HP Server Automation

Software Version: 10.23

User Guide: Server Automation

Document Release Date: June 2016
Software Release Date: June 2016

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 Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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.

Support

Visit the HP Software Support Online web site at: **http://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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1

Getting Started with the SA Client

Overview of the SA Client

The SA Client is a powerful Java client for the Server Automation (SA) system. It provides the look-and-feel of a Microsoft Windows desktop application with the cross-platform flexibility of Java.

The SA Client provides the following capabilities:

- Server Discovery and Agent Deployment
- Server Explorer
- Virtualization
- Audit and Remediation
- Compliance
- Server Automation Visualizer (SAV)
- Storage Visibility and Automation
- Software Management
- Patch Management for Windows
- Patch Management for HP-UX
- Patch Management for UNIX
- Patch Management for Solaris
- Application Configuration Management
- Global Shell
- NA/SA integration

Note: To visualize networking information with Network Automation (NA) inside of Server Automation Visualizer (SAV), you must have both a licensed version of NA integrated with your SA core, plus an additional license to run SAV showing NA data.

To visualize storage data in the SA Client, your SA core must be configured to connect to Storage Essentials (SE). For information, see the SA User Guide: Storage Visibility and Automation.

About the SA Client Launcher

The SA Client Launcher allows you to run the SA Client and connect to any of your SA cores. The SA Client lets you view, automate, and manage the devices in your data center.

The SA Client Launcher is a self-contained Java application that allows you to access the SA Client from any core in your mesh. You can use the SA Client Launcher to download the latest version of the SA Client. If the SA Client has been upgraded on a specific core or on a core in a different mesh, you can choose which core you would like to use for downloading the SA Client.

You also have the option of choosing which core you want to use to download the latest version of the SA Client, separate from the core you log in to. For example, when you log into a core and that core has a new version of the SA Client, the new version will automatically be downloaded when you log in. Using the launcher, you can choose one core to log in to and a separate core to download the latest client. This gives you the freedom to not have to download the SA Client every time you log into a different core.

The SA Client Launcher also allows you to configure advanced settings, such as debug settings, locale settings, proxy server settings, and more. See SA Client Launcher Advanced Options.

Note: If you are running the SA Client Launcher on Windows 2000, you may see a missing DLL error message when you log on. This error will not affect the log on procedure. To fix this so the error message does not appear, install this Microsoft update: http://support.microsoft.com/default.aspx?scid=kb;en-us;259403&Product=vc6.

SA Client and SA Client Launcher Requirements

The SA Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). The SA Client will not interfere with any other JRE versions installed on your system. The JRE will not be used (and is not usable) by any other Java application on the target computer, and it will not set itself as the default JRE on the target computer.

Note: The SA Client runs on most Microsoft Windows operating systems. For a list of the specific operating systems, versions, and system requirements for the SA Client, see SA Client Platforms in the SA Support and Compatibility Matrix.

You must download and install the SA Launcher (see the download button on the SA Client home page). In order to install the launcher, you must be a Windows user that has permission to install applications on your system.

Installing the SA Client Launcher

To run the SA Client, you first need to download and install the SA Client Launcher, which is a Java application that allows you to access the SA Client from any core in your mesh. When you install the SA Client Launcher, it installs all of the necessary Java applications (Java Web Start and JRE) you need to run the SA Client.

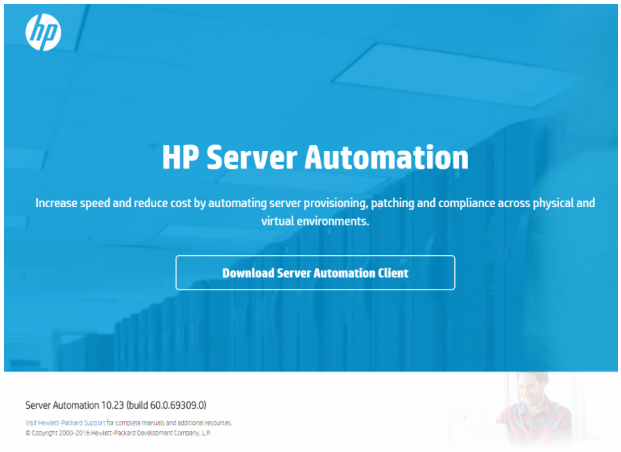
If you are upgrading, you will need to do the following:

a. Uninstall the previous version of the SA Client Launcher using the Windows uninstallation utility.
b. Ensure that there are no running instances of the Launcher.
c. Install the latest SA Client Launcher version, as described below.

To install the SA Client Launcher, perform the following steps:

1. Open any web browser and enter the URL to any SA core server. This displays the SA Web Client home page along with a button to download the SA Client launcher, as shown in Downloading the SA Client Launcher.

Downloading the SA Client Launcher



2. On the SA Web Client home page, click the **Download Server Automation Client** button.
3. Save the SA Client Launcher installation file. The installation file is typically named `hp_bsa_launcherinstaller_windows_x_x_x.exe`.
4. Locate and double-click the installation file to start the SA Client Launcher installer.
5. Follow the installation instructions.

Running the SA Client

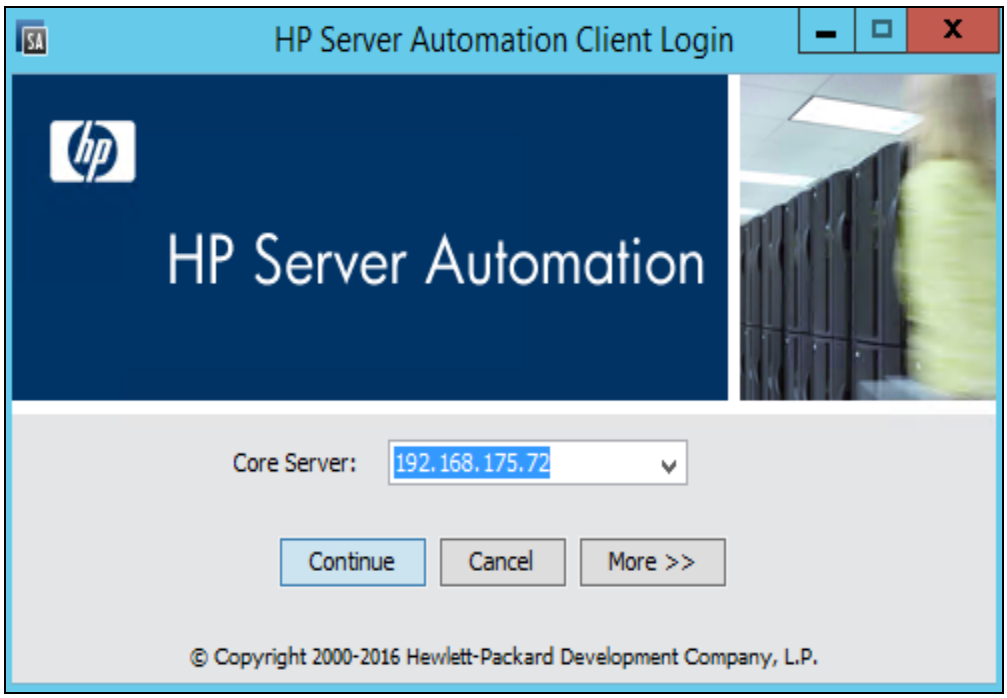
To run the SA Client, perform the following steps:

1. Start the SA Client from one of two locations:
   - On your desktop, double-click the HPE Server Automation Client icon.

   Or

   - From the **Start** menu, select > **All Programs** > **HP Business Service Automation** > **HP Server Automation Client**
2. The first time you open the SA Client, at the login window, enter the IP address for the SA Core server you want to log in to , as shown in SA Client Login Window .

SA Client Login Window

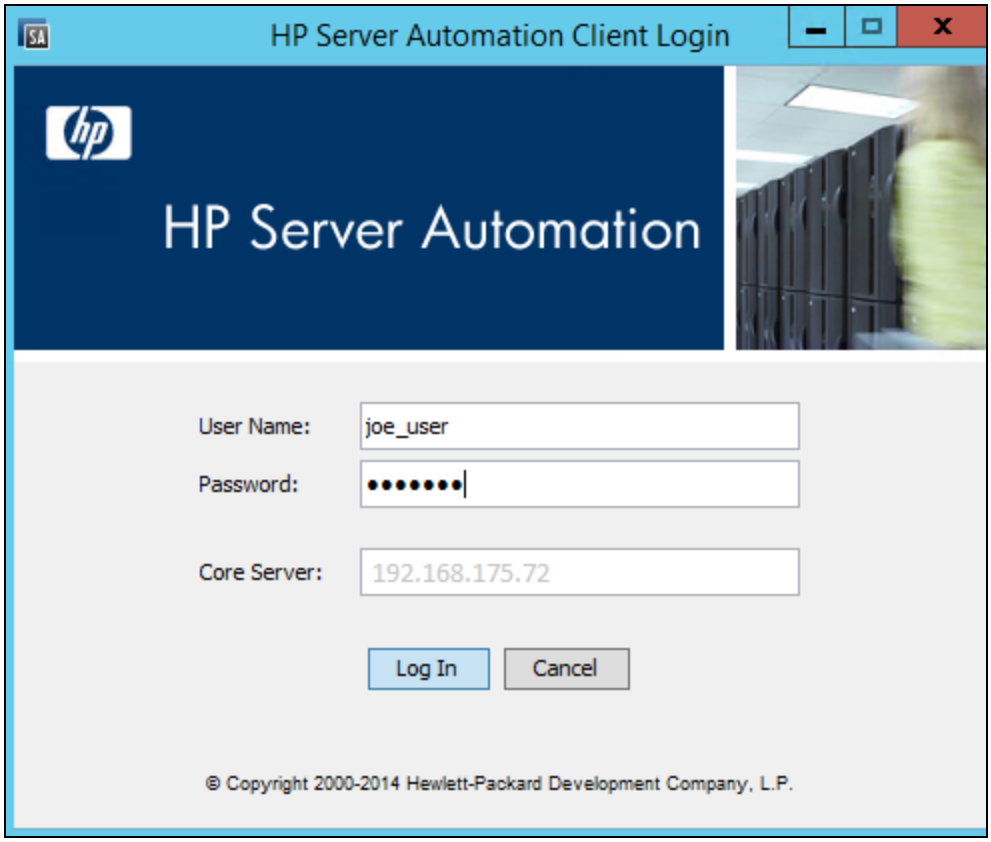


Press **Continue**. If this is the first time you are logging in to a specific core, the launcher will download the latest version of the SA Client when you log in. If you want to differentiate between the core you log in to and the core from where you download the latest version of the SA Client, you can change those options by clicking **More** in the log in window and configuring your Client Host Server.

For information on this and other advanced SA Client Launcher options, see SA Client Launcher Advanced Options.

3 If you are asked to trust the application, click **Start**. If the SA Client User Name and Password window does not appear, check your proxy settings and other settings. See SA SA Client Launcher Advanced Options.

4 After SA Client has been downloaded, a new window appears as shown in the following figure. If this is the first time you are logging in to SA Client, at the login window, enter the username **admin** and the password **opsware_admin**. You will be prompted to change the admin password. The user name is not case sensitive. If you have access to more than one core server in a mesh, you can enter the core server's IP address or name in the core server field. If you do not specify a port with the host:port notation, port 80 is used to download the SA Client.



5 Click **Log In**.

6 If you are asked to accept the certificate from the core server, click **Yes**. The SA Client appears.

SA Client Launcher Advanced Options

You can configure the following advanced options for the SA Client:

- **Debug Settings**: Gives you control over the level of detail as well as the type of information included in SA Client log file.
- **Client Download Server**: Allows you to change the host server from which you want to download the SA Client.
- **Proxies**: Allows you to configure the SA Client proxy server settings.
- **HPE Server AutomationHome**: Allows you to change the default location SA Client is downloaded and saved on your local computer, and to delete the SA Client's cache, and to change the location of SA Client log files.

To configure the SA Client Launcher's advanced options, perform the following steps:

1 Start the SA Client Launcher from one of two locations:

— On your desktop, double-click the SA Client Launcher icon

Or

— From the **Start** menu, select > **All Programs** > **HP Business Service Automation** > H**P Server Automation Client**

2 In the Log In to HPE Server Automation window, you can set the following configuration:
   - **Core Server**: Choose the SA core server to log in to.
3 Select the **More** button. In the expanded launcher window you can configure the following settings:
   - **Locale**: Select the version of the SA client to match your system's locale. English (en) is the default, but you can also select either Japanese (ja) or Korean (ko).

     Note that this locale setting is only used on cores previous to SA version 9.10. As of SA version 9.10 this setting is ignored and the setting in the user profile is used instead. For complete information on setting the locale in the user profile for each individual user, see the SA Administration Guide.
   - **Debug Settings**: Debugging options that are captured in the following log file: `<user_home>\Application Data\HP BSA\deployment\log\javaws\*.log`
     - **Enable Debug Logging (Fine)**: Enables debugging and sends SA Client operations and errors to the log file.
     - **Enable Server Method Call Logging**: Adds server method calls to the log file.
   - **Show Console**: Displays the Java Console window while the SA Client runs.
4 Click **Advanced Settings**.
5 In the Advanced Settings window, you can configure the following SA Client Launcher options:

   Client Download Server

   You can configure the SA Client Launcher so the default core you log in to is different from the core you use to access the latest version of the SA Client. This can be useful if you do not want to download a new version of the SA Client each time you log in to a different core running the same version of SA.
     - **Use Core Server**: Select this option to download the SA Client from the same server you want to log in to.
     - **Use**: Enter a core server you want to use to download the SA Client.

Note: The SA Client uses two ports: port 80 to download the SA client; port 443 to connect to the core specified in the main log in window. If you select the Use Core Server option, the connect port (443) cannot be overridden. If you select the Use option, the download port (80) can be overridden in the Use field and the connect port can be overridden in the Core Server field in the main log in window.

If you do not specify a port with the host:port in the Use field, port 80 is used to download the SA Client. In the Core Server field in the main log in window, if you do not specify a host:port, then port 443 is used to connect to the core.

   Proxies

   By default, the SA Client uses the proxy server settings configured for the default browser on your local system. For example, if your default browser has no proxy server settings configured, neither will the SA Client. You can change those proxy server settings here:
     - **None**: Do not use a proxy server to connect to the SA Client.

- **Use Browser**: Use the proxy server settings specified in your default browser.
- **Manual**: Enter the proxy server hostname and port.
- **No Proxy Hosts**: If you want to add proxy server overrides, add them here, separated by commas. (This is only enabled when proxy server settings is set to Manual.)

HPE Server Automation Home

- **Location**: The location where the SA Client is downloaded and saved on your local computer, along with all log files generated when the SA Client runs.

  Note that starting with SA 7.50, this location also controls where the SA Client data cache is stored.

Note: The default home location is `<user_home>\Application Data\HP BSA`, which is private to each user. If you choose to change this location, be aware that other users may have access to the new directory. You are responsible for setting the permissions on the new directory if you want to prevent unwanted access to your SA Client home.

- **Delete Application Cache**: Clicking this completely removes all downloaded copies of the SA Client. This ensures the launcher will download the latest SA Client from the core the next time the user logs in.
- **Delete Logs**: Delete all log files created by previous sessions of the SA Client. (All SA Client log files are located at: `<user_home>\Application Data\HP BSA\deployment\log\javaws\*.log`)

6 When you are finished setting the options, click **OK** to save your settings.

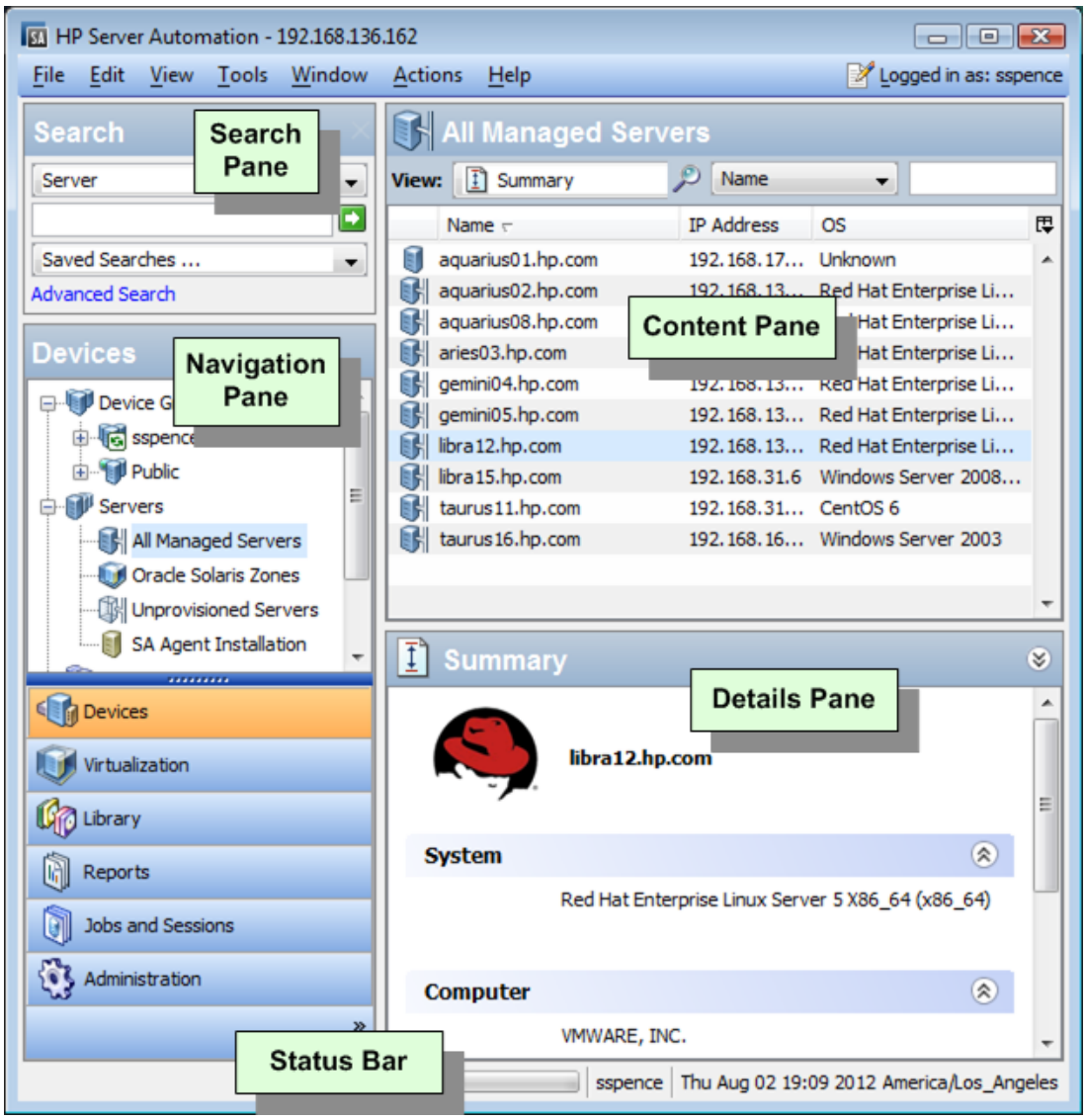
7 Click **Log In** to log in to the SA Client.

SA Client User Interface

The SA Client user interface has six main areas as shown in SA Client User Interface.

- Menus
- Navigation Pane
- Search Pane
- Content Pane
- Details Pane
- Status Bar

SA Client User Interface



Menus

The SA Client includes the following menus:

- **File**: This enables you to open a new SA Client window, or close the current window, or exit all open SA Client windows.
- **Edit**: This enables you to cut, copy, paste, delete text, and copy SA Client URLs.
- **View**: This refreshes the current view and shows the latest information from the core that you are currently logged into (such as compliance test information for the compliance dashboard). You can also access SA Client features in the Navigation pane, such as Devices (groups of devices, managed and unmanaged servers), Reports (Compliance Dashboard, Reports) Software Library (application configuration, patch management), OS sequences and OS installation profiles, Jobs and Sessions (job logs and shell

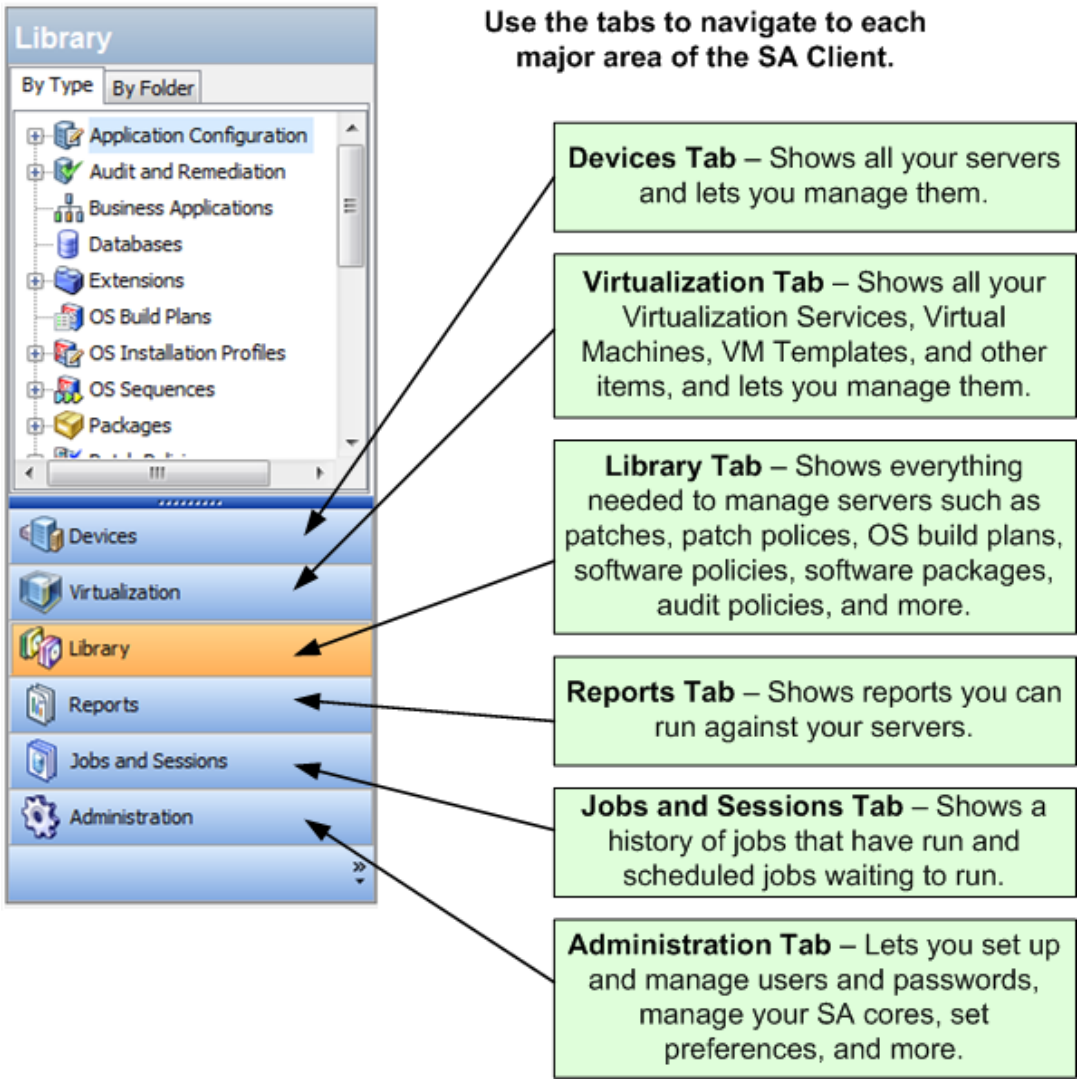
sessions), and Administration (patch settings and patch compliance rules). This also allows you to show or hide the Search pane and the Details pane.

- **Tools**: This enables you to open a Global Shell session, open the Server Automation Visualizer, or access the SA Client options.
- **Window**: This enables you to access multiple instances of SA Client windows, if more than one window is open.
- **Actions**: Depending on the feature that you have selected in the Navigation pane, this menu enables you to perform numerous functions related to all main SA Client features.
- **Help**: This menu provides help for the SA Client. Help F1 provides context-sensitive help relevant to the current feature window selected or opened (same as pressing the F1 key). The contents and index will open the SA Client help system to the main table of contents. (Select About HP Server Automation to see version and system information.)

Navigation Pane

The Navigation pane shown in SA Client Navigation Pane shows the tabs in the SA Client navigation pane. Each tab gives you access to one of the major areas of the SA Client. When you select an object, its contents appear in the top of the navigation pane and in the content pane. You can perform tasks related to the object with the right click menu and the Actions menu.

SA Client Navigation Pane



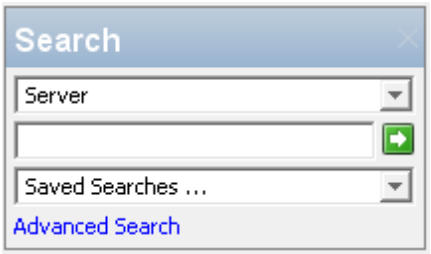
Search Pane

The Search pane allows you to search for any information in Server Automation, such as servers, device groups, folders in the SA library, jobs, software and software policies, patches and patch policies, application configurations, database and storage systems, audits, and snapshot results.

You can show or hide the Search pane by selecting the **View > Search Pane** menu item.

For more information on how to use the search tool, see Searching for Objects with the SA Client.

Search in the SA Client



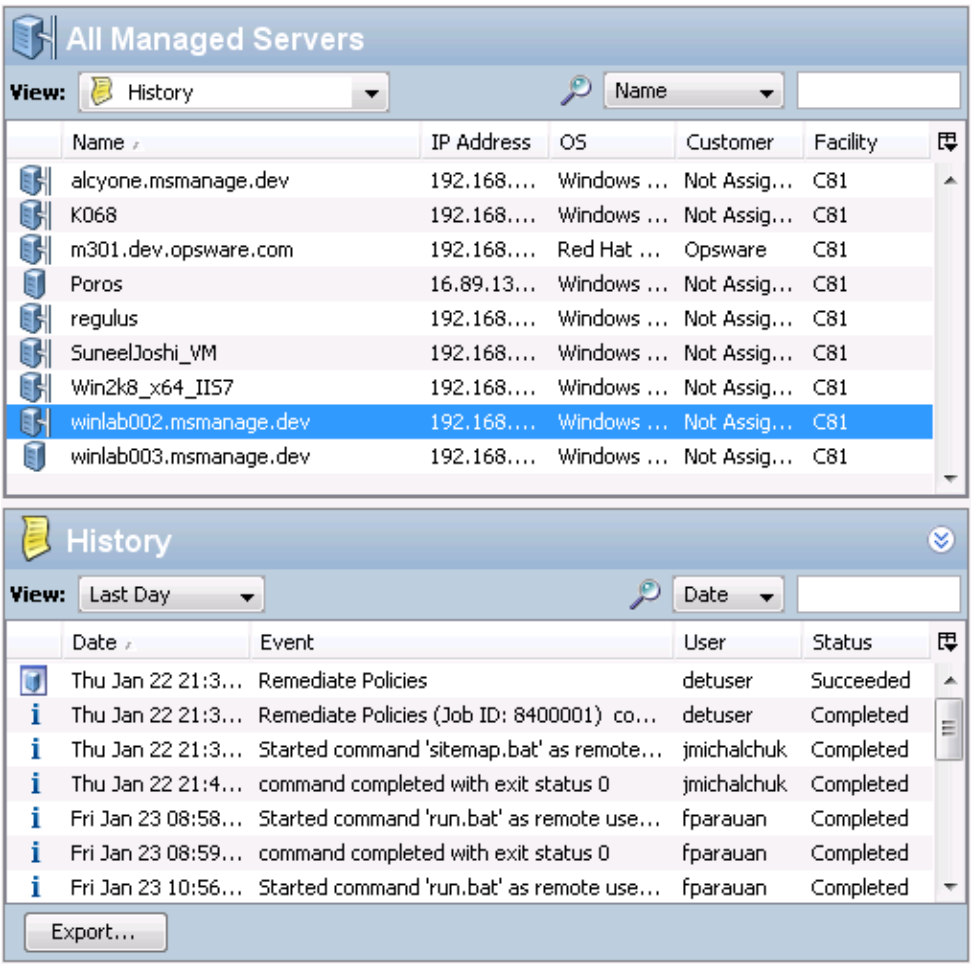
Content Pane

Depending on the selection in the Navigation pane – Devices, Virtualization, Library, Reports, Jobs and Sessions, Administration – the Content pane lists the following information:

- All managed servers and device groups, including agentless servers — both physical and virtual
- Virtualization Services and the virtualization inventory under them
- Agent installation information
- Application Configurations and configuration templates
- Software Policies
- Storage objects and their attributes
- Audit and Remediation audits, audit policies, and snapshots
- Patches and patch policies
- OS installation profiles and OS sequences
- Packages
- Reports and the Compliance Dashboard
- Custom attributes
- Jobs that the user has run
- Access to the Global Shell sessions
- Patch configuration and patch compliance rules

Content Pane Showing the Server History View is an example of the Content pane for managed servers. You can perform actions on features in the Content area using the Action Menu, or you can right-click to perform various actions or double-click to open.

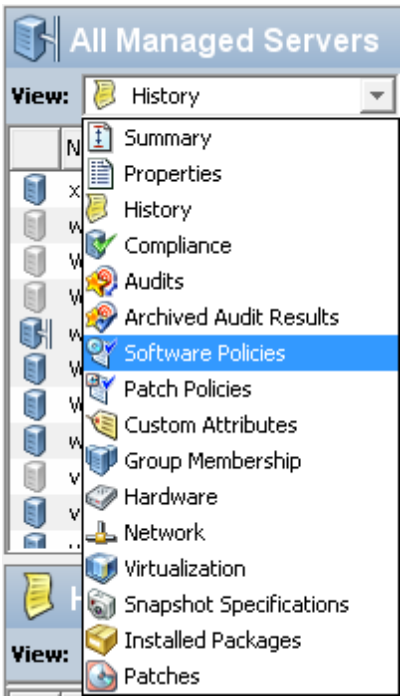
Content Pane Showing the Server History View



Views in the Content Pane

With the View drop-down list in the SA Client content pane, you can change the view of a selected feature. For example, you can select a server from the Content pane, and then from the View drop-down list, choose Software Policies. This shows all software policies attached to the server, as shown in View Drop-down List .

View Drop-down List

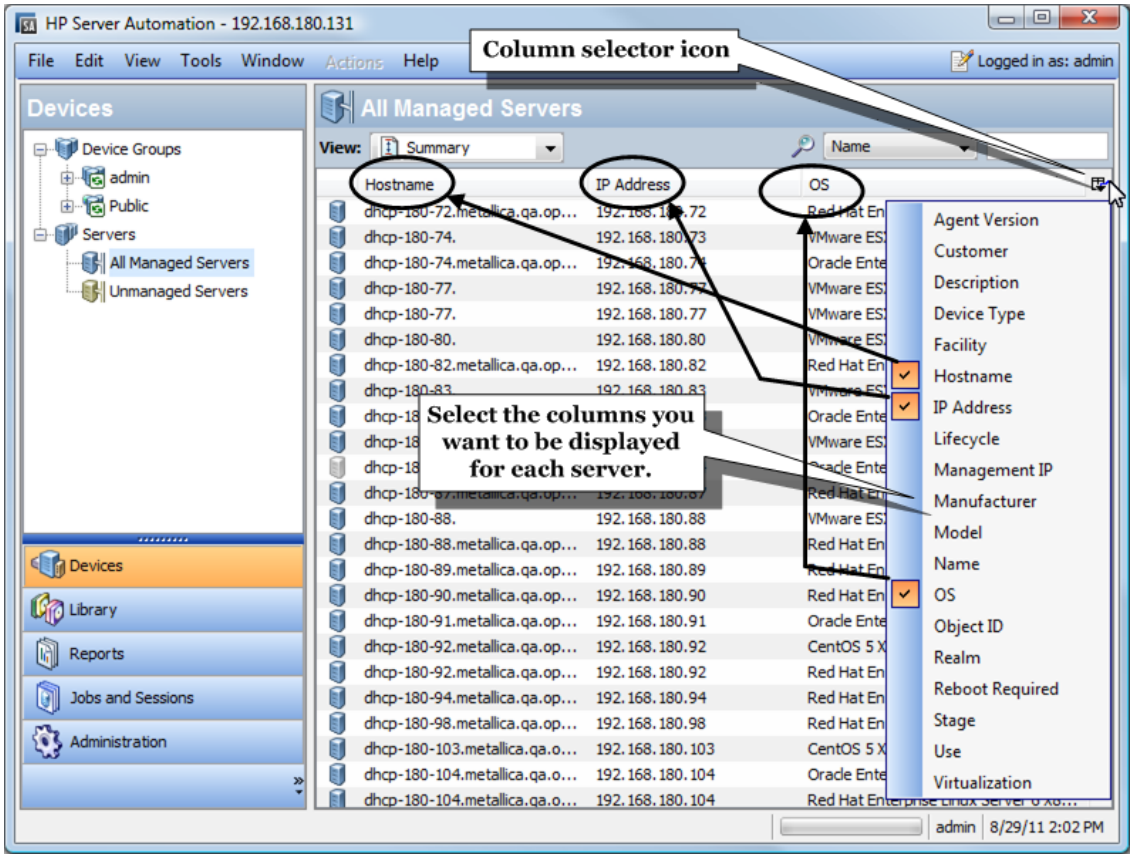


Columns in the Content Pane

You can click the column headings of the Content pane to sort data about a server. For example, for a managed server, you can sort by Hostname, IP address, Summary, OS, and so on. You can sort by additional columns by pressing the Ctrl key on the keyboard while clicking another column.

You can display more columns of information about the selected server by clicking the column selector and choosing the columns you want to display or hide, as shown in Column Selector - Columns Displayed for Each Server below.

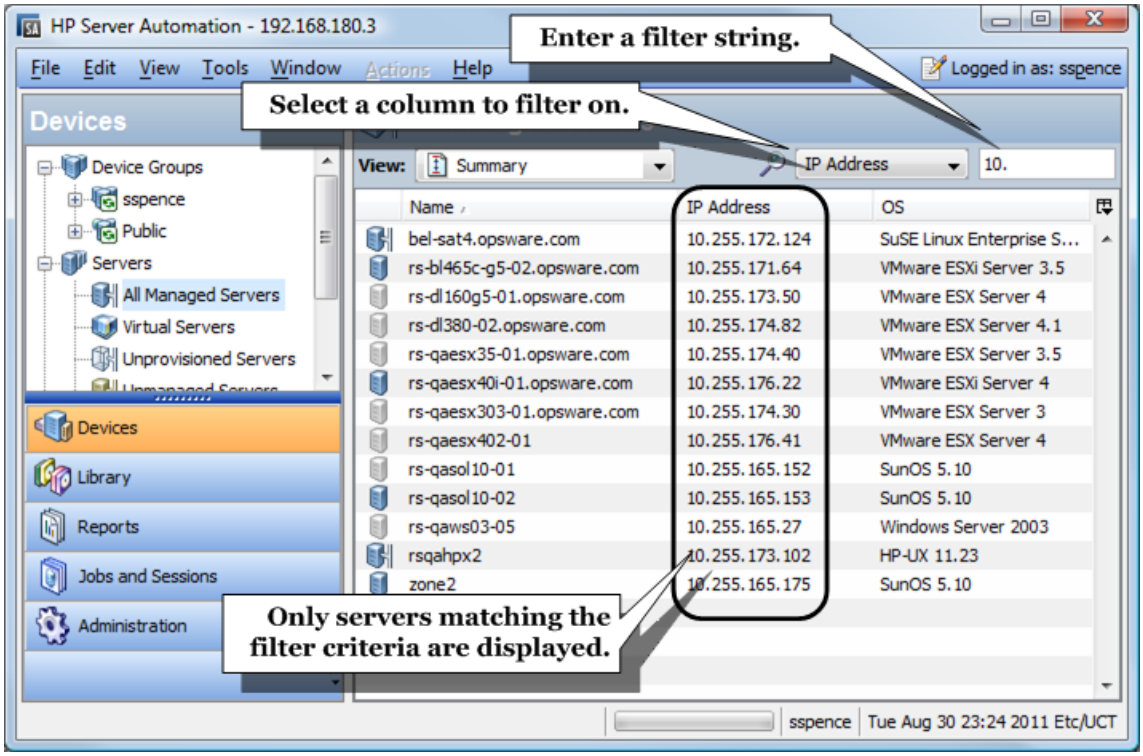
Column Selector - Columns Displayed for Each Server



Filter Tool in the Content Pane

With the SA Client filter tool, you can filter the information shown on the content pane by filtering on a single column with a substring search, as shown in Filter Tool below.

