the SA-uCmdb Connector:
`disable`

IMPORTANT: Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you edit the mapping file, you may encounter problems when you try to restart the Connector.

- 2 Write the customized conversation function code in java.

For example, see [Sample Conversion File – MyConvertVirtualizationType.Java](#). In this example, the conversion file's name is **MyConvertVirtualizationType.java**.

- 3 Modify the **mapping_custom.xml** file to utilize the conversion file that you just created.

For example, you would place the following line in the mapping_custom.xml file to point to the java file, MyConvertVirtualizationType.java:

Original text in mapping file

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='false'/>
```

Customized text in mapping file

```
<Attribute source='Node/VirtualizationTypeId' target-attr='device_isVirtual'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualiza
tionType'/>
```

This modified line of XML has the following values:

- **'device_isVirtual'** is the new attribute value for **target-attr**. Because this conversion changes the data type, it should be mapped to a different uCmdb attribute. However, if you are not changing the data type, then you should map to the same **target-attr** value.*
- **conversion-name** is the XML name for the conversion attribute. This is a verbatim label and cannot be substituted.
- **'com.hp.tell.ConversionMethod\$com.hp.tell.MyConvertVirtualizationType'** is the attribute value for conversion-name, and MyConvertVirtualizationType.java is the java conversion code file name.

The target-attr value is critical to the success of the conversion operation:

Changing data types

If the conversion is changing an attribute's data type, make sure that the destination attribute (specified by **target-attr**) has the same or compatible requirements, such as length and format. In the previous example, we modified the **target-attr** value because the conversion changes the actual data type. If, for example, you were merely converting the unit of measure (UOM), then you could specify the same **target-attr** value, because the actual data type did not change.

Unique filename per target-attr

Each **target-attr** conversion requires a unique java conversion code filename. The java conversion file represents a singular **target-attr** (output). For example, you can have multiple **target-attr** conversion scenarios for a single source attribute; however, each **target-attr** must be stated on an individual attribute tag in the mapping file, as shown in the following example:

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id1'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualiza
tionType1' />
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id2'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualiza
tionType2' />
```

- 4 Compile the customized conversion file (**MyConvertVirtualizationType.java** in this example). This generates the executable binaries.
- 5 Compress all of the conversion binaries into a jar file with the following name:
tell_conversions.jar.



You must use this exact jar filename for the SA-uCMDB Connector to recognize it.

-
- 6 Place the jar file in the SA Core directory, **/etc/opt/opsware/tell/lib**, prior to the starting up the uCMDB Connector.



You must use this exact directory path for the SA-uCMDB Connector to recognize it.

-
- 7 Start the SA-uCMDB Connector.

The conversion function will convert the data dynamically, at the time the SA-uCMDB Connector is restarted.

Sample Conversion File – MyConvertVirtualizationType.Java

This sample conversion file provides sample java code to use as a guideline. This java sample converts an SA **VirtualizationType** from Type: *Numeric* into Type: *String* for uCMDB.



You can only have one attribute conversion per java file. To convert multiple attributes, you need to have multiple java files. Each target attribute can only have one conversion.

Tip: Name the conversion file based on the attribute being modified. As in this example, the java filename is **MyConvertVirtualizationType** because it is modifying the **VirtualizationType** attribute.

```
package com.hp.tell;

import java.math.BigDecimal;
```

```

import com.hp.tell.ConversionMethod;

public class MyConvertVirtualizationType extends ConversionMethod {

    public Object convert(Object value) throws Exception{

        Integer vType = putInteger(value);
        String vValue;

        /*
         * Function to convert SA VirtualizationType (numeric) to string type For
uCMDB.
         */

        if (vType > 0) {
            vValue = "True";
        } else {
            vValue = "False";
        }

        return vValue;
    }

    private Integer putInteger(Object o) throws Exception {
        if (o instanceof String) {
            return Integer.valueOf((String) o);
        }
        if (o instanceof BigDecimal) {
            return ((BigDecimal)o).intValue();
        }
        if (o instanceof Integer) {
            return (Integer)o;
        }

        throw new Exception("Invalid conversion in putInteger
"+o.getClass().toString());
    }
}

```

Managing the SA-uCMDB Connector

Stopping and Disabling the SA-uCMDB Connector

If the SA-uCMDB Connector is running, you must stop and disable the Connector before making any kind of configuration change.

