

HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 9.10

Integration Guide

Document Release Date: June 2011

Software Release Date: June 2011



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 2000-2011 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.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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, go to:

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

Or 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.

Document Changes

Chapter	Date	Version	Changes
All	July 2010	1.0	Document Created
2	August 2010	1.1	Added changes to OO chapters
3	August 2010	1.2	Added changes to OO chapters
4	November 2010	9.02	Added SA–HP DMA integration chapter.
N/A	June 2011	9.10	Removed SA–HP DMA integration chapter. HP Database and Middleware Automation (HP DMA) is now automatically installed and fully integrated with SA. No additional integration steps are required. For information about using HP DMA with SA, see the following SA documents: <ul style="list-style-type: none">• <i>User Guide: Database and Middleware Automation</i>• <i>User Guide: Application Deployment Manager</i>

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site 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 web site 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

Contents

1	SA/NA Integration	9
	SA/NA Integration Overview	9
	SA/NA Integration Features	10
	How NA Data is Collected	10
	NA Topology Data Gathering Diagnostic	11
	NA Duplex Data Gathering Diagnostic	11
	NA Database/SA Database	11
	Authentication	11
	Prerequisites	11
	Time Requirements	11
	NA Integration Port Requirements	12
	SA/NA Integration Configuration Tasks	12
	SA Client Communication with NA	12
	Edit the jboss_wrapper.conf File	12
	SA Configuration Changes	14
	Configuring NA for Integration	15
	SA Gateway Requirements	15
	User Permissions	15
	NA Authentication Configuration	15
	Configuring SA/NA Integration with CiscoWorks NCM	17
	Gather Topology Data	18
	Troubleshooting Tips	18
	Resetting the NA Host in the SA Client	18
	Using SA/NA Integration	19
	Connections Between Network Devices and Servers	19
	Data Link Connections	19
	Physical Connections	20
	Network Device Information in SA	20
	Viewing Network Interfaces	21
	Viewing Network Ports	21
	Network Device Information in NA	22
	Viewing a Network Device Directly in NA	22
	Viewing Event History Directly in NA	23
	Duplex Mismatch	24
	Viewing Duplex Mismatches in the Dashboard	24
	Viewing Duplex Mismatches by Server	24
	Viewing Duplex Mismatches by Network Device	24
	Network Reports	25
	Connections by Network Device	25

Connections by Server	25
Duplex Compliance (All Servers)	25
Duplex Compliance by Customer	25
Duplex Compliance by Facility	25
Network Diagrams	26
Launching Service Automation Visualizer (SAV) (SAV)	26
Launching NA Diagramming	26
NA and the SA Global Shell	26
Launching OGFS	27
Remote Terminal (rosh)	27
Inferred Physical Connections	27
Device Groups and NA	28
Associating a NA Device Group	28
Combined Device History Log	28
Viewing a Combined Device Event History Log	29
2 SA-OO Integration – Running Flows	33
What’s New for SA-OO Integration	33
Ability to Run Flows from SA	33
Edit Flow Integration Settings Window	33
Displaying Real-Time Information	33
Replacing OO Connector File Functionality	34
New Required Permissions	35
Administrators: Setting Up Flows	35
Prerequisites	35
Prerequisites for Using OO	35
Environment	35
Importing the OO SDK Client Certificate	35
Permissions	36
Configuring or Editing a Flow Setting	37
SA-OO Integration Flows	38
Verifying Your Changes and Settings	40
Flow Edits and Flow Status	40
Users: Running Flows	41
Choosing a Flow to Run	41
Adding or Deleting Servers	43
Choosing Flow Input, Runtime Option, Scheduling Option, and Notification Parameters	43
Troubleshooting	45
SA-OO Connection Error	45
Flow Run Error	45
3 SA-OO Integration: Job Blocking and Approving	47
Blocking Jobs	47
What are Blocked Jobs?	47
Scenario 1	47
Scenario 2	47
Scenario 3	48
What SA Job Types Can be Blocked?	48

Required Permissions	49
How Do I Block and Unblock Jobs?	50
How Do I Designate Job Types to Block?	50
How Do I Disable Job Blocking?	51
How Do I View Blocked-Job Information?	51
Checking OO Connection Information in the SA Flow Integrations Panel	51
Checking Blocked-Job Status in the Job Log	52
Configuring or Editing a Flow Setting	52
Approving and Deleting Blocked Jobs	53
Java Methods for Handling Blocked Jobs	53
Job-Status Values	54

1 SA/NA Integration

SA/NA Integration Overview

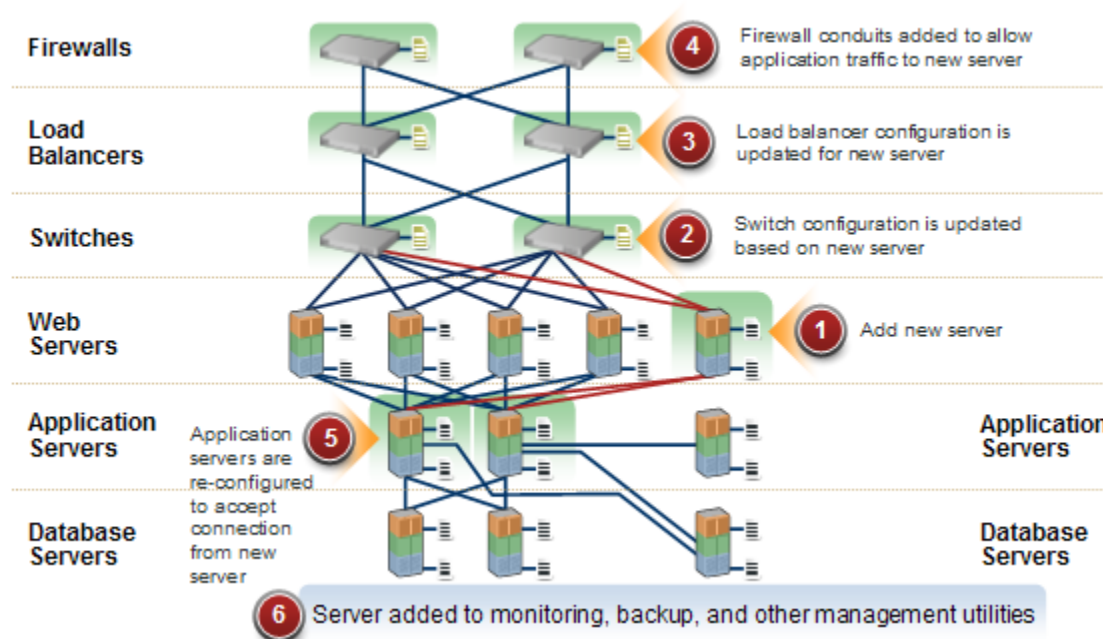
Implementing changes in an IT environment often requires a coordinated effort between network administrators, system administrators, and application architects who must manage an application environment that may consist of servers with different operating systems as well as network devices that can include 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 allowing you to see how servers are connected to network devices and enables them to closely examine managed servers. With this information, they can determine how all devices are related and coordinate and implement required changes.