Filter Tool



Details Pane

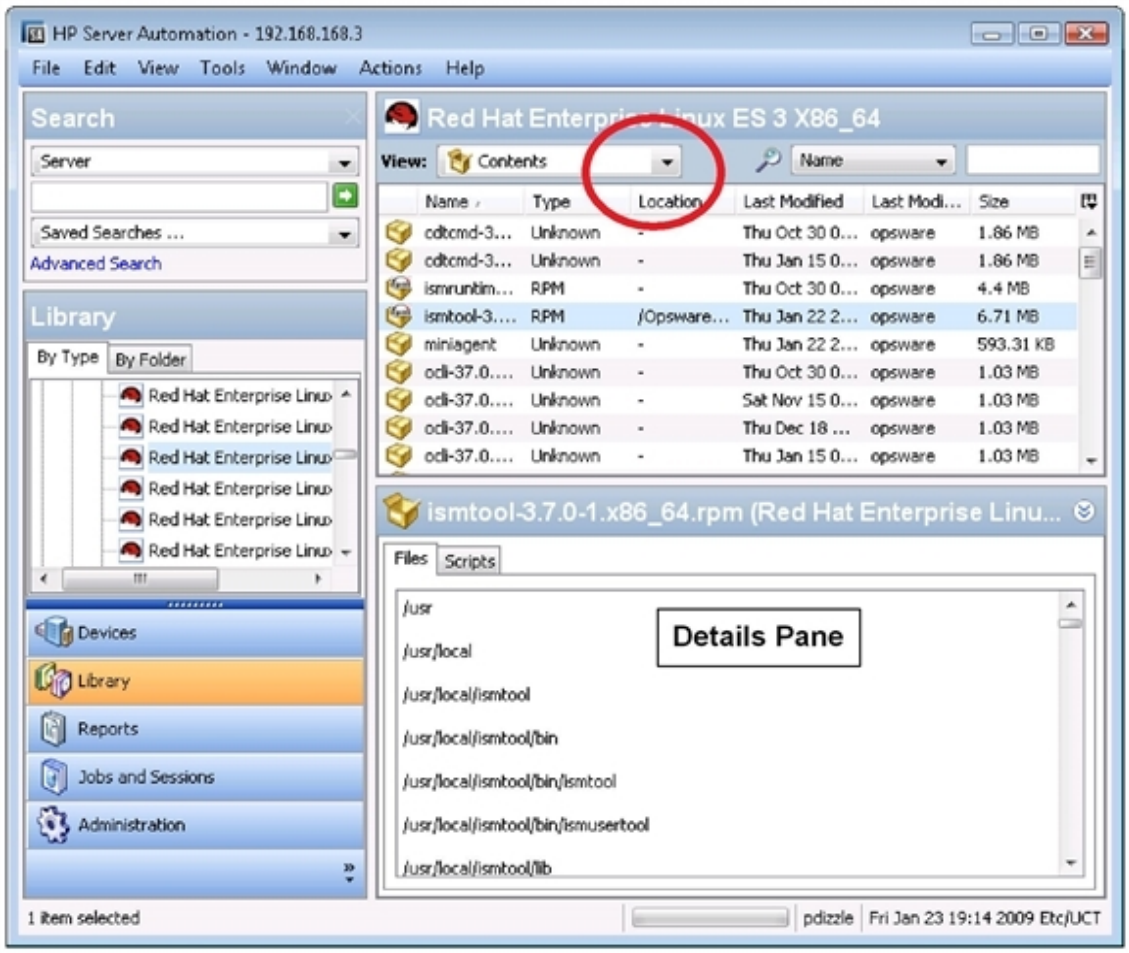
The Details pane allows you to preview information about servers, device groups, patches, and patch policies selected in the Content pane without having to open a new window.

You can use the Details pane to perform the following actions:

- Preview information about a server, device group, patch, or patch policy. To do so, select it in the Content pane.
- Select the type of information you view in the Details pane. From the top of the content area, choose a view from the View drop-down list.
- Deactivate the Details pane. To do so, from the **View** menu, select **Details Pane** > **Minimize**.

For example, if you are viewing Windows 2003 patches from the Library, you can select a patch in the Content pane and see information about the patch in the Details pane. This is shown in SA Client Showing Package Contents View in the Details Pane .

SA Client Showing Package Contents View in the Details Pane



To view other types of information about the selected patch, from the View drop-down list, choose a view.

Details Pane Show Filter

Some features displayed in the Details pane allow you to further filter the feature. Using the Show drop-down list, you can choose different views of the feature.

For example, if you are viewing all of the servers that the patch policy is attached to, in the Details pane, you can filter either Servers with Policies Attached or Servers with Policies Not Attached, as shown in Details Pane Show Drop-down List .

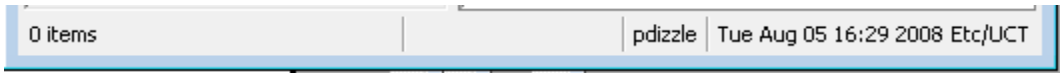
Details Pane Show Drop-down List

Status Bar

At the bottom of the SA Client window, the status bar provides the following information:

- Information about the selected object
- A progress bar that shows progress on retrieving information from the core
- Your user ID
- The current time

SA Client Status Bar



Sharing SA Client Objects with Drag and Drop

You can easily drag and drop servers and other SA Client objects out of the SA Client and into an email, a chat window, or a document editor. When you drag an object out of the SA Client, a URL is constructed that enables you to launch the object in the SA Client.

You can share such SA Client objects as servers, application configurations, audits, a Business Application, Patch Policies, OS Profiles, and more — basically, any device (server, storage, network, and so on) or any object from in the SA Library that is searchable.

You can also use the URL that is created during drag and drop as a link on a web page, which gives you easy access to those SA objects you are most interested in.

Note: In order to drag and drop networking devices from the SA Client, you must have a licensed version of Network Automation (NA) integrated with your SA core. Additionally, in order to drag and drop storage devices from the SA Client, SA core must be configured to connect to SE. For more information, contact your HP sales representative.

To drag and drop a SA Client object, perform the following steps:

1. From inside the SA Client, select a server, network or storage device, device group, Patch Policy, a Business Application, an audit, or any other object in a table.
2. CTRL+drag the selected object to one of the following locations:
   - Document editor
   - Chat window text entry box
   - Email
3. When you or another user clicks the link, you are asked to open or save the file. After the file is downloaded and saved, click **Open**.
4. In the HP Server Automation Client Login window, enter the SA core server you want to log in to and click **Continue**. In the next window, enter your SA user name and password and click **Log In**.

If the SA Client is already opened, and the object you are opening belongs to the core you are logged into, the object appears in its own window without requiring you to log in.

Besides CTRL+drag, you can also use the **Edit** > **Copy** menu, or SHIFT+CTRL+C to copy the link into the Windows clipboard, and then paste it into another application.

Copy and Paste Table Data

In this release, you can copy and paste data from tables inside the SA Client into other applications. For example, if you are viewing a list of managed servers, Windows Audits, Solaris 10 patches stored in the SA Client Library, or jobs scheduled to run in the next month, you can select one or more rows in the list, and then copy and paste them into a text file, email message, spreadsheet application, or other document processor.

The following restrictions to this capability:

- Column headings for a list are not selectable. This means that they are always copied.
- Values in the copied list might appear differently when pasted into a target application, depending on how the target application renders tables.
- The target application must understand a table description either in HTML format (with mimetype “text/html”) or as a tab/newline delimited string (with mimetype “text/plain”)

To copy and paste table data in the SA Client, perform the following steps:

1. From inside the SA Client, browse to the table that you want to copy.
2. Make sure that the application you want to paste the data into is open.
3. Select the rows you want to copy.
4. To copy the rows, perform one of the following actions:
   a. Press CTRL + C.
   b. From the **Edit** menu, select **Copy**.
   c. Use the cursor to drag the rows.
5. In the application you want to paste this data into, place the cursor and press CTRL + V or drop the rows if you are dragging them with the cursor. The data is copied.

Searching for Objects with the SA Client

In the SA Client, you can search for objects in your operational environment including physical and virtual servers, application configurations and templates, audits, business applications, device groups, SA extensions, folders, jobs, scripts, packages, patches, patch policies, snapshots, software policies, and many other objects.

Note: To search for storage devices in the SA Client, your SA core must be configured to connect to Storage Essentials. For more information, contact Support.

With the SA Client search you can:

- Perform a simple search by using keywords, or an advanced search using search queries.
- Save and reuse search queries.

- Perform various actions based on search results.
- Email search results.
- Print search results.
- Customize the formatting of your search results.

Performing a Simple Search

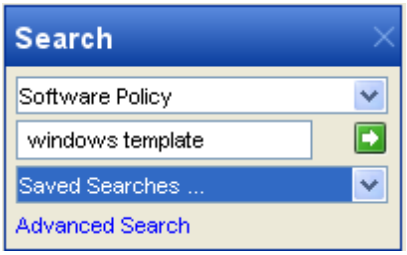
A simple search locates objects containing the text you entered.

Note: The search operation returns only items on which you have at least read permissions. To perform an action on an item, you must have write permission on that item. For more information on permissions, see the SA Administration Guide.

To perform a simple search, perform the following steps:

1. If the Search pane is hidden, select the **View > Search Pane** menu.
2. From the drop-down list in the Search Pane, select the type of object you want to search for, such as Software Policy, as shown in Simple Search in the SA Client .

Simple Search in the SA Client



3. Enter the search text in the text field. The text field does not support wildcards and the search is not case sensitive.
4. Click to perform the search. The results appear in the Content pane.
5. (Optional) Click on any column heading to sort the search results. You can also change the order of the columns by dragging the column heading and dropping it in the desired location.
6. (Optional) Click **Save** to save your search query. The Save As dialog appears. Enter the name of the search and then click **Save**. The name of the saved search cannot exceed 64 characters. See Creating a Device Group Using Search for more information about saving a search query as a device group.
7. (Optional) Click **Export** to export search results to a csv or html file. The Export Results window appears. Enter the location, file name, and file type and then click **Export Results**.
8. (Optional) To perform an action on the search results, select an item from the Content pane and then from the **Actions** menu, select the appropriate action.

About Advanced Searches

With advanced search you can create complex search queries. You can specify multiple search rules and combine each rule with a logical “And” or logical “Or” operator. You cannot use both the “And” and “Or” operator in a single search query.

Note: You can create more complex logical expressions using the SearchService interface in the com.opsware.search package of the SA Twister API. For more information on the SA Twister API, see the SA Platform Developer Guide.

Each rule is a combination of an attribute, operator, and value that enables you to search for a specific attribute value for the selected search item. Depending on the attribute that you select, the options for the operator and value are displayed. You can specify the attribute values by entering text or a numerical value in the text field, by selecting a value from the drop-down list, or by selecting multiple values from a list of values in the Select Values window.

The Select Values window appears when you need to specify multiple values for a rule containing an “equals” or “not equals” operator. In this window, you can select one or more values from a list of available values.

Format of Advanced Search Rules

Advanced search rules take the following form:

Search for: **<***Item***>**

Where: **<***Attribute***> <***Operator***> <***Value***>**

- <*Item*> is the object you are searching for, such as servers, patches, patch policies, storage devices, jobs, folders and other items in your managed environment.
- <*Attribute*> is data about the item you want the rule to examine.
- <*Operator*> is a comparison you want to perform between the <*Attribute*> and the <*Value*>.
- <*Value*> is the specific data you want to compare to the <*Attribute*> using the <*Operator*>.

Note: The search operation returns only items on which you have at least read permissions. To perform an action on an item, you must have write permission on that item.

Performing an Advanced Search

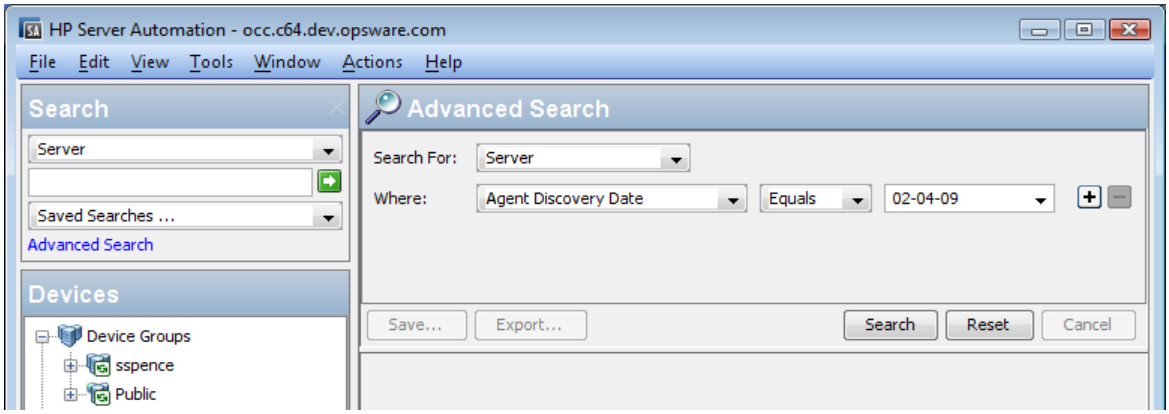
To perform an advanced search, complete the following steps:

1. If the Search pane is hidden, select the **View > Search Pane** menu.
2. From the SA Client navigation pane, select **Advanced Search**. The Advanced Search page appears in the Content pane.

   By default, the Search For “Server” item is selected in the first drop-down list and one search rule is added to the search.

3 From the Search For drop-down list, select the type of object you want to search for. SA Client Search shows "Server" as the item to search for.

SA Client Search



4 Create a rule by selecting the attribute from the first "Where" drop-down list. The figure above shows "Agent Discovery Date" as the search attribute. Depending on the attribute that you select, the operators and values for the rule will change.

5 Select the operator from the second "Where" drop-down list. The operator selected defines how the search text is treated. SA Client Search shows "Equals" as the operator.

6 Enter a value in the field or select a value from the drop-down list or click ... to select one or more values from the **Select Values** window. SA Client Search shows "02-04-09" as the value for the Agent Discovery Date.

The example in SA Client Search will search for all servers on which the agent discovery date is Feb 4, 2009.

7 (Optional) Click + to add rules and repeat steps 3 to 5.

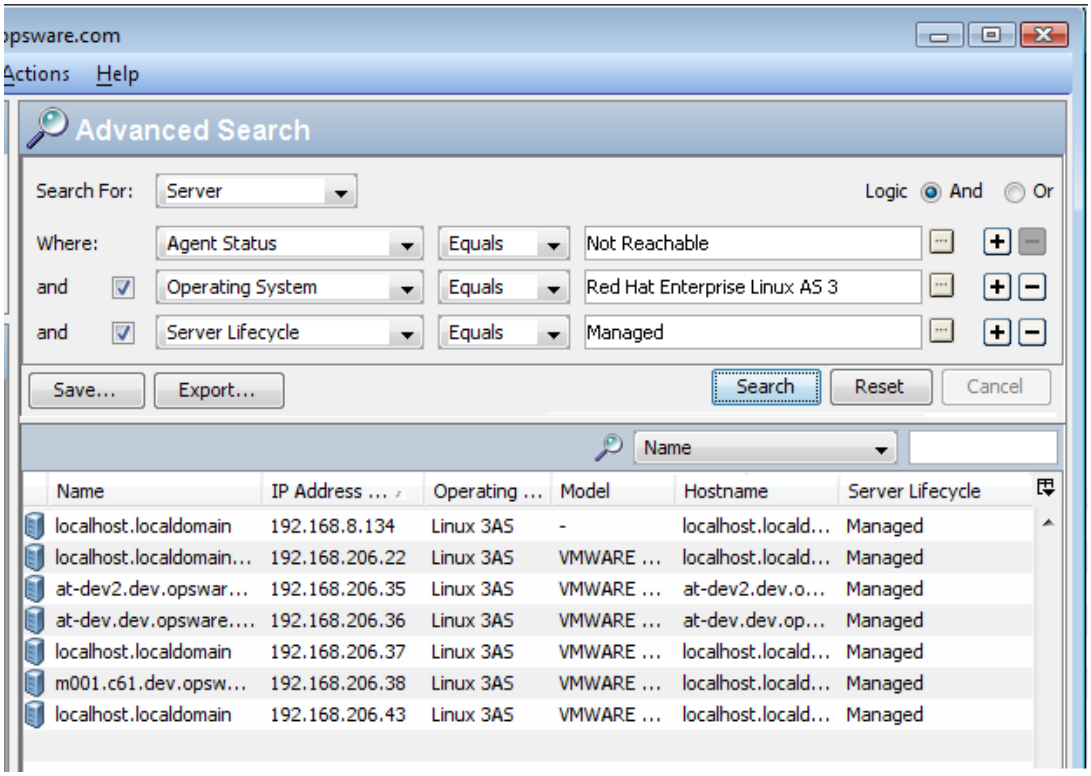
8 (Optional) Click − to delete any rules.

9 Select the Logic (logical And or logical Or) to be applied to the rules in the query.

10 Click **Search** or press Alt-S to run the search query. The search results appear in the Content pane.

Server Search Results for Servers with Unreachable Agents shows a search for all servers with unreachable agents that are running Red Hat Linux AS 3, with the Server Lifecycle value set to "Managed".

Server Search Results for Servers with Unreachable Agents



11 (Optional) Click **Reset** to clear the search query rules or click **Cancel** to cancel the search operation.

12 (Optional) Click on any column heading to sort the search results. You can also change the order of the columns by dragging the column heading and dropping it in the desired location.

13 (Optional) Click **Save** to save your search query as a csv or html file. The Save As dialog appears. Enter the name of the search query and click **Save**. The name of the saved search cannot exceed than 64 characters. The saved search query appears in the Saved Searches drop-down list. See Creating a Device Group Using Search for more information about saving a search query as a device group.

14 (Optional) Click **Export** to export search results to a csv or html file. The Export Results window appears. Enter the location, file name, and file type and then click **Export Results**.

15 (Optional) To perform an action on the search results, select an item from the Content pane and then from the **Actions** menu, select the appropriate action.

Running a Saved Search Query

To run a saved search query, perform the following steps:

1 If the Search pane is hidden, select the **View > Search Pane** menu.

2 From the Saved Searches drop-down list, select a search query. The query appears in the Advanced Search Content pane. The query is automatically executed and the search results appear in the Content pane.

Deleting a Saved Search

To delete a saved search query, perform the following steps:

1. If the Search pane is hidden, select the **View > Search Pane** menu.
2. From the Search pane, in the Saved Searches drop-down list, select a search query that has been previously saved. The saved search is displayed in the Advanced Search Content pane.
3. Click **Save** to display the Save As dialog box**.**
4. Select the saved search, right-click, and then select Delete.
5. In the "Delete existing search" dialog box, click **Delete**.
6. Click **Cancel** to exit the Save As dialog box.

Setting SA Client Options

You can configure the following options for the SA Client:

- General Options: This enables you to set options such as choosing the core you want to log into by default, how to handle caching, and so on.
- SA Agent Installation - Installer Options: This enables you to change the default behavior when installing server agents on your servers. The server agent enables SA to manage your servers. For more information, see Server Agent Management.
- Terminal and Shell Options: This enables you to configure your Terminal (UNIX) and RDP (Windows) client for the Global Shell and Remote Terminal connections.
- Patch Policy Options: This enables you to specify that a confirmation message will display when you try to remove a patch policy or a patch policy exception from a managed server.
- Network Automation Options: This enables you to reset the name of the NA host that you log into, restore the previously saved (default) host name, and launch the NA login window.
- Server Automation Visualizer (SAV) Options: This enable you to specify timeout values for launching SAV and the manner in which you want SAV to scan virtual server relationships.
- Displayed Platforms Options: This enables you to specify what Operating Systems are visible in the **By type view** of the SA Library.

To set SA Client options, perform the following steps:

1. In the SA Client, select the **Tools** menu, then select **Options**.
2. From the left side of the Set Options window, choose a view.
3. From the right side of the Set Options window, modify the desired setting.
4. Select the Save button.

General Options

The following general options enable you to select your default core:

Core Server Defaults

Specify the port number of the SA Client host that you log into by default. The default port is 443.

Cache

This option enables you to configure the caching of data displayed inside the SA Client. You can configure the following cache settings:

- **Check for updates every <xx> minute(s)**: This enables you to enter a value for how many minutes will lapse before the cache is refreshed.

  Enter a time interval for how often you want the SA Client to check the core for new compliance information. This check applies to all information accessed from the core by the SA Client, not just to compliance information. A longer interval increases the likelihood that the information you are viewing is out of date. A shorter interval increases network traffic flowing to and from your core—this means you are viewing more recent information. For more information, see the SA User Guide: Audit and Compliance.
- **Update Cache**: This enables you to check instantly for new information from the core.
- **Reload Cache**: This enables you to immediately reload (refresh) the cache.

Progress Information

Check this option to show the progress of a job. When a job finishes, the Progress window closes.

'Equals' Operator Limit in Search and Reports

This sets limits on the number of available value selections in the Advanced Search and Reports interfaces. To prevent delays and excessive system load, the list of available values is not populated when the number of values exceeds this setting. Values are added by entering them in a text box.

Client Default View

Specify which client you want to be the default view, SA or Application Deployment. See also the SA User Guide: Application Deployment Manager.

SA Agent Installation - Installer Options

In the SA Agent Installer Options pane, you can set options for the installation of a server agent on a server. The Installer Options window enables you to perform the actions listed below.

For more information on installing the agent on servers, see Server Agent Management.

- **Start the Agent after installation**: This enables you to start the Server Agent after installing it on the server. By default, the Agent Installer does not start the server Agent.
- **Ignore prerequisite check failures**: This enables you to ignore prerequisite check failures and forces server Agent installation.
- **Set the server's time from the Server Automation Core**: This enables you to synchronize the time on the server in which the Server Agent is installed with the SA core.

- **Install Windows Installer (MSI) if required**: This enables you to install MSI along with the Server Agent. If MSI is already installed, this option has no effect.
- **Reboot Windows servers after agent installation if warranted**: This enables you to reboot Windows servers after the Server Agent installation is complete.
- **Install Red Hat Package Manager (RPM) on AIX and Solaris**: This enables you to install the RPM handler with the Server Agent. SA recommends that you always include this option when you install Server Agents on Solaris and AIX servers.
- **Reset agent configuration, if present**: This enables you to replace the existing Server Agent configuration.
- **Delete gateway address list, if present**: This enables you to delete the SA Gateway address list, if present and no longer required.
- **Overwrite staged Server Agent installer**: This enables you to overwrite the existing Server Agent Installer.
- **Log Level**: This enables you to set the log level for log messages. With this option, you can specify levels for Errors, Warnings, Info, and Trace.

SA Agent Installation - Protocols

In the SA Agent Installation Protocols pane, you specify the standard port to use to connect to the servers for deployment.

For more information on installing the agent on servers, see Server Agent Management.

- **SSH**: This enables you to determine the standard port to connect to the servers for deployment using the SSH protocol.
- **SMB over NetBT**: This enables you to determine the standard port to connect to the servers for deployment using the Server Message Block over NetBT protocol.

SA Agent Installation - Advanced Options

The SA Agent Installation Advanced options pane allows you to set the options listed below.

For more information on installing the agent on servers, see Server Agent Management.

- **Immediately do a full hardware registration**: This enables you to force the Server Agent Installer to report full hardware information to the core.
- **Immediately do software registration**: This enables you to force the Server Agent Installer to report full software information to the core.
- **Suppress agent reachability check**: This enables you to disable this check during installation. By default, the installer triggers the core to check whether the server is reachable.
- **Disallow anonymous SSL connections if agent is dormant**: This enables you to configure the Server Agent so that browsers cannot connect without a valid certificate.
- **Force creation of new device record if conflict found**: This enables you to suppress this functionality. During registration, the Data Access Engine creates a new device record.

- **Fail if initial hardware registration fails (do not go dormant)**: This enables you to ensure that the Server Agent does not become dormant, if it fails to report hardware information.
- **Do not open Windows Firewall for core-agent communications**: By default, the Server Agent Installer will modify the Windows Firewall configuration on Windows XP and Windows 2003 (r2) servers to allow the SA core to contact the managed server on port 1002. If you select this option, the firewall configuration will not be modified. In this case, the server might not be manageable by SA.
- **Remediate Software Policies**: This enables you to remediate the server against any software policies that are attached to the server.
- **Attach to Software Policy ID**: This enables you to attach the server to the software policy ID.
- **Extra installer options**: This enables you to specify any other installer options, such as:

  `--logfile <path>` allows you to specify the path to the installer log file. By default, the installer log files are placed in the `/tmp` on UNIX or `%SYSTEMDRIVE%\WINDOWS\SYSTEM` on Windows.

  `--workdir <path>` allows you to specify the path to the working directory to use while the installation is in progress.
- **Core certificate fingerprint**: Specifies the fingerprint of the core certificate.

  If you specify a value for this option, the agent installer will verify that the Certificate Authority certificate used to sign the core's SSL certificate matches the value you provided. Specifying a value for this option increases security during the agent installation process by ensuring that the agent attaches itself to the correct core.

  To obtain the correct value for the core certificate fingerprint option, log on to the core as root (you may need to have an SA System Administrator perform this task for you) and run the following command:

/opt/opsware/bin/openssl x509 -in /var/opt/opsware/crypto/agent/opsware-ca.crt -fingerprint -noout

  The output looks like the following:

SHA1 Fingerprint=D2:3B:F8:72:B9:55:0D:

DE:97:04:D5:C2:A5:6B:B2:09:5C:0A:0D:7F

  The fingerprint is the string of hexadecimal numbers following the equal sign:

  D2:3B:F8:72:B9:55:0D:DE:97:04:D5:C2:A5:6B:B2:09:5C:0A:0D:7F
- **nmap parameter**s: This option allows you to specify parameters used when scanning for unmanaged servers, and to specify a different set of scan parameters if you find that SA is unable to locate and identify unmanaged servers due to network firewall configuration in your environment.The default values for the NMAP scan parameters in the SA Client can be set in the System Configuration menu by choosing the Opsware/adh product, and editing the contents of the `adh.scan.default_parameters` configuration parameter.

Terminal and Shell Options

These settings define the command that the SA Client invokes on your PC to open a Global Shell or start a remote terminal session. (For instructions on using an `ssh` client instead of the SA Client, see Opening a Global Shell Session.) See also Opening a Remote Terminal Session on an Agentless Server.

To view and change terminal and shell settings, perform the following steps.

1. In the SA Client, select the **Tools** > **Options** menu item. This displays the Set Options window.
2. In the View pane, select **Terminal and Shell**. This displays the commands that will be used when connecting to managed and unmanaged servers.

The following sections describe how the terminal and shell settings are used and how to set them.

Note: In order to use remote login capabilities to access unmanaged servers using the Secure Shell (ssh) or Remote Login (rlogin) protocols, you will need to install a client program capable of communicating via these protocols. Once you have installed these programs, you must configure the SA Client to invoke those programs.

Terminal Client Command

This setting specifies the terminal client that the SA Client uses for remote terminal sessions on UNIX managed servers and for Global Shell sessions. This setting is used when you select a managed UNIX server and select **Actions > Open With > Remote Terminal**. It is also used when you run the Global Shell using **Tools> Global Shell**. The default value is:

cmd /c start /w cmd /c "(telnet %h %p || echo > nul) && echo %m && pause > nul"

The `telnet` program emulates a command-line terminal session. The `%h` represents the host and the `%p` is for the port number. See Variables for the Terminal, RDP, Rlogin and SSH Client Options.

If you change the Terminal Client setting from the default value, make sure that the command blocks until the terminal application terminates. The terminal application must not run in the background. If you specify `cmd /c start`, include the `/w` switch to make `cmd` block until the underlying command (such as `telnet`) completes.

You are not required to use telnet as the terminal application. For example, you could use putty, the free Windows application that supports SSH, rlogin and telnet. To use a putty client, you could specify the following command:

"C:\\Program Files\\putty\\putty.exe" -telnet %h %p

RDP Client Command

This setting specifies the Remote Desktop Protocol (RDP) client that the SA Client uses for remote terminal sessions on Windows managed servers and unmanaged servers. This setting is used when you select a managed Windows server and select **Actions > Open With > Remote**

Terminal. It is also used when you select an unmanaged server and select **Actions > Log in with > Windows Terminal Services**. The default value is the Microsoft Terminal Services Client:

mstsc "%r"

The specified terminal client must be installed on your PC. To verify the existence of the terminal client, click the **Test** button.

The command can include variables such as `%h` and `%p` representing the host name and port number, respectively. When the terminal client is launched, these variables are replaced with the values shown in Variables for the Terminal, RDP, Rlogin and SSH Client Options. To override a replacement value, specify a constant instead of a variable. For example, you might specify 435 for the port instead of `%p`.

SSH Client Command

This setting specifies the terminal client and configuration settings that the SA Client uses to remotely log in to unmanaged Windows servers. This setting is used when you select an unmanaged server and select **Actions > Log in with > ssh**.

You must specify a client program that can communicate over the SSH protocol. For example you could use putty, the free Windows application that supports SSH.

For the SSH Client setting, specify the command line to invoke your SSH client.

The following shows a putty command you can use to remotely log in to an unmanaged server over SSH.

```
putty -ssh -l %u -P %p %h
```

Table: Variables for the Terminal, RDP, Rlogin and SSH Client Options

Variable	Description	Replacement Value
`%e`	The character encoding.	For Remote Terminal sessions, the encoding of the managed server. For Global Shell sessions, the value of the Encoding field.
`%h`	The host name that the client is to connect to.	The value of the `localhost` of the managed server.
`%m`	A locale-specific message on how to close the window.	For English locales, click the Enter key to close this window.
`%r`	The name of the Remote Desktop (RDP) connection file. This variable is used only for the Microsoft Terminal Services Client (`mstsc`).	A temporary RDP file generated at runtime by the SA Client.
`%t`	The title displayed in the terminal window.	For Remote Terminal sessions, the name of the managed server. For Global Shell sessions, the string “Global Shell.”

Variable	Description	Replacement Value
%u	The user name to pass to the client.	Specifying %u causes SA to display a dialog and request a user name. Enter the user name and select Log In. SA passes the specified user name to the client.

Encoding

This sets the encoding for Global Shell and the Remote Terminal sessions. This option is the replacement value of the %e variable in the command specified by the Terminal Client field. The default value of the Encoding option is UTF-8.

Patch Policy Options

This option allows you to specify that a confirmation message will display when you try to remove a patch policy or a patch policy exception from a managed server.

Network Automation Options

This options allows you to reset the name of the NA host that you log into, restore the previously saved (default) NA host name, and test whether SA can communicate with NA by using the new host name.

- **Host**: This option specifies the name of a server that is acting as a proxy for the NA host. Only the format of the host name is verified.
- **Restore Default**: This option restores the previously saved NA host name.
- **Test**: This option opens the NA login window to verify whether the host name is valid.

Server Automation Visualizer (SAV) Options

HP Service Automation Visualizer (SAV) allows you to manage the operational architecture and behavior of distributed business applications in your IT environment by displaying detailed application information in physical and logical drawings. For more information on SAV, see the SA User Guide: Service Automation Visualizer.

For SAV, you can specify the following options:

- Virtualization Settings
- Scan Time-Out Preference
- Discovery Settings
- Reset All Settings

Virtualization Settings

You can configure SA Client options that allow you to choose whether or not you want to perform a scan on any virtual servers or hypervisors related to the virtual server you want to open in SAV.

For example, if you want to visualize a VMware virtual machine (VM) or Solaris zone in SAV, by default you will be asked if you also want to scan any virtualization relationships — in other words, the system asks if you want SAV to also scan the hypervisor that is hosting the selected virtual server. Depending upon the virtual server you select, SAV might have to scan several related virtual servers in order to visualize a single virtual server in SAV.

Conversely, if you select a hypervisor to open in SAV, you are asked if you want to scan any virtualization relationships — in this case, SAV would need to scan all of the hosted virtual servers, which could take a long time to perform.

Note: Even if you do not request a virtual relationship scan, SAV will display the virtual machines it discovers. However, certain details such as the operating systems on those virtual machines will not be displayed unless you request a virtual relationship scan.

By default, SAV will always ask you if you want to scan virtual relationships, but you can set your own default behavior for scanning related virtual servers with the following virtualization options:

- Ask each time if you want to scan related virtual and host servers.
- Always scan related virtual and host servers.
- Never scan related virtual and hypervisor servers.

To change the virtualization settings, perform the following steps:

1. From the **Edit** menu, select **Options**.
2. In the Set Options window, in the Views pane, select **Service Automation Visualizer**.
3. Specify your desired Virtualization Settings, then click **OK** when you are finished.

Scan Time-Out Preference

SAV is optimized to scan a maximum of 50 servers. A number of factors affect the time it takes for a scan to complete, including the load on the scanned servers and the load on SA. The default scan time-out is set to 300 seconds. You can reset this time-out value to a minimum of 30 seconds or to a maximum of 3600 seconds.

To change the scan time-out, perform the following steps:

1. From the **Edit** menu, select **Options**.
2. In the Set Options window, in the Views pane, select **Service Automation Visualizer**.
3. In the Scan Time-out section, move the slider to increase or decrease the number of seconds at which you want the scanning process to stop.
4. Click **OK** to save your changes or click **Cancel** to close the window without saving your changes.

Discovery Settings

If servers are scanned and it is determined that they are dependent on external IP addresses, when this option is selected SAV attempts to determine which servers or network devices those IP addresses refer to.

Keep in mind that this could cause scan time to increase, depending on the numbers of servers you selected for the scan and how many remote dependencies are discovered.

For recurring background business application snapshots, this detection is always done and cannot be turned off.

Reset All Settings

Restores all SAV settings to their defaults, including resizing and repositioning all tabbed views.

Displayed Platforms Options

By default, the SA Client will display the operating systems that are supported according to the SA Support and Compatibility Matrix.

To change the list of operating systems that are displayed in the **By type view** of the SA Library, perform the following steps:

1. In the SA Client, select the **Tools > Options** menu item.
   This displays the Set Options window.
2. In the View pane, select **Displayed Platforms**.
   This displays the operating systems tree that is visible in the **By type view** of the SA Library.

The following sections describe how the Displayed Platforms settings are used and how to set them.

- In the Displayed Platforms pane, an operating system family tree is displayed. Check or uncheck the operating systems in the **By type view** of the SA Library. The list also includes operating systems that are no longer supported (such as AIX 5.3).
- **Show Unsupported** button – all operating systems that were supported in SA and are no longer supported will be displayed.
- **Restore Defaults** button – the list of operating systems that are displayed in the SA Library is restored to the default list of supported operating systems found in the SA Support and Compatibility Matrix.

Browsing Job Logs

To view information about jobs that have run, select the Jobs and Sessions tab in the SA Client. This displays jobs that have run as well as jobs scheduled to run in the future.

A job is any major process run by the SA Client, such as Audit Servers, Create Snapshot, Create Virtual Zone, Deploy Application, Install Software, Push Configurations, Run Communication Test, Run OS Sequence, Scan Configuration Compliance, Uninstall Patch, and so on.

The Job Logs window shows all jobs that the user is configured to see, based on his permissions. It also displays jobs scheduled to run, including the job ID, the job type, the start and end times, the number of servers and groups affected by the job, the status of the job, the ticket ID, and the user name of the person who ran the job.

If the job status is Pending Approval, then the job is blocked until it is approved by a process that is external to Server Automation. If jobs are blocked indefinitely, the SA Administrator should check the settings of the Approval Integration window or the configuration of the backend connector.

The format of the Start Time and End Time for a job is determined by the original user preferences set in the SA Client. These preference may be different than those of the current user.

Tip: If you are working in multiple time zones, make sure the preferences for Start Time and End Time are set to include the time zone in the date display.

To see the details of a finished job or recurring (scheduled to be run) job, open the job.You will only be able to modify a scheduled job if you created the job or have *Edit or Cancel Any Job* permissions. To obtain these permissions, contact your SA Administrator. See the SA Administration Guide for more information.

To view a job, select it, right-click, and select **Open**.

To cancel a non-recurring job, from the Job Logs window, right-click the job and select **End Job**. You cannot cancel a job while it is running (that is, when the job status is In Progress).

To cancel a recurring (scheduled) job, from the Recurring Schedules window, right-click the job and select **Delete Schedule**.

Note: In order to view a job in the SA Client, you must have permissions to run or execute the feature action. For example, if you wanted to view Application Configuration Push jobs in the SA Client and you had the Manage Application Configurations permission set to Read, but not Write, you would not be able to see any Application Configuration Push jobs in the SA Client.

At the top of the Job Logs window, you can filter jobs by specifying the following criteria:

- **Job Time Frame**: Enables you to limit the search for a job by a time restriction, such as jobs run anytime, in the last 24 hours, last week, last month, last quarter, and so on. Or, for scheduled jobs, you can filter the jobs list by those jobs scheduled to run in the next 24 hours, next week, and so on.
- **Job Status**: Enables you to search based on the status of a job, such as Succeeded  , Warning  , Failed  , Pending Approval, Cancelled, and so on.
- **Job Type**: Enables you to search for jobs by type, such as **Audit Servers, Modify Virtual Zone, Reboot Server, Remediate Policies, Run OGFS Script, and so on. These are jobs that have already run or are scheduled to run.**
- **Job ID**: Enables you to search by the job ID.
- **Ticket ID**: Enables you to search by the ticket ID, if one was given for the job.

- **User**: Enables you to enter a username to see only those jobs a certain user has run. Only users with the *View All Jobs* or *Edit or Cancel Any Job* permissions will be able to view jobs in the core. If you do not have these permissions, this filter will not appear.

  You must click Search to update the list based on the current filter settings.

After setting the filter criteria, click the **Search** button to filter the job table.

To perform an advanced search, click drop-down list on the Search button and select Advanced Search. For more information, see Performing an Advanced Search or Searching for Objects with the SA Client.

Recurring Job Schedules

The recurring schedules window shows all jobs that are scheduled to run on a recurring basis. You can choose to view all recurring jobs or filter the list of recurring jobs by specifying the following criteria:

- **Job Status**: Enables you to search for scheduled jobs by their status, such as Any Status, jobs that have been Cancelled, jobs that are Pending Approval, or all jobs that are Recurring.
- **Job Type**: Enables you to search scheduled jobs by their job type, such as Audit Servers, Create Snapshot, Push Configurations, and so on.
- **Job ID**: Enables you to search for recurring jobs by their job ID.
- **Ticket ID**: Enables you to search by the ticket ID, if one was given for the job.
- **User**: Enables you to enter a username to see only those jobs that a certain user has scheduled to run on a recurring basis. If a user is not specified, all recurring jobs will display.

Requirement: Only users with View All Jobs or Edit or Cancel Any Job permissions will be able to view all jobs in the core. If you do not have these permissions, you will not be able to see all jobs.

- **Search**: Enables you to perform a search query of scheduled recurring jobs. Click **Search** to display the detailed results.

Viewing and Deleting Recurring Job Schedules

To view a recurring job schedule, select it, right-click, and select **Open**.

To delete a recurring job, select it, right-click, and select **Delete Schedule**.

Job Notification Emails

If a job was configured to send an email notification to a recipient when the job has finished, either on success, failure, or both, the email provides the following information:

- **Job Information**: Provides data about the job, such as the Job ID, Status, and start and end time.

- **Job Type Information**: Provides data relevant to the specific job type that was run. For example, if the job run was an Audit, the job notification email will provide information, such as Audit task ID and audit results ID.
- **Job Results URL**: The job results URL launches the specific job type window. For example, if the job was an audit, the job type URL launches the audit results window. Other information in the notification email provides job results details, such as number of differences found in the audit results, source and target server information, and so on.

Finding Information in Job Results

To easily find key information in the Jobs and Sessions tab, you can filter, group, sort, search for, and highlight information in detailed job results.