To stop and disable the SA-uCMDB Connector:

- 1 Run the **stop** command to stop the SA-uCMDB Connector:


```
/etc/init.d/opsware-sas stop telldaemon
```

- 2 Run the **disable** command to disable the SA-uCMDB Connector:

```
disable
```

IMPORTANT: Make sure the connector is stopped and disabled before making any configuration change. If the connector is not stopped and disabled, you may encounter problems when you try to restart the Connector.

The stop Command

When you stop the SA-uCMDB Connector, it will stop transferring data from the SA database to uCMDB. To stop the SA-uCMDB Connector, enter the following command on an SA core server:

```
/etc/init.d/opsware-sas stop telldaemon
```

This stops the SA-uCMDB Connector.

If the SA-uCMDB Connector is disabled, the output will look like the following:

```
opsware-sas: One or more of the specified components does not exist
in the following file:
```

```
/opt/opsware/oi_util/startup/components.config
```

If you no longer need the SA-uCMDB Connector, you can disable it with the **disable** command. For more information, see [The disable Command](#).

The disable Command

Use the **disable** command to disable the SA-uCMDB Connector. If the SA-uCMDB Connector is running, the **disable** command will stop it before disabling it. If the SA-uCMDB Connector is disabled, you will not be able to start it.

The **disable** command modifies the file **/opt/opsware/oi_util/startup/components.config** and comments out the lines for the **telldaemon**, which is the process for the SA-uCMDB Connector.

Location of the disable Command

The **disable** command is located on your SA core server in the directory **/opt/opsware/tell/bin**.

Syntax of the disable Command

```
disable
```

Enabling and Starting the SA-uCMDB Connector

Before starting the SA-uCMDB Connector, you must enable it to make sure the most up to date configuration elements are engaged.

To enable and start the SA-uCMDB Connector:

- 1 Run the **enable** command to change the configurations of the SA-uCMDB Connector. There are multiple options for the enable command depending on your configuration.

The following is a simple example of this command:

```
enable --host myserver01.hp.com --port 8888 --user ucldb-admin  
--password 1eM93A3dme
```

For more information about the complete set of parameters, syntax, and options, see [The enable Command](#).

- 2 Run the **start** command to restart the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

- 3 Optionally check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

For more information, see [Displaying the Status of the SA-uCMDB Connector](#).

The enable Command

Before you can start the SA-uCMDB Connector, you must enable it with the **enable** command. When you enable it, you provide the uCMDB server name or IP address, port number, login, and password.

Use the **enable** command to configure and enable the SA-uCMDB Connector. This section describes the **enable** command. You must enable the SA-uCMDB Connector before you can start it.

The **enable** command does the following:

- Creates a custom SA-uCMDB Connector configuration file, **/etc/opt/opsware/tell/tell_custom.conf**, if it does not already exist. (By default, the custom configuration file does not pre-exist upon deployment unless one has been created manually.)
- Modifies the custom configuration file, **/etc/opt/opsware/tell/tell_custom.conf**, and enters the uCMDB server's host name or IP address, port number, and login into this file.
- Saves the user's password.
- Modifies the file **/opt/opsware/oi_util/startup/components.config** and uncomments the lines for the **telldaemon**, which is the process for the SA-uCMDB Connector.

If you modify any of the uCMDB configuration parameters while the SA-uCMDB Connector is running, you must stop and restart the SA-uCMDB Connector for your changes to take effect.

Location of the enable Command

The **enable** command is located on your SA core server in the directory **/opt/opsware/tell/bin**.

New Syntax in the enable Command

In SA 9.14, additional parameters were added to the SA-uCMDB Connector's **enable** command in order to support the new uCMDB Browser. The new parameters are described in this section and in [Table 10](#).

```
enable [--protocol <ucldb_protocol>] [--host <ucldb_host_ip>] [--port  
<ucldb_host_port_number>] [--browser_protocol <ucldb_browser_protocol>]  
[--browser_host <ucldb_browser_host_ip>] [--browser_port  
<ucldb_browser_host_port>] [--user <ucldb_admin_user>] [--password  
<ucldb_admin_password>] [--help]
```