Figure 1 shows some of the coordinated tasks you can perform through SA/NA Integration.

Figure 1 Overview of Coordinating Tasks Using SA/NA Integration



This section contains information about how to configure NA Integration with SA. Once 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 SA 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 HP Support. 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 24 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 15. 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) and 22 (Windows-based NA Servers).

- **RMI/JRMP 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/JRMP requires that the following ports are open:

- **Port 1099**

JNDI

- **Port 4444**

RMI Object

- **Port 8083**

RMI

- **Dynamic**

RMI

See the *NA User Guide* for information about how to set up these port requirements to access the NA API through a firewall.

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 can't communicate with the NA server, see [Resetting the NA Host in the SA Client](#) on page 18.

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 NA and the Web Service Data Access Engine for each slice.

- **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.

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



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` parameter must be enabled for NA integration.

To enable this parameter:

- a Log into the Command Center (OCC) as an SA Administrator.
- b Click on **Administration** ► **System Configuration**.
- c Select Data Access Engine from the SA component list.
- d Locate the parameter, `spin.cronbot.check_duplex.enabled`.
- e Click Use `value:` and enter 1 in the text box.
- f Click Save.

For more information about using the Command Center (OCC) to modify SA parameter values, 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 release notes for SA and NA.
-

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 User 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, it 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 3](#)):

- **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 Opware Server Automation System & TACACS+ (if used) as shown in [Figure 2](#).

Figure 2 External Authentication Type in NA

The screenshot shows the 'User Authentication' configuration page. The 'External Authentication Type' section is highlighted with a red circle around the 'Opware Server Automation System & TACACS+' radio button. Other options include 'None (Local Auth)', 'Opware Server Automation System', 'TACACS+', 'RADIUS', 'SecurID', and 'Active Directory'. The 'Additional User Password Restriction' section has three radio buttons: 'No additional restrictions' (selected), 'Must contain at least one non-alphabetic digit or special character', and 'Must contain both at least one digit and at least one special character'. The 'Maximum Consecutive Login Failures' is set to 0. The 'TACACS+ / RADIUS Authentication' section is partially visible at the bottom.

- 4 Scroll down and complete all fields in the Opware Server Automation System Authentication section shown in [Figure 3](#).

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 3 Opware Server Automation System Authentication

The screenshot shows the 'Opware Server Automation System Authentication' configuration page. The fields are: Twist Server (twist.c43.dev.opsware.com), Twist Port Number (1032), Twist Username (detuser), Twist Password (masked with dots), OCC Server (occ.c43.dev.opsware.com), 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 NA server.