Filtering the Display

Filtering enables you to control what displays in the Jobs and Sessions tab. You can narrow or expand the detailed job results. In the Jobs and Sessions tab, in the filter box, click on the filter menu to display a list of filtering criteria. The filter menu options display in the following 5 sections:

1. The first section is a list of the column names you can select to filter on. Depending on the Job type, the column names will vary. Select a column heading that you want to filter:

   All

   Item

   Status

   Only the following job types are filterable:

   - Audit Servers
   - Create Snapshot
   - Deploy Application
   - Install Software
   - Push Configurations
   - Remediate Audit Results
   - Remediate Policies
   - Reboot Server
   - Restore Configurations
   - Rollback Application
   - Undeploy Application
   - Uninstall Software
2. The next section is a list that specifies whether you want to filter with case sensitivity on or off:

   Case sensitive

   Case insensitive

3 This section specifies whether you want to filter using wildcards:

Use wildcards

If you enable wildcards, enter a string, using different wildcards, in the filter box. A wildcard is any character, including alpha, numeric, and special characters.

+ — The plus sign wildcard can be substituted for one or more of any character.

***** — The asterisk wildcard character can be substituted for zero or more characters.

? — The question mark wildcard character can be substituted for one character.

4 This section specifies where in the field to match the string:

Match from start

Match exactly (This means you want to match the entire line.)

Match anywhere

5 This section specifies how to keep the grouping when it filters a string. If neither is selected, it just keeps the rows that have the string:

Keep parent row if any of the children match — This will display the parent row along with all the children rows that contain the string that the filter requested.

Keep the children if any of their ancestors match — This will display the children rows along with all the parent rows that contain the string that the filter requested.

Grouping and Ungrouping Columns

You can group any one or multiple columns. When you group multiple columns, you create nested groups.

1 Right-click on the column heading you want to create a group of and then select **Group This Column**.

2 To ungroup a column, right-click on any column heading and then select **Ungroup Column <name>**.

Expanding and Collapsing Information in Columns

You can expand or collapse information in a column.

1 Right-click on a column heading and then select **Expand All**.

2 Right-click on a column heading and then select **Collapse All**.

Resizing Columns

You can auto resize one or all columns in the display.

1 To auto resize one column, right-click on the column heading and then select **Auto Resize This Column**.

2 To auto resize all columns, right-click on any column heading and then select **Auto Resize All Columns**.

3 (Optional) Double-click on the edge of a column heading in the job results display. This action will auto resize the column width to fit the data.

4 (Optional) You can also drag the vertical line between column headings to resize them.

5 (Optional) You can also drag-and-drop a column heading to change its horizontal position.

Sorting Columns

You can sort information displayed in a column.

1 To sort column information, click on the column heading.

2 To reverse sort column information, click on the column heading again.

3 To add a secondary, tertiary (and so on) sort, press CTL-Click.

Finding & Highlighting

You can use the **Find** tool to narrow your search and highlight what you see in the table or in the details pane.

1 To find key information in the table view, click in the table and then press CTRL-F to open the Find bar. Enter any string in the Find text box. This action finds the string you entered, whether it is an entire string or part of a string.

2 To find key information in the details pane, select a row in the table to open the details pane. Click in the details pane and then press CTRL-F to open the Find bar.

   Example:

   a Enter “ORA” in the Find text box. This will highlight the first occurrence of “ora” in the details pane.

     If you enter text that does not have any matches, “Phrase not found” will display next to the Find bar.

   b (Optional) You can have either one or both Find bars open at the same time. If you have both Find bars open simultaneously, one displays at the bottom of the table and the other one displays at the bottom of the details pane.

   c (Optional) Click **Highlight** to highlight all occurrences of “ora”.

   d (Optional) Click **Find Next** or **Find Previous** to jump forwards or backwards to the next occurrence of “ora” and highlight it.

   e (Optional) Click **Match Case** to narrow the find to “ORA” database errors in this example.

3 To close the Find bar, click the **X** in front of the Find text box or position the cursor in the Find text box and then press **Esc**.

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.

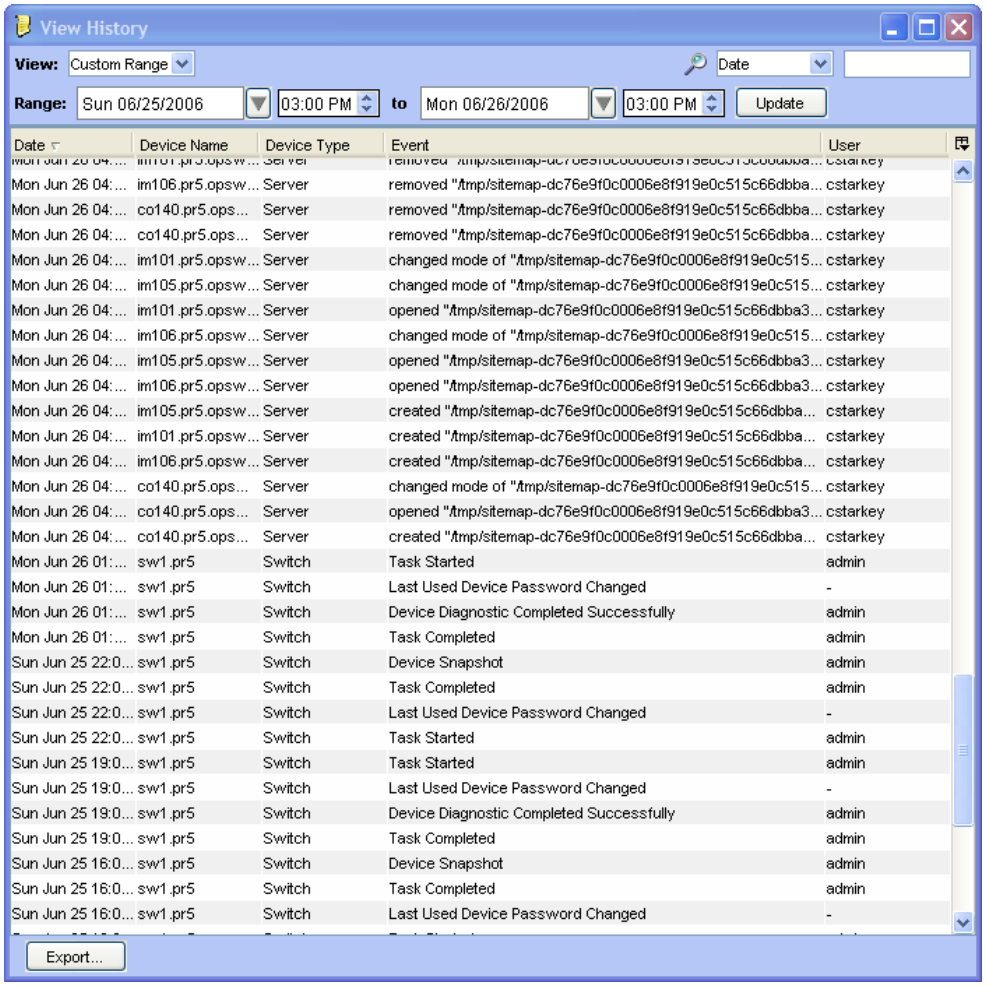
You can view a combined device history log for one or more managed servers or for a device group that contains managed servers and network devices.

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.

Right-click and then select View History to list events that occurred on the selected devices.

Combined Device Event History


View History
View: Custom Range
Date
Range: Sun 06/25/2006 03:00 PM to Mon 06/26/2006 03:00 PM Update
Date | Device Name | Device Type | Event | User
Mon Jun 26 04:... im106.pr5.opsw... Server removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba... cstarkey
Mon Jun 26 04:... co140.pr5.ops... Server removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba... cstarkey
Mon Jun 26 04:... co140.pr5.ops... Server removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba... 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-dc76e9f0c0006e8f919e0c515c66dbba... cstarkey
Mon Jun 26 04:... im101.pr5.opsw... Server created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba... cstarkey
Mon Jun 26 04:... im106.pr5.opsw... Server created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba... 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-dc76e9f0c0006e8f919e0c515c66dbba... 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 -
Export...

Chapter 2 Exploring the SA Library

The SA library provides a secure folder hierarchy for organizing and sharing all your server resources.

- The SA Library allows you to organize your server resources - packages, scripts, software policies, OS build plans, and many other server objects - in a folder hierarchy.
- Folder permissions enable you to control which user groups can view, use, and modify folder contents.
- Policies can specify various resources. Yet each resource can be located in any of various different folders. Because folder permissions determine user group access, each resource can be managed by an number of different user groups.

The ability to perform specific actions in SA is governed by your permission settings. For information about permissions, see the SA Administration Guide.

About Server Resources in the SA Library

The SA Library stores server resources such as OS build plans used for OS provisioning, software packages and policies for installing software, application configurations for configuring software, patches and patch policies for installing patches, scripts for running on your servers and many other resources for managing your servers quickly and efficiently. The SA Library is organized **by resource type** and **by folder location**. You can view server resources either by their type or by their location in the folder hierarchy.

- The **By type view** is organized by the type of object (policy, package, OS, patch, script). This view is a popular starting point for most of the software management activities, such as creating application configurations, running scripts, attaching policies to servers.
- The **By folder view** allows you to manage user group access to the software resources and is organized by operating system as a default. Folders can be added, moved, etc. It is where the admin can organize and manage permissions to shared resources. When you add or import resources, you specify a folder location. The location you specify will determine which user groups can access it.

When you install SA, the SA Library contains the default folders and resource types, as described below.

- The *Home* folder contains a folder for every SA user. Users can only see their own user directory under the home folder.
- A folder that contains the tools required to upload ISMs to SA.
- The *Package Repository* folder contains software packages that are organized by operating system families.
- In addition to using the default folders, you can create new folders in the library to manage your software resources. See Creating a Folder for more information.

Default Resource Types:

- Application Configurations
- Audit and Remediation
- Business Applications
- Databases*
- Extensions
- OS Build Policies
- OS Installation Profiles
- OS Sequences
- Packages
- Patch Policies
- Patches
- Scripts
- Software Policies
- UNIX Users and Groups
- Windows COM +
- Windows Hyper-v Manager
- Windows IIS 7 Settings
- Windows IIS Metabase
- Windows Local Security Settings
- Windows Registry
- Windows Services
- Windows Users and Groups
- Web Applications*

*Except for Web Applications and Databases, all of these resources can be added to folders.

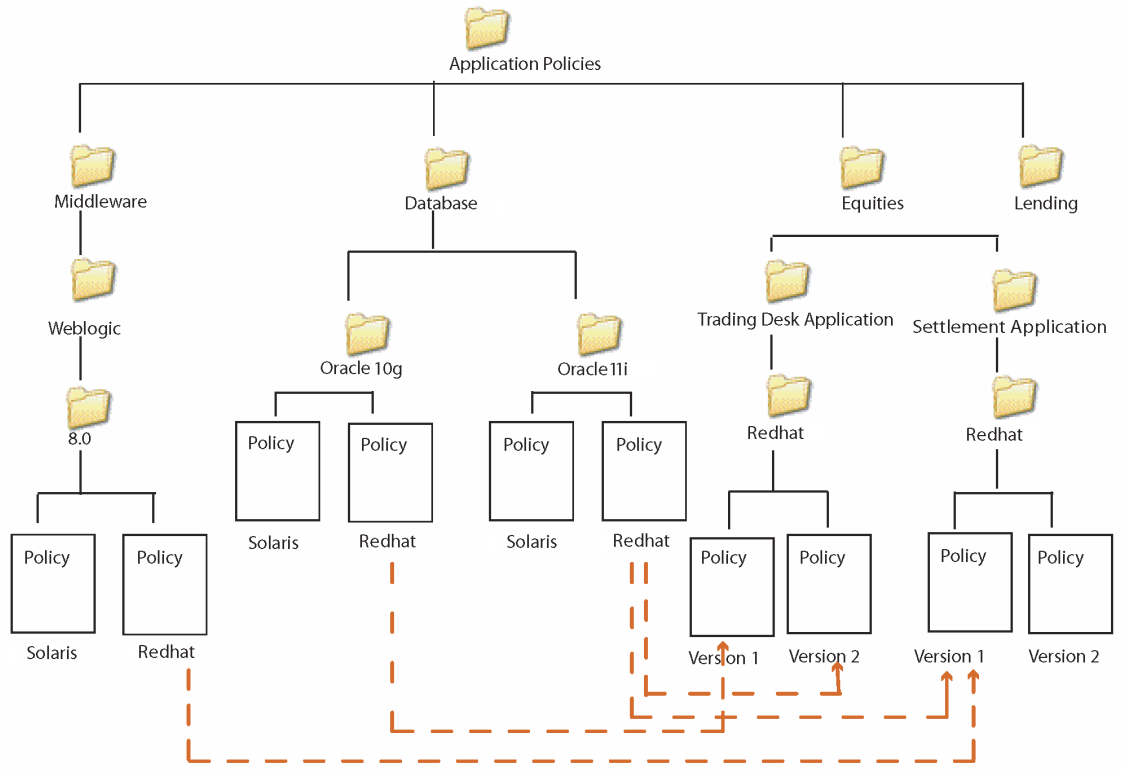
The SA Client search tools can find managed servers, software policies, folders, application configurations, patches, and software, and let you perform actions on the results.

About Managing Folders

The folder hierarchy in the SA Client provides a way to organize your software resources and allows you to define security permissions to control access to the contents of a folder. Folders can contain packages, patches, scripts, policies, server objects, and OS sequences. They can also contain other subfolders to form a hierarchal structure.

Use folders to organize and manage your software resources to correspond to your operational environment. For example, you can organize the folders by functionality (Finance, Engineering, Operations, or Marketing), by applications (Web Servers, Web Application Servers, Database Servers, or Middleware), or by operating system versions (UNIX or Windows).

Example of a Hierarchical Folder Structure in the SA Library



SA not only provides you with the flexibility of organizing folders based on functionality, applications, or OS versions, but it also allows you to share content among user groups. In this example, all policies related to database servers are organized in the Database folder. The Database folder contains subfolders for different versions of Oracle, which contain policies for different platforms.

Similarly, the Settlement Application subfolder contains the policies necessary for that functionality. The policies in this folder are organized based on operating system versions.

When you attach the Version 1 policy to a server, all the software in policy Version 1 is installed in addition to the software in policy Oracle, Redhat and Weblogic.

Folders cannot be attached to a server directly. Instead, you have to add the software resources in folders to a policy and attach the policy to a server. Folders also do not support inheritance, which means that the subfolders do not inherit the resources of a parent folder. See Creating a Folder.

About Folders and Permissions

Folders allow you to define security boundaries to control access to their content across user groups. You can assign permissions to folders to determine who can access the contents of the folder such as policies, packages, patches, server objects, and OS Sequences. A folder's permissions determine the user groups that can view, create, modify, and delete items within the folder. A folder's permissions apply only to the items directly under the folder. They do not apply

to items lower down in the hierarchy, such as the subfolders and subfolders of subfolders (grandchildren).

In addition to the Folder permissions, a user must have the appropriate SA Client Feature permissions to access the contents of a folder. SA Client Feature permissions determine what actions users can perform with the SA Client, whereas the Folder permissions specify which folders users have access to.

You can assign the following permissions to a folder, by associating a user group with each folder:

- **List Contents of Folder**: Enables a user to navigate to the folder in the hierarchy, view the folder's properties, and view the names of the folder's children.
- **Read Objects Within Folder**: Enables a user to view and use the contents of a folder.
- **Write Objects Within Folder**: Enables a user to view, use, and modify the contents of a folder.
- **Edit Folder Permissions**: Enables a user to modify the folder permissions or add customers to a folder. This permission delegates the management of folder permissions to another user group.
- **Execute Objects Within Folder**: Enables a user to execute the scripts contained in the folder and view the names of the folder's children. This permission allows users to run scripts, but not to read or write them.

In addition to folder permissions, you can assign customer constraints to folders. See the SA Administration Guide for more information about folder permissions and customer constraints.

Creating a Folder

Perform the following steps to create a folder in the SA Client:

1. From the Navigation pane, select **Library** > **By Folders**.
2. From the **Actions** menu, select **New** > **Folder**.

   The name of the folder that you just created is New Folder (n), where n is a number based on the number of new folders already in existence.
3. Enter the name of the folder in the Content pane.
4. From the Navigation pane, select **Save** to save a folder.

Note: To create a folder in a specific location, navigate to the desired location in the folder hierarchy and select **New Folder** from the **Actions** menu.

Note: You can also rename, move, cut, and copy folders by selecting **Rename**, **Move**, **Cut**, and **Copy** from the **Actions** menu.

Setting Folder Properties

After you create a folder, you can view and modify the properties of the folder. You can view the folder properties, such as the SA user who created the folder, the date when the folder was created, the location of the folder in the Library, and the number of subfolders and feature objects present in the folder. You can also modify the name and the description of the folder.

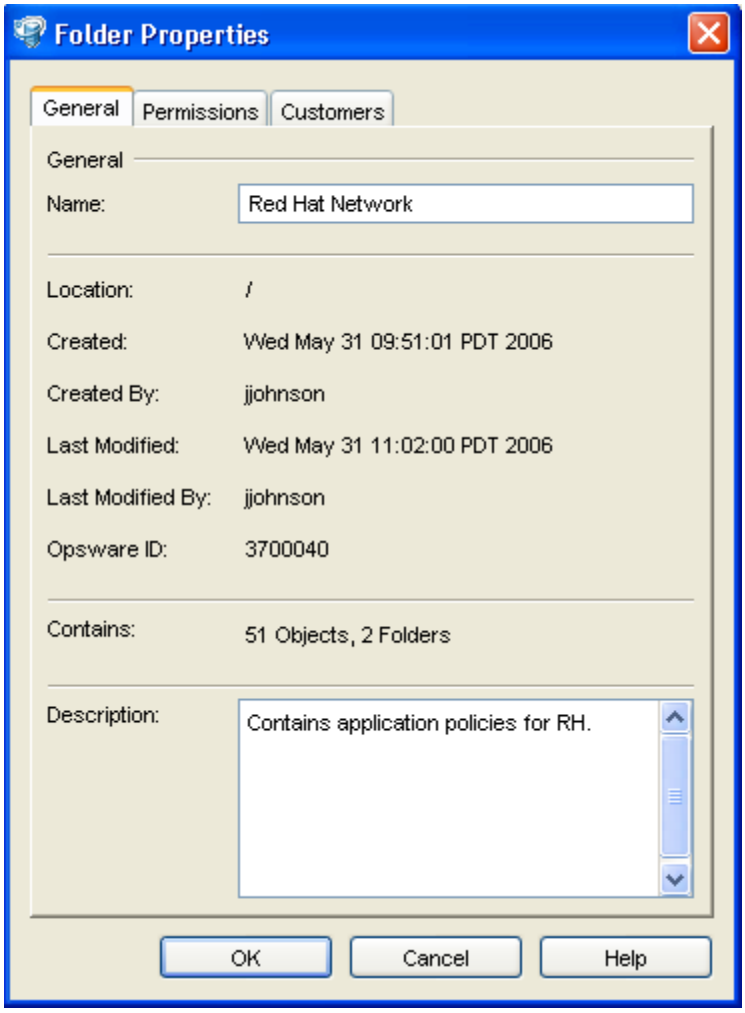
You can also set the Folder permissions and Customer permissions on the folder. See the SA Administration Guide for information about setting Folder and Customer permissions.

Perform the following steps to manage the properties of a folder in the SA Client:

1. From the Navigation pane, select **Library** > **By Folders**.

   All the folders in the Library appear in the Content pane.
2. From the Content pane, select a folder.
3. From the **Actions** menu, select **Folder Properties**. The Folder Properties window appears as shown in Setting Folder Properties in the SA Client .

Setting Folder Properties in the SA Client



4. Select the General tab to view the folder properties, such as the location of the folder in the Library, the SA ID associated with the folder, and the features and subfolders contained in the folder.
5. In the Name field, modify the name of the folder. In the Description field, enter a description of the folder.
6. Click **OK** to save the changes or click **Cancel** to close this window without saving the changes.

Copying a Folder

You can copy and paste a folder in the SA Library which copies the contents of the folder to the new location, however, not all file types are copied.

Copying a folder copies the following types of files: audit policies, CML files, configuration files, OGFS script files, OS build plans, OS sequences, server scripts, and software policies. Other file types are not copied, such as zip files, RPM files, executable files, shell scripts, and files of unknown type. These types of files can be large and making copies can waste storage space. Proliferating copies of certain types of files can make keeping track of the official files more difficult. As a best practice, keep related files in one place for easier tracking.

Note that you can move a folder and all its contents by using cut and paste.

If you need to make a copy of a file, you can export the file to your local system, then import it to the new folder. Perform the following steps.

1. Locate the file in the SA Library and select it.
2. Right click or select the Actions menu and select Export Software. This displays a window where you can specify a location in which to store the file.
3. Specify the location where you want to save the file.
4. In the SA Client, navigate to the destination folder in the SA Library.
5. Right click or select the Actions menu and select Export Software. This displays a window where you can specify a location in which to store the file.
6. Use a similar process to import the file to the new location in the SA Library.

Deleting a Folder

Note: To delete a folder containing subfolders, you must have the required permissions for the subfolders as well as the parent folder.

Perform the following steps to delete a folder in the SA Client:

1. From the Navigation pane, select Library > By Folders.

   All the folders in the Library appear in the Content pane.
2. From the Content pane, select the folder that you want to delete.
3. From the **Actions** menu, select **Delete**. The Confirmation window appears.
4. Click **Delete** to delete the folder.

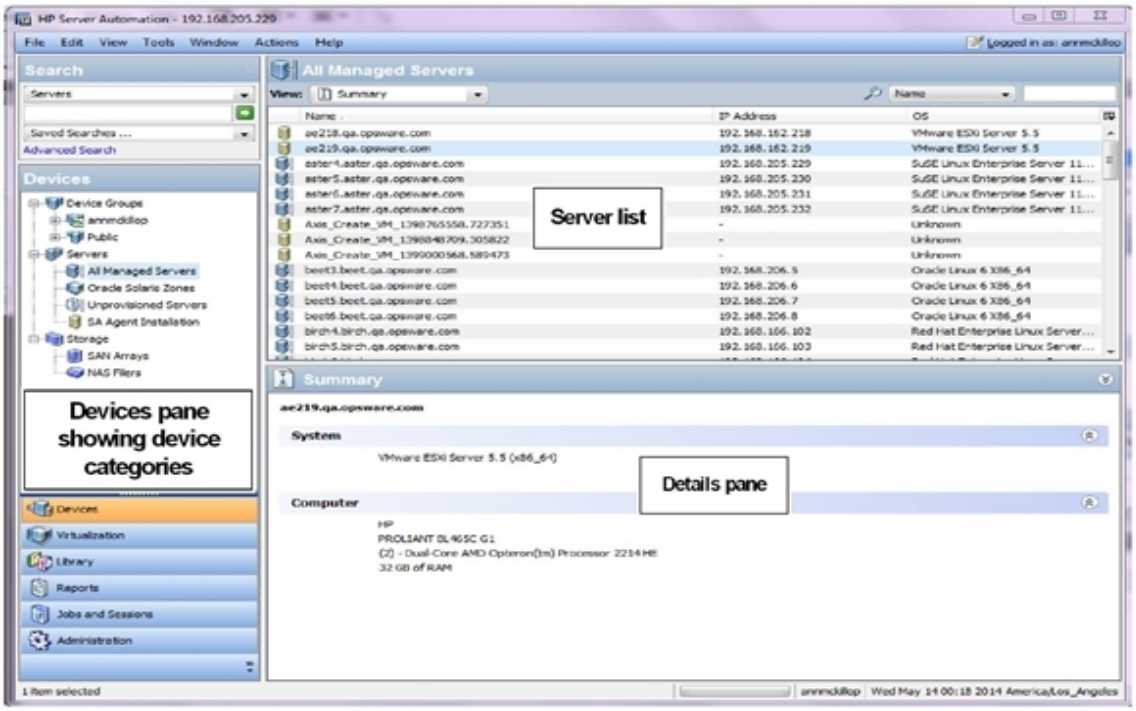
Chapter 3

Exploring Servers and Device Groups in the SA Client

Exploring Servers in the SA Client

The SA Client allows you to view a list of all your servers in your data center, which can exist in various states of SA management. All your servers can be accessed from the Devices pane in the main SA Client interface, as shown in Servers in the Devices Panel.

Servers in the Devices Panel



Note: To visualize networking information with Network Automation (NA) inside of the SA Client, you must have both a licensed version of NA integrated with your SA core, plus an additional license for NA.

To view storage devices and SAN information inside of the SA Client, Storage Essentials (SE)

version 6.1.1 or later and the Server Automation SE Connector component must be installed and configured your SA core. For more information, contact your HP SA sales representative.

Server Status Icons

In the SA Client, you can determine the status of a server by the type of icon next to the server, as defined in Server Status Icons in SA . See the Server List in Servers in the Devices Panel.

Table: Server Status Icons in SA

Server Icon	Description
	**Planned** Indicates that a device record has been created for the server, but an OS Build Agent has not yet been installed on it. Servers in this stage cannot be provisioned until the OS Build Agent is installed. In the SA Client, appears in the Unprovisioned Server list.
	**Unprovisioned — Unreachable** Indicates a server that has been registered with the core via the OS Build Agent, but has not reported as ready for provisioning recently. This may be due to networking problems between the server and the SA core or the server having been disconnected or powered off. In the SA Client, appears in the Unprovisioned Server list.
	**Unprovisioned — Reachable** Indicates a server that has been registered with the core via the OS Build Agent and is available to have a target OS installed on it. In the SA Client, appears in the Unprovisioned Server list.
	**Provisioning — Unreachable** Indicates a server on which the OS Provisioning feature was in the process of installing the target OS, but for some reason stopped because the server is unable to communicate with the SA core. In the SA Client, appears in the Unprovisioned Server list.
	**Provisioning — Reachable** Indicates a server on which the OS Provisioning feature is in the process of installing the target OS. In the SA Client, appears in the Unprovisioned Server list.

Server Icon	Description
	**Provisioning Failed — Unreachable** Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS, and that the server is not able to communicate with the SA core. In the SA Client, appears in the Unprovisioned Server list.
	**Provisioning Failed — Reachable** Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS. In the SA Client, appears in the Unprovisioned Server list.
	**Agent Managed — Reachable** Indicates a server has a Server Agent is running on it and that it is able to communicate with the SA core. In the SA Client, appears in the All Managed Servers list, Virtualization tab, and Oracle Solaris Zones.
	**Agent Managed — Unreachable** Indicates a managed server cannot communicate with the SA core (it is Not Reachable). If you want to discover reasons why the managed server is unreachable, you can run a Communication Test. See Running Server Communication Tests for more information. In the SA Client, appears in the All Managed Servers list, Virtualization tab, and Oracle Solaris Zones.
	**Agentless** Indicates the server does not have a Server Agent installed on it. For virtual servers, this means that someone created a virtual machine (VM) outside of SA so it does not have a Server Agent installed on it. For virtual servers, this state could also mean that the VM has not yet been provisioned, or that your user belongs to a group that does not have permissions to perform operations on this virtual server. For more information on installing a Server Agent on an unmanaged server, see Server Agent Management.
	**Deactivated** Indicates a server that was deactivated in Server Automation by deactivating its SA Agent so that it is currently not managed and is no longer

Server Icon	Description
	reachable. Appears in the Manage Servers list and in the server lists in the SA wizards (however, it is not selectable in the wizards).
	**Scheduled** Indicates a server that is scheduled for an operation (install software, uninstall software, and so forth). In the SA Client, appears in the Job Logs list.
	**Error** Indicates a managed server on which an error occurred while Server Automation was installing or uninstalling software.
	**Warning** Indicates a managed server on which a warning occurred while Server Automation was installing or uninstalling software. Appears in the My Jobs panel in the home page and in the list in the My Jobs page.
	**Application Configuration Out of Sync** Indicates a managed server on which the configuration file on the server is out of sync with the Application Configuration Template (SA model). Appears only in the Application Configuration feature and the server list in the SA Client.

Device Group Status Icons

Device groups let you gather servers into logical sets to make performing actions on groups of servers easier and more efficient. The following table shows the icons displayed for device groups. See About Device Groups for more information.

Table: Device Group Status and Icons
Table:

Device Group Icon	Description
	**Static Device Group** Indicates a static server group. The same states that apply to single servers apply to groups. See About Device Groups for more information about the different types of server groups.

Device Group Icon	Description
	**Dynamic Device Group** Indicates a dynamic server group. The same states that apply to single servers apply to groups.
	**Public Static Device Group** Indicates a public and static server group. The same states that apply to single servers apply to groups.
	**Public Dynamic Device Group** Indicates a public and dynamic server group. The same states that apply to single servers apply to groups.

VM Template Status Icons

The following table shows the icons displayed for virtual machine (VM) templates. VM templates are only visible and manageable from the Virtualization tab of the SA Client. For complete details, see the SA User Guide: Virtualization Management.

Table: VM Template Status Icons

VM Template Icon	Description
	**Agent-Managed VM Template** This template includes the SA agent. When you deploy a VM from this type of VM template, the resulting VM will be agent-managed. As a best practice, always use agent-managed VM templates and agent-managed VMs.
	**Agentless VM Template** This template does not include the SA agent. When you deploy a VM from this type of VM template, the resulting VM will not be agent-managed.

Running Server Communication Tests

You can run a set of communication tests to assess the connection between the SA core and your managed servers. For details, see Running Server Communication Tests.

Ways to Use the Device Explorer

The Device Explorer allows you to browse and manage servers, devices (such as network or storage), and groups of servers in your environment.

Using the Device Explorer you can perform the following actions on individual servers:

- Browse basic device system information, such as device, operating system, memory, Server Agent version, and more.
- View device compliance information and view the details of any policies attached to the server, such as all audits, patch policies, software policies, as well as any application configurations attached to the server.
- Run audits of the server, remediate any software policies attached to the server, and push application configurations on to a server.
- Browse live and up to date information about a server's file system, registry, hardware inventory, hardware, ethernet and SAN connections, installed software and patch lists, runtime state, user and user group membership, services, snapshots, and more
- View server group membership.
- View virtual server hypervisors and virtual machines (VMware, Solaris, and Microsoft Hyper-V).
- Add and delete custom attributes.

Note: Some Device Explorer features are not available for VMware ESXi servers because SA does not install a Server Agent on ESXi servers. For more information on ESXi servers, see the SA User Guide: Virtualization Management. For more information on Server Agents, see Server Agent Management.

Network and Storage Devices in the Device Explorer

For more information on the types of information you can view in the Device Explorer for network and storage devices, see the following:

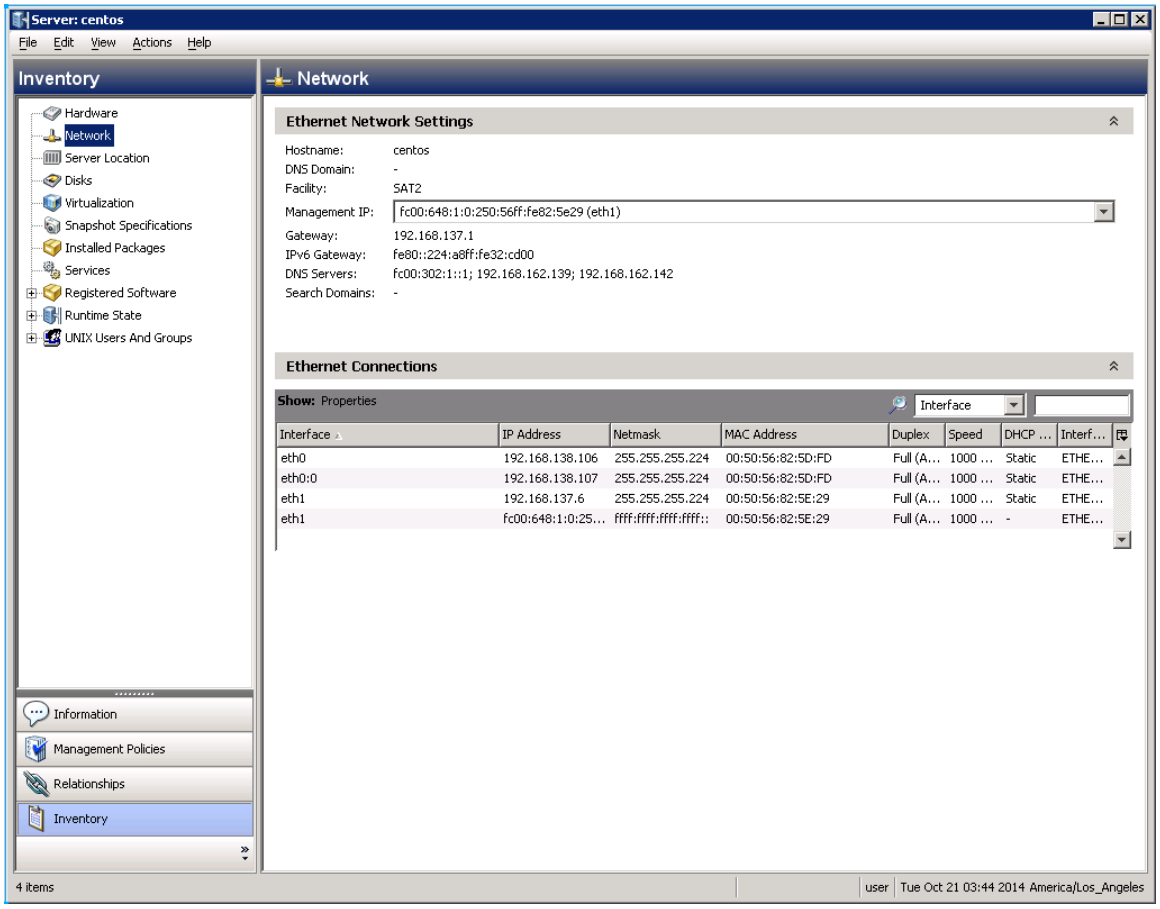
- SA Integration Guide for network devices
- Storage

For more information on storage in the SA Client, see the Storage Visibility and Automation User Guide.

Device Explorer Interface

The Device Explorer consists of two main sections: the Views pane and the Content pane. The Views pane lists server objects from the managed server, and the Content pane displays content for each of the server's objects. When you select a server object in the Views pane, its corresponding content appears in the Content pane. See Device Explorer Interface .

Device Explorer Interface



Device Explorer Views Tabs

The Device Explorer Views tabs organize four different types of information about your device:

- Information About Servers: Shows general property and system information, such as computer manufacturer, hardware type, system, processor and memory, OS version, Server Agent version and status (for those managed servers that have a Server Agent installed), SA customer assignment, history of changes to the server, and more.
- Server Management Policies: Displays a roll up of all compliance policies attached to the server, as well as compliance for individual compliance policies, such as audits, software and patch policies, application configurations, and any custom user-create policies. It also shows any custom attributes created on the server.
- Relationships with Other Devices: Shows all groups that the selected server is a member of and allows you to modify group membership (if your user has sufficient permissions).
- Inventory of Server Information: Displays a list of live server configuration objects and server modules captured directly from the server, such as registered hardware, network connections, snapshots taken of the server, installed packages, patches, discovered software, runtime information about processes running on a server, local security settings, users and groups memberships, and so on.

Accessing the Device Explorer

To access the Device Explorer, perform the following steps:

1. Launch the SA Client and then from the Navigation pane, select **Devices** > **All Managed Servers**.
2. A list of servers will display in the Content pane.

   If the list of servers is long, use the filter tool  to locate a server (upper right corner) by name, IP address, OS, customer, facility, or description. If you filter by user name, the text entry is case insensitive.

   You can also sort the list by clicking a column heading, such as name, IP address, OS, customer, and so on. To reverse sort, click the column heading a second time.
3. Open a server from the Content pane. This opens the Device Explorer. From the **Actions** menu, you can perform many types of operations, such as:
   - Open in Server Automation Visualizer (SAV) if your core is licensed to run SAV
   - Run a script on the server
   - Create or run an audit or snapshot of the server
   - Scan software, application configuration, or patch compliance
   - Add to a device group
   - Export patch information to a .csv file
   - And more

   Action menu items change according to the server object selected.

   For example, if you select the Configured Applications object from the server object tree, then from the **Actions** menu, you can add, remove, or open an application configuration, create a package, and so on.

Note: For VMware ESXi servers, some actions are not available because the SA Server Agent is not deployed on VMware ESXi servers. For more information on ESXi servers, see SA User Guide: Virtualization Management. For more information on Server Agents, see Server Agent Management.

Opening a Remote Terminal

You can open a remote terminal and log in to any managed server. Perform the following steps:

1. From the SA Client Navigation pane, select **Devices** > **All Managed Servers**.
2. Select a managed server.
3. Select the **Actions** menu or right click and select **Open With** > **Remote Terminal**.
4. Log in to the remote server.

See also the Server Status Icons.

Information About Servers

The Information tab for a server provides the following information:

- Summary of Server Information
- Properties of Servers
- Custom Attributes Defined for a Server
- History of Server Changes
- Server Location

Note: For VMware ESXi servers, some Device Explorer information is not displayed because the SA Server Agent is not deployed on VMware ESXi servers. For more information on ESXi servers, see SA User Guide: Virtualization Management. For more information on Server Agents, see Server Agent Management.

Summary of Server Information

The Summary view in the Device Explorer lists the following information:

- **System**: This displays operating system information.
- **Computer**: This displays server manufacturer, hardware, and system details.
- **Agent**: This displays communication status, the time when the server was last registered, and the number of SA applications. Servers that do not use an SA agent, such as VMware ESXi, will not display agent information. For more information on ESXi servers, see SA User Guide: Virtualization Management.

Properties of Servers

The Properties view in the Device Explorer lists the following information for the server that you are viewing:

- Management Information for Servers
- Custom Fields Defined for Servers
- Reported Information for Servers
- Server Modules

Management Information for Servers

The Management Information view in the Device Explorer lists the following information about the server that you are viewing:

- **Name**: This displays the name of the managed server.
- **IP Address**: This displays the IP address of the managed server.
- **Description**: This displays a text description of the server.

- **Customer**: This displays an account within Server Automation that has access to designated resources, such as servers and software.
- **Facility**: This displays the location of the server. Users can manage servers in any facility from a SA Client.
- **Realm (link speed)**: This displays the minimum bandwidth limit between the Server Agent and the core (if the agent is going through gateways).
- **Server Use** (sometimes abbreviated to just **Use**): This property displays how an organization is using the managed server; for example, a server could be a staging server, a production server, a development server, and so on. You can set this value for your servers and use it to group and filter servers for management tasks or as a condition for inclusion in dynamic groups. For example, you could use this property to quickly locate all your staging servers. The predefined values are:
  - Not Specified - This is the default value for all servers.
  - Development - Servers are being used to develop business services.
  - Staging - Servers are in preparation before going into production.
  - Production - Servers are in production providing business services.