Table 10 New Parameters for the enable Command

Parameter	Description	New
--protocol <ucmdb_protocol>	uCMDB server protocol, http or https. Default is http.	New
--host <ucmdb_host_ip>	This option gives the IP address or host name of your HP uCMDB server. The default value is localhost.	—
--port <ucmdb_host_port_number>	This option gives the port number of your HP uCMDB server. The default value is 8080.	—
--browser_protocol <ucmdb_browser_protocol>	uCMDB Browser server protocol, http or https. Default is http.	New
--browser_host <ucmdb_browser_host_ip>	This option gives the IP address or host name of your HP uCMDB Browser host name or IP. The default value is localhost.	New
--browser_port <ucmdb_browser_host_port>	This option gives uCMDB Browser host port. The default value is 8080.	New
--user <ucmdb_admin_user>	This option gives the user name of an administrative user for your HP uCMDB server. The default value is admin.	—
--password <ucmdb_admin_password>	This option gives the password for the user provided in the --user option. The default value is admin.	—

Example of **enable** command without SSL enabled:

```
enable --protocol http --host 192.168.8.93 --port 9999 --browser_protocol
http --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb
--password mypass1234
```

Example of **enable** command with SSL enabled for the uCMDB Server and the uCMDB Browser:

```
enable --protocol https --host 192.168.8.93 --port 9999 --browser_protocol
https --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb
--password mypass1234
```

Displaying the Status of the SA-uCMDB Connector

To display the status of the SA-uCMDB Connector, enter the following command on an SA core server:

```
/etc/init.d/opsware-sas status telldaemon
```

If the SA-uCMDB Connector is enabled but not running, the output will look like the following:

```
Verify "telldaemon" running: FAILURE (pidfile does not exist)
Failed to perform "status" operation on Opsware SAS components.
```

If the SA-uCMDB Connector is disabled, the output will look like the following:

```
opsware-sas: One or more of the specified components does not exist in the
following file:
/opt/opsware/oi_util/startup/components.config
```

SA-uCMDB Data Relationship and Transfer

CI Relationships Maintained

Table 11 lists the Configuration Item (CI) relationships maintained by the SA-uCMDB Connector.

Table 11 CI Relationships Maintained

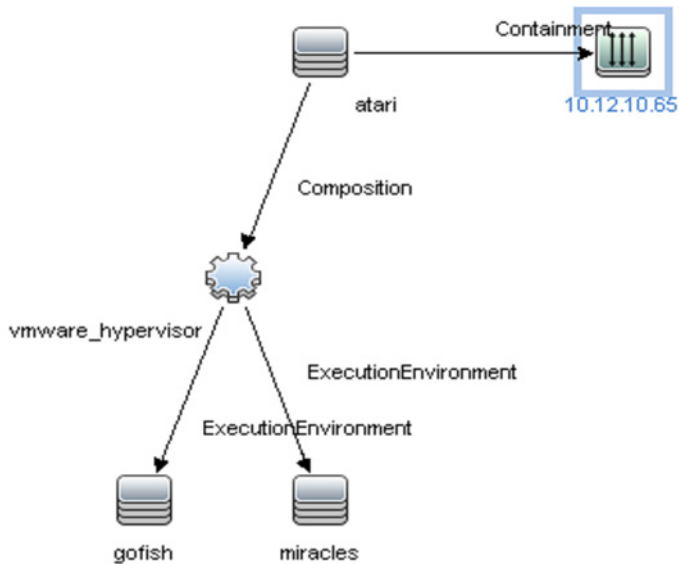
From uCMDB CI	Via	From uCMDB CI
Node	containment	IpAddress
Node	composition	InstalledSoftware
Node	composition	Hypervisor
Node	aggregation	PolicyResult
Hypervisor	ExecutionEnvironment	Node
Policy	composition	PolicyResult
SaSystem	aggregation	Node
SaSystem	aggregation	Policy

Example: uCMDB Showing an SA Managed Server

Figure 25 is from an HP uCMDB screen and it shows:

- One SA managed server named “atari.”
- The managed server’s IP address 10.12.10.65.
- The managed server “atari” is running a VMware hypervisor.
- Two virtual machines are running on the hypervisor named “gofish” and “miracles.”