2 Open the XML file:

```
<NAS_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 **Opware NAS**.

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 NA.
- 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.opsware.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**.

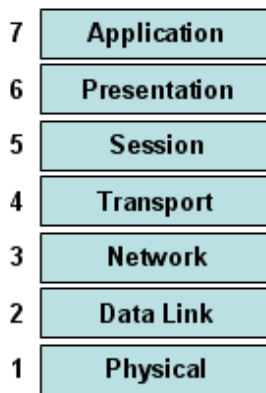
Using SA/NA Integration

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 4](#) for definitions of the OSI Model layers.

Figure 4 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 27. 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. See the *NA User Guide*.

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 22 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 5](#).

Figure 5 Hardware View in the Server Explorer

The screenshot shows the 'Hardware' view in the Server Explorer for a server named 'm263.dev.opsware.com'. The interface is divided into a left 'Views' pane and a main 'Hardware' pane. The 'Views' pane lists various system components, with 'Hardware' selected. The 'Hardware' pane displays detailed information for several components, each in a collapsed section:

- General:** Manufacturer: DELL COMPUTER CORPORATION, Model: POWEREDGE 1750
- Processors:** A table with columns: Vendor, Model, Speed, Cache. Two entries for Intel(R) Xeon(TM) CPU 2.80GHz at 2,787 MHz with 512 KB cache.
- Memory:** A table with columns: Type, Capacity. Entries for SWAP (1.95 GB) and RAM (1.96 GB).
- Storage:** A table with columns: Storage, Media, Model, Bus Type, Capacity. Entries for sda (SCSI DISK, SEAGATE ST3146707LC, SCSI, 136.73 GB) and hdc (CDROM, TEAC CD-ROM CD-224E, IDE, 1,024 GB).
- Network Interfaces:** A table with columns: Interface, IP Address, Netmask, MAC Address, Connected To, VLAN, Duplex, Speed. Two entries: eth0 (192.168.194..., 255.255.255.0, 00:0B:DB:92..., sw3548_13..., VLAN101, Full (Auto), 100 (Auto)) and eth1 (-, -, 00:0B:DB:92..., -, -, -).

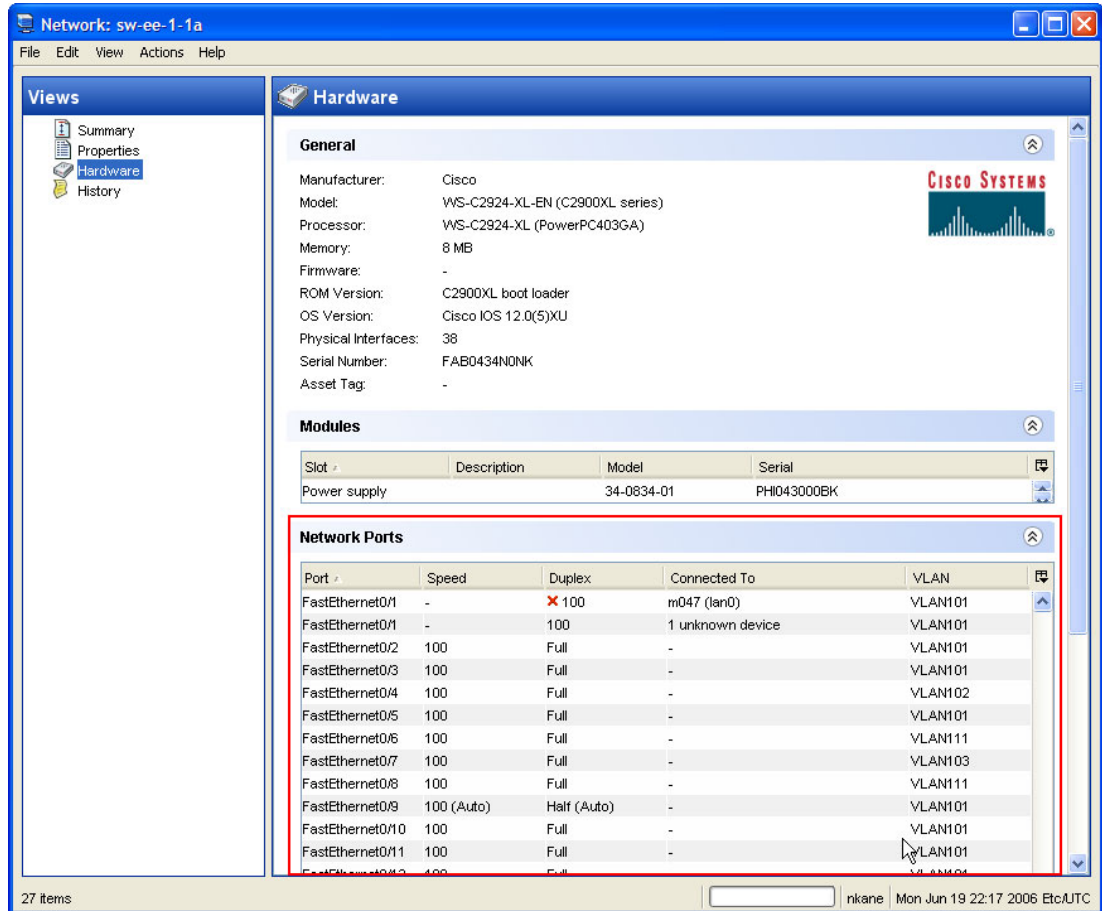
The 'Network Interfaces' section is highlighted with a red border in the original image. The status bar at the bottom shows '2 items', a search box, the user 'nkane', and the date 'Mon Jun 19 21:57 2006 Etc/UTC'.

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 6](#).

Figure 6 Hardware View in the Network Device Explorer



Network Device Information in NA

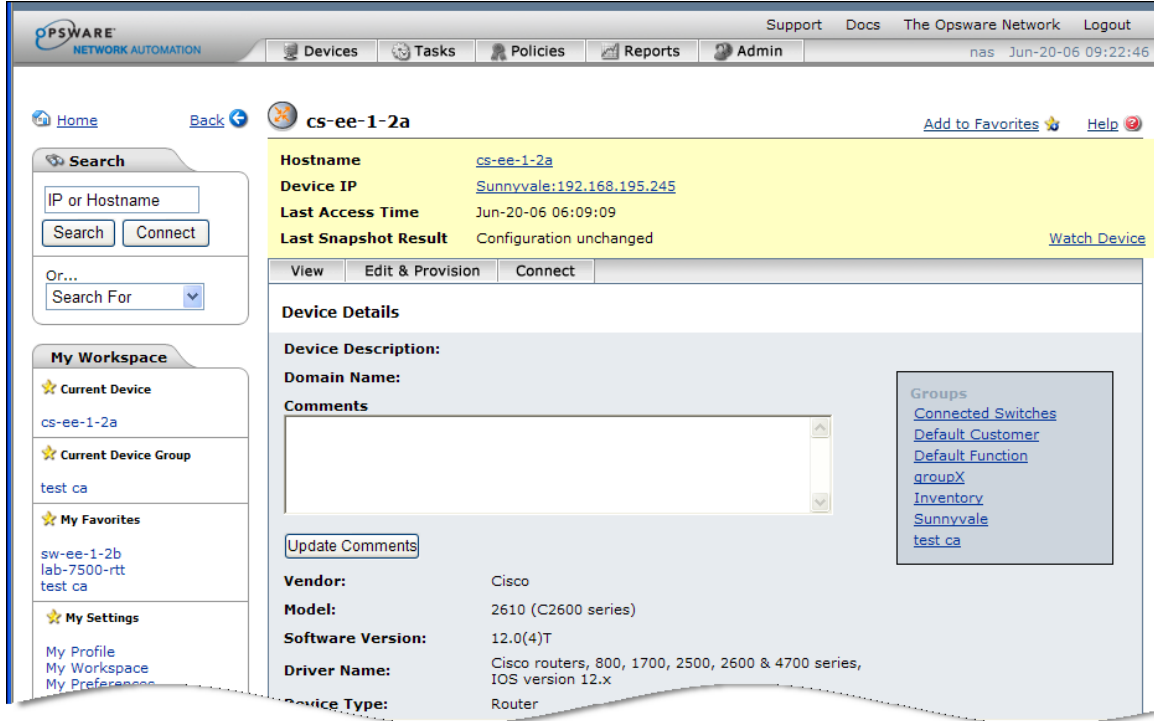
To help you with troubleshooting tasks that involve network devices in your environment, you can examine additional network device details and network device event history by logging directly in to NA. The SA/NA Integration feature provides a login option to access detailed information about network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

Viewing a Network Device Directly in NA

If you want to view detailed information about a network device directly in NA, perform the following steps:

- 1 From the Navigation pane, select **Devices** ► **Device Group** ► **Public**.
- 2 In the Content pane, select a network device.
- 3 Right-click and select **Open with** ► **HP Network Automation** to display the NA login window.
- 4 Enter your user name and login, and then click **Login** to display device details in NA.

Figure 7 Network Device Details in NA



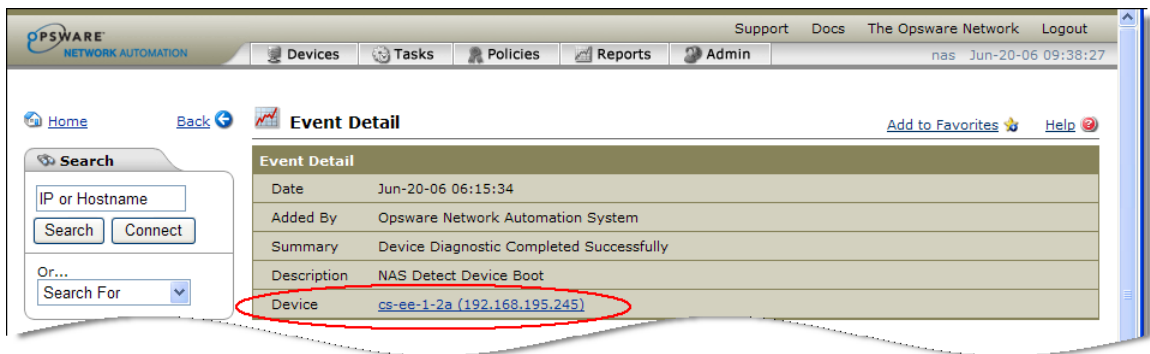
- 5 Click **Logout** to exit NA.

Viewing Event History Directly in NA

If you want to view event details directly in NA, perform the following steps:

- 1 In the Event Details window, click **Open with** ► **HP Server Automation** to display the NA login window. See **Figure 12 on page 31**.