  You can add, delete or change the server use categories as follows:

a. Log in to the SA Client as a user who has the Server Attributes permission set to Yes. This permission is required to change server use categories. For more information on permissions, see the SA Administration Guide.

b. Select the Administration tab.

c. Select Server Use which is under the Server Attributes node in the navigation pane. This displays all your currently defined server use categories.

d. Use the **Actions > New**, **Actions > Open** and **Actions > Delete** menus or the New and Delete icons to create, modify and delete server use categories. You cannot modify or delete the Not Specified category.

- **Server Lifecycle**: This displays the server's stage in the managed server lifecycle; for example, unprovisioned, available, managed, or deactivated.
- **Reboot Required**: This indicates whether or not the server needs to be rebooted, for example because a patch has been installed.
- **OS Version**: This displays the operating system (platform) that the managed server is running on.
- **Deployment Stage** (sometimes abbreviate to just **Stage**): This property displays the stages of deployment for a server; for example, a server could be live or offline or in deployment. You can set this value and use it to group and filter servers for management tasks or as a condition for inclusion in dynamic groups. For example, you could use this property to quickly locate all servers that are offline. The predefined values are:
  - Not Specified - This is the default value for all servers.
  - Offline - Servers are not in use.
  - In Deployment - Servers are being prepared for use.

- Ops Ready - Servers are ready to be used.
- Live - Servers are being actively used.

You can add, delete or change the deployment stage categories as follows.

a. Log in to the SA Client as a user who has the Server Attributes permission set to Yes. This permission is required to change deployment stage categories. For more information on permissions, see the SA Administration Guide.
b. Select the Administration tab.
c. Select Deployment Stage which is under the Server Attributes node in the navigation pane. This displays all your currently defined deployment stage categories.
d. Use the **Actions > New**, **Actions > Open** and **Actions > Delete** menus or the New and Delete icons to create, modify and delete deployment stage categories. You cannot modify or delete the Not Specified category.

— **Locale**: This displays the server's current locale setting.

— **UUID**: A unique identifier for the managed server.

— **Object ID**: This displays the internal identifier that SA uses to identify the server.

— **Status**: This displays whether or not the server is reachable and thus managed by SA. "OK" means that the server (its Server Agent) is reachable; unreachable means that there is a communication problem and SA cannot communicate with the server.

Custom Fields Defined for Servers

This view lists the custom fields defined for the server and the value of each custom field and lets you edit the values.

SA can store a large amount of information about your managed servers. Custom fields provide a way for you to store additional information about your servers quickly and easily. Custom fields are data elements you can create for servers and other objects in SA.

For more information about custom fields, see Comparing Custom Fields and Custom Attributes and About Custom Fields.

Tip: Custom attributes are similar to custom fields. For more information about custom attributes, see Custom Attributes Defined for a Server.

Reported Information for Servers

This view displays information about the server reported by the server agent. For more information on the server agent, see Server Agent Management.

— **Reporting**: This displays information about the ability of the server's agent to communicate with the core. Statuses include Has not reported, OK, Registration in progress, and Reporting error.

— **Agent Version**: This displays the version number of the agent. This only applies to managed servers where a Server Agent is installed.

— **Hostname**: This displays the host name of the managed server.

- **Reported OS**: This displays the operating system (platform) that the managed server is running on.
- **MAC Address**: This displays the Media Access Control (MAC) address. This is the network interface card's unique hardware number. The MAC address is used as the server's physical address on the network.
- **Serial Number**: This displays the serial number of the system. Server Automation attempts to report a chassis ID if possible.
- **Chassis ID**: This displays a unique hardware-based identifier that the Server Agent discovers, typically derived from some property of the server's chassis. As a common source for this ID, Server Automation uses an interface's MAC address or the host ID on Solaris servers, or the serial number for one of the interfaces.
- **Encoding**: This displays the character encoding of the managed server, such as Shift_JIS (Japanese) or Windows 1252 (Western).

From this window, you can also open a remote terminal on the selected server.

Server Modules

Server Modules are software modules that work with and extend the server agent to provide additional management capabilities for your servers. Most server modules are installed and managed automatically by the SA core and the server agent and do not require any administration or maintenance.

For example, the extensible discovery software module is installed automatically on servers when you perform an extensible discovery operation. For more information about extensible discovery, see the Running Extensible Discovery on Managed Servers.

The software discovery server module discovers and creates an inventory of unlicensed software, unregistered software, custom-built software and nonstandard software on your servers. For more information about software discovery, see the SA User Guide: Software Management.

Custom Attributes Defined for a Server

This view displays the custom attributes attached to a server. You can add, edit or remove custom attributes from this view.

Custom attributes can be locally defined or inherited:

- **Inherited**: Custom attribute value inherits from another source, such as a customer, a facility, a software policy, ISM control, and so on.
- **Locally Specific Value**: Custom attribute is created directly on a servers.

To create a new custom attribute, click the Add  icon, and then enter a value.

Overriding Inherited Custom Attribute Values

For all custom attributes that a server inherits from another source, such as from a customer or facility or device group, you can choose to override the inherited attribute's value.

To override inherited custom attribute values, perform the following steps:

1. In the SA Client, select Devices All Managed Servers.
2. Select a server.
3. Select the Actions menu or right click the server and select Open. This displays information about the selected server.
4. Select the Information tab.
5. Select Custom Attributes in the navigation pane. This displays all the custom attributes defined for the server. The Source column indicates where the custom attribute is defined, whether it is defined locally on the server or is defined by and inherited from another object.
6. For the inherited custom attribute you want to override, from the Source column select Overridden with Specified Value from the drop down list.
7. Enter a value in the Value field.

Tip: Custom fields are similar to custom attributes. For more information and a comparison of custom fields and custom attributes, see Comparing Custom Fields and Custom Attributes and About Custom Fields.

History of Server Changes

The History view shows changes made to the selected server. For example, it displays who modified a server, what change was made, when it was modified, and so on. Server History specifically shows when a user has performed one of the following actions:

- Added the server to a group
- Removed the server from a group
- Reassigned the server from one group to another
- Login sessions
- Jobs that were run on the server, such as snapshots, audits, patch and software policy remediations
- Custom attributes changes for servers

Entries are generated when actions are performed for managed servers in the SA Client. The History is read-only. Double-click an entry to see more detailed information, such as:

- **Date**: The date when the last change occurred.
- **Device Name**: Name of the server or device where the change was made.
- **User**: The user who made the change.
- **Details**: A description of the change.

Use the View drop-down list to sort the server history list according to a range of time, such as last week, the last two months, and so on.

Server Location

The Server Location node shows an HP ProLiant server's (BL Models only) physical location. The General category displays the following information:

- **Rack:** Rack number
- **Enclosure:** Enclosure name
- **Bay:** Server bay number

Note: Note: If the server is moved, the SA agent updates the server-location information during full hardware registration.

Server Management Policies

The Device Explorer — Management Policies provides the following information:

- Compliance
- Audits
- Archived Audit Results
- Software Policies
- Patch Policies
- This window displays all patch policies associated with the selected managed server (or groups of server group).

Compliance

The Compliance view of the Device Explorer displays overall compliance levels — a roll up of all compliance policies attached to the server — and compliance for individual compliance policies, such as audits, software and patch policies, application configurations, and any custom user-created policies.

You can select and expand a compliance category and view all tests in each category. For each test you can view policy details and remediate any tests that are out of compliance. Each compliance category contains an expandable list that contains all the policies of this type. The top-level node shows the rollup compliance status of all policies in this category. If you expand the list, you can see each individual policy and its compliance status as well, for a detailed breakdown of compliance for the server.

You can also sort the list to show all policies, or filter it to show only the policies for one compliance categories, such as all Audit policies and their compliance statuses. You can also sort by status filter, such as, show all compliance tests that are compliant, non-compliance, are currently scanning, and so on.

For more information on server and device group compliance, see the SA User Guide: Audit and Compliance.

Compliance Categories

Compliance categories a server include:

- **Audit**: A roll up compliance status of all scheduled audit that target this server appears by on the top node of the Audit category in the Details pane. This category displays the overall compliance status of all recurring audits that run on this server. To see the individual audits that use this server as a target, expand the Audit list, which shows each audit's compliance status in the Status column.
- **Software**: A roll up compliance status of all software policies attached to the server appears the top node of the Software category in the Details pane. Software compliance indicates whether or not all software policies attached to the selected server are compliant with the actual server configuration.

  A software policy can include installed packages and patches, application configurations, and other software policies. If the actual server configuration does not match the software policy definitions, then the server's software policies are considered out of compliance. To see the individual software policies attached to this server, expand the Software list, which shows each software policy's compliance status in the Status column.
- **App Config**: A roll up compliance status of all application configurations attached to the server appears the top node of the App Config category in the Details pane. An Application Configuration (App Config) policy defines how specific application configurations files should be configured on a managed server. Application Configuration compliance indicates whether or not all of the Application Configurations attached to a server are compliant with the actual application configuration files on the server. If the actual server configuration does not match the Application Configuration definitions, then the server's Application Configurations are out of compliance. To see the individual application configurations attached to this server, expand the App Config list, which shows each application configuration s compliance status in the Status column.

  Patch: A roll up compliance status of all patch policies attached to the server appears the top node of the Patch category in the Details pane. Patch compliance determines whether all patches in a patch policy and a patch policy exception were installed successfully. To test patch compliance, servers are scanned to determine whether they conform to their attached policies and exceptions, based on compliance status and rules. If any of the patches defined in the patch policy do not match what is actually installed on the server, then the server's patch policies are out of compliance. To see the individual patch policies attached to this server, expand the Patch list, which shows each patch policy's compliance status in the Status column.

Audits

Audits view shows a list of all audits associated with the server, where the selected server is either the source or the target of an audit.

Show Options

- **Audit - Server is Target**: Shows all audits where the selected server is the target of an audit.

- **Audit - Server is Source**: Shows all audits where the selected server is used as the source of an audit.

For more information, see the SA User Guide: Audit and Compliance.

Archived Audit Results

This list displays all audits results associated with this server that have been deliberately archived by a user. In some cases, audits that run regularly can accumulate many audit results. In the main Audit and Remediation feature, you can select to archive audit results if you want to save them for later viewing. All audit results for the selected server are displayed here.

Software Policies

This window displays all software policies associated with the selected server (or device group). You can perform actions such as attaching a policy, detaching a policy, remediating a server, and scanning software compliance from the **Actions** menu.

Note: (Optional) Show "Last Successful Remediation" column, to check when was a Software Policy last remediated successfully on the server.

For more information, see the SA User Guide: Software Management.

Patch Policies

This window displays all patch policies associated with the selected managed server (or groups of server group).

Show Options

The Show drop-down list displays the following patch policy information:

- **Policies Attached to the Server**: This displays all policies attached to the server, or policies attached to a server group to which the selected Windows managed server belongs.
- **Policies Not Attached to the Server**: This displays a list of all patch policies relevant to the selected server that are not attached to the server.

Configured Applications

The Configured Applications screen shows all the Application Configurations attached to the managed server. Each node under the Configured Applications node represents an application configuration attached to the server. Each subnode under each application configuration lists all the instances of the application configuration defined for the server.

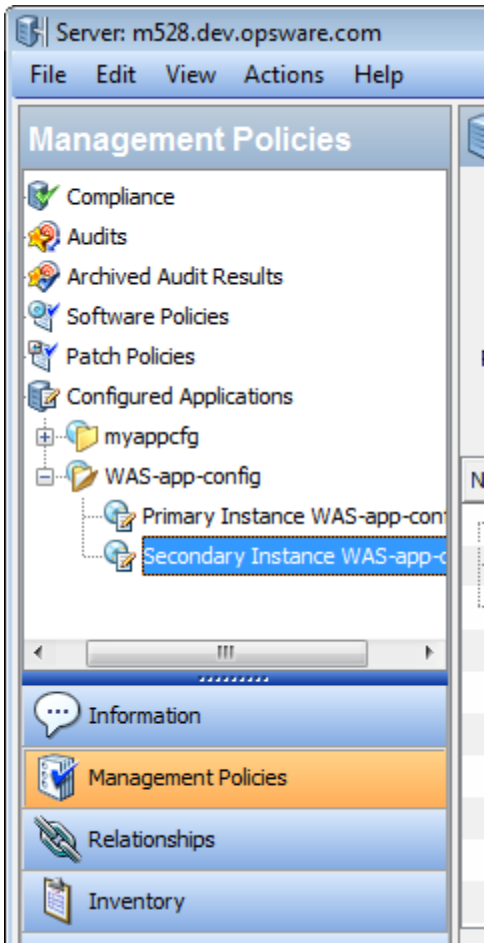
You can edit the value sets at the server level and the server instance level.

- Selecting the Configured Applications node displays all the application configuration instances available to be pushed to the selected server.
- Selecting an application configuration displays the value set in the value set editor at the server level for the selected template.

- Selecting an instance of an application configuration displays the value set in the value set editor at the server instance level for the selected template.

For complete information on managing software and application configurations, see the SA User Guide: Application Configuration.

The example below shows two application configurations attached to the server m528 named myappcfg and WAS-app-config. Two instances are defined for WAS-app-config named “Primary Instance WAS-app-config” and “Secondary Instance WAS-app-config”.



Running a Script on the Server

The **Run Script** button executes the selected Application Configuration’s data-manipulation script. If the application configuration contains no data-manipulation script, the **Run Script** button is disabled. For more information, see the SA User Guide: Application Configuration.

Previewing an Application Configuration Push Operation

The Preview button compares the configuration file on the server with the configuration file defined by the selected instance and shows the two files. For more information, see the SA User Guide: Application Configuration.

Push an Application Configuration to the Server

Thie Push button saves any changes you have made to the Application Configuration and starts the Push Configurations wizard to push the selected instance of the configuration file to the server. For more information, see “About Pushing Application Configurations to Servers” in the SA User Guide: Application Configuration.

Relationships with Other Devices

The Relationships view of the Device Explorer lists all device groups of which this server is a member. Members of a group can include servers, network devices (for NA-enabled cores), storage devices and assets (for SE-enabled cores), and other device groups.

You can select a group, right-click and select **Open** to view its contents. You can also select to Add to Group to select other devices to add to the group.

If the list of groups is long, use the search tool  to locate a server (upper right corner) by name, description, access, type, modified by, and so on. If you search by device group name, the text entry is case insensitive.

Storage Relationships

If your core is configured to connect to SE, Device Explorer view also gives you viewing access to various storage objects such as SAN switches, SAN fabrics, storage targets, and databases. For more information on these storage objects and relationships, select an object and press F1, or see the Storage Visibility and Automation User Guide.

Inventory of Server Information

The Inventory tab provides the following information about the selected server:

- Hardware
- Network
- Storage
- Disks
- Virtualization View
- Snapshot Specifications
- Installed Packages
- Patches for the Server
- Files on the Server
- Windows COM+ Objects
- Windows IIS Metabase
- Windows IIS 7.0
- Internet Information Server (IIS)

- Windows Registry
- Services (Windows and Linux)
- Windows .Net Framework Configuration
- Local Security Settings
- Registered Software
- Runtime State
- Users and Groups

Hardware

The Hardware view lists all the reported hardware on the selected managed server. This includes the following information:

- **Processors**: This lists the processor information for all processors on the managed server.
- **Memory**: This lists the total amount and the types of memory on the managed server.
- **Storage**: This lists all storage devices on the managed server.
- **Network Interfaces**: This lists the network interfaces on the managed server, including Ethernet cards (NICs) and any Fibre Channel Adapters, ports—including the switch ports that a port is connected to as well as any zones.

Network

The Network view shows all network connections (or SAN, for Storage-enabled cores), providing the IP address, subnet mask, MAC address, duplex and speed settings, DHCP settings and the interface type for all network interfaces.

This view also shows the network configurations for the selected server including the host name, the DNS domain, the SA facility, the name and IP address of the management interface, the IP address of the gateway, the IP addresses of the DNS servers and the search domains.

Storage

If your core is configured to connect to SE, the Inventory tab includes a Storage view that provides information about SAN, NAS and DAS (Direct Attached Storage) assets related to the selected server.

This view also provides a summary of the storage (if applicable) consumed by and allocated to the selected server, as well as insight into Database storage (if applicable) consumed by the selected server.

Note: In order to view storage devices and SAN information inside of the SA Client, Storage Essentials (SE) version 6.1.1 or later and the Server Automation SE Connector component must be installed and configured your SA core. For more information, contact your SA sales representative.

This Storage view provides details about the following storage assets:

- **File Systems**: Shows a list of local and remote file systems (SAN-based storage). It provides information such as mount location, type of file system, storage capacity and free space. From the View drop-down list, you can select four different views into File Systems:
  - **Properties**: Displays information like mount location, description for mount point; mount point, type of file system, storage capacity and free space.
  - **Volumes**: Displays a list of volumes based on the selected file system.
  - **Disks**: Displays a list of disks on which the selected file system is dependent.
  - **Connectivity**: Displays supply chain information for the selected file system in a tree format.
- **Volumes**: Shows a list of volumes consumed by the selected server. These volumes could be local or remote (SAN volumes). From the View drop-down list, you can select four different views into Volumes:
  - **Properties**: Displays the name, type, service type, status and storage capacity for the selected volume.
  - **Composition**: Displays *upstream* and *downstream* storage dependencies. Upstream storage dependency means that the storage asset depends on the selected volume; downstream storage dependency means that the selected volume is dependent upon other storage assets.
  - **Disks**: Displays the list of disks on which the selected volume is dependent.
  - **Access Path**: Displays data which is mostly interesting if the selected volume is a remote SAN volume. This sub-view provides LUN Mapping information for the remote SAN Volume — the target storage array, target storage array port, target storage volume, LUN number and initiator port.
  - **Connectivity**: Displays the supply chain information for a volume in a tree format. This view is useful in the context of remote SAN volumes.
- **Unmounted Volumes**: Shows a list of volumes that are available to the selected server but that are not used by the server. These volumes are typically remote SAN volumes which are mapped to the selected server but the server is not using them. From the View drop-down list, you can select four different views into Unmounted Volumes:
  - **Properties**: Displays name, type (raid type), service type, status, storage capacity and target device for the selected Unmounted volume.
  - **Composition**: Displays *downstream* storage dependencies, which means that the unmounted volumes are dependent upon the selected storage asset.
  - **Disks**: Displays the list of disks on which the selected unmounted volume is dependent.
  - **Access Path**: Displays data which is mostly interesting if the selected unmounted volume is a remote SAN volume. This sub-view provides LUN Mapping information for the remote SAN Volume — the target storage array, target storage array port, target storage volume, LUN number and initiator port.

  - **Connectivity**: Displays the supply chain information for a unmounted volume in a tree format. This view is useful in the context of remote SAN volumes.
- **Disks**: Shows information about local and remote (SAN-based) disks. Detailed information includes name, manufacturer, model, device (server), storage capacity, status and if its spare or not. From the View drop-down list, you can select two different views into Disks Volumes:
  - **Volumes**: Displays list of volumes based on the selected disk.
  - **File Systems**: Displays a list of file systems based on the selected disk.
- **Manager Software**: Shows information about Volume Manager software and MultiPath software on the selected server, including vendor, version and details about logical volumes managed like name, type (RAID Type), service type, status, storage capacity and number of paths.

Disks

The Disks views provides local disk information for the managed server, including such information as disks names, manufacturer, the device that contains the disk, model number of the disk, its capacity, its status (identifies the disk health, such as OK, ONLINE, Disable, Not Ready, Error, READONLY), and whether the disk is used as a spare (Yes) or not used as a spare (No).

Virtualization View

The Virtualization view shows you the following details about the selected item in your virtualization inventory:

- Cluster - Number of hosts and processors in the cluster, CPU and memory resources available in the cluster, and resource allocation settings.
- Datacenter - Datacenter name, technology, and the VS managing it.
- Folder - Folder name, and the VS it resides on.
- Host - Hypervisor name, VS it is running on, CPU and memory usage, virtual networks, and storage configured on the host.
- **Host Groups** – In SCVMM, containers you can create to group a set of virtual machine hosts for easier management. Host groups are hierarchical and can contain other host groups.
- Projects – A project is a logical grouping of users that defines quotas and access to VM images.
- **Resource Pool** – In VMware, a way to divide the resources of a host or a cluster into smaller pools. A resource pool contains a set of CPU and memory resources that all the VMs running in the resource pool share. Resource pools provide the ability to balance workloads across the resource pool.
- Virtual Machine (VM) - VM name, VS it is being managed by, host it is running on, CPU and memory information, guest OS, power state, how it was created, virtual networks, and storage configured on the VM.
- **VM Template** – A specification for a virtual machine. You can create a virtual machine from a VM template and you can create a VM templates from a virtual machine. A VM template

typically includes an OS Build Plan for installing an operating system, patch policies that specify patches to be installed, software policies that specify software to be installed, application configurations that specify how the software should be configured, audit policies that specify rules that define compliance, and the SA agent for managing the virtual machine. VM templates allow you to control what type of virtual machines get created and they allow you to keep your virtual machines in compliance.

- Virtualization Service - VS name, VS vendor, VS version, IP address, port number, and administrative user.

For more information on managing virtual machines, hypervisors, and virtualization services, see the SA User Guide: Virtualization Management. For a list of icons and their meanings, see Server Status Icons.

Solaris Zones — Device Explorer

You can use the Device Explorer to view a Solaris global zone hypervisor and local zone server information. A global zone or local zone as seen through the Device Explorer looks nearly the same as a regular physical server, except that it has an extra property named “Virtualization,” which provides the following information:

- **Hypervisors**: When you view a Solaris global zone hypervisor in the Device Explorer, the Virtualization view shows all hosted local zones. From here, you can also stop and start the local zones.
- **Solaris Local Zones**: When you view a Solaris local zone in the Device Explorer, the Virtualization view indicates the name of its hypervisor, its reserved CPU shares, and virtual hardware information.

VMware ESX — Device Explorer

You can use the Device Explorer to view a VMware vCenter Server (virtualization service), a VMware ESX hypervisor’s server information, and VM (virtual machine) information. A VM as seen through the Device Explorer looks nearly the same as a regular physical server, except that it has an extra property named “Virtualization,” which provides the following information:

- **Virtualization Service: For servers hosting a VMware vCenter Server or OpenStack, the Device Explorer gives the vCenter or OpenStack version, IP address, port number, user name, and other information about the server.**
- **Hypervisors**: For servers hosting a VMware ESX hypervisor, the Device Explorer shows the virtualization service hosting the server, the connection state of the server, the virtual networks attached to the server, the datastores attached to the server, and other information about the server.
- **VMware VMs**: When you view a VMware VM in the Device Explorer, the Virtualization view shows you the hypervisor hosting the VM, the virtualization service managing the hypervisor, the VMs genealogy - how it was created, the VMs memory and CPU allocations, its virtual network configuration, its storage configuration, and other information about the VM.

Windows Hyper-V — Device Explorer

You can use the Device Explorer to view a Windows Hyper-V partition or a hypervisor’s server information. A partition, as seen through the Device Explorer, looks nearly the same as a regular

physical server, except that it has an extra property named “Virtualization,” which provides the following information:

- **Virtualization Service: For servers hosting a Microsoft System Center Virtual Machine Manager or OpenStack, the Device Explorer gives the SCVMM version, IP address, port number, user name, and other information about the server.**
- **Hypervisors**: For servers hosting a Windows Hyper-V hypervisor, the Device Explorer shows the virtualization service hosting the server, the connection state of the server, memory information, the virtual networks attached to the server, and other information about the server.
- **Windows Hyper-V VM**: When you view a Windows VM in the Device Explorer, the Virtualization view shows you the Hyper-V hypervisor hosting the VM, the virtualization service managing the hypervisor, the VMs genealogy - how it was created, the VMs memory and CPU allocations, the power state, its virtual network configuration, its storage configuration, and other information about the VM.

Snapshot Specifications

The Snapshot Specifications view shows a list of all Snapshot Specifications where the selected server is listed as a target. To view the results of one of the Specifications, select it in the Contents pane (right side). When you select a Snapshot Specification, a list of all snapshot results appear in the pane below (for all servers that are targets of the Snapshot Specification).

To open a Snapshot Specification, select one, right-click, and select **Open** (or double-click it). To view the results of a snapshot, select one from the lower pane, right-click, and select **Open** (or, double-click it).

Installed Packages

The Installed Packages view enables you to view any installed packages on the selected managed server that are managed by SA. For each package, you can view name, type, size, last modified, and description. To sort the list by these categories, click the title of each column. See the SA User Guide: Software Management for information on how to create a package.

For information about using the Device Explorer to see packages that exist on the manager server but are not yet managed by SA, see Patches for the Server.

Patches for the Server

This window displays all patches associated with the selected managed server.

Show Options – Windows

You can use the Show drop-down list to filter the following types of patch information:

- **Patches Installed**: This option displays all patches that have been installed on the server.
- **Patches Recommended By Vendor**: This option displays all application and operating system patches that have been recommended by the Windows patch database for the selected server. If multiple patches have the same QNumber, Patch Management detects the

application files that are already installed on a managed server and, subsequently, recommends the correct patch to install.

- **Patches with Policies or Exceptions**: This option displays patches in policies attached to the selected server, or patches that have 'always install' or 'never install' exceptions, *and* have one of the following conditions:
  - The patches are not currently installed and are recommended by the vendor.
  - The patches are currently installed.
- **Patches Needed**: This option displays all patches that should be installed on the selected server but are not. These include patches that are in policies attached to that server, or patches that have always install exceptions, *and* are recommended by the vendor.
- **Patches with Exceptions**: This option displays all patches that have exceptions (such as always install or never install) a*nd* have one of the following conditions:
  - The patches are not currently installed and are recommended by the vendor.
  - The patches are currently installed.
- **All Patches**: This option displays all patches that are associated with the operating system of the server.

Show Options – UNIX

The Show options for UNIX patches display the following information:

- **All Patches**: This option displays all patches that are associated with the operating system of the server.
- **Patches Installed**: This option displays all patches that have been installed on the server.

Patch Contents – Windows

The Show options for Windows patches display the following information:

- **Icon**: A dimmed icon means that the patch has not yet been uploaded to the Software Library.
- **Name**: This is the QNumber of a patch that is a hotfix or an update rollup. Service pack patches do not have a QNumber.
- **Compliance**: This shows one of the following three levels of patch policy compliance, as defined by a patch administrator:
  - Policy Only: Compliance that includes the policy only.
  - Policy and Exception: Compliance that includes the policy and the policy exceptions.
  - Customized: Customized compliance.
  - **Non-Compliant** (red): This indicates that the patch is installed on the server, but is not in the policy, or that the patch is not installed on the server but is in the policy.
  - **Partial** (yellow): This indicates that the policy and exception do not agree, and the exception does not have data in the Reason field.
  - **Compliant** (green): This indicates one of the following conditions:

  - A patch is installed on the server and is in a policy, or a patch is not installed on the server and is not in a policy.
  - A patch is installed on the server and there are additional patches with the same QNumber in a patch policy or exception. In this case, all patches with the same QNumber are considered installed when Patch Management calculates patch compliance.
  - A patch is not installed on the server and is in a patch policy or has an always install exception, and is not recommended by the vendor. In this case, the patch has a never install exception, because it is not recommended by the vendor.

  In the Preview pane, move the cursor over the icon or text in the Compliance column to view patch compliance information about a server.
- **Type**: This shows the type of patch, such as Windows Hotfix or Windows Update Rollup.
- **Bulletin**: (Optional) This shows the Microsoft Security Bulletin ID number for this patch.
- **Severity**: (Optional) This shows one of the following three Microsoft severity ratings for this patch:
  - **Critical**: This indicates a patch whose exploitation could allow the propagation of an internet worm, without user action.
  - **Important**: This indicates a patch whose exploitation could result in a compromise of the confidentiality, integrity, availability of user data, or of the integrity or availability of processing resources.
  - **Moderate**: This indicates a patch whose exploitability is mitigated to a significant degree by certain factors, such as default configuration, auditing, or the difficulty of exploitation.
  - **Low**: This indicates a patch whose exploitation is extremely difficult, or whose impact is minimal.
- **Release Date**: This displays the date that Microsoft released this patch.
- **Exception**: This displays the type of patch policy exception set for the selected server.
- **Installed**: This shows if the patch is installed on the selected server.
- **Recommended**: A check mark indicates that this patch was recommended by the vendor (Windows patach databae) during the last software registration.
- **Description**: This displays a description of the server.
- **Opsware ID**: (Optional) This displays a unique Opsware ID that identifies the patch object.
- **Locale**: (Optional) This displays the encoding of the patch contents.
- **OS**: (Optional) This displays the operating system version of the server.

Patch Contents – UNIX

This shows the following Unix patch content information:

- **Icon**: A dimmed icon means that the patch has not yet been uploaded to the Software Library.
- **Type**: This shows the type of patch, such as Solaris Patch, HP-UX Patch Fileset, and so on.

- **Installed**: This shows if the patch is installed on the selected server.
- **Description**: This displays a description of the server.
- **Install Date**: This displays the date the patch was installed on the server.
- **Opsware ID**: (Optional) This displays the unique Opsware ID that identifies the patch object.
- **OS**: (Optional) This displays the operating system version of the server.

Files on the Server

The Files view enables you to browse the file system of a managed server. The File System has two main sections (similar to the Windows file system explorer): the server's directories and the contents of the selected directory.

The left side navigation panel of the Device Explorer shows all the directories of the selected server, and the right side of the Device Explorer lists the contents of the selected directory.

For each file, the SA Client lists the file's name, size, type, and date modified. To sort the files by any of these categories, click on the top of the column.

Note: Depending upon your user permissions, you might not have access to a particular server's file system. In such a case, you cannot select and view the server's file system in the Device Explorer. If you have access to a server's file system, then you will see user names, such as Administrator, root, and Local System. These are user names used to access that server's file system as the selected user.

Viewing File Contents

To view file contents, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select **Devices** > **All Managed Servers**.
2. A list of servers will display in the Content pane. Select a server and open it. This opens the Device Explorer.
3. From the left side of the Device Explorer, select a File System object.
4. Select a user name to log into the computer, such as Administrator, LocalSystem, or root. Select a user.
5. To view the contents of disk drives or folders, expand the icon. Select a directory.
6. From the **Actions** menu, select **View Contents**. The file content view pane appears at the bottom of the window.
7. To change the character encoding, select an item from the Encoding drop-down list.

Ways to Copy Files

You can copy files from a server to another directory on the same server, to a directory on another SA-managed server, or to your local computer (where the SA Client is running). You can also copy a file from your local computer to a directory on the managed server. A few restrictions apply when copying files on a managed server's file system using the Device Explorer:

- You cannot copy folders/directories.

— You can only copy to servers that you have permissions to write to and to view.

— You can only copy one file at a time.

— You cannot undo a deletion — once you delete a file, it's gone.

Copying Files Between Managed Servers

To copy files between managed servers, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select the **Devices** > **All Managed Servers**.
2. To launch the Device Explorer, open a server from the server list.
3. From the left side of the Device Explorer, select a File System object. To view the contents of disk drives or folders, expand the icon.
4. Navigate to the directory that contains the file that you want to copy and select it.
5. From the **Actions** menu, select **Copy To**.
6. In the Copy To dialog box, select from the following locations in the drop-down list:
   - Managed Servers (other managed servers in the core)
   - This Server
   - Local File System
7. Navigate to the desired directory.
8. Click **Select**.

Copying Files from Your Computer to a Managed Server

To copy files from your computer to a managed server, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select **Devices** > **All Managed Servers**.
2. To launch the Device Explorer, open a server from the server list.
3. From the left side of the Device Explorer, select a File System object.
4. Navigate to the target directory where you want to copy the file.
5. Use your system's file system explorer to select the file that you want to copy, then drag the file to the desired location in the Device Explorer.

Deleting Files

Once you delete a file, it cannot be recovered. (However, before you delete, you are prompted with a confirmation dialog box.)

To delete a file, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select the **Devices** > **All Managed Servers**.
2. To launch the Device Explorer, open a server from the server list.
3. From the left side of the Device Explorer, select a File System object.
4. Select a file to delete from the Content pane.
5. From the **Actions** menu, select **Delete**.
6. Click **Yes** in the confirmation dialog box.

Renaming Files

To rename a file, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select the **Devices** > **All Managed Servers**.
2. To launch the Device Explorer, open a server from the server list.
3. From the left side of the Device Explorer, select the File System object. To view the contents of a folder, expand the folder.
4. Select the file that you want to rename, and from the **Actions** menu, select **Rename**.
5. Enter a new name for the file, then press ENTER. Pressing the ESC key on your keyboard will cancel the rename operation.

Creating a Configuration Template from a File

For any file on a managed server, you can create a configuration template.

To create a configuration template from a file, select the file. From the **Actions** Menu, select **Create Configuration Template**. See the SA User Guide: Application Configuration for more information.

Creating a Package from a File

For any file on a managed server, you can create an installable software package. For each package, you can specify the customer assignment, the reboot requirements, and the pre/post install and pre/post uninstall scripts.

To create a package from a file on the managed server file system, select the file. From the **Actions** menu, select **Create Package**. See the SA User Guide: Software Management for information on how to create a package.

Windows COM+ Objects

This window displays a read-only view of all the COM+ objects on the selected managed server. In the Server Explorer window, the Views pane displays the following two folders for browsing COM+ objects:

- **All Objects**: This is a flat list of all the COM+ objects on the managed server.
- **Component Categories**: This contains an alphabetical list of all COM component categories.

To view the contents of a COM+ object, perform the following steps:

1. Select the All Objects or the Component Categories folder. In the Content pane, expand the folder until you reach an object.
2. To view the contents of a COM+ object, from the **Actions** menu, select **View Contents**. The contents will then display.
3. If the content of the COM+ object uses a different encoding, choose the appropriate encoding type from the Encoding drop-down list.
4. You must have specific user permissions to view Windows COM+ objects. If you are unable to access the Windows Registry, contact your SA administrator.

Windows Registry

This window displays a read-only view of the Windows registry on the selected Windows managed server. You can navigate to this registry much like the regedit tool on the Windows operating system.

Folders on the left side of the window represent keys in the registry. Clicking a folder on the left displays entries in a key in the right window.

To view Windows Registry items, select the top-level Windows Registry icon in the Server Explorer and select a user from the menu. Your user must have proper permissions to view Windows Registry keys. If your user is unable to access the Windows Registry for the selected managed server, contact your SA Administrator.

Note: The HKEY_CLASSES_ROOT might have thousands of entries and can take time to load.

Services (Windows and Linux)

The Services window shows you a list of all running services on the selected managed server. Depending on the installed operating system, you can perform different operations on the services:

- For Windows services, you can start, stop, pause, resume, and restart a service. You can also set the service to start manually, to start automatically when the system is rebooted, or to be disabled altogether.
- For Linux servers (supported by Red Hat, SuSE and Ubuntu versions), you can perform any action that a particular service supports. Supported actions can vary based on the specified service, for example, start, stop, restart, condrestart, or status. You can also specify the run level for a service.

  Note that *Upstart* managed services, on Red Hat Enterprise Server 6 and Ubuntu 12.04, or *systemd* managed services, on Red Hat Enterprise Server 7, will only display the run level; not change it.

To perform an operation on a service, select the service and right-click.

Discovered Software

The Discovered Software feature provides a signature-based software discovery mechanism for Windows and UNIX managed servers to help you manage applications and software that are not managed by SA.

Specifically, Discovered Software:

- Discovers unregistered software which is not currently managed by SA.
- Creates an inventory of software that is not installed as part of an OS-registered application, or that was custom built

- Provides system administrators the ability to create snapshots of the discovered software on a server and then periodically audits against the snapshots over time.
- Enables system administrators to track in-house or custom built software.
- Gives auditors a convenient method for discovering unsupported or unlicensed software installed on a server.

To enable this feature, you need to create an “inventory” snapshot of a server, which takes a picture all of the software and application information on the server. Additionally, you can also use an audit to capture the current state of a server’s software installations and, by running the audit on a regular schedule, you can monitor any installation changes over time.

For more information on creating an inventory snapshot, see the SA User Guide: Audit and Compliance.

Windows IIS Metabase

This window displays a read-only view of the IIS Metabase on the selected Windows managed server. You can use this window to browse the IIS Metabase much like one of the metabase browsing tools such as metaedit or the IIS Metabase Browser.

The left side of the Metabase window displays the hierarchical layout of the metabase tree. Selecting an item in the tree on the left shows the data items associated with the selected key in the right hand view. Clicking the (+) symbol to the left of a key item will expand the item's child keys.

To view Windows IIS Metabase items, select the top-level Windows Metabase icon in the Server Explorer, right-click, and select a user. Your user must have permissions to view Windows Metabase items. If your user is unable to access the Windows Registry, contact your SA Administrator.

Windows IIS 7.0

The Windows IIS 7.0 server module allows you to view various elements and configuration of a server’s IIS 7.0 application, such as Application Pools, Web Sites, and Features.

Add to Library/Add to Software Policy

From inside a server’s Device Explorer > Inventory, you can add selected IIS 7.0 configuration items to the SA library or to a software policy.

For example, you can expand the IIS 7.0 Application Pools hierarchy in the Device Explorer, select an AppPool, right-click, and select **Add to Software Policy**. Using software policies, you can create a policy based upon the Application Pool configuration, attach it to other servers, and then remediate (install) onto other servers running IIS 7.0 and force them to conform to your company’s standards.

If you select Add to Library, the IIS 7.0 configuration item becomes accessible to other users on your data center, for use specifically in software policies.

For more information on using Software Policies, see the SA User Guide: Software Management.

Using with Audits and Snapshot Specifications

You can also use IIS 7.0 inside of audits and snapshot specifications. In a snapshot specification, you can capture the state of your IIS configuration on a server you know to have a good configuration (a "golden" server), and use that to compare against other "target" servers running IIS 7.0. If any target server IIS 7.0 configurations do not match the golden server's IIS 7.0 configuration, you can remediate those servers to ensure they are configured how you want them to be.

You can also use Audits to check a server's IIS 7.0 configuration on a time or regular basis, so you can keep track of a server's IIS 7.0 configuration, and remediate the server if it ever becomes "non-compliant."

For more information on creating audits and snapshot specifications for auditing and snapshotting IIS 7.0 configurations, see the SA User Guide: Audit and Compliance.