Figure 25 SA Managed Servers Displayed in the uCMDB



SA Data Transferred to uCMDB

The following data from the SA database is transferred to the uCMDB Configuration Items (CI) and Attributes (see [Table 12](#)):

Table 12 uCMDB CIs and Attributes Populated by SA

uCMDB CI	uCMDB Attribute
Node	Name
Node	Description
Node	BiosAssetTag
Node	DefaultGatewayIpAddress
Node	NodeModel
Node	SerialNumber
Node	BiosUuid
Node	NetBiosName
Node	MemorySize
Node	OsDescription
Node	OsFamily
Node	TenantOwner
IpAddress	Name
IpAddress	RoutingDomain

Table 12 uCMDB CIs and Attributes Populated by SA (cont'd)

uCMDB CI	uCMDB Attribute
InstalledSoftware	Name
InstalledSoftware	Vendor
InstalledSoftware	BuildNumber
InstalledSoftware	DmlProductName
Hypervisor	Name
Hypervisor	Description
Hypervisor	ProductName
Policy	Name
Policy	Description
Policy	PolicyCategory
Policy	PolicyDefinedBy
PolicyResult	Name
PolicyResult	PolicyResultDateTime
PolicyResult	ComplianceStatus
PolicyResult	RulesCompliant
PolicyResult	RulesNonCompliant
PolicyResult	ComplianceLevel
SASystem	Name
SASystem	Description
SASystem	Version

Frequency of Data Transfer to uCMDB

When the SA-uCMDB Connector first starts running, it queries the SA database, creates the CIs in the uCMDB and transfers the data from SA to the uCMDB. After that, whenever the data in the SA database changes, the SA-uCMDB Connector automatically detects the changes and transfers the modified data to the uCMDB. The connector logs information in the log file `/var/log/opsware/tell/LOAD_STATS.0.log`.

For the complete list of data transferred from SA to the uCMDB, see [SA Data Transferred to uCMDB](#).

Accessing the uCMDB Browser from the SA Client

The uCMDB Browser Window

You can view server details in the uCMDB Browser window.

To view server details:

- 1 Log in to the SA Client.
- 2 Go to **Devices > All Managed Servers**.
- 3 Select any server and click **Actions > Open with uCMDB Browser**.

Optional: You can also use the context menu here or on the search panel. Select the server, then right-click and choose **Open With > uCMDB browser**.

Sample URL that SA uses to open the uCMDB Browser for a specific Managed Server:

```
http://my-ucmdb.mycomp.com:8080/ucmdb-api/ucmdb-browser/  
?locale=en&theme=LIGHT#refocus-selection=<global_ucmdb_id>
```

- 4 If you are not already logged in to the uCMDB Browser, this will invoke the uCMDB Browser Login screen. Complete using your uCMDB login credentials. You will only need to sign in once per session.

Tip: If a blank page or a Page Not Found error occurs when you open the uCMDB Browser, it could mean that either uCMDB is not set up or the uCMDB server is not running or configured correctly. Make sure that the uCMDB server is configured and that the Tellconnector is running.

If the SA-uCMDB Connector has not been configured and you need to disable the ‘Open with uCMDB Browser’ menu item, go to **System Configuration > Opsware > Tell** and set the values to no value for **uCMDB Browser URL** and **uCMDB URL**.

Configuring the uCMDB Browser

If the uCMDB Browser needs to be invoked from the SA Client, the uCMDB Browser’s related parameters need to be specified after enabling the SA-uCMDB Connector using the following **/opt/opsware/tell/bin/enable** parameters:

<code>--browser_protocol</code>	- uCMDB Browser server protocol, http or https
<code>--browser_host</code>	- uCMDB Browser host name or IP
<code>--browser_port</code>	- uCMDB Browser host port

Also, by default the SA Client invokes the uCMDB Browser via the uCMDB 9.05-compatible URL prefix.

For example, to use the uCMDB 10.01-based Browser:

- 1 Stop the SA-uCMDB Connector by running the **stop** command:

```
/etc/init.d/opsware-sas stop telldaemon
```
- 2 Disable the SA-uCMDB Connector by running the **disable** command:

```
disable
```

IMPORTANT: Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you revise the configuration file, you may encounter problems when you try to restart the Connector.

- 3 Update the uCMDB Browser prefix in the custom SA-uCMDB Connector configuration file `/etc/opt/opsware/tell/tell_custom.conf` to indicate the correct uCMDB version.

For example:

Change from the following uCMDB 9.05 default:

```
com.hp.sa.tell.ucmdb.browser.path.suffix=/ucmdb-api/ucmdb-browser
```

To the uCMDB 10.01 prefix:

```
com.hp.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser
```

- 4 After the configuration file is updated, enable the SA-uCMDB Connector by running the **enable** command.