- 2 Enter your user name and login, and then click **Login** to display event details in NA.

Figure 8 Event Details for a Network Device in NA



- 3 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. See **Figure 13**.
- 4 Click **Logout** to exit 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 HP Support.

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 11.

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, Hewlett Packard recommends 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, it 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 5](#).

Network Reports

To help troubleshoot problems that involve physical connections and duplex compliance, you can run and examine several network reports. By using the Reports feature in the SA Client, you can produce the following network reports that identify layer 1 connections and configuration mismatches (duplex compliance) 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.

Duplex Compliance (All Servers)

This report groups all managed servers by duplex compliance level to show configuration mismatches between servers and network devices. Click on a section of the chart to display a list of servers in a certain compliance level. Double-click on a server for more details or to perform an action.

Duplex Compliance by Customer

This report lists all managed servers by customer and then by duplex compliance level to show configuration mismatches between servers and network devices. Double-click on a server for more details or to perform an action.

Duplex Compliance by Facility

This report lists all managed servers by facility and then by duplex compliance level to show configuration mismatches between servers and network devices. Click on a section of the chart to display a list of servers in a facility with a certain compliance level. Double-click on a server for more details or to perform an action.



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) (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 Remote Shell (`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**.

Combined Device History Log

The combined device history log records events performed on servers and network devices in your environment. These events are recorded in detail as actions performed on a certain date, by a certain user, on a certain server, or on a certain network device.

In many troubleshooting tasks, this type of information is critical because some of these actions (changes) might be the root cause of problems. This log provides detailed information, such as the date the action occurred, the name and type of the device that the action was performed on, and a description of the action, that can help you perform root cause analysis, capacity planning, and compliance remediation tasks.

For example, if an application in your environment has suddenly stopped running and you know exactly when it was previously running, you need to examine a combined event history log for the affected servers and network devices, for that time period. This information can help you determine why the application stopped working.

Viewing a Combined Device Event History Log

You can view a detailed list of events that occurred on a server or network device, such as all changes made to an application. You can narrow the time frame of the log display to see changes that occurred daily, weekly, monthly, quarterly, or in a custom range of dates. You can also dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.