Internet Information Server (IIS)

The Internet Information Service (IIS) window allows you to view the real time information about IIS for a Windows server. For a Windows server you can view IIS information such as Server name, Server type, Server state, Log file path, and Document file path.

Note: For servers running IIS 7.0 or greater, the IIS information is available in the Windows IIS Settings module. In this module, you can view IIS information such as Application Pools, Sites, and Features. See the *SA Administrators Guide* for information on permissions.

Note: When you access the Internet Information Server for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

Using the Audit and Remediation feature you can specify audit rules for the Internet Information Service to compare Internet Information Service configurations against a baseline server, or user-defined values, or a server snapshot. For more information, see the SA User Guide: Audit and Compliance.

Local Security Settings

The Local Security Settings window allows you to view the real time information about security settings for a Windows managed server. For every Windows server you can view security settings such as Password policy, Audit policy, User rights, and Security options.

To view the information for the Local Security Settings server object, you will need the appropriate permissions. See the SA Administration Guide for information about the permissions required for the server object.

Note: When you access the Local Security Settings for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

In the SA Client you can manage the Local Security Settings information by adding it to a software policy or audit.

- Using the Software Management feature, you can deploy the Local Security Settings on a managed server. See the SA User Guide: Software Management for information.
- Using the Audit and Remediation feature you can specify the audit rules for the Local Security Settings and then remediate any differences found between the target server and the audit rule. See the SA User Guide: Audit and Compliance.

Registered Software

The Registered Software view allows you to view real time information of all the packages and patches installed on a managed server. For each package or patch you can view information such as Name, Version, Release, Unit Type, and Installed Unit.

To view the information for Registered Software, you will need the appropriate permissions. See the SA Administration Guide for information about the permissions required for the server object.

Note: When you access Registered Software for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

Using the Audit and Remediation feature you can specify the audit rules for Registered Software to compare package and patch configurations against a baseline server, or user-defined values, or a server snapshot. For more information, see the SA User Guide: Audit and Compliance.

Runtime State

The Runtime State window allows you to view real time information about the run time data for a managed server. It provides information about the DNS servers, Routes, and Processes for every managed server.

To view the information for the Runtime State server object, you will need the appropriate permissions. See the SA Administration Guide for information about the permissions required for the server object.

Note: When you access the Local Security Settings for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

Using the Audit and Remediation feature you can specify the audit rules for the Runtime State to compare Runtime state configurations against a baseline server, or user-defined values, or a server snapshot For more information, see the SA User Guide: Audit and Compliance.

Windows .Net Framework Configuration

The Windows .Net Framework Configuration window allows you to view real time information about Assembly Cache and Configured Assembly List for a Windows server.

For each Assembly Cache you can view information such as Assembly Name, Version, Locale, Public Key Token, Cache file (GAC or ZAP), Processor Architecture, Custom, and File name.

For every Configured Assembly List, you can view information such as Assembly Name, Public key token, Codebases, Binding policy, File name, File data.

To view the information for the Windows .Net Framework Configuration server object, you will need the appropriate permissions. See the SA Administration Guide for information about the permissions required for the server object.

Note: When you are accessing the Windows .Net Framework Configuration for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

In the SA Client you can manage Windows .Net Framework Configuration information by adding it to a software policy or audit.

- Using the Software Management feature, you can deploy the Windows .Net Framework Configuration on a managed server. See the SA User Guide: Software Management for more information.
- Using the Audit and Remediation feature you can specify the audit rules for assembly cache and configured assemble list and then remediate any differences found between the target server and the audit rule. For more information, see the SA User Guide: Audit and Compliance.

Users and Groups

The Windows Users and Group window allows you to browse and manage users and groups information on a Windows server. The UNIX Users and Group window allows you to browse and manage users and groups information on a UNIX server.

For every SA User you can view information such as Name, Description, Country code, Home directory, Password, Number of Logons, and Last logoff and logon time.

For every SA User Group you can view information such as Group Name and Description.

To view the information for the User's and Groups server object, you will need the appropriate permissions. See the SA Administration Guide for information about the permissions required for the server object.

Note: When you access the Users and Groups for the first time, it may take a few minutes to load the server object. Subsequent usage of the server object will be significantly faster.

In the SA Client you can manage the Users and Group information by adding it to a software policy or audit.

- Using the Software Management feature, you can deploy the Users and Groups on a managed server. See the SA User Guide: Software Management for information about the Software Management feature.

- Using the Audit and Remediation feature you can specify the audit rules for the Users and Groups and then remediate any differences found between the target server and the audit rule. For more information, see the SA User Guide: Audit and Compliance.

Basic Server Management Tasks

You can perform the following basic server management tasks in the SA Client:

- Refreshing Server Status
- See "Deactivating a Server"
- Rebooting a Server
- Opening a Remote Terminal
- Changing User Passwords on Managed Servers
- Running Server Communication Tests

Refreshing Server Status

Refresh a server to see if anything has changed on the server since you last looked at it in the SA Client. Refreshing a server retrieves the latest server information from the model repository and displays it. Refreshing a server's status is good idea from time to time to make sure you are looking at current data on the server.

For more information on server statuses, see Ways to Use the Device Explorer.

To refresh a server's status, perform the following steps:

1. Launch the SA Client. From the Navigation pane, select **Devices**.
2. Select one of the server categories, such as Device Groups, All Managed Servers, Unprovisioned Servers, or Virtual Servers. (You cannot refresh server status of unmanaged servers or a device group.)
3. Select one or more servers.
4. Right-click or select the **Actions** menu and select **Refresh Server**.

Deactivating a Server

Perform the following steps to deactivate a server:

1. From the navigation panel, click Servers > Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to deactivate.

   Or

   Search for the server that you want to deactivate.

   See See "Searching for Servers or Other Resources" and See "Server Searching by IP Address" for more information.
2. Select the servers that you want to deactivate.
3. Choose Edit > Deactivate Server from the menu above the Manage Servers list. A confirmation dialog box prompts you to confirm the deactivation.

4 Click OK. The Manage Servers list refreshes and the server appears with a deactivated icon.

Note: You cannot deactivate an SA Core server, only managed servers.

Rebooting a Server

You can reboot a single server or a group of server immediately, or schedule the reboot for a later time. If you choose to reboot a group of servers, all servers contained in the group will be rebooted.

Note: In order to be able to reboot a server, your user needs to belong to a user group that has the Reboot Server permission. For more information, contact your SA Administrator.

Caution: If you are rebooting a hypervisor server that is hosting other virtual servers, then all virtual servers being hosted by that hypervisor will be shut down as well. Whether or not the hosted virtual servers get rebooted depends upon the individual virtual server's configuration.

To reboot a server, perform the following steps:

1 Launch the SA Client.

2 From the Navigation pane, select **Devices** > **All Managed Servers** or > **Device Groups**.

3 Include these scripts in a software policy related to the server you want to reboot: `reboot_script.txt`, `to_MAINTENANCE`, `to_OK`.

4 Alternatively, before you reboot, run the following script to set the server to maintenance mode before you reboot the server: `to_MAINTENANCE`.

5 Select a server or group of servers, right-click, and select **Reboot Server**.

6 In the Reboot Server window, step one lists the server or servers you have selected to reboot. Click **Next**.

7 In the Scheduling page, choose if you want to reboot the server or group of servers immediately, or at some later time and date. To run the reboot at a later time, select **Run Task At**:, and then choose a day and time.

8 Click **Next**.

9 In the Notifications page, by default your user will not have a notification email sent when the reboot finishes, whether or not the reboot job is successful. To add an email notifier, click **Add Notifier** and enter an email address.

10 (Optional) You can specific if you want the email to be sent upon success of the reboot job ( ) and/or failure of the reboot job ( ).

11 (Optional) You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when SA Professional Services has integrated SA with your change control systems. It should be left blank otherwise.

12 Click **Next**.

13 In the Summary View page, click **Start Job** to reboot the selected server or group of servers. When the job has run, click **View Results** to view the results of the reboot job.

14 In the Job Status page, you can see the progress of the job if you ran the job immediately. If the job is scheduled to run, you can close the window, and to view the job details, from the left side of the SA Client, select **Jobs and Sessions** > **Job Logs**.

15 Run the `to_OK` script to reset the server to normal mode.

SA Tasks that Reboot a Server

There are a few other SA tasks that will initiate a server reboot, depending on the options set in the task:

- Installing or uninstalling a patch on Windows or UNIX servers. See the SA User Guide: Server Patching for more information.
- Remediating a Patch policy. See the SA User Guide: Server Patching for more information.
- Installing a package and remediating a software policy. See the SA User Guide: Software Management for more information.

Opening a Remote Terminal

To open a remote terminal for any managed server, perform the following steps:

1 From the SA Client navigation pane, select the **Devices** tab**.**

2 In the navigation pane, select **All Managed Servers**.

3 Select a managed server.

4 Select the Actions menu or right click and select **Open With** > **Remote Terminal.** For some operating systems, this displays a menu of users with which to log in, typically root, Administrator and root administrator. Otherwise this opens a window to the managed server.

5 If a menu of users is displayed, select the desired user to log in with. Otherwise skip this step.

6 Log in to the remote terminal.

Changing User Passwords on Managed Servers

You can change the password of any user on any of your managed servers using the SA Client. Perform the following steps.

1 In the SA Client, select the Devices tab. This displays the Device Groups node and the Servers node in the navigation panel.

2 Under the Servers node, select All Managed Servers or Virtual Servers. This displays all the corresponding servers. Select one or more servers

   Or under Device Groups, select one or more device groups.

3 Select the **Actions** menu or right click and select **Run Extension** > **Change User Passwords for Selected Servers**.

   Or, if **Run Extension** > **Change Passwords** is not shown, select **Run Extension** > **Select Extension**. This displays the Select Extension window and lists the available extensions.

Select **Change User Passwords for Selected Servers** in the Select Extension window then select OK.

This displays the Run Program Extension window showing the servers and device groups you selected.

4. You can optionally add servers and device groups with the Include Devices button or remove selected servers and device groups with the Remove button.
5. Select the Next button to display the Program Properties with the name of the extension you are running. Verify that it is the Change User Passwords for Selected Servers extension.
6. Select the Next button to display the Options screen.
7. **Run as root or Administrator:** This setting specifies the login credentials to use on the managed servers to perform the change password action. Select Yes to use root or Administrator. Select No to perform the operation as the user whose password you are changing. If you selected No, you must enter the user's current password.
8. **User:** Enter the user name whose password you want to change. This user must be a valid user on all the selected servers.
9. **Current Password:** If you selected No for "Run as root or Administrator, enter the current password of the user whose password you want to change. If you selected Run as root or Administrator for the credentials, the current password is not needed.
10. **New Password:** and **Confirm New Password:** Enter the new password.
11. **Program Timeout:** This specifies how long to allow the job to run before aborting if it does not finish. This setting can be useful to ensure the job runs within a maintenance window.
12. To skip the remaining settings and start the job immediately, select Start Job. Otherwise, select the Next button to schedule when to run the password change job.
13. **Schedule** - Specify whether you want the job to run immediately or in the future. If you want the job to run in the future, specify the start time and date.
14. Select Next to display the Email Notifications screen.
15. **Email Notifications** - You can request that an email message be sent when the job finishes. Use Add Notifier and Remove to change the recipients.

    You can optionally add a ticket identifier to the job for tracking purposes. The ticket identifier is retained with the job information.
16. Select Next to display the Job Status screen.
17. **Job Status** - Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.

    Once the job finishes, you can view the results. Select a server to display the results for that server.
18. Select Close. At any time you can view the job results by selecting the Jobs and Sessions tab in the SA Client navigation panel and locating the job in the job history.

About Device Groups

Device groups let you organize servers and other types of network and storage devices into logical sets. A device group is simply a container of a set of servers and other devices. Grouping

servers lets you perform actions such as installing patches or remediating servers on all of the servers in a device group simultaneously, instead of having to perform the action on each individual server one at a time.

Below are some recommended ways of grouping servers.

- Grouping servers by OS version
- Grouping servers by customer
- Grouping servers by facility
- Grouping servers by deployment stage category
- Grouping servers by server use category
- Group servers by virtual technology
- Grouping servers by operational boundaries, for example, grouping together all servers that require identical application configurations
- Grouping servers to control access, for example, creating device groups that are associated with a specific user group

Characteristics of Device Groups

Device groups contains the following characteristics listed in Device Group Characteristics:

Table: Device Group Characteristics

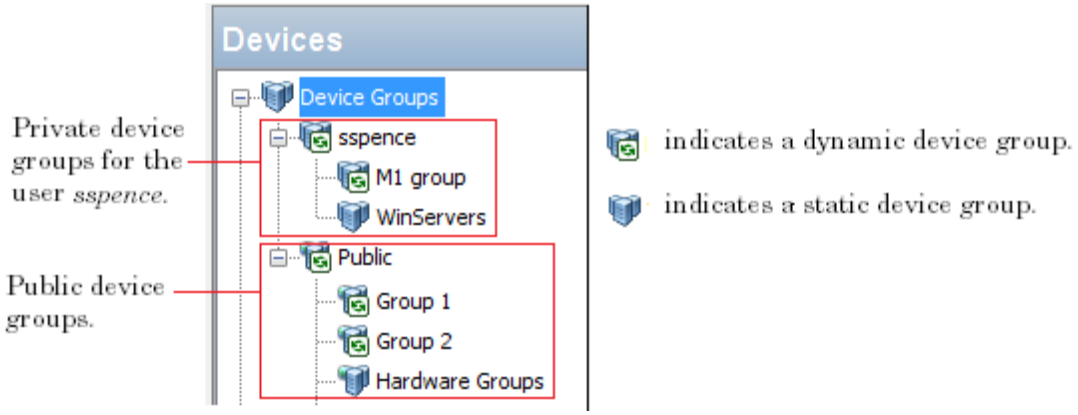
	Public Groups	Private Groups
Static Groups	Access: Visible to all. Membership: Fixed.	Access: Visible only to the owner. Membership: Fixed.
Dynamic Groups	Access: Visible to all. Membership: Based on rules.	Access: Visible only to the owner. Membership: Based on rules.

- All device groups are either public or private.
  - **Public groups** are accessible to all users with the Manage Public Device Groups permission.
  - **Private groups** are accessible only to the user who created the group.
- All device groups are either static or dynamic.
  - **Static groups** contain a fixed set of devices that you add manually to the group.
  - **Dynamic groups** contain all the servers that satisfy a set of rules that you define. Dynamic groups automatically add or remove servers based on whether or not the servers satisfy the defined rules.
- Individual servers can be included in multiple device groups or not included in any device groups.

— Adding a server to a device group does not remove the server from the All Managed Servers list in the SA Client.

Device Group Types shows these four types of device groups in the SA Client. The group named “M1 group” is a private, dynamic group. The group named “Hardware Groups” is a public, static group.

Device Group Types



Device Groups and Subgroups

Device groups can contain other device groups, called subgroups. In other words, device groups are hierarchical, meaning they can be nested, with the following caveats:

- Private and public groups cannot be mixed in a hierarchy. That is, a private group cannot be a member of a public group and vice versa.
- Static and dynamic groups can be mixed in a hierarchy. That is, a static group can be a member of a dynamic group and vice versa.
- The rules for a dynamic group are not inherited from a parent dynamic group to a child dynamic subgroup. Each group defines its own set of rules, independent of whether or not it is part of another group.
- Groups do not inherit custom attributes from their parent groups.
- When you run an operation on a device group that contains subgroups, the operation also applies to all the servers in the subgroups. For example, remediating a device group remediates all servers in its subgroups, but the subgroups do not inherit the software policy attached to the device group. However, when an Application Configuration operation within the SA Client is applied to a device group that contains subgroups, the operation does not apply to all the servers in the subgroups. It only applies to the servers in the group upon which the operation was directly applied.

Public Device Groups

Public groups are visible to all users, and can be used by any SA user. Public device groups can also be used for modeling. For more information on modeling, see Public Device Group Modeling below.

Public device groups can be created, edited, or deleted by any user who has Manage Public Device Groups permissions. Only users with Manage Public Device Group permission can add members to a static public device group or change the rules that govern the dynamic public device group.

Accessing servers in a public device group also depends on the Device Group permission in the SA Client. See the SA Administration Guide for more information about setting device group permissions.

Public Device Group Modeling

With SA modeling, the desired state of a server is defined and then applied to servers. In the case of public device groups (static and dynamic), you can define a model consisting of application configurations, patch policies, software policies, and custom attributes, which will be applied to all servers in the group. The modeling information is attached to the group, but not to any subgroups.

If the modeling information changes, the servers in the group are not affected until the remediation operation runs on those servers. If the model has already been remediated on that server when it is removed from the group, the installed material will be removed during the next remediation.

Private Device Groups

Each SA user automatically gets their own private device group area with the same name as their SA user name. Only the user who creates the private device groups can see and manage them. These groups are not visible to the other SA users. Private groups behave the same way as public groups, with the exception that modeling is not available for private groups.

Private device groups can be created by any user belonging to a user group that has access to the Servers list.

Static Device Groups 

A static group has servers that are added to and removed from the group manually. When using static groups, you first create the group, and then select the servers to populate it.

Dynamic Device Groups 

Dynamic device groups contain servers and other devices that are added to or removed from the group based on a set of user-defined rules. Once the rules have been created, SA will search for servers and devices that match the rules and add them to the group.

If the rules are changed and if the servers in the environment change or if servers are added to or removed from the managed environment, servers will be added to or removed from the group automatically. SA automatically recalculates dynamic group membership every hour.

Rules apply only to the group being created or modified and not to any of its subgroups.

Ways to Create Device Groups

In the SA Client, you can create a device group from the All Managed Servers list or by performing a server search, and saving the resulting list of servers or the rules as a group.

You can create the following types of device groups:

- Creating a Static Device Group
- Creating a Dynamic Device Group
- Creating a Device Group Using Search

About Static Device Groups

This section describes static device groups. Static device groups contain a fixed set of devices that you add manually to the group.

Creating a Static Device Group

This section describes how to create a static device group. Static groups contain a fixed set of devices that you manually add to or remove from the group. Static device groups must be either public or private.

Note: To create a public static device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

To create a static device group, perform the following steps:

1. From the navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane. All the public device groups are under Public. All your private device groups are under your user name.
2. Navigate to the location where you want to create your group.
   - To create a public group, select Public or an existing group under Public.
   - To create a private group, select your user name or an existing group under your user name.
3. From the **Actions** menu, select **Device Group** > **New Static Group**.

   This creates an empty device group named New Device Group (n), where n is a number based on the number of new device groups already in existence.
4. You can rename the device group by selecting it and either right clicking on it and selecting **Rename** or by selecting the **Actions** > **Rename** menu item.

   After you create a static device group, you can add servers to the group. See Adding a Server to a Static Device Group below.

Adding a Server to a Static Device Group

You can use either of the following two methods to add a server to a static device group: Method 1 - Select Device Group First, then Servers or Method 2 - Select Servers First, then Device Group.

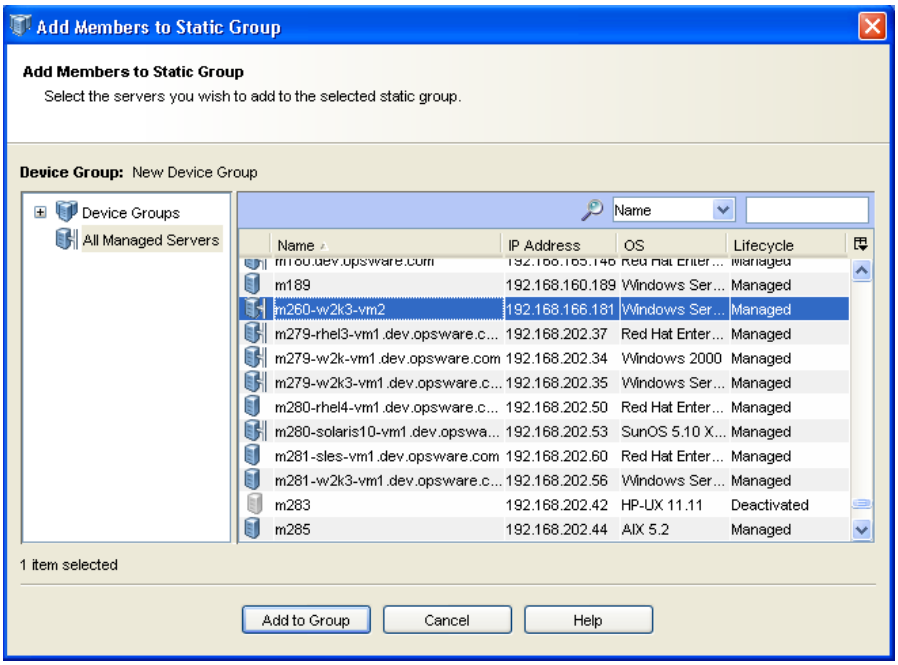
Note: To add a server to a public static device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

Method 1 - Select Device Group First, then Servers

To add a server or device group to a static device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Group**. The device groups appear in the Content pane. You can distinguish between static and dynamic device groups by their icon. See Device Group Status and Icons.
2. Navigate to the desired static device group. Select the device group in the Content pane, and from the **Actions** menu, select **Open**. The Device Group Explorer appears.
3. From the Views pane of the Device Explorer window, select Device Membership. This displays a list of servers in the group.
4. From the **Actions** menu, select **Add**. The Add Members to Static Group window appears.

The Add Members to Static Group Window in the SA Client



5. Select one or more servers to add to the static device group.
6. Click **Add to Group**. The selected severs are added to the device group and appear in the Device Group Browser.
7. From the **File** menu, select **Save** to save the device group.

Method 2 - Select Servers First, then Device Group

Perform the following steps to add a server to a static device group:

1. From the Navigation pane, select **Devices** > **All Managed Servers**. The list of managed servers appears in the Content pane.
2. From the Content pane, select one or more servers and then from the **Actions** menu, select **Add to Device Group**. The Add to Group window appears.
3. Select the static device group to add the servers to.
4. Select **Add to Group**. The selected servers are added to the static device group.

Method 3 - Import CSV File

You can add servers to a static device group by importing a CSV (comma-separated value) file containing the host names of the servers you want to add to the group. The CSV file contains a single column of string data representing server host names. The following characters have special meanings:

- The asterisk (*) indicates zero or more of any legal character (letters, numbers, the underscore character and dot).
- Lines that start with the "#" character are ignored. You can use them to insert comments.
- Blank lines are ignored.

For example, the following shows a CSV file that specifies a server named "myhost.hp.com", all servers that start with the string "ca", and all servers that end with ".mycustomer.com":

This is a comment line.
myhost.hp.com
ca*

*.mycustomer.com

The following shows a list of hosts and which hosts would be selected by this CSV file:

myhost.hp.com This host would be selected.
myhost2.hp.com This host would not be selected.
ca23.hp.com This host would be selected.
ca28.hp.com This host would be selected.
carl.hp.com This host would be selected.
acam.hp.com This host would not be selected.
host01.mycustomer.com This host would be selected.

To add servers to a device group from a CSV file, perform the following steps.

1. From the Navigation pane, select **Devices** > **Device Group**. The device groups appear in the Content pane. You can distinguish between static and dynamic device groups by their icon. See Device Group Status and Icons.
2. Navigate to the desired static device group. Select the device group in the Content pane, and from the **Actions** menu, select **Open**. The Device Group Explorer appears.
3. From the Views pane of the Device Explorer window, select Device Membership. This displays a list of servers in the group.

4. From the **Actions** menu, select **Import...**. The Import window appears.
5. Select the CSV file and click Open. This displays the Add Members to Static Group window that lists the servers that can be added to the device group.
6. Select the servers you want to add to the device group.
7. Select **Add to Group**. This adds the selected servers to the device group.

Removing Servers from a Static Device Group

In a static device group, servers must be removed manually. Removing a server only removes the server from the device group and not from the All Managed Servers list. Servers can belong to more than one device group, so if you want to remove a server from each device group that it belongs to, then you must locate and remove each instance of the server from all the device groups it is a member of.

Note: To remove servers from a public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

Method 1 - From the Device Group Explorer

To remove a server from a static device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane.
2. Navigate to the desired static device group. Select the device group in the Content pane, and from the **Actions** menu, select **Open**. The Device Group Explorer appears.
3. From the Views pane, select Device Membership. The list of servers in the device group appears in the Content pane.
4. Select the server you want to delete. From the **Actions** menu, select **Remove**. Or right click on the server and select Remove. The selected server is removed from the static device group.
5. From the **File** menu, select **Save** to save the device group.

Method 2 - From the SA Client

To remove a server from a static device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane.
2. Navigate to the desired static device group. Select the device group and double-click to display its members.
3. Select the server displayed in the Content pane. From the **Actions** menu, select **Remove Member**. The server selected is removed from the static device group.

Method 3 - From the Device Explorer

To remove a server from a static device group, perform the following steps:

1. From the Navigation pane, select **Servers** > **All Managed Servers**. The list of servers appears in the Content pane.

2. Navigate to the desired server. Select the server and double-click to display it in the device explorer window.
3. Select Relationships in the Navigation pane. This displays all the static groups the server belongs to.
4. Select a static device group from the Content pane.
5. From the **Actions** menu, select **Remove from Group**. Or right click the server and select Remove from Group. The server selected is removed from the static device group.

About Dynamic Device Groups

This section describes dynamic device groups. Dynamic device groups contain all the servers that satisfy a set of rules that you define. Dynamic groups automatically add or remove servers based on whether or not the servers satisfy the defined rules.

SA automatically recalculates the members of every device group every hour and whenever any device attribute changes or when a dynamic device group rule changes. SA examines the rules you have defined and determines which servers satisfy the rules. The SA Client displays when the last recalculation occurred in the Properties view for each dynamic device group.

Creating a Dynamic Device Group

Dynamic device groups are defined by one or more rules. The servers in a dynamic group are added or removed automatically based on the rules that you define. This section describes how to create a dynamic device group. The following section describes how to create rules that determine the members of the group.

Note: To create a public dynamic device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

To create a dynamic device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of existing device groups appears in the Content pane. All the public device groups are under Public. All your private device groups are under your user name.
2. Navigate to the group where you want to create your new group.
   - To create a public dynamic device group, select Public or navigate to a group under Public.
   - To create a private dynamic device group, select your user name or navigate to a group under your user name.
3. From the **Actions** menu, select **Device Group** > **New Dynamic Group**.

   This creates an empty device group named New Device Group (n), where n is a number based on the number of new device groups already in existence.
4. You can rename the device group by selecting it and either right clicking on it and selecting **Rename** or selecting the **Actions** > **Rename** menu item. Enter the name of the device group in the Content pane.

5 After you create a dynamic device group, you need to define the rules for the group. For more information, see About Rules for a Dynamic Device Group below.

Recalculating the Members of a Dynamic Device Group

SA automatically recalculates the members of every device group every hour and whenever any device attribute changes or when a dynamic device group rule changes. SA examines the rules you have defined and determines which servers satisfy the rules. The SA Client displays when the last recalculation occurred in the Properties view for each dynamic device group.

You can also manually recalculate the members of a dynamic device group by performing the following steps.

1 In the SA Client, select the **Devices** tab.

2 Navigate to the desired device group under the Device Groups node in the navigation pane.

3 Select one or more dynamic device groups.

4 Select the **Actions** menu or right-click and select **Device Group** > **Recalculate**. SA examines the dynamic device group rules, determines all the managed servers that match the rules and updates the members of the device group.

About Rules for a Dynamic Device Group

Servers and other devices are automatically added to and removed from dynamic device groups by SA based on the rules you create for the group. You can change the membership of a dynamic group by adding, deleting, or modifying these rules. See also Adding Rules for a Dynamic Device Group and Modifying Rules for a Dynamic Device Group.

A rule is a condition that specifies values for some attribute of servers such as IP address, server name, operating system, and many others. Servers either comply with each rule or not. For example, the following are example rules and example servers that demonstrate how servers would be included in the group or excluded from the group.

- All servers with a name that begins with the string “pro”. A server named “provision1.hp.com” would be included by this rule. A server named “approval4.hp.com” would not.
- All servers that are in the subnet 192.168. A server at IP address 192.168.123.7 would be included by this rule. A server at IP address 192.167.43.18 would not.
- All servers with operating system HP-UX version 11.31. All servers with this operating system would be included by this rule. Servers with any other operating system or any other version of HP-UX would not.
- All servers attached to a particular software policy named “AccountingDB”.
- All servers that have a particular patch installed.

You can define a wide variety of rules and create as many device groups as you need to make managing your IT environment faster, easier and more efficient.

Format of Rules for Dynamic Device Groups

Rules for dynamic device groups take the following form:

Search for: **<***Device***>**

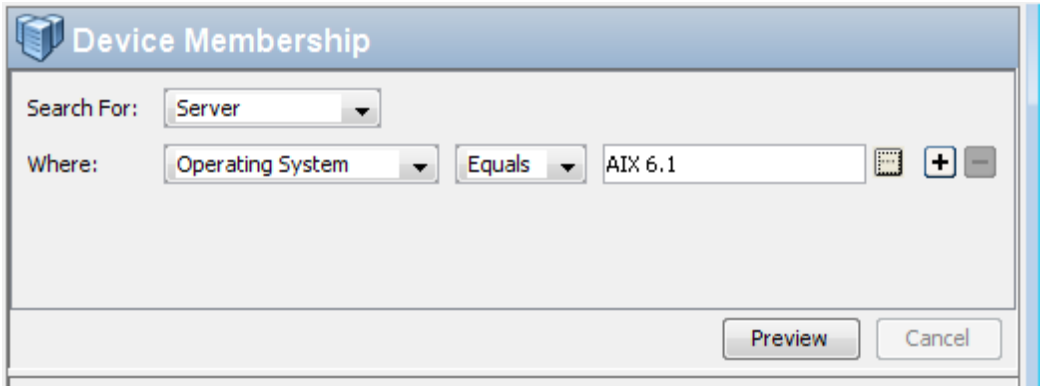
Where: **<***Attribute***> <***Operator***> <***Value***>**

- <*Device*> is typically Server because device groups contain servers, but it can also be other kinds of devices.
- <*Attribute*> is some piece of data about the device you want the rule to examine.
- <*Operator*> is a comparison you want to perform between the <*Attribute*> and the <*Value*>.
- <*Value*> is the specific data you want to compare to the <*Attribute*> using the <*Operator*>.

Example Rule 1 - Servers Running a Particular OS

Select All Servers Running AIX 6.1 Device Group Rule displays a dynamic device group rule that selects all servers running the AIX 6.1 operating system and places them into the device group:

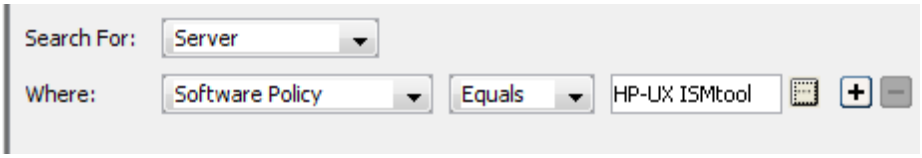
Select All Servers Running AIX 6.1 Device Group Rule



Example Rule 2 - Servers Attached to a Software Policy

Servers Attached to a Software Policy Device Group Rule displays a dynamic device group rule that selects all servers attached to the software policy “HP-UX ISMTool”:

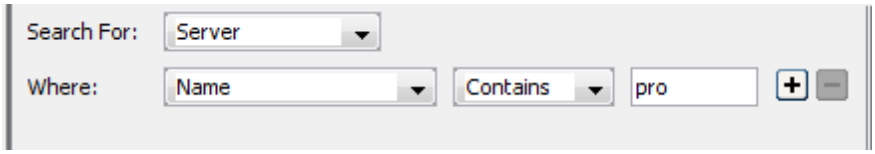
Servers Attached to a Software Policy Device Group Rule



Example Rule 3 - Servers with a Particular Name

Servers with a Particular Name Device Group Rule displays a dynamic device group rule that selects all servers with a name beginning with the characters “pro”:

Servers with a Particular Name Device Group Rule



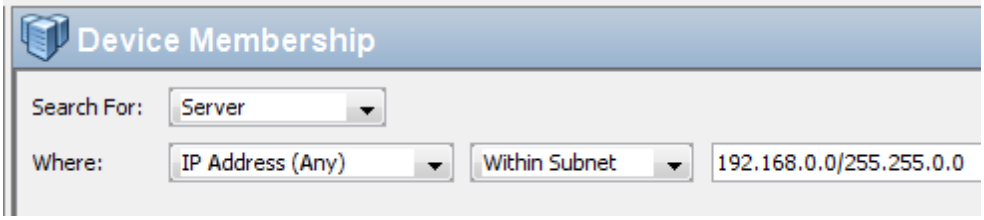
Example Rule 4 - Servers in a Subnet

You can create device groups containing servers on a particular subnet. You can use an IP address and either a **subnet mask** or a **CIDR number** to specify the network address of the subnet. When you select IP Address as the server attribute to search on and Within Subnet as the operator, you must enter an IP address and either a subnet mask or a CIDR number as follows:

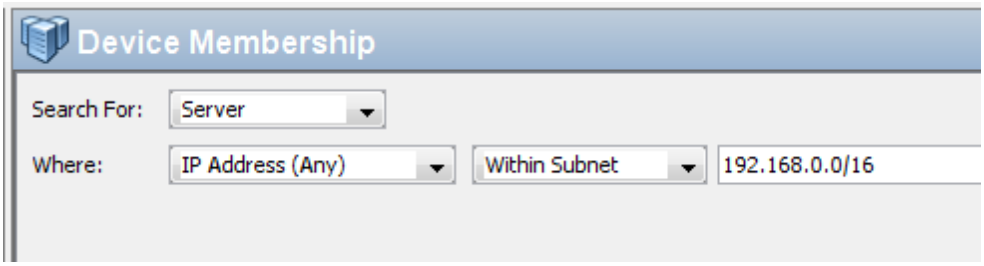
- <IP address>/<Subnet mask>
- <IP address>/<CIDR number>

For example, both of the following examples specify a subnet of 192.168:

- Subnet mask: `192.168.0.0/255.255.0.0`



- CIDR block: `192.168.0.0/16`



Configuring Multiple Rules for Dynamic Device Groups

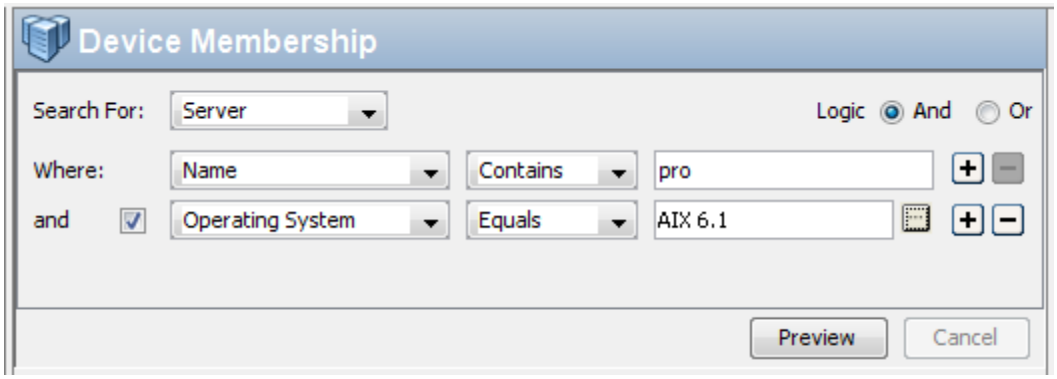
You can configure multiple rules and combine them with a logical And or a logical Or. Select ⊞ to add a rule. Select ⊟ to remove the selected rule or rules. Select either Logical And or Logical Or to logically combine the rules.

Note: You can create more complex logical expressions using the SearchService interface in the com.opsware.search package of the SA Twister API. For more information on the SA Twister API, see the SA Platform Developer Guide.

Example of Multiple Rules

Multiple Dynamic Device Group Rule displays a dynamic device group rule two rules combined with a logical And to select all servers that both have a name that begins with the characters “pro” and run AIX 6.1:

Multiple Dynamic Device Group Rule



Adding Rules for a Dynamic Device Group

Rules determine which servers are included in a dynamic group.

Note: To add a server to a dynamic public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

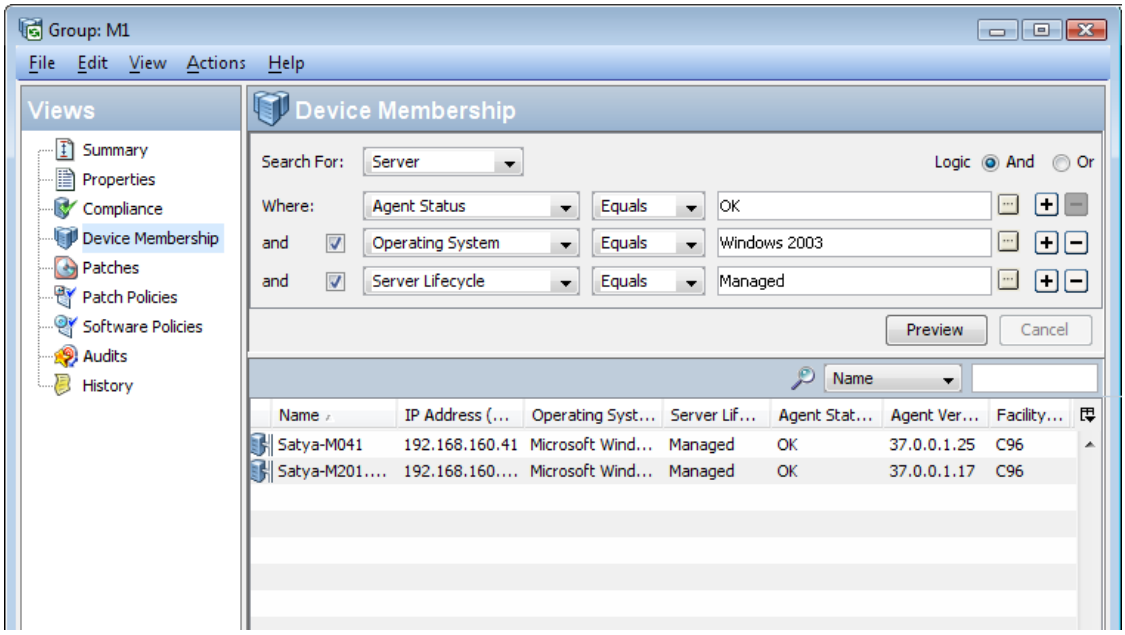
To add a rule to a dynamic group, perform the following steps.