The syntax of the enable command varies depending on your environment. See [The enable Command](#) in this document for an explanation of the enable command syntax and options.

- 5 Restart the uCMDB Connector. Enter the following command to start the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

- 6 Optionally check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

Support for uCMDB Server Versions 9.05 and 10.01

For the SA-uCMDB Integration, SA 9.14 or later supports the following uCMDB Server integrations:

- uCMDB 9.05 Content Pack 10 or higher, Cumulative Update Package 6 or higher
- uCMDB 10.01 Content Pack 12



Version support and compatibility information is subject to change. For complete and up-to-date support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online web site:

http://support.openview.hp.com/sc/support_matrices.jsp

You can also download the HP Server Automation Support and Compatibility Matrix for this release from the HP Software Support Online Product Manuals web site:

<http://support.openview.hp.com/selfsolve/manuals>

Global uCMDB IDs

With uCMDB 9.04 and earlier, only the local uCMDB IDs as known to that uCMDB server were synchronized in SA.

With uCMDB 9.05 and later, the uCMDB Servers can be configured as uCMDB Global ID generators, where the uCMDB IDs generated are *global* and *unique* in multi-uCMDB server environments. In such environments, these global IDs are needed to invoke the uCMDB Browser properly.

The SA 9.14 SA-uCMDB Connector was enhanced to automatically use the global uCMDB ID of CIs if the uCMDB Server is configured as a global ID generator. No special configuration is needed for the SA-uCMDB Connector.

SSL Connectivity to the uCMDB Server and the uCMDB Browser

The SA-uCMDB Connector supports SSL protocol for the uCMDB Server and the uCMDB Browser.

When enabling Secure Sockets Layer Communication (SSL), the appropriate certificate and keystore need to be in place for the SA-uCMDB Connector.

To enable SSL:

- 1 Follow the instructions in the *uCMDB Deployment Guide*, “Enabling Secure Sockets Layer Communication,” to create a uCMDB keystore and export the certificate to a file.
- 2 Import exported certificate from step 1 to where the SA-uCMDB Connector is installed. For example, the keystore must be placed in **/var/opt/opsware/crypto/tell** with the keystore filename: **tell.keystore** and the keystore password: **hppass**.

Example of import command:

```
/opt/opsware/jdk1.6/bin/keytool -import -noprompt -alias hpsaucmdb -file  
<path_to_the_exported_hpcert> -keypass hppass -keystore /var/opt/opsware/  
crypto/tell/tell.keystore -storepass hppass
```

Configurable Files Archived During Upgrade

During upgrade, certain customizable and configurable files will be archived for preservation.

If you are upgrading from the SA-uCMDB Connector 9.14 to 10.0 following files will be archived in **/var/opt/opsware/install_opsware/config_file_archive/<respective path for file>**

- tell.conf
- mapping.xml
- logging.properties
- tell_conversions.jar
- tell.pwd
- tell.keystore

For example, the **tell_custom.conf** residing in **/etc/opt/opsware/tell/tell_custom.com** will be archived to **/var/opt/opsware/install_opsware/config_file_archive/etc/opt/opsware/tell/tell_custom.com<time_stamp_of_upgrade>**

For the SA-uCMDB Connector 10.0 and future upgrades, **tell_custom.conf** and **mapping_custom.xml** will also be archived for preservation.

Troubleshooting Tips

Running the SA-uCMDB Connector on a Second Core

In some cases, a particular core in a multi-master SA Mesh needs to be deactivated and it becomes necessary to run the SA-uCMDB Connector from a different core in that mesh. Sometimes this is also needed if network performance from another core to the uCMDB server is preferred. In those scenarios, the following steps are necessary:

To run the connector on a second core:

- 1 Stop the SA-uCMDB Connector on the first core and remove its affinity to it.

```
/etc/init.d/opsware-sas stop telldaemon  
/opt/opsware/tell/bin/tell --release
```
- 2 On the second core, enable the SA-uCMDB Connector by running the **enable** command.



The syntax of the enable command varies depending on your environment. See [The enable Command](#) in this document for an explanation of the enable command syntax and options.

- 3 Take responsibility of the SA-uCMDB integration, and then start the SA-uCMDB Connector.

```
/opt/opsware/tell/bin/tell --take  
/etc/init.d/opsware-sas start telldaemon
```

To enable additional logging:

- 1 Start the SA-uCMDB Connector.