You can view a combined device history log for one or more managed servers or for a device group that contains managed servers and network devices.

To view a combined device history log for a device group, perform the following steps:

- 1 From the Navigation pane, select **Devices** ► **Device Group**, and select a device group.
- 2 In the Content pane, select one or more devices in the group.
- 3 Right-click and then select View History to list events that occurred on the selected devices.

Figure 9 Combined Device Event History

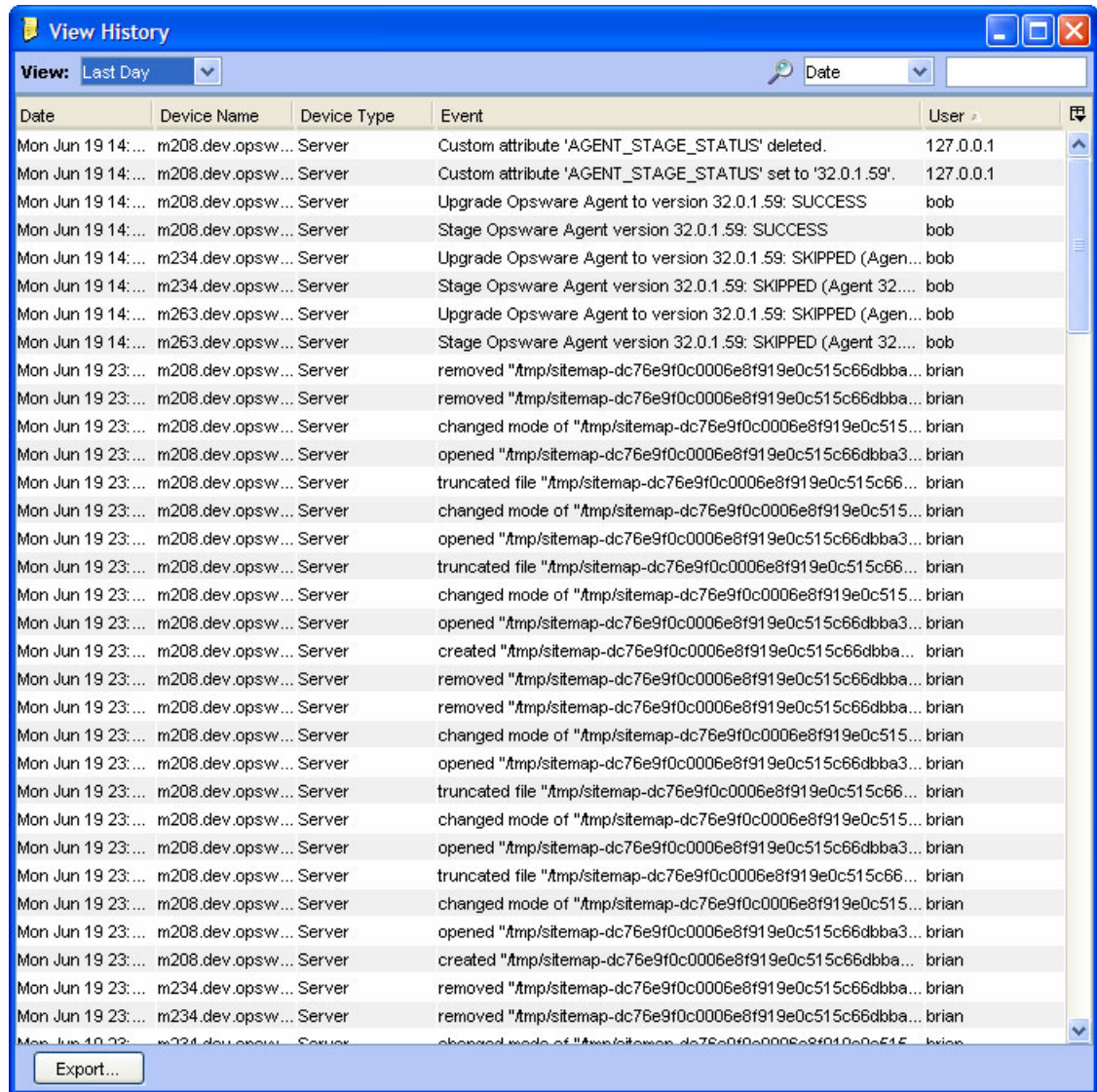
Date	Device Name	Device Type	Event	User
Mon Jun 26 04:...	im101.pr5.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 01:...	sw1.pr5	Switch	Task Started	admin
Mon Jun 26 01:...	sw1.pr5	Switch	Last Used Device Password Changed	-
Mon Jun 26 01:...	sw1.pr5	Switch	Device Diagnostic Completed Successfully	admin
Mon Jun 26 01:...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Device Snapshot	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Last Used Device Password Changed	-
Sun Jun 25 22:0...	sw1.pr5	Switch	Task Started	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Task Started	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Last Used Device Password Changed	-
Sun Jun 25 19:0...	sw1.pr5	Switch	Device Diagnostic Completed Successfully	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Device Snapshot	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Last Used Device Password Changed	-

Viewing an Event History Log for Servers

To view a combined device history log for one or more managed servers, 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 Right-click and select View History to list events that occurred on the selected server(s).

Figure 10 View History of Servers



The screenshot shows a window titled "View History" with a "View:" dropdown set to "Last Day" and a search icon. The table below represents the data shown in the window.

Date	Device Name	Device Type	Event	User
Mon Jun 19 14:...	m208.dev.opsw...	Server	Custom attribute 'AGENT_STAGE_STATUS' deleted.	127.0.0.1
Mon Jun 19 14:...	m208.dev.opsw...	Server	Custom attribute 'AGENT_STAGE_STATUS' set to '32.0.1.59'.	127.0.0.1
Mon Jun 19 14:...	m208.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SUCCESS	bob
Mon Jun 19 14:...	m208.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SUCCESS	bob
Mon Jun 19 14:...	m234.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SKIPPED (Agen...	bob
Mon Jun 19 14:...	m234.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SKIPPED (Agent 32....	bob
Mon Jun 19 14:...	m263.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SKIPPED (Agen...	bob
Mon Jun 19 14:...	m263.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SKIPPED (Agent 32....	bob
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian


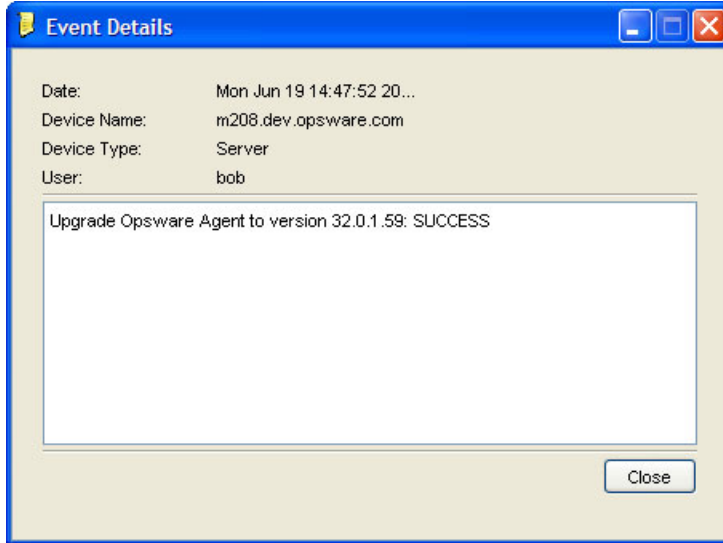
- 4 (Optional) In the View History window, select an option in the View drop-down list to list events by a time period, such as Last Day, Last Week, Last Month, or Custom Range.
- 5 (Optional) In the View History window, use the search tool  to dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.
- 6 (Optional) To identify the device name and type for a certain event, double-click on the event listed in the View History window to display the Event Details window.

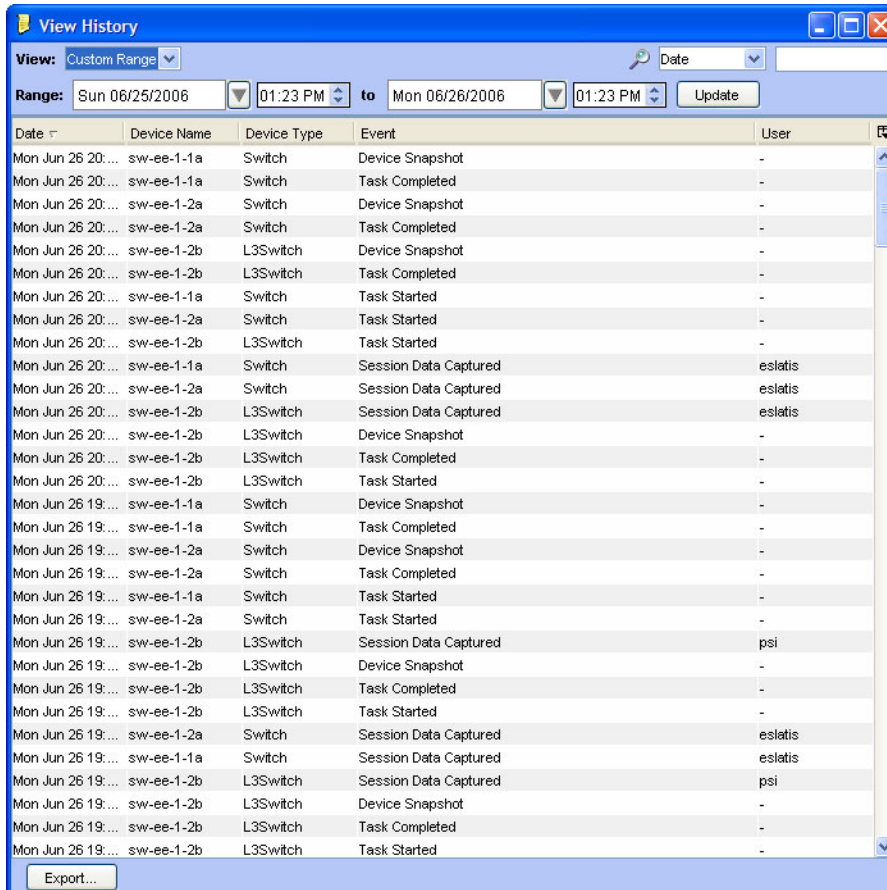
Figure 11 Event Details for a Selected Server