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Navigation pane and the Content pane.
2. In the Navigation pane, navigate to the dynamic device group you want to modify.

   You can determine whether a device group is static or dynamic from the icon next to its name as described in Device Group Status and Icons.
3. From the Content pane, select the device group and then select the **Actions** > **Open** menu item. This opens a Group View window.

   You can determine whether a group is static or dynamic from the Summary View, under Properties.
4. From the Views pane, select Device Membership. This displays the rules defined for the group in the Content pane. See Defining Rules for a Dynamic Device Group below.

Defining Rules for a Dynamic Device Group



5 Create a rule by first selecting the type of device you want to include in the device group from the “Search For:” drop-down list. Depending on the type of device you select, the other drop-down lists change to correspond to the device type. Defining Rules for a Dynamic Device Group shows Server selected.

6 Select the attribute to search on from the “Where:” drop-down list. Depending on the attribute that you select, options available for the operator and values for the rule in the remaining drop-down lists will change.

7 Select the operator from the next drop-down list.

8 Enter a value in the field, or select a value from the drop-down list, or click ... to select one or more values from the Select Values window.

9 Click + to add additional rules and repeat steps 6 to 8. Click − to delete a rule.

10 Select the logic (logical And or logical Or) to be applied to the set of rules.

11 Click **Preview** to view the servers that satisfy all the rules and are therefore members of the device group.

12 From the **File** menu, click **Save** to save your rules in the dynamic device group.

Modifying Rules for a Dynamic Device Group

Rules determine which servers are included in a dynamic group. To modify a rule in a dynamic group, perform the following steps.

Note: To modify rules for a dynamic public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

1 From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Navigation pane and the Content pane.

2 In the Navigation pane, navigate to the dynamic device group you want to modify.

   You can determine whether a device group is static or dynamic from the icon next to its name as described in Device Group Status and Icons.

3 From the Content pane, select the device group and then select the **Actions** > **Open** menu item. This opens a Group View window.

   You can determine whether a group is static or dynamic from the Summary View, under Properties, or from the Properties view next to Type.

4 From the Views pane, select Device Membership. This displays the rules defined for the group in the Content pane. See Defining Rules for a Dynamic Device Group below.

5 Modify the rules for the device group as needed. For more information on rules, see About Rules for a Dynamic Device Group and Adding Rules for a Dynamic Device Group.

6 Click **Preview** to see the list of servers that satisfy all the rules and are therefore members of the device group.

7 From the **File** menu, click **Save** to save your rules in the dynamic device group.

Converting a Dynamic Group to a Static Group

You can convert a dynamic device group to a static device group. When a dynamic device group is converted to a static device group, all the servers that match the rules at that time are placed in the static device group, but the rules used to define the server membership are lost. To convert a dynamic group to a static group, perform the following steps.

1 From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appear in the Content pane.

2 From the Navigation pane, navigate to a dynamic device group.

   You can determine whether a device group is static or dynamic from the icon next to its name as described in Device Group Status and Icons.

3 From the Content pane, select the dynamic device group.

4 Select the Actions > Open menu item. This displays information about the device group in a new window.

5 In the Views navigation panel on the left, select Properties. This displays detailed information about the device group.

6 Locate the Type row and drop-down list next to it. In the drop-down list, select Static.

7 Select the File **>** Save menu item. This saves the group as a static group. All the rules that were used to define the dynamic group are lost.

More Device Group Tasks

This section describes additional tasks you can do with device groups.

Creating a Device Group Using Search

Note: To create a public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

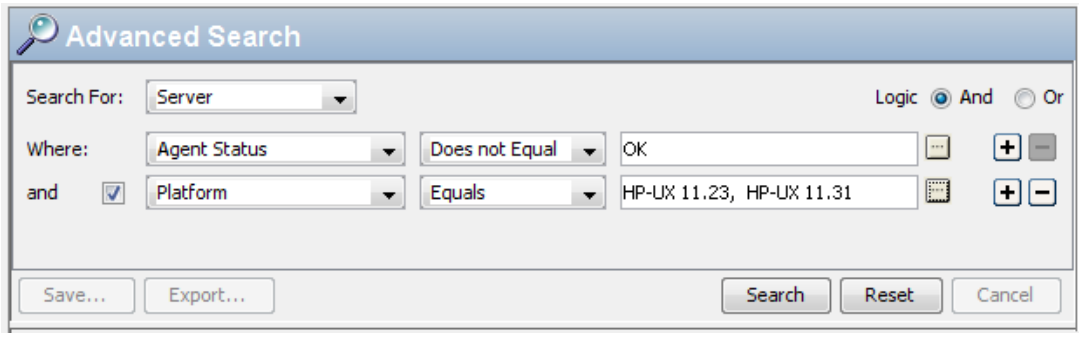
You can create a search for servers and use the search results to create a device group. To create a device group using search, perform the following steps:

1. From the Navigation pane, select **Advanced Search**. The Advanced Search page appears in the Content pane.

   For more information on advanced search, see the About Advanced Searches.
2. From the first drop-down list, select Server.
3. Create your search criteria by setting up a rule in the "Where:" line. Select a server attribute to search on from the first drop-down list. Depending on the attribute that you select, options in the remaining two drop-down lists (operator and value) will change.
4. Select the operator from the second drop-down list. The operator selected defines how the search value is treated.
5. Enter a value in the third field or select a value from the drop-down list or click (only shown for some attributes) to select one or more values from the Select Values window.
6. Click to add rules and repeat steps 3 to 6. Click to delete any rules.
7. Select the logic (logical And or logical Or) to be applied the set of rules in the search.

   Advanced Search with Two Conditions Logically Anded Together shows an advanced search with two conditions logically Anded together:

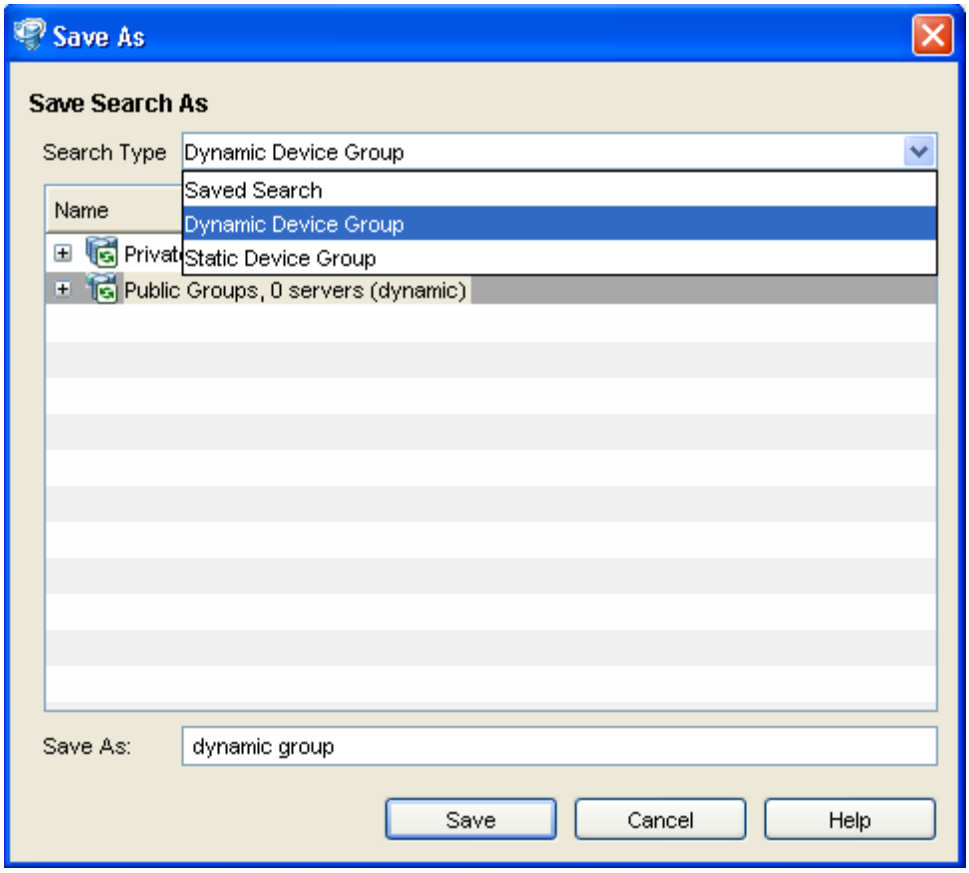
Advanced Search with Two Conditions Logically Anded Together



8. Click **Search** to run the search. The results appear in the Content pane.
9. Click **Save** to save your search. The Save Search window appears as shown in The Save Search Window in the SA Client below.
10. In the Search Type drop-down list, select Dynamic Device Group or Static Device Group.
11. Navigate to the location where you want to save the group, either under Private Groups or under Public Groups.
12. Enter the name of the new device group in the Save As text box.

13 Click **Save** to save your new device group.

The Save Search Window in the SA Client



Note: When you save the device group as a dynamic group, if the rules change or the servers in the environment change, servers will be added to or removed from the device group automatically. When you save the device group as a static group, the servers will be added to the device group, but all rules will be lost.

Note: If the search query does not return any results, then you can only save the device group as a dynamic device group.

Moving a Device Group

You can move device groups to a different location under Device Groups. You can move device groups from a private group to a public group, but you cannot move device groups from a public group to a private group. If you move a device group containing subgroups, the subgroups are also moved.

Note: To move a public device group or to move a private group to a public group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

To move a device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane.
2. From the Navigation pane, navigate to the desired group.
3. From the Content pane, select the device group you want to move.
4. From the **Actions** menu, select **Device Group** > **Move...**. The Move Group window appears.
5. Select the desired new location for the device group.
6. Click **Move Group**. The device group is moved to the new location.

Duplicating a Device Group

When you duplicate a device group, the servers are copied to a new group and they remain in the original group. In the SA Client, you can only select one device group at a time to duplicate.

Note: To duplicate a public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

To duplicate an existing device group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane.
2. From the Navigation pane, navigate to the desired group.
3. From the Content pane, select the device group you want to duplicate.
4. From the **Actions** menu, select **Device Group** > **Duplicate**. This creates a copy of the device group.
5. You can rename the group by selecting it and selecting **Actions** > **Rename**.

Deleting a Device Group

Deleting a device group removes the group, but the servers in the group still remain in the All Managed Servers list and in any other groups they are members of.

A group cannot be deleted when any of the following conditions apply:

- The device group contains other device groups.
- Software policies or patch polices are attached to the group.
- Access controls are set for the group. For more information on controlling access to device groups, see “Setting the Device Group Permissions” in the SA Administration Guide.

Note: To delete a public device group, you must have Manage Public Device Group permissions. To obtain these permissions, contact your SA Administrator.

To delete a server group, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The list of device groups appears in the Content pane.
2. From the Navigation pane, navigate to the desired group.
3. From the Content pane, select the device group you want to delete.
4. From the **Actions** menu, select **Device Group** > **Delete**.
5. Click **Delete Selected Groups** on the confirmation dialog to delete the device group.

Device Group Explorer

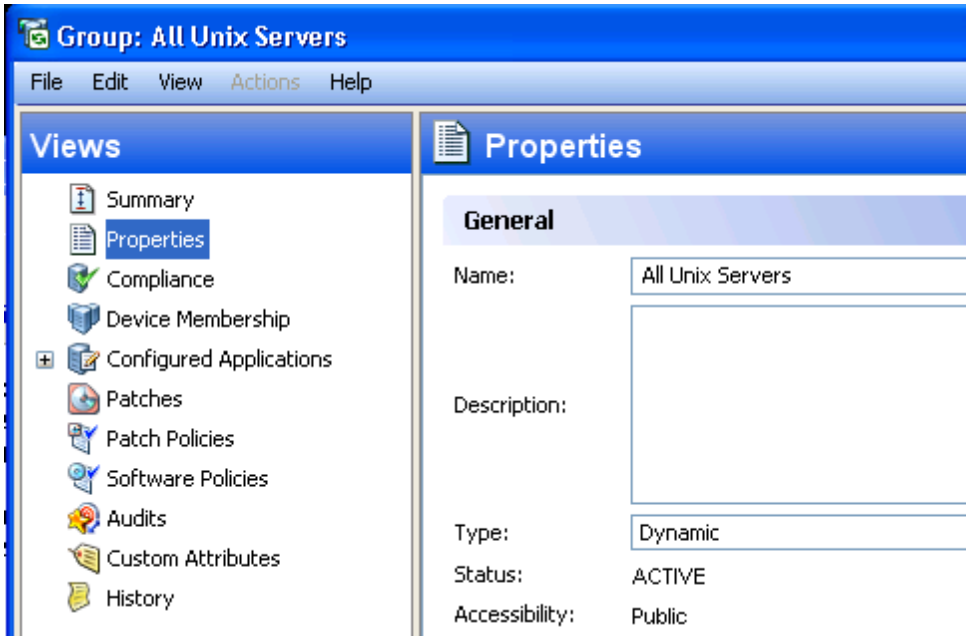
The Device Group Explorer allows you to view and manage the properties of a device group in the SA Client. From the Device Group Explorer, you can perform the following actions:

- View the properties and members of a device group.
- Change a dynamic device group to a static device group.
- Add or remove members from a device group.
- View rollup compliance information for group members targeted by compliance policies such as Audit, Software, App Config, and Patch.
- Add application configurations to a device group.
- View and manage patches, patch policies and software policies associated with the servers in the group.
- Create an audit.
- Take a snapshot.
- View and create custom attributes.
- View server history.

To access a Device Group Explorer, perform the following steps:

1. From the Navigation pane, select **Devices** > **Device Groups**. The device groups appear in the Content pane.
2. Select a device group and from the **Actions** menu select **Open**. The Device Group browser appears as shown below.

The Device Group Explorer Window



3 To view the properties or perform an action on the device group, select one of the following views:

- Summary
- Properties
- Compliance
- Device Membership
- Configured Applications
- Patches for Device Groups
- Patch Policies for Device Groups
- Software Policies for Device Groups
- Audits
- Custom Attributes for Device Groups
- History Properties for Device Groups

Summary

The Summary view lists the following information:

— **Properties**: This displays if the device group is Private, Public, Dynamic or Static.

— **Members**: This displays the total number of members in the device group.

Properties

The Properties view lists the following property information such as name, type, status, accessibility for the group of servers that you are browsing.

Compliance

The Compliance view provides a summary of how the servers in the device group comply with the patch, software, and audit policies attached to the device group. For more information, see the SA User Guide: Server Patching, the SA User Guide: Software Management, and the SA User Guide: Audit and Compliance.

Device Membership

From inside each device group, you can view all members — managed servers and other groups of servers and other devices — that belong to the group. For each server that belongs to the group, the system displays its name, IP address, OS, customer, facility, and any description.

Configured Applications

If the device group is public, then you can add an Application Configuration to the group. The Application Configuration applies to all servers and groups in this group.

- The Installed Configurations tab allows you to browse and edit all Application Configurations attached to the device group.
- The Backup Configurations tab provides a history of all changes made to the selected application configuration template, and allows you to revert to a previous version of the configuration.

See the SA User Guide: Application Configuration for more information.

Patches for Device Groups

For complete information on patching servers, see the SA User Guide: Server Patching.

This window displays all patches associated with the selected server group.

Show Options

You can use the Show drop-down list to filter the following types of patch information displayed in the Device Groups Explorer:

- **Patches with Exceptions (Windows Only)**: This option displays all patches that have exceptions for Windows servers (such as always install or never install) a*nd* has one of the following conditions:
  - The patches are not currently installed and are recommended by the vendor.
  - The patches are currently installed.

- **All Patches**: This displays all patches that are associated with the operating system of a server.

Patch Contents

This section displays the following patch contents information:

- **Icon**: A dimmed patch icon indicates that the patch has not yet been uploaded to the Software Library.
- **Name**: The QNumber of a patch that is a hotfix or an update rollup. Service pack patches do not have a QNumber.
- **Compliance**: The patch compliance level, as defined by your patch administrator:
  - **Non-compliant** (red): The patch is installed on the server and is not in the policy or the patch is not installed on the server and is in the policy.
  - **Partial** (yellow): The policy and exception do not agree and the exception does not have data in the Reason field.
  - **Compliant** (green): This indicates any of the following conditions:
    - A patch is installed on the server and is in a policy or a patch is not installed on the server and is not in a policy.
    - A patch is installed on the server and there are additional patches with the same QNumber in a patch policy or exception. In this case, all patches with the same QNumber are considered installed when SA calculates patch compliance.
    - A patch is not installed on the server and is in a patch policy or has an always install exception, and is not recommended by the vendor. In this case, the patch has a never install exception because it is not recommended by the vendor.

  In the Preview pane, move the cursor over the icon or text in the Compliance column to view patch compliance information about a server.
- **Type**: The type of patch, such as Windows Hotfix or Windows Update Rollup.
- **Bulletin**: (*Optional*) The Microsoft Security Bulletin ID number for this patch.
- **Severity**: (*Optional*) The Microsoft severity rating for this patch:
  - **Critical**: This indicates a patch whose exploitation could allow the propagation of an internet worm, without user action.
  - **Important**: This indicates a patch whose exploitation could result in a compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources.
  - **Moderate**: This indicates a patch whose exploitability is mitigated to a significant degree by factors, such as default configuration, auditing, or difficulty of exploitation.
  - **Low**: This indicates a patch whose exploitation is extremely difficult or whose impact is minimal.
- **Release Date**: The date that Microsoft released this patch.
- **Exception**: The type of patch policy exception set for the selected server.
- **Installed**: Indicates whether the patch is installed on the selected server.

- **Recommended**: A check mark indicates that this patch was recommended by the vendor during the last software registration.
- **Description**: A brief description of the managed server.

Patch Policies for Device Groups

For complete information on patching servers with patch policies, see the SA User Guide: Server Patching.

This window displays all patch policies associated with the selected device group. You can use the Show drop-down list to filter the type of patch policies to display in the Server Explorer.

Show Options

This section displays the following patch information:

- **Policies Attached to Device Group**: This displays all policies attached to the device group, or policies attached to a server group to which the selected managed server belongs.
- **Policies Not Attached to the Server**: This displays a list of all patch policies relevant to the selected server group that are not attached to the group.

Patch Contents

This section displays the following patch content information:

- **Name**: This displays the name of the patch policy.
- **OS**: This displays the operating system associated with the patch policy.
- **Description**: This shows a description of the patch policy.

Software Policies for Device Groups

This Software Policies view displays all software policies associated with the selected server (or group of servers). You can perform actions such as attaching a policy, detaching a policy, remediating a server, and scanning software compliance from the **Actions** menu. For more information, see the SA User Guide: Software Management.

Audits

This window allows you to create and run audits and snapshots. For more information, see the SA User Guide: Audit and Compliance.

Custom Attributes for Device Groups

This window displays the custom attributes set to a server or device group. You also can add, edit or remove custom attributes from this window.

Custom attributes can be one of the following two types:

- Inherited from another source, such as a customer, a software policy, group of servers, ISM control, and so on.

- Attached directly to the server.

To override inherited custom attribute values, click the inherited arrow icon once, and enter a new value in the value field. Press ENTER. The inherited arrow changes to indicate that the custom attribute value has been overridden.

History Properties for Device Groups

The History view shows changes made to the selected device group. Entries are generated when actions are performed on a device group in the SA Client. The History is read-only. Each entry shows the following information:

- **Date**: The date when the last change occurred.
- **Event**: A description of the change.
- **User**: The user who made the change.

Use the View drop-down list to sort the device group history list according to a range of time, such as last week, the last two months, and so on.

The History view also displays custom-attribute changes for device groups.

Chapter 4 Server Agent Management

Server Agent Management topics describe the SA Agent and how to install it.

The SA Agent is software that is installed on most servers and it enables SA to manage your servers. There are four ways to install the agent on your server:

- By scanning IP addresses to locate agentless servers. Use the Devices tab, and Servers > SA Agent Installation. See Discovering Agentless Servers and Installing the SA Agent.
- By locating agentless servers among your managed servers. Use the Devices tab, and Servers > All Managed Servers. See Installing the SA Agent.
- By locating agentless servers managed by your virtualization services. Use the Virtualization tab. Installing the SA Agent. see also the SA User Guide: Virtualization Management.
- By using the agent installation command. See Agent Installation and Upgrade Utilities.

Note: SA does not install a server agent on VMware ESXi servers. Instead, SA manages ESXi servers through a VMware vCenter virtualization service. For more information, see the SA User Guide: Virtualization Management.

Permissions Required for Server Discovery and Agent Installation

To discover agentless servers and install agents you must have certain permissions. See the SA Administration Guide for more information about the permissions. To obtain the required permissions for scanning and deploying agents, contact your SA administrator.

Installing the SA Agent

This section describes how to install the SA agent on servers to bring under SA management.

The SA Client shows agentless servers with the server icon  . See Server Status Icons.

Agentless servers may be physical servers that are not running the agent, or they may be virtual machines (VMs) not running the agent, but managed by a virtualization service. For more information, see the SA User Guide: Virtualization Management.

1. In the SA Client, under Devices > SA Agent Installation, select the servers on which you want to install the SA agent. See Discovering Agentless Servers.

   Or under Devices > All Managed Servers, select the servers on which you want to install the SA agent.

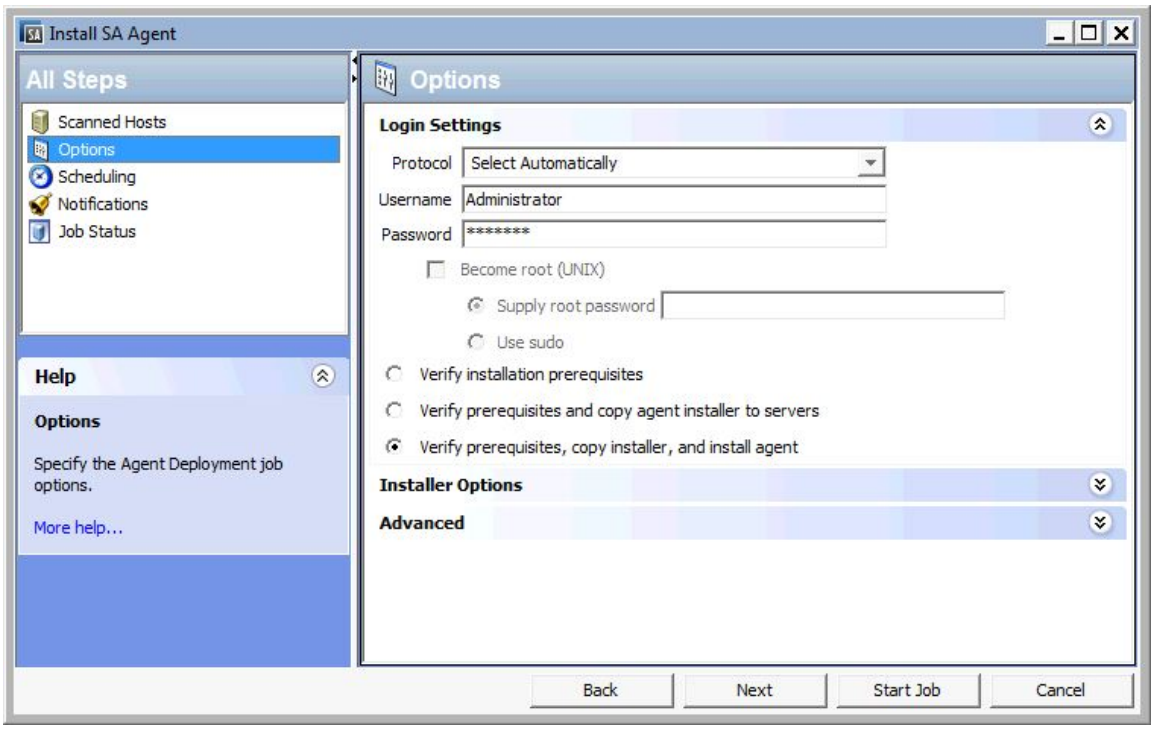
   Or under the Virtualization tab, select the VMs on which you want to install the agent. All VMs are managed under a virtualization service.

   The server icon  indicates agentless servers. See Server Status Icons.

   The servers must be powered on. Otherwise the Install SA Agent menu item will be disabled.

2 From the Actions menu, select Install SA Agent. This displays the Install SA Agent dialog box as shown in Install SA Agent Dialog.

Install SA Agent Dialog



3 Select a network protocol to use for connecting to the server from the drop-down list.

In most cases, choosing Select Automatically to allow SA to select an appropriate protocol for each server is recommended.

4 Enter a user name and password to use for logging into the managed server.

For Windows-based systems, specify the Windows administrator user name and password.

For UNIX systems, specify a `root` user and password. If logging in as `root` is not permitted, select the checkbox Become root (UNIX). Select Supply root password and enter the password, or select Use sudo if `sudo` access is enabled for that account.

If you log in using `sudo`, the sudo user's configuration file (typically `/etc/sudoers`) must allow the account to run any command with root privileges. This is typically accomplished by using the "ALL" alias in the `sudoers` file.

If you are unable to deploy the agent to a UNIX server by logging in as root, the system you are deploying to may be configured to disallow direct root logins. In such cases SA allows you to log in as a non-root user and then escalates your privileges via either the "su" command or the "sudo" command.

Perform the following steps to deploy agents as a non-root user:

a Enter the unprivileged user name in the Username field to log into the server.

b Enter the unprivileged password in the Password field.

c Select the Become root (UNIX) checkbox. Select “Supply root password” and enter the password or select “Use sudo”. If you use sudo, the unprivileged account must be able to run any command as root.

5 Select one of the following deployment actions:

- Verify installation prerequisites.
- Verify prerequisites and copy agent installer to servers.
- Verify prerequisites, copy installer, and install agent.

See Setting Agent Installation Actions for Each Server for more information.

6 Specify the agent installer options to control the way the agent is installed on a server. See Agent Installer Options for more information.

7 Select OK to perform your selected actions.

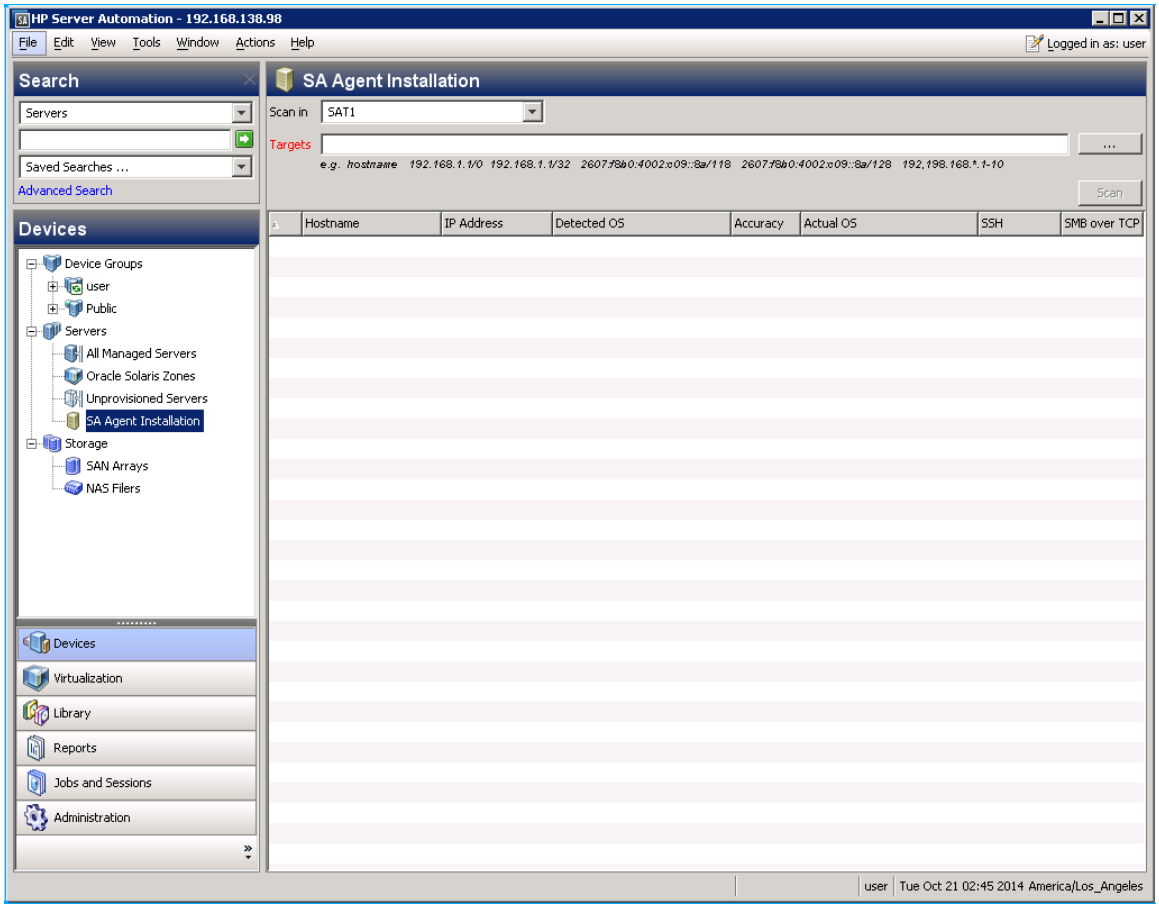
8 After the agent installation is complete, the SA Client displays the results and updates the status icons for the servers. You can view information on an unmanaged server and generate reports on agent installation status. See Reports on Agent Installation for more information.

9 You will see a checkbox for enabling the --r option. Resets the Agent configuration file to the default settings.Specifies the path to the RPM handler to use for RPM operations. Use this option, when an RPM handler is already installed on the server.If an RPM handler is not already installed on the server, use the --withrpm option instead to install one.It is not necessary to use this option with the --withrpm option.

Discovering Agentless Servers

You can use the SA Client to install agents on a large number of servers. To discover agentless servers, you specify a location to scan for servers and a set of IP addresses. SA performs a network scan to locate and identify servers. Instead of entering addresses into the input field, you can import a file containing of IP addresses or IP address ranges. When the scan is complete, SA displays a list of scanned servers.

SA determines the status of each server, its IP address, its host name, detected operating system, and open ports used to connect to the server.



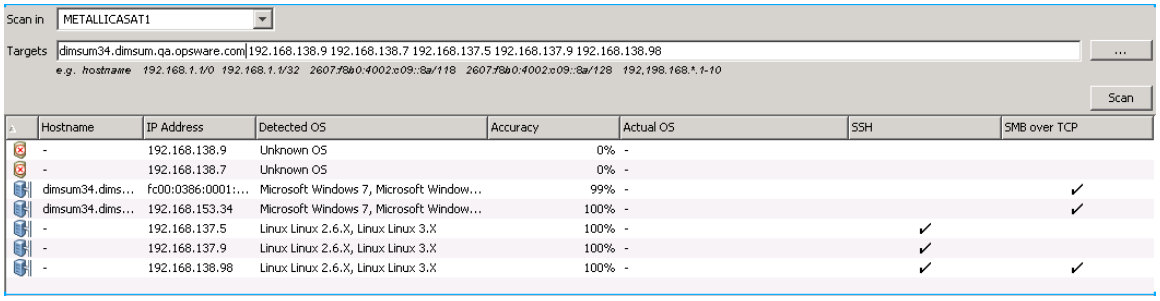
To scan for agentless servers and install agents on them using the SA Client, perform the following steps.

1. From the SA Client navigation pane, select the Devices tab and then select Servers > SA Agent Installation.
2. Select a realm to scan for servers from the “Scan in” drop-down list. For more information about realms, see the SA Administration Guide.
3. In the Targets field, click the ... button to select a realm and enter as many IPv4 or IPv6 addresses as you want to scan.
4. Click Scan to scan for servers. When the scan is complete, the list of servers is shown. For each server, SA determines the status of the server, its IP address, its host name, the detected operating system and open ports that can be used to connect to the server. You can click on any of the column headings to sort the server list by that column.

   Note: If you have a firewall enabled, SA may not be able to accurately detect a server’s actual installed operating system. Some firewalls can interfere with the methods SA uses to detect the operating system. SA must be able to access at minimum one open port and one closed port to gather the information needed to determine the operating system. If you find that SA has not identified any operating system or has misidentified

the operating system, you may need to configure your firewall to allow network packets from the SA core.

The following figure shows the results of a network scan for servers. The actual operating system of the server can be only determined if SA is able to successfully log into the server.



5. Install the SA agent on these servers, as described in Installing the SA Agent.

Upgrading the Server Agent

When a new version of HP SA is released, it may include a new version of the SA agent. The new agent may be required to gain access to some new functions in SA. For instructions on upgrading the SA agent, see Agent Upgrade - SA Client.

Note: If you attempt to upgrade an agent on a server that acts as an SA Core host, you will see warning message. Core host agents are upgraded when the core itself is upgraded and you should not need to manually upgrade them.

Setting Agent Installation Defaults

The server agent enables SA to manage your servers. You can specify the default behavior for agent installation by selecting the **Tools > Options** menu in the SA Client. For more information, see SA Agent Installation - Installer Options, SA Agent Installation - Protocols, and SA Agent Installation - Advanced Options.

Starting and Stopping a Server Agent

Once the SA agent is installed and running on your managed servers, you rarely need to stop or restart them.

To start a server agent, log onto the managed server and enter one of the following commands.

UNIX:

```
/etc/init.d/opsware-agent start
```

HP-UX:

/sbin/init.d/opsware-agent start

AIX:

/etc/rc.d/init.d/opsware-agent start

Windows:

```
net start opswareagent
```

To stop an agent, enter the same command, specifying `stop` instead of `start`.

Viewing Server Agent Information

You can view information about the agent in the SA Client by selecting a server, selecting the Properties view and scrolling to the Reported Information in the SA Client.

The Reporting field indicates the status of the Agent's reporting capability and tells you whether or not the agent is reporting regularly and successfully. The possible reporting states for the agent are as follows:

- OK: The Agent is reporting properly.
- Registration in progress: The Agent is currently registering server hardware information.
- Reporting error: The Agent encountered an error while trying to report hardware information.
- Has not reported in <*number*> days: This indicates when the Agent last reported.
- **Has not reported**: Indicates the Agent has not yet reported.

Searching for Servers Based on Agent Information

You can also perform an advanced search and specify the search criteria as Agent Discovery Date, Agent Encoding, Agent Reporting, Agent Status or Agent Version.

You can access Agent reporting information in Server Properties.

If the Agent experiences an error in reporting, or has not reported within 24 hours, you can run a communication test to troubleshoot the problem. See Running Server Communication Tests for more information.

If you modify the server hardware, it could take up to 12 hours for the change to appear in the SA Client user interface, depending on the time that the agent for that server contacted the core.

If you install or uninstall software on a managed server outside of Server Automation, it could take up to 24 hours for the change to appear in the SA Client user interface. For example, if you update the Microsoft Patch Database, it could take up to 24 hours for all managed servers to display whether they need new patches based on the updated Microsoft Patch Database.

In some cases, not all of a server's hardware information is reported. For example, if the agent was installed with its default settings, not all hardware information is reported to the SA Client until an hour after the agent is installed. There also might be a problem retrieving certain hardware information, such as a disk failure, that could prevent some hardware information from being reported. In these cases, the server's property page lists unreported information as not set.

Security for Agents Running on Managed Servers

Agents act as both clients and servers when they communicate with the SA core. All communication is encrypted, integrity-checked, and authenticated using X.509v3 client certificates using SSL/TLS. A small number of core components can issue commands to the agent over a well-defined TCP/IP port. The agent can also call back to core components, each with its own well-defined port.

Agent Functionality on Managed Servers

The server agent:

- Only discovers information about its own managed server and no others.
- Cannot make changes on a server unless explicitly instructed to do so by the SA core.

SA runs with administrator privileges (root on UNIX servers and Local System on Windows servers), because it performs tasks that require administrator privileges, such as installing patches and rebooting.

The core performs client authentication and checks to see if the presenting certificate belongs to that particular server. Server Automation does this by comparing the certificate to the server's IP address that is generated when the agent is initially installed. If the certificate is not valid or the originating IP address does not match the IP address stored in the Model Repository, authentication fails and the agent cannot continue communication with Server Automation. If an unauthorized user were able to log on to a managed server with administrator privileges and compromise a server's security, the user would have only limited access to the following information in the SA core:

- The server's hardware inventory (already available to someone logged on with administrator privileges)
- The server's software inventory (already available to someone logged on with administrator privileges)
- The custom attribute information

Software and Hardware Inventory

When the server agent is first installed, it performs a full software and hardware inventory and stores this information in the SA core. It automatically performs the following inventories:

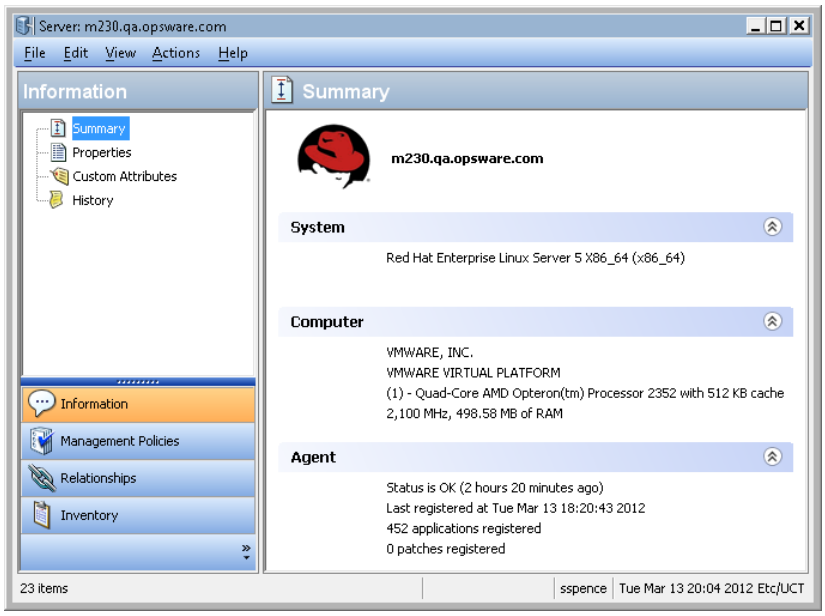
- Every 12 hours the agent performs a minimal hardware inventory and stores the updated information in the SA core. It reports information such as the OS version, the chassis ID, the SA agent version and the SA object ID.
- Every 7 days the agent performs a full hardware inventory and stores the updated information in the SA core. It reports all the information from the minimal hardware inventory plus information such as CPU, memory, storage and networking information.
- Every 24 hours, the agent performs a software inventory and stores the updated information in the core. It reports the software found on the server and the core determines any differences. A

- A hardware inventory is also performed during software installation.