Normal log files are stored in the **/var/log/opsware/tell** directory. Default file names include the following:

```
tell.0.log           (normal startup log)  
ucmdb_failure.*.log (ucmdb failures seen during synchronization)  
LOAD_STATS.*.log    (number of processed data)
```

- 2 To request additional logging details, specify the requested information in the **/etc/opt/opsware/tell/logging.properties** file as shown in [Table 13](#).

Table 13 **/etc/opt/opsware/tell/logging.properties** Fields

Field	Description
java.util.logging.FileHandler.limit	Specifies the maximum number of bytes to write to any one file. Default value is 10000000.
java.util.logging.FileHandler.count	Specifies the number of files to use. Default value is 10.
java.util.logging.FileHandler.append	Specifies append mode, defaults to true.
java.util.logging.FileHandler.pattern	Specifies the pattern for naming the output file where the log file can be found. Defaults to /var/log/opsware/tell/tell.%g.log



CAUTION: Use caution when modifying the file limit. Large numbers might impact performance.

On-Demand Synchronization

Upon SA restart, the SA-uCMDB Connector normally continues synchronizing SA data to uCMDB from where it ended before the restart. The connector also runs a full sync, periodically. However, in some cases, such as when there are networking or server issues that prevent the updates from reaching the uCMDB server, you may need to trigger the full sync on demand.

To trigger the synchronization on demand:

- 1 Stop the SA-uCMDB Connector.
- 2 Restart the SA-uCMDB Connector with the following option:

```
/opt/opsware/tell/bin/tell --startfresh
```

Viewing Log Files

The SA-uCMDB Connector generates the following text log files. You can view these log files in a text editor to get more information.

- **/var/log/opsware/tell/tell.0.log** is the main log file for information, warnings and errors encountered by the SA-uCMDB Connector.
- **/var/log/opsware/tell/LOAD_STATS.0.log** contains the status and statistics of the initial data load, and approximate times to complete the initial data load.
- **/var/log/opsware/tell/ucmdb_failure.0.log** contains uCMDB errors, primarily reconciliation errors if the SA data is incomplete, for example, if the required uCMDB keys are missing. This could happen if a server did not have a serial number or an IP address, for example. This log file contains the uCMDB exception, the reason why it failed and a trace of the CIs that caused the exception.

SA-uCMDB Connector Daemon

The SA-uCMDB Connector runs the daemon **/etc/opt/opsware/startup/telldaemon** on your SA core server. Make sure this process is running on your SA core server.

If it is not running, start it as described in [Enabling and Starting the SA-uCMDB Connector](#).

If it is running, check the status as described in [Displaying the Status of the SA-uCMDB Connector](#).

EXAMPLE – SA-uCMDB Connector Mapping File

```
<DB-UCMDB-HIGHLEVEL-MAPPING>
  <!-- generates installed_software.xml -->
  <Model-Definition model-name='sa' enable='true'>
```

```

        <CI ucmdb-ci-type-name='server_automation_system' enable='true'
base-class='server_automation_system'>
        <Attribute source='SA/Description' target-attr='description'
enable='true' />
        <Attribute source='SA/Name' target-attr='name' enable='true' />
        <Attribute-Default target-attr='version' target-attr-value='9.14'
enable='true' />
        </CI>
    </Model-Definition>

    <!-- generates node.xml -->
    <Model-Definition model-name='hosts' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true' />

        <CI ucmdb-ci-type-name='ip_address' enable='true' base-class='node'>
            <Attribute source='IpAddress/PrimaryIpName' target-attr='name'
enable='true' />
            <Attribute source='IpAddress/RoutingDomain'
target-attr='routing_domain' enable='true' />
        </CI>

        <CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
            <Attribute source='Node/Name' target-attr='name' enable='true' />
            <Attribute source='Node/Description' target-attr='description'
enable='true' />
            <Attribute source='Node/BiosAssetTag' target-attr='bios_asset_tag'
enable='true' />
            <Attribute source='Node/BiosSerialNumber'
target-attr='serial_number' enable='true' />
            <Attribute source='Node/BiosUuid' target-attr='bios_uuid'
enable='true' />
            <Attribute source='Node/DefaultGatewayIpAddress'
target-attr='default_gateway_ip_address' enable='true' />
            <Attribute source='Node/NetBiosName' target-attr='net_bios_name'
enable='true' />
            <Attribute source='Node/NodeModel' target-attr='node_model'
enable='true' />
            <Attribute source='Node/MemorySize' target-attr='memory_size'
enable='true' />
            <Attribute source='Node/OsDescription'
target-attr='os_description' enable='true' />
            <Attribute source='Node/OsFamily' target-attr='os_family'
enable='true' />
            <Attribute source='Node/TenantOwner' target-attr='TenantOwner'
enable='true' />
            <Attribute source='Node/Facility' target-attr='facility'
enable='false' />
            <Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='false' />
            <Attribute source='IpAddress/ManagementIpName'
target-attr='ip_address' enable='false' />
            <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>