To view the combined device history log for a device group, perform the following steps:

- 1 From the Navigation pane, select **Devices ► Public**.
- 2 In the Content pane, select one or more devices in the group.
- 3 Right-click and then select View History to list events that occurred on the selected network devices.

Figure 12 View History of Network Devices




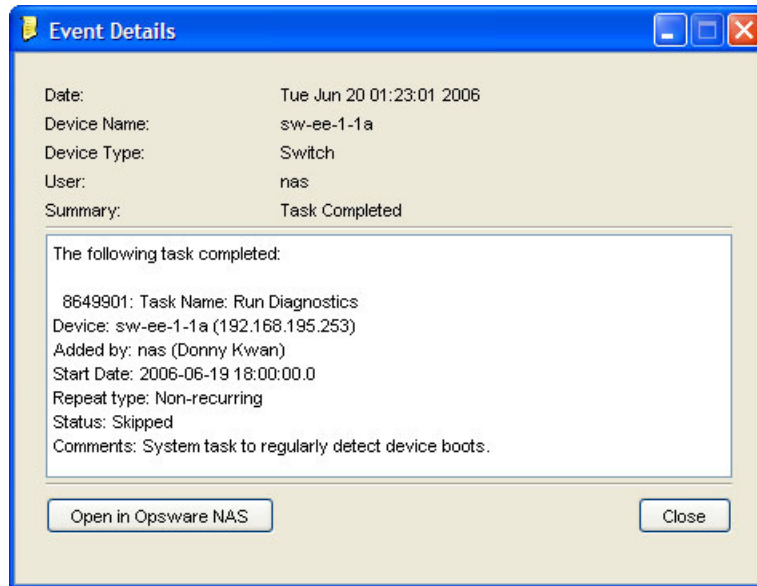
- 4 (Optional) In the View History window, select an option in the View drop-down list to list events by a time period, such as Last Day, Last Week, Last Month, or Custom Range.
- 5 (Optional) In the View History window, use the search tool  to dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.
- 6 (Optional) To display details for a certain event, double-click on the event listed in the View History window to display the Event Details window.

Figure 13 Event Details for a Selected Network Device



Exporting a Combined Device History Log

If you need to use the log file in different applications, you can export the list of combined device history events to a .csv or an .html file.

To export the combined device history log, perform the following steps:

- 1 From the View History window, click **Export** to display the Export Dashboard window.
- 2 In the Look in field, enter the location of where you want to save the file.
- 3 (Optional) From the Encoding drop-down list, select a character encoding option. The default is Unicode (UTF-8).
- 4 In the File name field, enter a name for the file.
- 5 In the Files of type field, select .csv or .html.
- 6 Click **Export** to save the file in the selected format or click **Cancel** to close this window without saving.

2 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 33
- [Administrators: Setting Up Flows](#) on page 35
- [Users: Running Flows](#) on page 41

What's New for SA-OO Integration

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

Ability to Run Flows from SA

Users can now run flows from SA. See [Users: Running Flows](#) on page 41 for more information on running flows as a user.

Edit Flow Integration Settings Window

This window, its subwindow, 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 [Configuring or Editing a Flow Setting](#) on page 37.

Replacing OO Connector File Functionality

OO Connector Configuration file functionality has been replaced with the Edit Flow Integration Settings SA window, where administrators can enter configuration inputs into the SA interface.

If you are upgrading 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 1](#) for mapping information for the connection settings. See [Configuring or Editing a Flow Setting](#) on page 37 for more information on the interface.

Table 1 Mapping Configuration File Inputs to Integration Window Fields

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

New Required Permissions

The following new permissions (one for administrators, one for users) are required to work with flows:

- Administer Flow Integrations

This permission allows administrators to configure the OO integration settings.

- Run Flow

This permission allows users to run flows in SA.

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 9.0
- HP Operations Orchestration (OO) version 7.60.X or 9.X
- OO installation server networked to SA core server
- Reserved Port 8443 on the OO server
- Valid OO SDK Client Certificate to communicate with OO



NOTE: SA version 9.0 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:

```
/opt/opsware/jdk1.6/jre/bin/keytool -exportcert -alias pascert -file /tmp/oocentral.crt -keystore /var/opt/opsware/twist/ooCERT
```

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

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

- 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

The following new administrator permission is required: Administer Flow Integration. This permission allows administrators to configure the OO integration settings.

To set this permission, access the Administration section of the SA Web Client. To learn more about permissions, see the permissions section of the *Server Automation Administration Guide*.

Use the following table as a guide to check if the proper permissions have been granted.

Table 2 Checking User Permissions

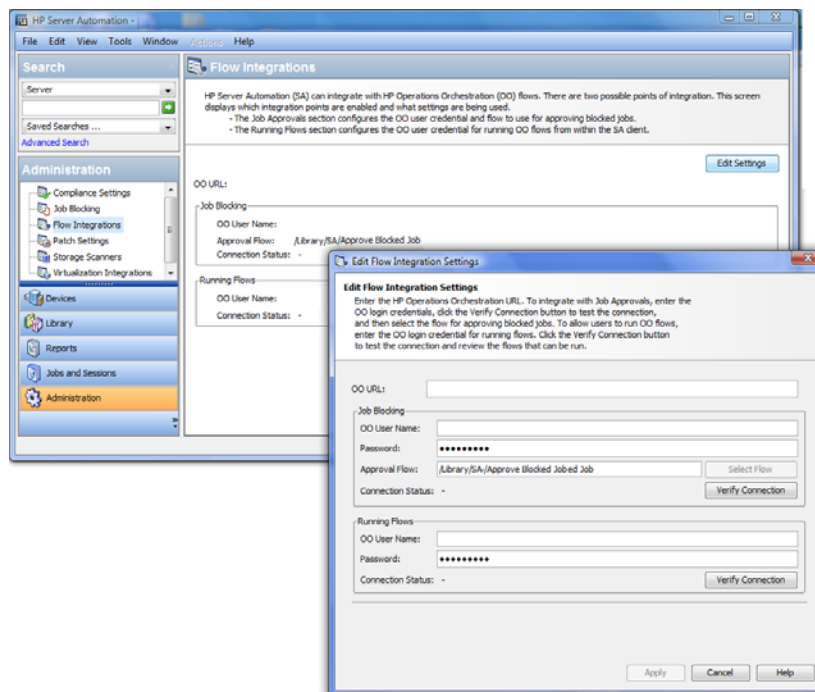
Permission	Description	Check in the SA Client
AdministerFlowIntegrations	Configure the OO integration settings	Select Administration in the navigation panel. If the Flow Integrations option appears in the list of choices in the navigation tree, the permission has been granted.
RunFlowOption (for users 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.

Configuring or Editing a Flow Setting

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 14 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 1](#) 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.

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 3](#), 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 3 Flow Inputs

Flow Inputs	Related to	Automatically Assigned Values (by SA)
coreHost and coreIPAddress	SA Core	Host and IP address of the SA core associated with the SA user who is logged in to the SA Client
coreUsername or coreUser	SA Core	User name associated with the SA user who is logged in to the SA Client
corePassword	SA Core	Password associated with the SA user who is logged in to the SA Client The contents of the field are encrypted.
coreVersion	SA Core	Current SA core version SA provides these values
saServerIdentifier	SA Managed Server	Selected server identifiers: You can set two possible values (in OO): <ul style="list-style-type: none"> • Not Assigned (for one value) • List of Values (for multiple values) - Define the input as a freeFormList type in OO.
saServerScriptName	SA Managed Server	Name of the server script that is available in the SA core for that particular server's operating system Automatically assigned values: None Instead, the SA Client provides a widget that enables users to select a server script (excluding the OGFS script).

Table 3 Flow Inputs (cont'd)

Flow Inputs	Related to	Automatically Assigned Values (by SA)
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>

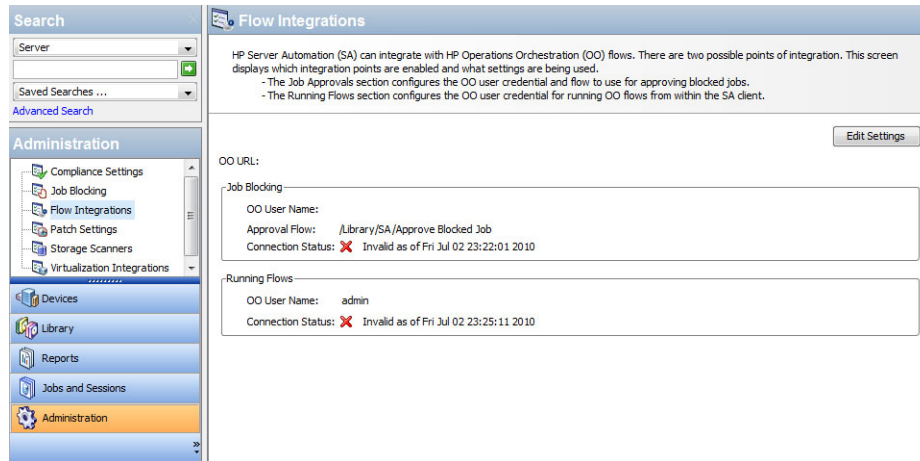
Verifying Your Changes and Settings

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 15 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.

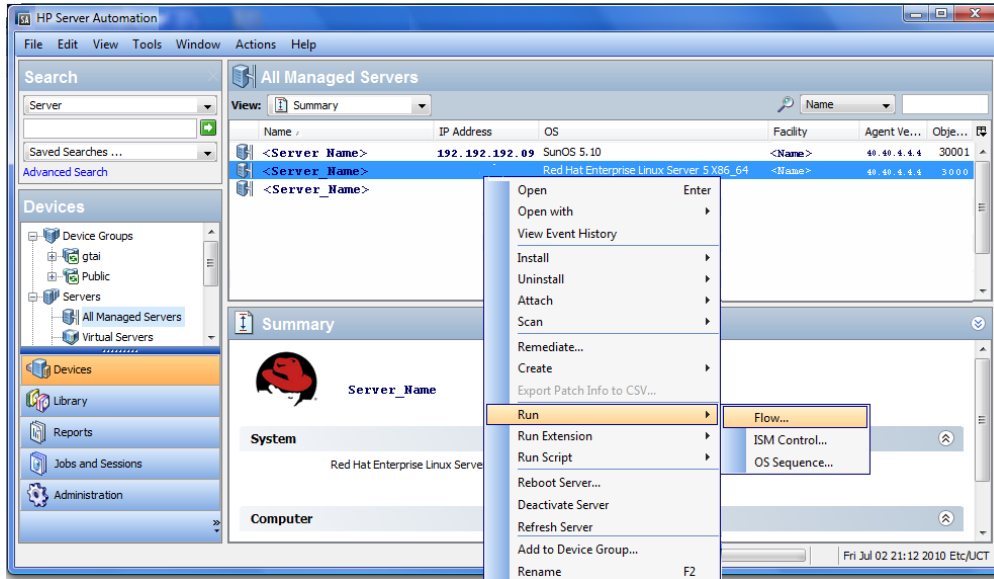
Users must have the Run Flow permission to run flows in SA.

Choosing a Flow to Run

This section describes how to choose a flow to run.