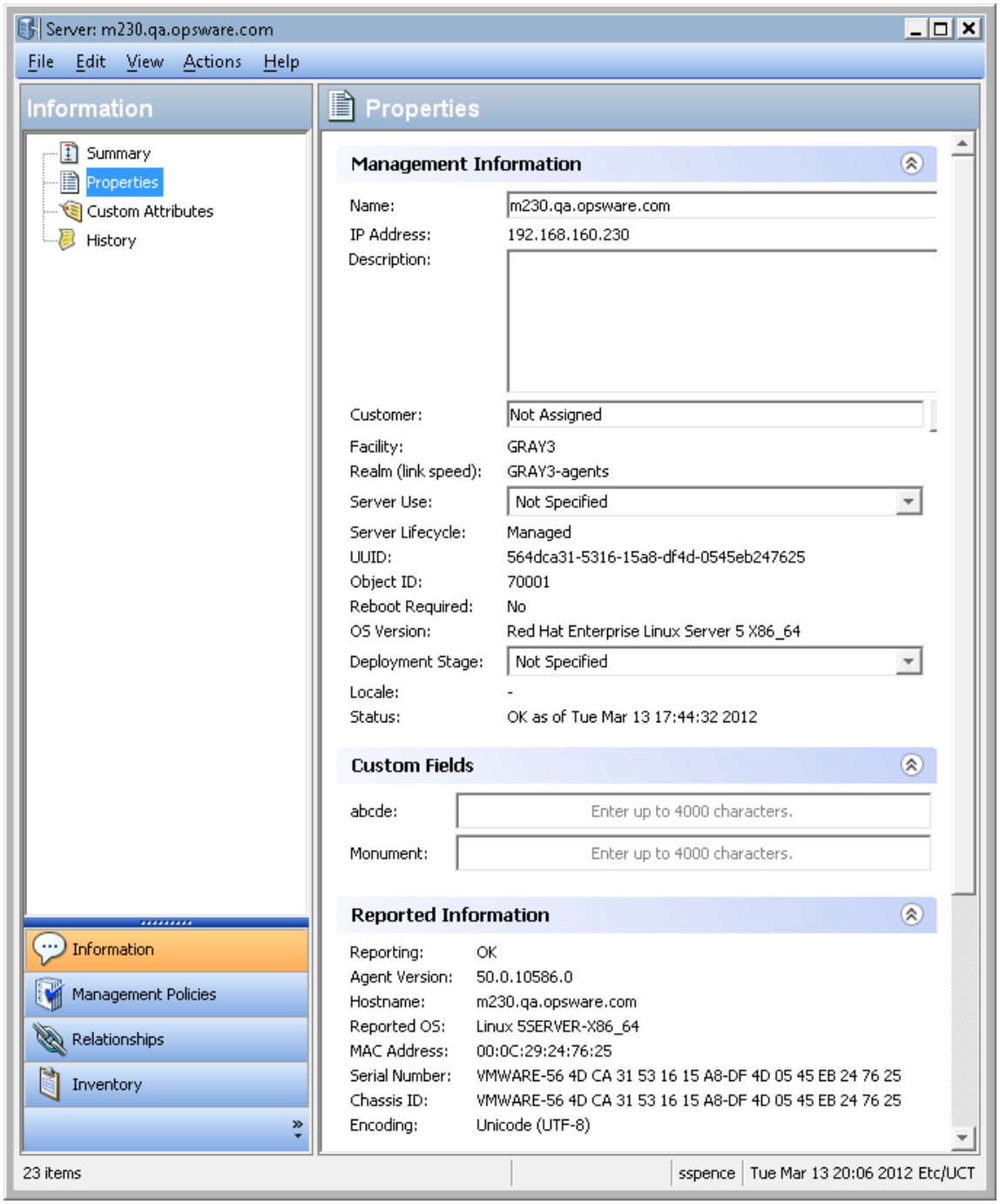
Server Information that the Agent Tracks

For each managed server, the agent reports software, networking, and hardware information, as shown in Server Information - Summary and Server Information - Properties. By communicating with the core and reporting the installed hardware and software for the server, SA determines what software should be *installed* on a server.

Server Information - Summary



Server Information - Properties



Software Information

The software that installed on the server is recorded in SA Library. To display the list of software installed on the server, select the Inventory tab, then select Installed Packages. For more information, see the SA User Guide: Software Management.

Hardware Information

SA tracks hardware information in a variety of ways. Hardware Information that the Agent Reports for Servers shows how the agent obtains the server and hardware information about each managed server.

Table: Hardware Information that the Agent Reports for Servers

Attribute	Description	How Obtained
Name	The user-configurable name for the server. By default, Server Automation uses the configured host name of the server until a user edits it.	**Windows**: Uses the fully qualified DNS name of the server. **Linux, Solaris, AIX, HP-UX**: Uses the current host name of the server that the `hostname` command returns.
Reported OS	The version number of the server's operating system.	**Windows:** Uses the Windows version number as reported by the operating system. This information includes the major version number, the minor version number, the Windows build number, and the Service Pack level. **Linux, Solaris, AIX, HP-UX**: Uses the operating system version that the `uname` command returns.
OS Version	The OS version specified for the OS definition.	Specified by the user who prepared the OS with the Prepare Operating System Wizard. See the SA User Guide: Provisioning for more information.
Serial Number	The serial number of the system. Server Automation attempts to report a chassis ID, if possible.	**Windows, Linux**: Obtained from the system BIOS. **Solaris, AIX, HP-UX**: Obtained from the system ROM.
Manufacturer	The manufacturer of the server if available.	**Windows, Linux:** Obtained from the system BIOS. **Solaris, AIX, HP**: Obtained from the system ROM.
Model	The model of the server if available.	**Windows, Linux**: Obtained from the system BIOS. **Solaris, AIX**: Obtained from the system ROM. **HP-UX**: Output of model command (which is

Attribute	Description	How Obtained
		read from the system ROM).
Memory	The amount of physical RAM and the total amount of virtual memory paging space configured.	**Windows**: Uses the Windows 2000 API `GlobalMemoryStatus()`. **Linux**: Obtained from information in the file `/proc/meminfo`. **Solaris**: Obtained from the `sysconf` and `swapctl` APIs. **AIX**: Uses the `lsattr` command for memory information and the `lsps` command for paging space. **HP-UX**: Uses the `pstat` system call.
CPUs	Information about each of the processors in the system. See CPU Properties.	
Storage	Information about each installed disk drive or RAID array.	**All Platforms**: Uses system APIs to discover and probe disk drives and RAID arrays.
Server ID or Object ID	The internal ID that Server Automation uses to identify the server.	In most cases, the server ID is the same as the MID.

In addition to hardware and software reporting, the agent reports networking information. This information can be accessed in the Server Browser under Inventory panel in the Network tab.

CPU Properties

The following CPU properties are displayed in the SA Client in the Inventory > Hardware window for platforms that provide the information to SA:

Table: CPU Properties

CPU Property	Description
# of Logical Cores	The processing unit capable of executing its own thread.
# of Physical Cores	An actual physical processor core, which has its own circuitry and caches, and can read and execute independently from other physical cores.

CPU Property	Description
Cache Memory	Memory that can be accessed more quickly than regular RAM, and is described in levels of closeness and accessibility to the microprocessor (L1, L2, L3), where L1 cache is on the same chip as the microprocessor, and other levels are on a separate static chip.
Family	Groupings of processors that have similar feature sets (such as processor model or stepping level), defined by the processor vendors.
Feature Flags	For CPU-specific flags, see the documentation from your CPU's manufacturer.
Model	Model number
Slot	Mechanical and electrical connections found between microprocessors and a printed circuit board. The Slot column is unique for each physical socket. For example, if a device has four chips on the board, it will have four entries in the Slot column.
Speed	Speed in Megahertz
Status	ONLINE or OFFLINE
Stepping	(A-0 for core step, incremented for improvement releases)
Vendor	Vendor name

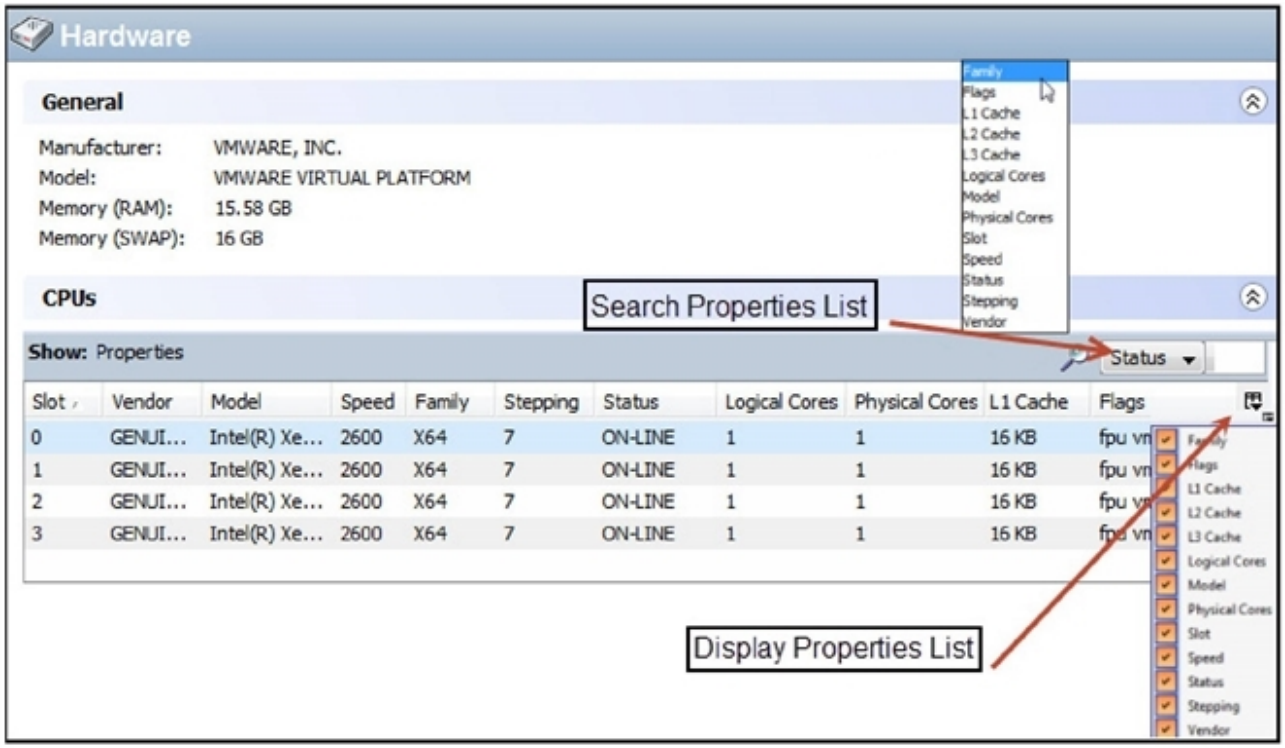
To view CPU information for a server:

1. In the SA Client, select Devices > Servers > All Managed Servers to view the server list.
2. From the content pane, right-click the server and choose Open.

   The server's Summary window is displayed.
3. Select **Inventory** > **Hardware**.

   The Hardware window displays both general server information (such as the model), and CPU information.

Hardware Window Displaying General and CPU Information



4 To search by property, choose a property from the search properties drop-down list, then enter the search string in the adjacent field.

5 To control which properties are displayed, click the icon to display the properties list. Deselect the properties that should not appear in the window.

6 To change the column order, drag a column to a new location.

About Server Discovery and Agent Installation

SA can install agents on a large number of servers through the SA Client. SA can identify servers on which to install an agent, specify the agent configurations for each server, select the login protocols to connect to each server, specify the agent installation options, install the agent and generate reports on agent installation status.

This section contains the following topics:

- Setting Agent Installation Actions for Each Server
- Specifying Login Settings
- Agent Installer Command
- Reports on Server Status

See Discovering Agentless Servers for more information about how to install an agent.

Setting Agent Installation Actions for Each Server

Once you have identified the servers, you can perform the following deployment actions:

- Verify installation prerequisites including:
  - Checking for sufficient disk space for agent installation on the server.
  - Verifying that no other application is using port 1002.
  - Verifying if ports to the Gateway are accessible.
- Copy the agent installer to servers.
- Install the agent on the server.

Specifying Login Settings

When installing the SA agent, you can select the network protocols to connect to the server and specify the user name and password to log in to each server. Agent installation is performed as root on UNIX operating systems and as administrator on Windows operating systems so. SA attempts to log in to each of the selected servers with the specified user name and password and performs the specified deployment actions.

The agent requires administrator-level privileges (root on UNIX servers and administrator on Windows servers) to manage a server.

Agent Installer Command

You can use the agent installer command to manually install agents on servers. For more information, see Agent Installation and Upgrade Utilities.

Reports on Server Status

After the SA agent is installed, the SA Client displays the results and updates the status icons for the servers as shown in Server Status

Table: Server Status

Icons	Server Status
	The server is agentless, but reachable
	The server is agentless and unreachable
	The server is agent managed
	The server failed prerequisite checks

Icons	Server Status
	The server passed prerequisite checks
	The server passed prerequisite checks and the agent installer was copied to the server
	The agent was successfully deployed
	The agent was not successfully deployed

Note: A server is considered to be managed when SA determines that the agent is listening for TCP connections on port 1002.

For a failed deployment action, you can view the errors on each server. You can also log in to the server and correct the errors.

You can also create the following reports:

- All the servers in the current network scan
- Selected servers in the current network scan
- All the servers in the current network scan with successful deployments
- Servers in the current network scan with failed deployments

You can save and export the reports to a CSV, HTML, or text format file.

Troubleshooting Agent Installation Errors

After the agent is installed, you can review the results and generate reports. For a failed agent installation, you can view the errors on each server. You can also log into the server from SA and correct the errors.

This section discusses the following topics:

- Viewing Unmanaged Server Information
- Opening a Remote Terminal Session on an Agentless Server
- Reports on Agent Installation

Viewing Unmanaged Server Information

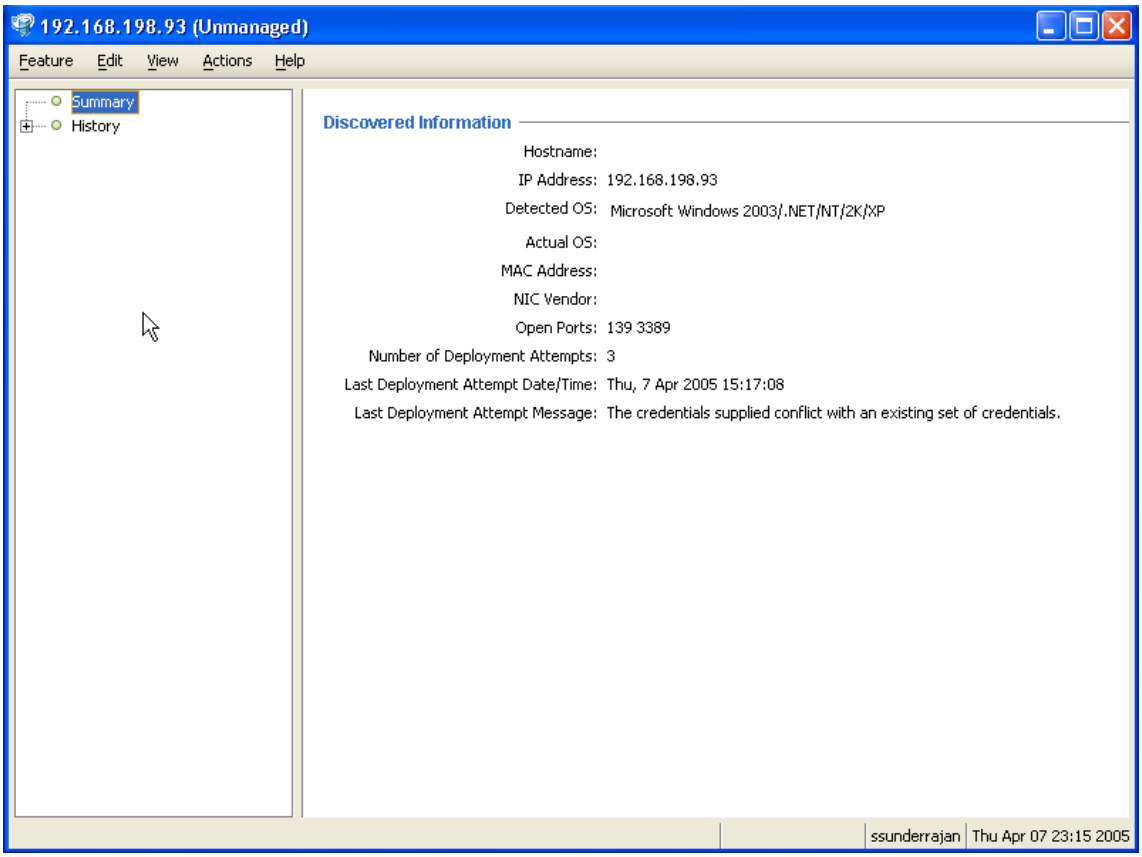
Unmanaged physical servers are any physical servers that do not have an SA agent installed on them.

Virtual machines (VMs) are always managed by a virtualization service. It is highly recommended that you make all virtual machines (VMs) agent-managed servers to have maximum visibility, control, and compliance for these VMs. For more information, see the SA User Guide: Virtualization Management.

To view information about unmanaged, agentless servers, perform the following steps.

1. From the SA Client navigation pane, select Devices and then select SA Agent Installation. This lets you search for agentless servers to install the SA agent on. For more information, see Discovering Agentless Servers.
2. From the SA Agent Installation screen, select an agentless server. From the Actions menu, select Open. This displays information about the agentless server as shown in Unmanaged Server Summary Page below.

Unmanaged Server Summary Page



The Summary View of an Unmanaged Server

The Summary view of the agentless server gives the following information.

- **Hostname**: The host name of the agentless server, if defined in the Domain Name System (DNS).
- **IP Address**: The IP address of the server.
- **Detected OS**: The operating system detected on the server after performing the network scan. The listed operating system is a *"best guess"* made by comparing the server's response

to a network probe of a list of known operating system *"fingerprints"*. The listed operating system may not always be accurate, for example when a firewall exists between the Server Automation Core and the server and does not allow or alters the network probe.

- **Actual OS**: The actual operating system detected on the server after the agent is installed. This entry will be blank until SA can successfully log on to the managed server and identify the operating system type and version.
- **MAC Address**: The Media Access Control (MAC) address, which is the network interface card's unique hardware number of the server. The MAC address is used as the server's physical address on the network. The MAC address is only detected if the server is on the same physical network as the Gateway.
- **NIC Vendor**: The vendor name for the Network Interface Card (NIC) driver. The NIC vendor is only detected if the server is on the same physical network as the Gateway.
- **Open Ports**: The discovered open ports on an unmanaged server. SA does not perform a comprehensive search for open ports. There may be open ports not listed.
- **Number of Deployment Attempts:** The number of attempts to install the SA agent on the server.
- **Last Deployment Attempt Date/Time**: The date and time of the last attempt to install the SA agent.
- **Last Deployment Attempt Message**: The message stating the possible cause for the failure of the last attempt to install the SA agent.

The History View of an Unmanaged Server

The History view of a server shows a history of all actions executed on the server.

Opening a Remote Terminal Session on an Agentless Server

You can open a remote terminal session on an agentless server and log in to the server using the appropriate protocol and correct any errors on the server or perform any other operations.

To open a remote terminal session on an agentless server perform the following steps.

1. Log into the SA Client.
2. From the navigation pane, select Devices and then select SA Agent Installation.
3. Select an agentless server.
4. Either right click or select the Actions menu, select **Log in with** and select the appropriate protocol.

The specific commands that SA uses to log in to the remote server are specified in the Terminal and Shell options. Select **Tools > Options**. For more information, see Terminal and Shell Options.

Reports on Agent Installation

You can create the following reports as described below.

- All the servers in the current network scan

- Selected servers in the current network scan
- Servers in the current network scan with successful deployments
- Servers in the current network scan with failed deployments

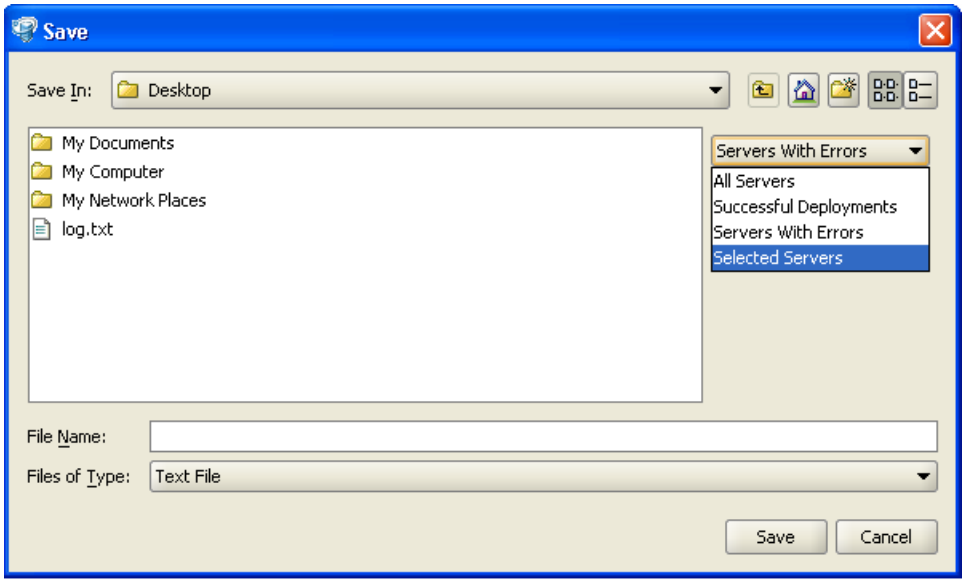
You can also save and export the reports to a CSV, HTML, or text file format.

Creating Reports on Failed Agent Installation

Perform the following steps to create reports:

1. Log in to the SA Client.
2. From the navigation pane, select Devices and then select SA Agent Installation.
3. From the SA Agent Installation page, select the agentless server. From the Actions menu, select Export to the desired report format. The Save Report dialog box appears.
4. From the drop-down list, select the type of report as shown in Generating Reports .

Generating Reports



5. Enter the location and file name to save the report.

Example Report

The following example shows a report of servers with failed deployments.

```
Server List:


Name : dhcp-183-154.aqua.qa.hp.com
Address : 192.168.183.154
Detected Operating System : Microsoft Windows 2008
Accuracy : 100%
```

```
Actual Operating System : Unknown
Open Ports : 3389
MAC Address : 00:50:56:8A:13:58
NIC Vendor : VMWare
# of Deployment Attempts : 0
Last Deployment Message : "No Message"
Managed by HP Server Automation: No
```

About Communication between the Server and the SA Core

The server agent communicates with the SA core to provide information about the server to the core and to receive commands from the core.

- The server agent gathers information about the server and sends it to the SA core. The SA core stores this information about all managed servers.
- When you initiate an action on the server — for example, a software installation or removal, a patch installation, a software or hardware configuration change, an audit or any other server management action — the SA core sends a command to the server agent. The server agent receives the command from the core and initiates the corresponding actions on the server.

The server agent opens a secure communication channel to the core, presents its IP address and public-key certificate for authentication purposes. If properly authenticated, the agent updates the information about the server in the SA core.

Running Server Communication Tests

This section describes how to assess the communication between the SA core and your managed servers.

- About Server Communication Tests
- Running Server Communication Tests - SA Client
- Communication Test Results
- See also Troubleshooting Server Communication Tests.

Note: The communication test is not available on VMware ESXi servers because SA does not install a server agent on ESXi servers. You can determine if an ESXi server is reachable from its virtualization service by selecting the server and selecting the Virtualization view. The Virtualization view displays the virtualization service managing the ESXi server and its connection state. For more information about virtual servers, see the SA User Guide: Virtualization Management.

About Server Communication Tests

Sometimes a server agent can become unreachable and the SA core cannot communicate with the agent. To identify managed servers that have unreachable agents, the SA core runs periodic communication tests with all managed servers and saves the results. You can check the reachability of agents by looking at the server's Properties or by viewing the current agent reachability status for all managed servers since the last communication test was run.

You can also manually run communication tests on one or more servers. When the test finishes, the results for each server are displayed. In some cases, the failure of one test might prevent other tests from being executed.

The results of each communication test job are saved under the Jobs and Sessions tab. You can search and view the results of previously run communication tests.

The communication test works by testing communication and data exchange between the specific components of the SA core and each managed server. To manage servers, the core needs to be able to communicate with the server agent on each managed server.

Types of Server Communication Test

The communication test performs the following diagnostic tests:

- **AGT Test** (Command Engine to Agent Communication) - Tests if the SA core can communicate with the SA agent running on the server.
- CRP Test (Crypto Match) - Tests the encryption and security of the connection between the SA core and the managed server. Checks that the agent's SSL cryptographic files are valid.
- CE Test (Agent to Command Engine Communication) - Tests if the server can retrieve commands to be executed from the SA core.
- DAE Test (Agent to Data Access Engine) - Tests if the server can retrieve its stored device information from the SA core.
- SWR Test (Agent to Software Repository Communication) - Tests if the server can retrieve software and patches from the SA core.
- MID Test (Machine ID Match) - Verifies that the server's machine ID is the same as the machine ID stored in the SA core.

Running Server Communication Tests - SA Client

You can run communication tests on one or more managed servers. Perform the following steps.

1. In the SA Client, select the Devices tab.
2. In the navigation pane, select one or more servers.
3. Either select the **Actions** menu or right click and select **Run** > **Communication Test**. This runs the communication test on the selected servers and displays the results in a separate Run Communication Test screen.
4. Optionally select the Run in Background button. This closes the Run Communication Test screen and redisplays it when the test completes.

5 If any tests fail, see Troubleshooting Server Communication Tests.

Communication Test Results

The icons shown in Agent Reachability Status Icons below indicate the success or failure of agent reachability test. For more information, see Troubleshooting Server Communication Tests.

Table: Agent Reachability Status Icons

Status Icons	Test Results
	The communication test passed. The server is reachable.
or 	The communication test did not execute. This is typically because one of the other tests failed.
 or 	The communication test failed. The server is unreachable.
 or 	The communication test is still running.

Chapter 5

Creating and Managing Customers

SA provides several ways to organize your managed servers:

- Creating **Customers** in SA and assigning servers to those customers. Customers provide a way to group your servers and provide access control boundaries.
- Creating **Device Groups** and placing servers in the device groups either manually or by a set of rules that automatically determine membership. Device groups provide a way to group your servers and provide access control boundaries. For more information about device groups, see Exploring Servers and Device Groups in the SA Client.
- Creating and modifying **Server Use** categories and **Deployment Stage** categories so you can identify categories of servers and what they are used for, as well as to describe their various stages of life cycle deployment. For more information, see See "Server Use Categories and Deployment Stage Categories".

About Customers

Many enterprises have consolidated disparate IT operations into a single operation, yet they still need separate reporting, billing, and management for different business units, groups or customers. For example, one company may separate activities for their West Coast Office, East Coast Office, and London Office. A service provider company may organize their IT operations by their customers such as Customer A, Customer B, Customer C and so forth.

SA accommodates these requirements by letting you create separate **customers** and assign each managed server to a specific customer.

A customer in SA is a logical group into which you can place servers. You can then perform IT management tasks on all servers belonging to a customer. Customers also provide security and authorization boundaries. Each SA user must be given access to one or more customers to gain access to the servers belonging to each customer.

IT resources such as patches and patch policies, software packages and policies can also be assigned to customers. Only resources assigned to a customer can be used on servers assigned to the same customers. Resources assigned to a special category “Customer Independent” can be used on any servers regardless of their customer assignment.

About Customers and Facilities

A facility is all the servers managed by an SA core or satellite. You may have one facility or you many have multiple facilities. Each facility is managed by a separate SA core or satellite. If you have multiple cores and facilities, all your SA cores are connected in a multimaster mesh for reliability, redundancy, scalability and performance. All cores and satellites communicate with each

other to keep all your data redundantly stored. If one core goes down, the other cores automatically provide services to the servers managed by that core.

Customers are a way to organize your servers and provide access control boundaries based on the users of your servers. A customer represents a set of servers associated with a business organization, such as a division or a company. Typically a server is associated with a customer because it runs applications for that customer.

You can define as many customers as you need and assign managed servers to each customer. However, you must first associate a customer with one or more facilities before you can place servers from a facility into a customer. A customer can span more than one facility and a facility can contain one or more customers. To associate a customer with one or more facilities, see Viewing or Modifying a Customer - SA Client.

Predefined Customers

SA defines the following customers:

- **Not assigned**: Default "customer" that servers belong to when they are not assigned to a "real" customer. When you bring a server into SA, the server is associated with the Not Assigned customer.
- Opsware (customer): SA infrastructure component hosts belonging to the Opsware customer. The Opsware customer is a system-provided customer designation that is used exclusively for servers (or VMs) that host the SA infrastructure: cores, satellites, and slices. This customer designation allows you to give infrastructure servers their own set of access controls to keep them logically separate from your other servers and prevents you from accidently deleting them.

  Opsware Customer can be renamed, but the qualities that belong to the Opsware Customer are carried over to the newly named entity.

Caution: The Opsware customer should only contain Server Automation infrastructure servers. If you accidentally assign a non-infrastructure server (or VM) to the Opsware customer, change its customer status to Not Assigned before you delete it.

- **Customer Independent**: Resources such as software and patches can be specified as customer independent. Servers cannot be assigned to this "customer". These customer independent resources can be installed on any managed server, no matter what customer the server is assigned to.

You can install software and patches that are Customer Independent on Not Assigned servers. However, you cannot install any resources associated with a customer on a server that is not assigned to a customer. That is, the resources and servers need to be owned by the same customers.

Customer Security, Authorizations and Permissions

Setting up separate customers and assigning servers and IT resources to separate customers allows you to set up security boundaries and user authorization capabilities. Only users who have

permission to access a customer's servers and IT resources are authorized to manage those servers and resources. A user who does not have access to a customer's servers and IT resources can neither see nor manage that customer's servers.

Access is granted or denied based on user groups. Each user belongs to one or more user groups. Each user group has access to one or more specific customers. This combination of customers and user groups gives you full control over security and authorization.

For more information on users, user groups and setting permissions, see the SA Administration Guide.

Permissions to Create, Delete, and Modify Customers

An SA user must have the Super Administrator permissions to create or delete customers. An SA user must have the Customers Feature permission to modify customers. For more information on permissions, see the SA Administration Guide.

Customer Tasks - SA Client

This section describes how you can use SA customers to manage your servers through the SA Client.

Assigning a Server to a Customer - SA Client

All managed servers must be assigned to exactly one customer, even if they are assigned to the special customer "Not Assigned". To assign the server to a different customer, perform the following steps.

1. In the SA Client, select the Devices tab.
2. Navigate to the desired server under the Servers node in the navigation pane.
3. Select the server.
4. Select **Actions** or right click and select **Open**. This displays a new window with information about the server.
5. Select Properties in the navigation pane. This displays a list of management information about the server including the customer the server is assigned to.
6. Select the Change button next to the Customer field. This displays a list of available customers.
7. Select a customer.
8. Select the Select button.
9. Select **File > Revert** to discard your changes.
10. Select **File > Save** to save your changes.

Creating a New Customer - SA Client

To create a new customer, you need to log in as a super administrator. For more information on permissions, see the SA Administration Guide.

To create a new customer, perform the following steps.

1. Log in to the SA Client as a user with the Customers Feature permission.
2. Select the Administration tab in the navigation pane. This displays the Customers node at the top of the navigation pane.
3. Select the Customers node in the navigation pane. This displays all the customers that have been defined.
4. Select **Actions > New**. This displays the new customer window. If you do not have the proper permissions, this menu is disabled.
5. Enter a name and a short name for the new customer. The name is the display name that is used throughout the SA Client. The short name is the name used internally by SA.
6. Optionally add one or more facilities by selecting the "+" icon. Only servers from facilities associated with the customer can be assigned to the customer. For more information, see About Customers and Facilities.
7. Select **File > Save** to create the new customer.

Viewing or Modifying a Customer - SA Client

To modify a customer, you need appropriate permissions. For more information on permissions, see the SA Administration Guide.

To view or modify a customer, perform the following steps.

1. Log in to the SA Client as a user with the Customers Feature permission.
2. Select the Administration tab in the navigation pane. This displays the Customers node at the top of the navigation pane.
3. Select the Customers node in the navigation pane. This displays all the customers that have been defined.
4. Select the customer you want to view. Information is displayed in the lower pane.
5. From the View list, select either Properties or Custom attributes.
6. To open the customer in a separate window, select **Actions** or right click and select **Open**. This displays the customer in a separate window.
7. Select Properties to view or modify the name of the customer or to view or change the facilities associated with the customer.
8. Select Custom Attributes to view, modify or delete the custom attributes defined by the customer. Select the value of any custom attribute to modify it. Select the "+" icon to add a new custom attribute. Select one or more custom attributes and select the "-" icon to delete them.
9. Select **File > Revert** to discard all your changes.
10. Select **File > Save** to save your changes to the customer.

Deleting a Customer - SA Client

To delete a customer, you need appropriate permissions. For more information on permissions, see the SA Administration Guide.

To delete a customer, perform the following steps.

1. Log in to the SA Client as a user with the Customers Feature permission.
2. Select the Administration tab in the navigation pane. This displays the Customers node at the top of the navigation pane.
3. Select the Customers node in the navigation pane. This displays all the customers that have been defined.
4. Select one or more customers you want to delete.
5. Select **Actions** or right click and select **Delete**. This deletes the selected customers. If you do not have the proper permissions, this menu will be disabled.

Chapter 6 Running SA Extensions

HPE Server Automation(SA) gives you the capability to extend its functionality by creating **Automation Program Extensions** (**APX**s). This section describes the APX extensions feature and how to run extensions.

Tip: For information on how to create APX extensions, see "Extending SA with Automation Platform Extensions (APXs)" in the SA Platform Developer Guide.

APX extensions provide a framework that allows anyone familiar with script-based programming tools such as shell scripts, Python, Perl, and PHP, to extend the functionality of SA and create applications that are tightly integrated into SA. SA provides two types of APX extensions:

- **Program APX Extensions** run in the Global File System (OGFS) and can use all of the OGFS functionality. You can use typical programming practices to leverage the SA API and access a core's Managed Servers to implement new custom functionality. For example, you could write an APX extension that gathers BIOS information from managed servers and populates custom fields using shell commands.
- **Web APX Extensions** allow you to create a web-based application, where either an Apache 2.x process or a CGI/PHP script is called using GET or POST URL. Web APX extensions can contain static web resources such as images, and can employ CGI or PHP for dynamic content generation.

APX extensions allow you to access data about your managed environment and share and process that data with web applications, scripts, programs and other custom applications.

Methods of Running Extensions

You can run extensions in any of the following ways.

- **From Managed Servers, by selecting a server first:** Select one or more servers in the SA Client, right click or select **Actions**, then select **Run Extension**. This applies only to certain program extensions. For details, see Run Extensions on Managed Servers.
- **From the SA Client Library:**
  - In the SA Client, select **Library** > **By Type** > **Extensions > Web** or **Program** to run an extension. Choose an extension, then:
    - Double-click the extension.
    - Right-click the extension and select **Run...**.
    - Select **Actions** > **Run...**.
  - In the SA Client, select **Library** > **By Folder** to run an extension, then navigate to the extension and open it: select **Actions** > **Run...**.
- **From the Global Shell (program extensions only):** From the Global Shell, run `/opsw/apx/bin/<extension name>` where <extension name> is the unique name of

the extension. Provide any parameters the extension requires. For more information on the Global Shell, see SA Global Shell.

- **From a web browser (web extensions only):** From a web browser, enter the URL *https://<SA core>/webapp/<extension name>* where `<SA core>` is the IP address or host name of your SA core and `<extension name>` is the unique name of the web extension.
- **From the SA API (program extensions only):** From the SA API, use the method `ProgramAPXService.startProgramAPX()`. For more information on the SA API, see the SA Platform Developer Guide.

Note: Most extensions cannot run on VMware ESXi hypervisor servers because SA does not install an agent on ESXi servers. Instead, SA manages ESXi servers through the VMware vCenter virtualization service. For more information, see the SA User Guide: Virtualization Management.

Tip: When using the global shell to run an APX that seeks information on a managed server, such as the System Diagnostics APX, the agent for that server must be running. Attempting to run the APX when the agent is turned off will result in an error.

Run Extensions on Managed Servers

Some extensions take one or more managed servers as input and perform some operation or gather some information from those managed servers. For example, an extension could gather certain information about devices on the servers using a script. You can run this extension by selecting one or more servers and selecting the extension to run. This extension describes how to run extensions that take one or more managed servers as input to the extension.

Note: Only program extensions that implement the “com.hp.client.server.RightClickToRun” interface can be run using this method. This interface indicates that the extension takes one or more servers as input parameters.

Only extensions you have permission to execute will be shown in the SA Client. For more information on permissions, see the SA Administration Guide.

For details on creating extensions, the RightClickToRun interface and permissions, see “Extending SA with Automation Platform Extensions (APXs)” in the SA Platform Developer Guide.

To run an SA program extension by first selecting one or more servers, perform the following steps.

1. From the SA Client Navigation pane, select **Devices** > **All Managed Servers**.
2. Select one or more servers in the Contents pane.
3. Right click the server or select **Actions > Run Extension > Select Extension...**.