```

```

        </CI>

        <Relation ucmdb-relation-type-name='containment'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='ip_address' enable='true'
ucmdb-relation-id-link='true'/>
        <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='server_automation_system'
ucmdb-relation-to-ci-type-name='node' enable='true'
ucmdb-relation-id-link='false'/>
    </Model-Definition>

    <!-- generates installed_software.xml -->
    <Model-Definition model-name='software' enable='true'>
        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='installed_software' enable='true'
base-class='installed_software'>
            <Attribute source='InstalledSoftware/DmlProductName'
target-attr='dml_product_name' enable='true'/>
            <Attribute source='InstalledSoftware/Name' target-attr='name'
enable='true'/>
            <Attribute source='InstalledSoftware/Version'
target-attr='version' enable='true'/>
            <Attribute source='InstalledSoftware/Vendor' target-attr='vendor'
enable='true'/>
        </CI>

        <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='installed_software'
ucmdb-relation-id-link='true' enable='true'/>
    </Model-Definition>

    <!-- generates policy.xml -->
    <Model-Definition model-name='compliance' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='policy' base-class='policy' enable='true'>
            <Attribute source='Policy/Name' target-attr='name' enable='true'/>
            <Attribute source='Policy/Description' target-attr='description'
enable='true'/>
            <Attribute-Default target-attr='policy_defined_by'
target-attr-value='SA' enable='true'/>
            <Attribute-Default target-attr='policy_category'
target-attr-value='audit' enable='true'/>
        </CI>

```

```

        <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='server_automation_system'
ucmdb-relation-to-ci-type-name='policy' enable='true'
ucmdb-relation-id-link='false' />
    </Model-Definition>

    <!-- generates hypervisor.xml -->
    <Model-Definition model-name='hypervisor' enable='true'>
        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true' />

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor'
enable='true'>
            <Attribute source='Hypervisor/Name' target-attr='name'
enable='true' />
            <Attribute source='Hypervisor/Description'
target-attr='description' enable='true' />
            <Attribute source='Hypervisor/ProductName'
target-attr='product_name' enable='true' />
        </CI>

        <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='hypervisor' ucmdb-relation-id-link='true'
enable='true' />
    </Model-Definition>

    <!-- generates hypervisorRelation.xml -->
    <Model-Definition model-name='vmrelations' enable='true'>
        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor'
reference-ci='true' enable='true' />

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true' />

        <Relation ucmdb-relation-type-name='execution_environment'
ucmdb-relation-from-ci-type-name='hypervisor'
ucmdb-relation-to-ci-type-name='node' ucmdb-relation-id-link='false'
enable='true' />
    </Model-Definition>

    <!-- generates policyResult.xml -->
    <Model-Definition model-name='compliance_status' enable='true'>
        <CI ucmdb-ci-type-name='policy' base-class='policy'
reference-ci='true' enable='true' />

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true' />

        <CI ucmdb-ci-type-name='policy_result' base-class='policy_result'
enable='true'>
            <Attribute source='PolicyResult/Name' target-attr='name'
enable='true' />

```

```
        <Attribute source='PolicyResult/ComplianceStatus'
target-attr='compliance_status' enable='true' />
        <Attribute source='PolicyResult/PolicyResultDateTime'
target-attr='policy_result_date_time' enable='true' />
        <Attribute source='PolicyResult/RulesCompliant'
target-attr='rules_compliant' enable='true' />
        <Attribute source='PolicyResult/RulesNonCompliant'
target-attr='rules_non_compliant' enable='true' />
        <Attribute source='PolicyResult/ComplianceLevel'
target-attr='compliance_level' enable='true' />
    </CI>

    <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='policy'
ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='false'
enable='true' />
    <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='true'
enable='true' />
</Model-Definition>
</DB-UCMDB-HIGHLEVEL-MAPPING>
```