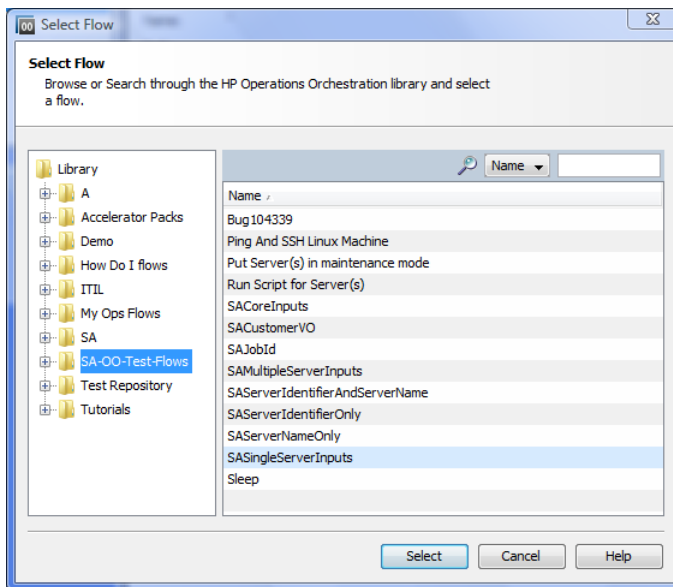
- 1 In the SA Client navigation panel, select Devices.
- 2 In the top panel, select **Servers** ► **All Managed Servers**.
You must select a server before you can select a flow.
- 3 Right-click a server name.

Figure 16 Run Flow Option



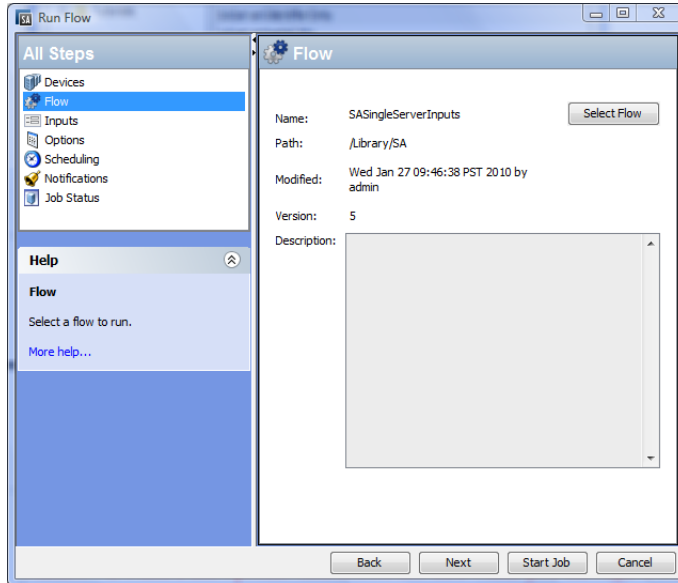
- 4 Select **Run** ► **Flow...** to display the Select Flow OO window.

Figure 17 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 18 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 43.

Adding or Deleting Servers

To add or delete servers, first follow the steps in [Choosing a Flow to Run](#) on page 41, then:

- 1 In the All Steps navigation panel of the Run Flow Window, select Devices.
- 2 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.

- 3 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

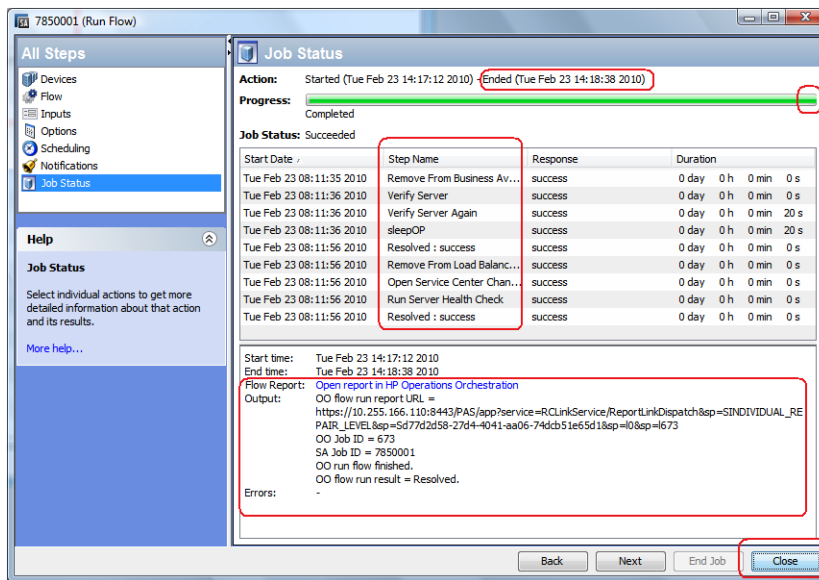
You can enter values for flow inputs, runtime options, scheduling, and notifications. Some parameters will be automatically filled in already.

- 1 Follow the steps in [Choosing a Flow to Run](#) on page 41, 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 3](#) 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 19 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 [Configuring or Editing a Flow Setting](#) on page 37.)
- 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 [Configuring or Editing a Flow Setting](#) on page 37.

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 [Configuring or Editing a Flow Setting](#) on page 37 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.

3 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 47
- [Approving and Deleting Blocked Jobs](#) on page 53

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

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 4 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 4 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?

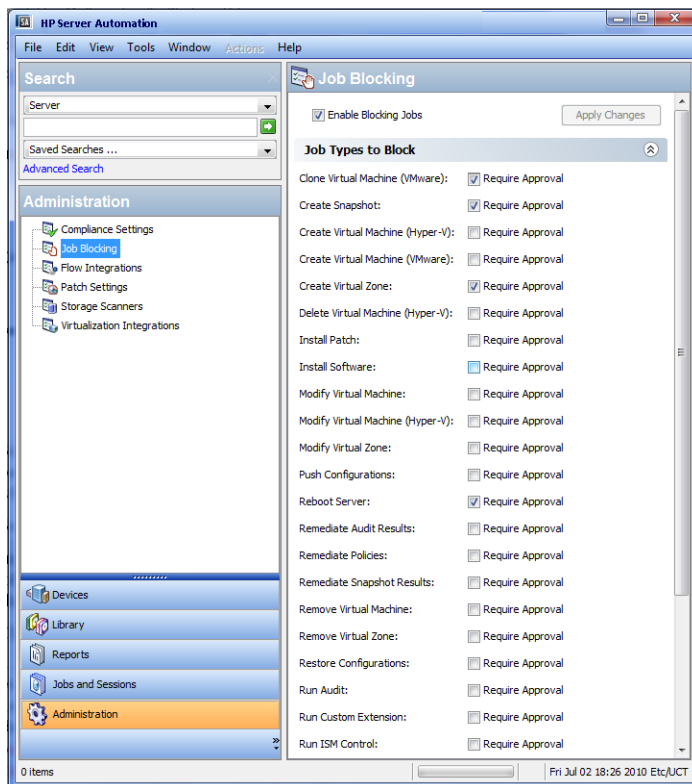
This section describes how to designate job types to block and how to disable job blocking.

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 20 Blocking SA Job Types



See [Table 4](#) 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 20](#).)
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.

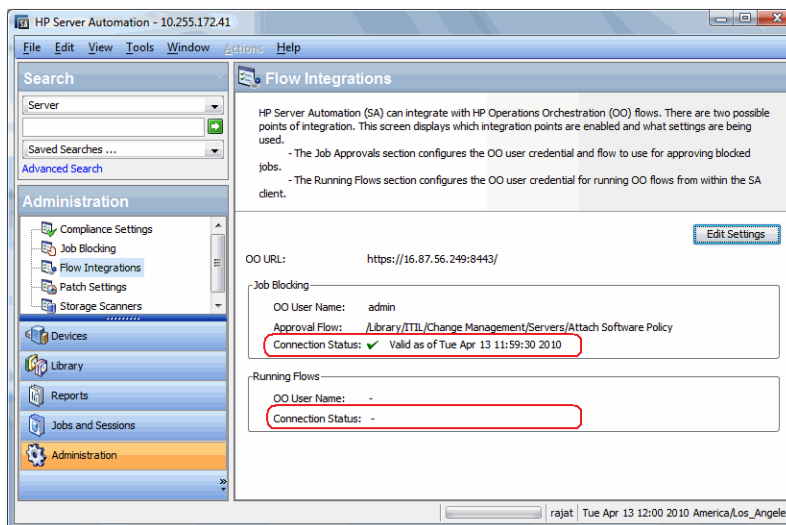
How Do I View Blocked-Job Information?

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 21 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 6](#).

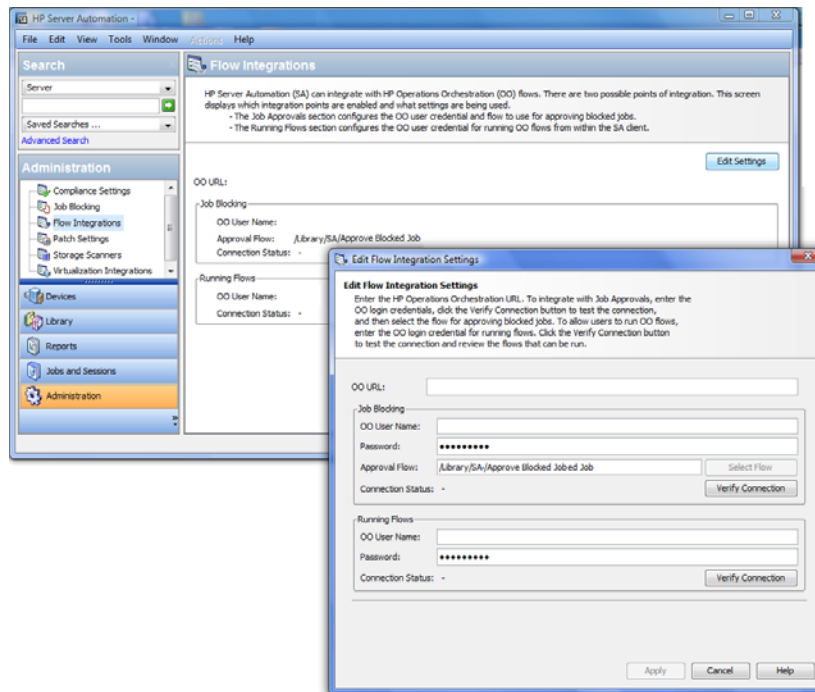
Configuring or Editing a Flow Setting

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 22 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 1](#) 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 (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 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 5 SA JobService Java Methods

Java Method	Method Description	OCLI 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 6 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 6 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	