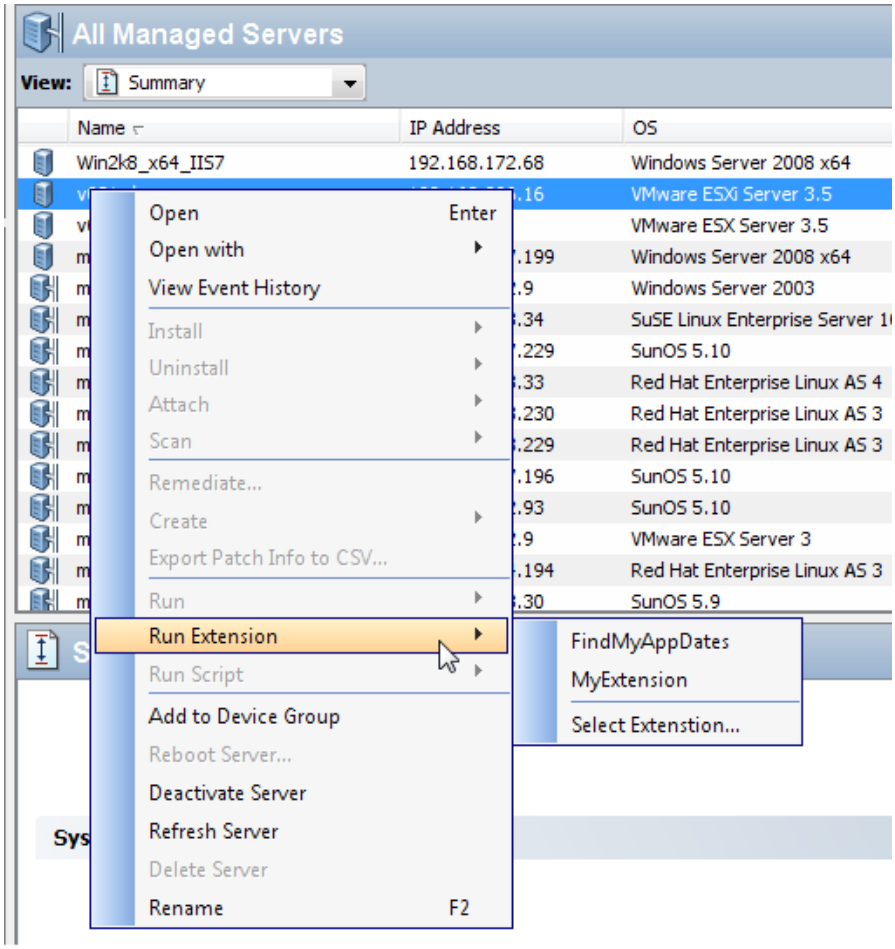
   Or

Right click the server or select **Actions > Run Extension >** and select a named extension, if any are shown in the menu.

Run Extension lists all of the program extensions that have been run at least once before. You can select one of these extensions without having to use the **Select Extension...** window.

For example, the following shows the **Run Extension** menu item selected, two sample program extensions named **MyExtension** and **FindMyAppDates**, and the **Select Extension...** menu item.

The Run Extension Menu

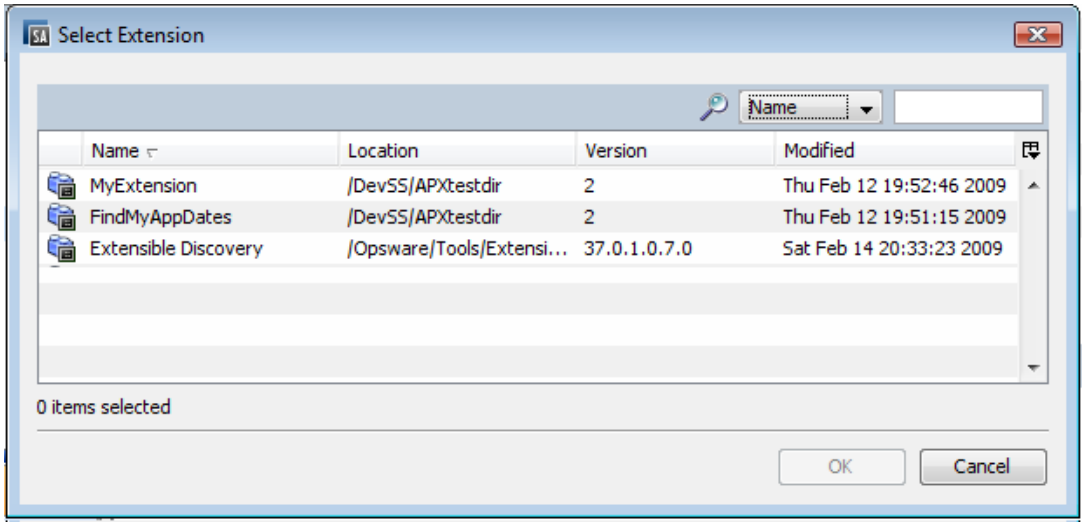


Note: Extensions appear under **Run Extension** only after they have been run at least once using **Select Extension...**. That is, to make your extension appear under **Run Extension**, you must first select **Select Extension** to run your extension, then choosing your extension as described in step 4 below.

4 If you selected a particular extension **Run Extension** in Right click the server or select Actions > Run Extension > Select Extension...., skip ahead to Once you have chosen a particular extension to run, the SA Client displays the Run Program Extension screen as shown below. This screen shows the devices the extension will run against. below.

If you chose **Select Extension...**, the SA Client displays the available extensions. The following screen shows three extensions: MyExtension, FindMyAppDates and Extensible Discovery. Select an extension and click OK.

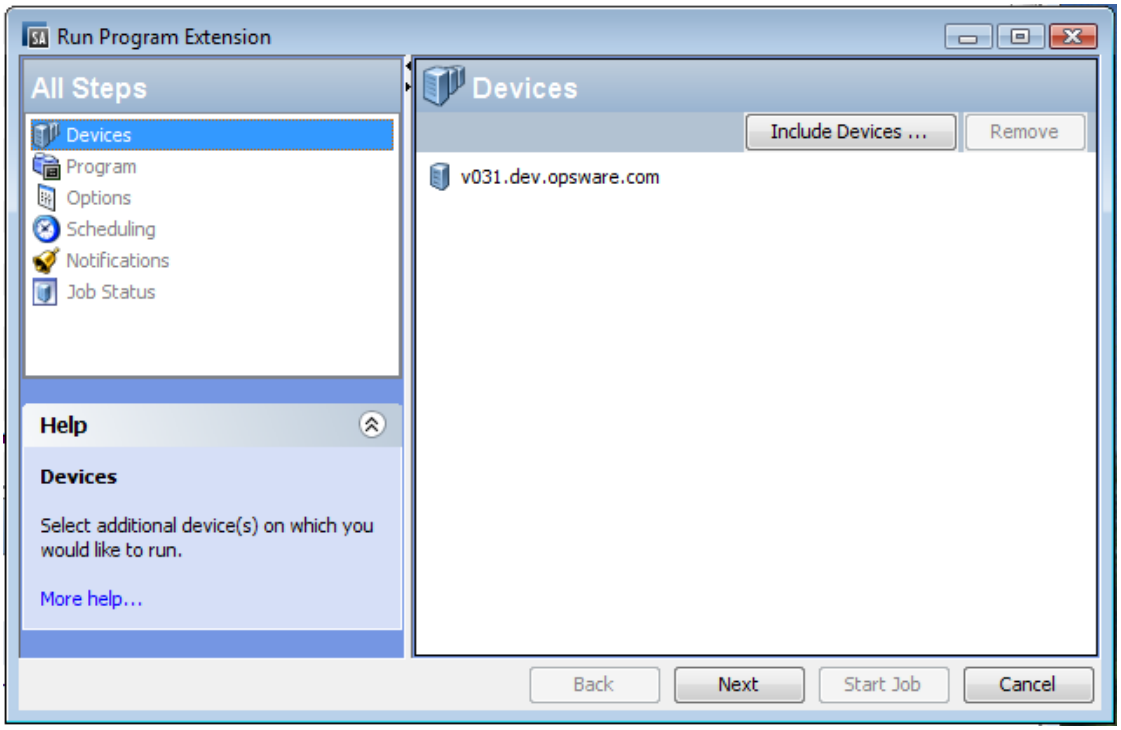
The Select Extension Window



5 Once you have chosen a particular extension to run, the SA Client displays the Run Program Extension screen as shown below. This screen shows the devices the extension will run against.

If you want to run the extension against more devices, select the Include Devices... button and select additional devices or device groups. To remove devices, select the devices and click Remove.

Select Devices on the Run Program Extension Window



6 Click the Next button. This displays the Program Properties and Program Execution Path. Optionally edit the program execution path and click Next to display the Runtime Options and Output Options.

7 Optionally change the Runtime Options and Output Options and click Next to display the Schedule Frequency and Time and Duration.

Or you can click Start Job to skip the remaining options and run the extension with default options.

8 Optionally specify how frequently to run the extension and click Next to display Email Notifications and Ticket Tracking.

9 Optionally change the email notifications and add a ticket ID and click Next to display the Job Status screen.

10 Click Start Job to run the extension. The Run Program Extension screen displays the progress of the extension. When the extension finishes, click the Close button.

Running Extensible Discovery on Managed Servers

SA can gather a large amount of information from your servers by default. Extensible Discovery lets you gather additional information about your servers quickly and easily. Extensible Discovery is a feature that you can customize and use to discover and obtain custom information about servers in your managed environment.

This section describes how to run Extensible Discovery. To customize Extensible Discovery and add your own scripts, see Adding Scripts to Extensible Discovery.

Note: To run Extensible Discovery, you must have write access to the managed servers where you want to run Extensible Discovery and you must have execute access to the Extensible Discovery folder in the SA Library. For more information on permissions, see the SA Administration Guide.

Note: You cannot run Extensible Discovery on VMware ESXi hypervisor servers because SA does not install an Agent on ESXi servers. Instead, SA manages ESXi servers through the VMware vCenter virtualization service. For more information, see the SA User Guide: Virtualization Management.

To run Extensible Discovery, perform the following steps.

1. Run the Extensible Discovery extension as described in Run Extensions on Managed Servers. This does the following:
   a. Remediates the software policies "Customer Provided Scripts" and "HP Provided Scripts" on the selected servers. This copies all the scripts in these policies to all the managed servers. It places the scripts on the managed servers.
   b. Runs all the scripts in the Extensible Discovery directory on the selected servers.
   c. Places the output from the scripts either in custom attributes or custom fields.

Note: The first time you run Extensible Discovery on a server will typically take longer than subsequent runs because it needs to install scripts on the server the first time you run it.

2. Examine the results by viewing the Custom Attributes or Custom Fields for each server.

   If an error occurs, check the following custom attributes for more information.

   — HPSW_ED_error: If an error occurs on a server, this custom attribute will be created for the server and it will contain any relevant error messages. To determine which servers had an error, you can search for servers with this custom attribute.

   If Extensible Discovery runs without errors on the server later, this custom attribute will be removed.

   — HPSW_ED_warning: This custom attribute will be created on servers where a non-fatal warning occurs.

   If Extensible Discovery runs without warnings on the server later, this custom attribute will be removed.

   For more information, see Comparing Custom Fields and Custom Attributes.

Running Extensible Discovery from the OGSH

You can also run Extensible Discovery from the Global Shell (OGSH) using the command interface as follows:

```
/opsw/apx/bin/com/opsware/extensible_discovery -d <server ids> -g
<group ids>
```

The following table describes the options to this command. For more information on the Global Shell, see *SA Global Shell*.

Table: Options to the extensible_discovery Command

Option	Usage
-h --help	Displays help for this command.
-d <server ids> --deviceids=<server ids>	Specifies one or more server IDs or server names separated by commas. Runs Extensible Discovery on the specified servers.
-g <group ids> --groupids=<group ids>	Specified one or more device group IDs or device group names separated by commas. Runs Extensible Discovery on all the servers in the specified groups.

To find a server ID or a device group ID in the SA Client, display the server or device group and locate the ID in the Object ID column. The Object ID is an integer value.

Adding Scripts to Extensible Discovery

SA can gather a large amount of information from your servers by default. Extensible Discovery lets you gather additional information about your servers quickly and easily. Extensible Discovery is a feature that you can customize and use to discover and obtain custom information about servers in your managed environment. With Extensible Discovery you can:

- Write scripts that gather custom information from your servers and easily incorporate your scripts into Extensible Discovery.
- Schedule the execution of your scripts.
- Search and generate reports on the resulting custom information.
- Export the resulting information to other tools for further analysis and decision support.
- Automatically update all servers when your scripts change.

Scripts Provided with Extensible Discovery

The following scripts are included with Extensible Discovery. These scripts are automatically executed on the selected managed servers when you run Extensible Discovery.

Table: Scripts Included with Extensible Discovery

Script Name	Operating System	Description
get_oslevel.sh	AIX	Returns the operating system level. (Uses the AIX command `oslevel -s`.)
get_install_date.sh	HP-UX	Returns the date the operating system was installed. The date value is formatted to be placed

Script Name	Operating System	Description
		in a custom attribute or a string type custom field, but not a date type custom field.
get_firmware_version.sh	Linux	Returns the BIOS version.
get_firmware_version.sh	Solaris	Returns the EEPROM (or OBP) version when run on Sparc servers. Otherwise returns the BIOS version.
get_firmware_version.vb	Windows	Returns the BIOS version.

These scripts will create custom attributes with the name `HPSW_ED_firmware_version` or `HPWS_ED_oslevel`. If you want the return values to be placed in custom fields, you must create custom fields named `HPSW_ED_firmware_version` and `HPWS_ED_oslevel` before running the extension, and the return values will be stored in the custom fields you created. If the custom fields don't exist, Extensible Discovery will create custom attributes on each server and place the data in the custom attributes.

These scripts are in the SA Library under `/Opsware/Tools/Extensible Discovery/HP Provided Components`. To view these scripts, in the SA Client select Library, By Folder and navigate to the `HP Provided Scripts` folder. Select a .zip file and select **Actions** > **Export Software**.

If you do not want these scripts to execute on managed servers, remove them from the "HP Provided Scripts" software policy as described in Software Policies Provided with Extensible Discovery below.

Software Policies Provided with Extensible Discovery

Extensible Discovery uses two software policies that contain the scripts it runs to gather information from managed servers. Extensible Discovery automatically remediates these policies on managed servers and runs the scripts in them.

- **HP Provided Scripts**: This software policy contains the HP-provided scripts listed in Scripts Included with Extensible Discovery. It is located in the SA Library under `/Opsware/Tools/Extensible Discovery/HP Provided Components`.
- **Customer Provided Scripts**: This software policy is initially empty. You can place your custom scripts in this software policy as described below and Extensible Discovery will use your scripts. It is located in the SA Library under `/Opsware/Tools/Extensible Discovery/Customer Provided Components`.

When you run Extensible Discovery, it remediates these policies on the selected managed servers and runs all the scripts in these policies. If you don't want any of the scripts in these policies to run, remove them from the policy.

Extensible Discovery copies the scripts in these policies to the following directories on the managed servers:

- `/var/opt/opsware/extensible_discovery/scripts/` on UNIX systems.

- `%SYSTEMDRIVE%\Program Files\Common Files\Opsware\extensible_discovery\scripts\` on Windows systems.

Extensible Discovery runs all the scripts in these directories regardless of how the scripts got there.

You can use these software policies or create your own software policies, but if you create your own, you must remediate them on managed servers where you want to run Extensible Discovery. For more information on software policies, see the SA User Guide: Software Management.

Writing Your Own Scripts for Extensible Discovery

This section describes requirements and guidelines for writing scripts for use with Extensible Discovery. For instructions on how to add your scripts to Extensible Discovery, see Adding Your Own Scripts to Extensible Discovery.

- HP provides several sample scripts you can use in the software policy "HP Provided Scripts". You can view these scripts in /Library/Opsware/Tools/Extensible Discovery/HP Provided Components. For more information, see Scripts Provided with Extensible Discovery.
- A best practice is to store your script in a version control system.
- Your script needs to handle error situations within your script and return an accurate exit status. The following explains various error situations and how Extensible Discovery handles them.
  - The exit status of a shell script is the exit status of the last command in the script. A script that returns zero status is considered successful.
  - A script could return zero status but also send some output to stderr. This case is treated as a success. The output from stderr will be treated the same as stdout.
  - A script that returns zero status and outputs nothing to stdout or stderr will be considered a success and the blank value will be written to the appropriate custom attribute or custom field. You could use this method to set the custom attribute or custom field to ““.
  - A script that returns a non-zero value is treated as an error. A message including the script's stdout and stderr will be stored in the HPSW_ED_error custom attribute.
  - A script that is not executable or has syntax errors is treated as an error. A message including the script's stdout and stderr will be stored in the HPSW_ED_error custom attribute.
  - If a script determines that it has nothing to collect on a server (for example, if the get_eeprom_version.sh is run on a Solaris x86 server, where there is no EEPROM), it should return an exit status of 3, which will be interpreted by Extensible Discovery as not applicable, and will return nothing for that particular data item.
  - For UNIX shell scripts, if you want the script to fail when any individual command in the script fails, start the script with the line `#!/bin/sh -e`. For more information, see the documentation for the UNIX shell.

Adding Your Own Scripts to Extensible Discovery

To customize extensible discovery, you need to write one or more scripts that gather the custom data you want, then import your scripts into SA. For requirements and guidelines on writing scripts, see Writing Your Own Scripts for Extensible Discovery.

Note: This section presumes you are familiar with software policies. For details on software policies, see the SA User Guide: Software Management.

Note: To add scripts to Extensible Discovery, you must have write access to the Extensible Discovery folder and the ability to create software policies. For more information on permissions, see the SA Administration Guide.

To create and add your script to Extensible Discovery, perform the following steps.

1. Decide where you want the output of your script to go. It can go either in a custom attribute or in a custom field.
   - For more information on custom attributes, see See "Custom Attributes for Servers".
   - For more information on custom fields, see See "Custom Fields for Servers".
2. Decide on the name of the custom attribute or custom field. Extensible Discovery will place the output of your script in the named custom attribute or custom field.
   - For a custom attribute, the name will be in the following format: HPSW_ED_<name> where <name> is any string you choose.
   - For a custom field, use any value for the <name> of the custom field.

   You must use the <name> string in the name of your script as described in the steps below.
3. Write your script such that the output of the script is the data you want to capture. You can write any of the following types of scripts:
   - UNIX shell scripts in a file ending with `.sh`.
   - Visual Basic scripts in a file ending with `.vbs`.
   - Windows batch scripts in a file ending with `.bat`.

   For more information how to write these scripts for Extensible Discovery, see Writing Your Own Scripts for Extensible Discovery.
4. Test your script to make sure it is functioning properly.
5. Name your script `get_<name>.sh` or `get_<name>.vbs` or `get_<name>.bat`, where `<name>` is from Decide on the name of the custom attribute or custom field. Extensible Discovery will place the output of your script in the named custom attribute or custom field. above. Extensible Discovery uses <name> to locate the custom attribute or custom field for the output of the script.
6. Make sure your script file has execute permissions. For example, for UNIX scripts use the `chmod` command.

7 If you want the output to go into a custom attribute, skip this step and go to Wrap your script into a .zip file. Include any other files your script needs in the .zip file. below. Extensible Discovery creates and places the output in the custom attribute named `HPSW_ED_<name>` by default.

   If you want the output to go to a custom field, you must create a custom field named "`<name>`" where `<name>` is the string you used in Decide on the name of the custom attribute or custom field. Extensible Discovery will place the output of your script in the named custom attribute or custom field. and Name your script get_<name>.sh or get_<name>.vbs or get_<name>.bat, where <name> is from Decide on the name of the custom attribute or custom field. Extensible Discovery will place the output of your script in the named custom attribute or custom field. above. Extensible Discovery uses <name> to locate the custom attribute or custom field for the output of the script. above. Extensible Discovery first checks for an existing custom field of the specified name. If that custom field exists, Extensible Discovery places the script output there. If that custom field does not exist, Extensible Discovery creates and stores the output in a custom attribute named "`HPSW_ED_<name>`".

   For example, if you create a script named `get_mysysdata.sh`, the output from the script will be placed into the custom field named `mysysdata`, if it exists. Otherwise the output will be placed in the custom attribute named `HPSW_ED_mysysdata`.

   For instruction on creating custom fields, see About Custom Fields.

8 Wrap your script into a .zip file. Include any other files your script needs in the .zip file.

   As a best practice, include a version string in the name of your .zip file and increment the version string with each subsequent version of your script. For more information, see Upgrading Your Scripts in Extensible Discovery.

9 Import your .zip file into a package in SA.

   For convenience, you can place your packages in /`Opsware/Tools/Extensible Discovery/Customer Provided Components`. Make sure your imported package specifies the proper target operating system.

   For instructions on importing packages, see the SA User Guide: Software Management.

10 Open your package in the SA Client and set the Default Install Path property to one of the following and save your changes.

   — UNIX: /var/opt/opsware/extensible_discovery/scripts

   — Windows: %ProgramFiles%\Common Files\Opsware\extensible_discovery\scripts\. SA replaces %ProgramFiles% with the appropriate system Program Files directory.

11 Add your package to a software policy. Add it either to the software policy named "Customer Provided Scripts" or add it to your own software policy.

   Extensible Discovery remediates the "Customer Provided Scripts" policy by default whenever it runs.

Note: Make sure the software policy to which you add your package has the proper target operating system(s). Note that any user who has write access to the "Customer Provided Components" folder can run arbitrary code on any servers that Extensible Discovery is run on. For

greater security, use your own software policy and set security on your software policy to meet your security requirements.

12 If you added your script to your own software policy, you must remediate your policy on all servers where you want Extensible Discovery to run.

   If you added your script to the policy named “Customer Provided Scripts”, you can skip this step.

13 Run your script as described in Running Extensible Discovery on Managed Servers below.

Tip: If you intend to use a custom field but inadvertently run your script without having created the custom field and it creates custom attributes on many servers, you can use the following OGSH command to remove the custom attributes from all servers.

```
rm /opsw/Server/@/*/CustAttr/<custom attribute name>
```

For more information on the SA Global Shell (OGSH), see SA Global Shell.

Upgrading Your Scripts in Extensible Discovery

This section describes how to upgrade your scripts that are used with Extensible Discovery. The following steps presume you have already created and installed a script called `get_mysysdata.sh` and wrapped it in the file `get_windows_data_v1.0.zip` and imported it into Extensible Discovery as described in Adding Your Own Scripts to Extensible Discovery. To upgrade this script, perform the following steps.

1 Create the new version of your script and give it the same name as the original script file. For example, use `get_mysysdata.sh`. Follow the instructions in `Writing Your Own Scripts for Extensible Discovery`.

2 Wrap your script in a .zip file and increment the version string of the .zip file. For example, you could use `get_windows_data_v1.1.zip`.

3 Import your .zip file into a package in SA.

   For convenience, you can place your packages in /`Opsware/Tools/Extensible Discovery/Customer Provided Components`. Make sure your imported package specifies the proper target operating system.

   For instructions on importing packages, see the SA User Guide: Software Management.

4 Open your package in the SA Client and set the Default Install Path property to one of the following and save your changes.

   — UNIX: /var/opt/opsware/extensible_discovery/scripts

   — Windows: %ProgramFiles%\Common Files\Opsware\extensible_discovery\scripts\. SA replaces %ProgramFiles% with the appropriate system Program Files directory.

5 Open the software policy “Customer Provided Scripts”. If you have used another software policy, open that policy.

Note: Make sure the respective software policy has the proper target operating system(s).

6 Remove the old .zip file from the policy, `get_windows_data_v1.0.zip` in this example.

7 Add your new .zip file to the policy, `get_windows_data_v1.1.zip` in this example.

8 If you are using the "Customer Provided Scripts" policy, run Extensible Discovery as described in Running Extensible Discovery on Managed Servers. This remediates your new script on the managed servers.

   If you are using another policy, remediate the servers with that policy. This remediates your new script on the managed servers so Extensible Discovery can be run.

Removing Your Scripts from Managed Servers

When you run Extensible Discovery, it copies your scripts in "Customer Provided Scripts" to the specified managed servers. To remove the scripts from the managed servers, perform the following steps. For this scenario, assume you have a script named `get_mysysdata.sh` wrapped in the file `get_mysysdata_v2.5.zip`.

1 Create a new version of your .zip file with a new version number, for example `get_mysysdata_v2.6.zip`.

2 Copy everything from the old .zip file into the new .zip file, except for the script you want to remove from managed servers, `get_mysysdata.sh` in this example.

3 Import your .zip file into a package in SA.

   For convenience, you can place your packages in /`Opsware/Tools/Extensible Discovery/Customer Provided Components`. Make sure your imported package specifies the proper target operating system.

   For instructions on importing packages, see the SA User Guide: Software Management.

4 Open your package in the SA Client and set the Default Install Path property to one of the following and save your changes.

   — UNIX: /var/opt/opsware/extensible_discovery/scripts

   — Windows: %ProgramFiles%\Common Files\Opsware\extensible_discovery\scripts\. SA replaces %ProgramFiles% with the appropriate system Program Files directory.

5 Open the software policy "Customer Provided Scripts". If you are using your own software policy, open your policy.

6 Remove the old .zip file, `get_mysysdata_v2.5.zip` in this example.

7 Add your new .zip file, `get_mysysdata_v2.6.zip` in this example.

8 If you are using the software policy "Customer Provided Scripts", Run Extensible Discovery as described below. This removes your script from the managed servers.

   If you are using your own software policy, remediate the managed servers. This removes the scripts from the managed servers.

Output from Extensible Discovery Scripts

Each script being used by Extensible Discovery provides output that is placed either in a custom attribute or a custom field. The maximum size of this output is 1000 bytes. To save more than 1000 bytes, perform the following steps.

1. Follow step 1 through Make sure your script file has execute permissions. For example, for UNIX scripts use the chmod command. under Adding Your Own Scripts to Extensible Discovery.
2. Create a configuration file the same name as your script except ending with "`.cfg`". For example, if your script is named `get_mysysdata.sh`, create the file `get_mysysdata.cfg`.
3. Enter the following line in your configuration file.

   `MAXBYTESTOCAPTURE=<number of bytes>`

   where <number of bytes> is the maximum number of bytes your script will produce.
4. Wrap your script file and the configuration file into a .zip file.
5. Follow the remaining steps under Adding Your Own Scripts to Extensible Discovery.

Comparing Custom Fields and Custom Attributes

SA can store a large amount of information about your managed servers. Custom Attributes and Custom Fields provide a way for you to store additional information about your servers quickly and easily. Custom Attributes and Customer Fields are data elements you can create for servers and other objects in SA.

Custom Attributes and Custom Fields are similar but they have several differences as described in the following table. In general, you should use custom fields when all servers require the data to be stored and you should use custom attributes when only a subset of servers require the data to be stored. However, see the following table for other differences before you decide which to use.

Table: Comparison of Custom Attributes and Custom Fields

	Custom Attributes	Custom Fields
Data Type:	String only.	Typed. Must be one of the types listed in Custom Field Data Types.
Objects Allowed for:	Allowed for any object: servers, device groups, customers, facilities, OS installation profiles, and software policies.	Allowed only for servers and device groups.
Number:	Each custom attribute is for one object only.	Each custom field creates an instance for all servers or device groups. All managed servers have the same named

	Custom Attributes	Custom Fields
		custom field, but the value can vary with each server. Similarly for device groups.
Searches Allowed:	Search is only allowed on the custom attribute name, not on its value. That is, you can search for all servers that define a particular custom attribute.	Search is allowed based on custom field values, including different matching criteria for different data types. For example, if you have a custom field of type date, you can search for all servers where the date value is one month old or older.
Inheritance:	Inherited from more general objects. For example, servers inherit custom attributes defined for device groups they belong to.	No inheritance.
Permissions Required to View:	Read permission on the server, device group or other object.	Read permission on the server or device group.
Permissions Required to Modify the Value:	Write permission on the server, device group or other object.	Write permission on the server or device group.
Permissions Required to Create or Delete:	Write permission on the server or device group where you are creating the custom attribute.	Manage Virtual Columns permission. Write permission on the server or device group.

For more information on Custom Attributes and Custom Fields, see See "Custom Fields for Servers" and See "Custom Attributes for Servers".

About Custom Fields

SA can store a large amount of information about your managed servers. Custom Fields provide a way for you to store additional information about your servers quickly and easily. Custom Fields are data elements you can create for servers and device groups.

When you create a custom field for servers, every server in your managed environment gets an instance of the custom field. When you create a custom field for device groups, every device group gets an instance of the custom field. The value of the custom field can be different for each server or device group.

For example, if your managed environment contains 500 servers and you create a custom field for servers, you would have 500 separate custom fields, one for each server. If you had 75 device groups and you created a custom field for device groups, you would have 75 separate custom fields, one for each device group.

Tip: Custom attributes are another way to store additional information about your servers. For more information on custom attributes, see Creating and Managing Custom Attributes. See also Comparing Custom Fields and Custom Attributes.

Data Types in Custom Fields

Custom fields are typed. Each custom field you create must be of one of the following types.

Table: Custom Field Data Types

Custom Field Type	Description
String	Any characters, up to a maximum of 3999 characters.
Long String	Any characters. Use this type for strings longer than 3999 characters.
URI	A string representing a Uniform Resource Identifier.
Date	A date.
Number	A positive or negative integer.
File	An attached file.

Creating a Custom Field with the Custom Field Management Web Extension

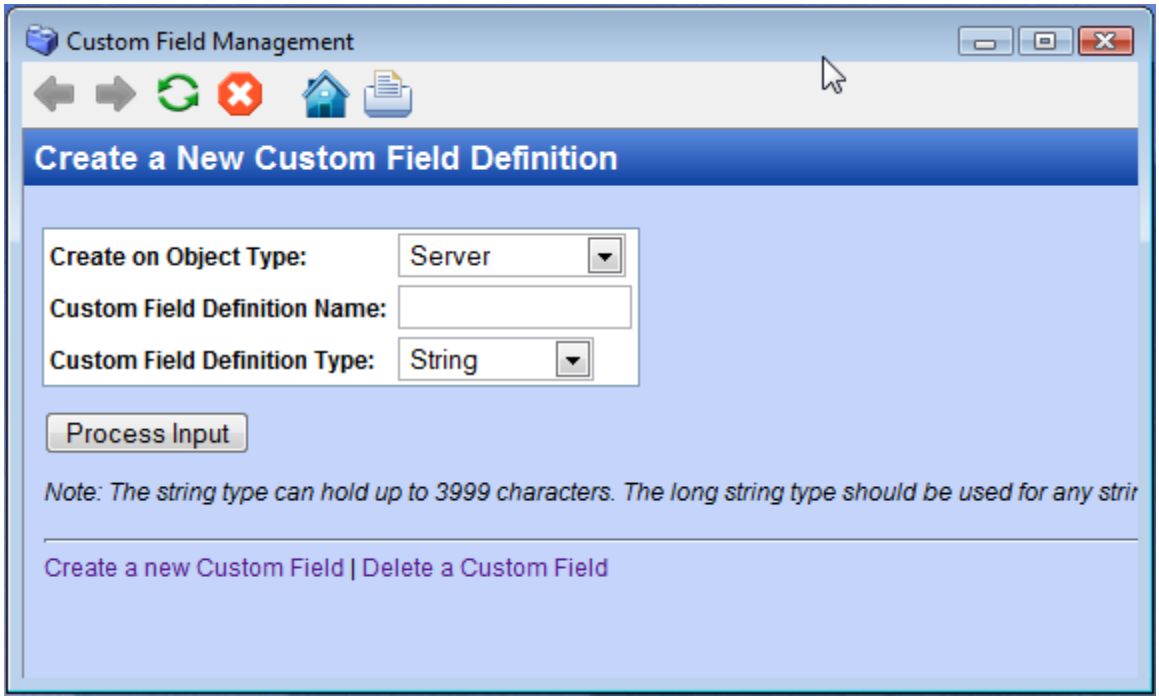
The Custom Field Management web extension lets you create and delete custom fields.

Note: To create or delete custom fields, you must have the following permissions: Manage Virtual Columns, Execute permission on the Web Extensions folder in the Library, and Read access to at least one managed server. For more information on permissions, see the SA Administration Guide.

To create a custom field, perform the following steps.

1. In the SA Client navigation pane, select Library and the By Type tab.
2. Select Extensions, then select Web.
3. Select the Custom Field Management extension and either right click or select **Actions > Run...**. This displays the Custom Field Management window as shown below.

Custom Field Management Web Extension - Create a Custom Field



4. In the first drop-down list, select the object you want the new custom field to be associated with. If you select Server, every server will get an instance of the custom field. If you select Device Group, every device group will get an instance of the custom field.
5. Enter the name of the new custom field in the text input field.
6. In the second drop-down list, select the data type of the custom field. See Custom Field Data Types.
7. Select Process Input to create the custom field.

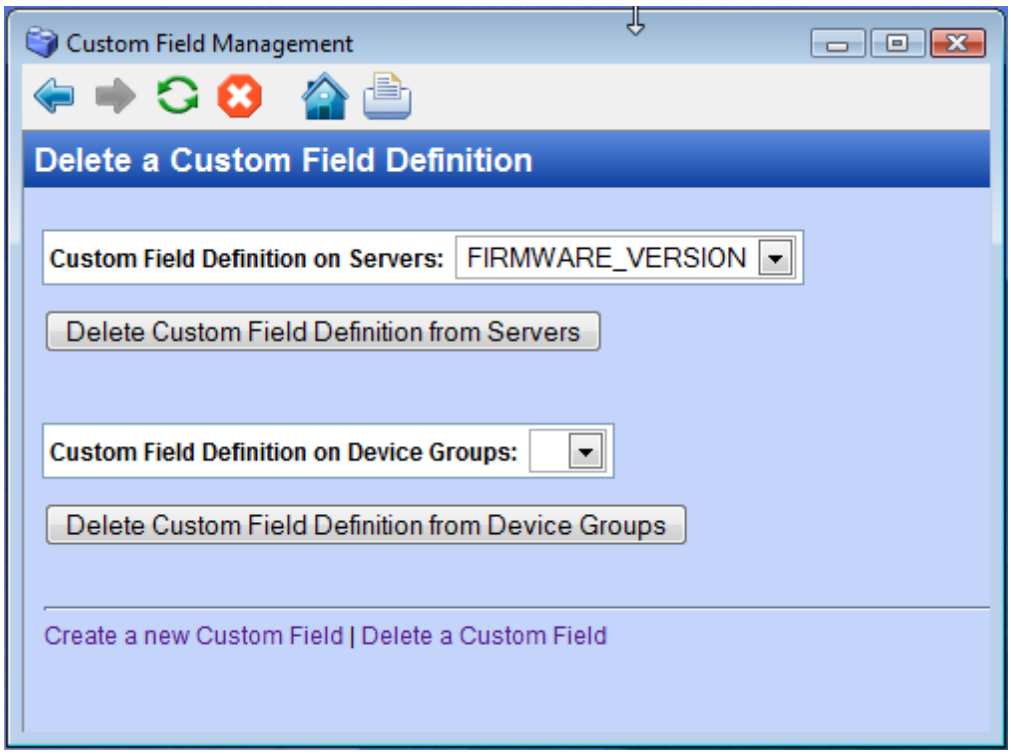
Deleting a Custom Field with the Custom Field Management Web Extension

The Custom Field Management web extension lets you create and delete custom fields. To delete a custom field, perform the following steps.

> **Caution:** When you delete a custom field, you delete all the values stored by all the servers or device groups associated with the custom field.

1. In the SA Client navigation pane, select Library and the By Type tab.
2. Select Extensions, then select Web.
3. Select the Custom Field Management extension and either right click or select **Actions** > **Run...**. This displays the Custom Field Management window as shown in Custom Field Management Web Extension - Create a Custom Field.
4. Select the “Delete a Custom Field” link. This displays the Delete a Custom Field Definition window as shown below.

Custom Field Management Web Extension - Delete a Custom Field



5 To delete a custom field defined for servers, select a custom field name in the first drop-down list. The example above shows the custom field FIRMWARE_VERSION selected.

   To delete a custom field defined for device groups, select a custom field name in the second drop-down list.

6 To delete a custom field defined for servers, select Delete Custom Field Definition from Servers.

   To delete a custom field defined for device groups, select Delete Custom Field Definition from Device Groups.

Editing Custom Field Values

To edit custom field values for a server, perform the following steps.

1 In the SA Client navigation pane, select the Devices tab.

2 Select the All Managed Servers node.

3 Select a server.

4 To view the custom fields and values, select Properties from the View drop-down selector. This displays several different properties of the server including all the custom fields defined for the server.

5 Select Actions > Open to open the server browser, or right click the server and select **Open**. This displays information about the server. Select the Information tab, then select Properties in the navigation pane. This displays several different properties of the server including all the custom fields defined for the server.

6 Locate the custom field you want to modify.

7 The way you modify the value of the custom field depends on the type of the custom field. Modify the value of the custom field.

8 Select **File > Revert** to discard all your changes to custom field values.

9 Select **File > Save** to save the modified custom field value.

Creating and Managing Custom Attributes

SA can store a large amount of information about your managed servers. Custom attributes provide a way for you to store additional information about your servers quickly and easily. Custom attributes are data elements you can create for servers and device groups.

You can create custom attributes for servers, device groups, customers, facilities, OS installation profiles, and software policies. Custom attributes values are string values.

Tip: Custom fields are another way to store additional information about your servers. For more information on custom fields, see About Custom Fields. See also Comparing Custom Fields and Custom Attributes.

To add, delete or modify the value of a custom attribute for a server, perform the following steps.

1 In the SA Client navigation pane, select the Devices tab.

2 Select the All Managed Servers node.

3 Select a server.

4 To view the custom attributes defined for the server, select Custom Attributes from the View drop-down selector. This displays all the custom attributes defined for the server.

5 Select Actions or right click the server and select Open. This displays information about the server.

6 Select the Information tab in the navigation pane.

7 Select Custom Attributes in the navigation pane. This displays all the custom attributes defined for the server.

8 To add a new custom attribute, select the “+” icon and enter the name of the custom attribute.

9 To delete a custom attribute, select the custom attribute and select the “-” icon.

10 To change the value of a custom attribute, double click the value column in the appropriate row and enter the new value.

11 Select **File > Revert** to discard all your changes.

12 Select **File > Save** to save your changes.

Note: Custom attributes changes are reflected in the History panel for servers, device groups, OS installation profiles, and software policies.

Chapter 7

Script Execution

Overview of Script Execution

The Script Execution feature allows you to automate the management and execution of scripts in the SA Client. It also allows you to organize your scripts in folders and define security permissions around them. From the SA Client, you can create or upload a script, set it up to run simultaneously across multiple UNIX or Windows servers, and monitor it as it executes on each server. After a script is executed, you can view the results for every server and then export the script results. You can also modify, delete, and rename a script. You can also execute scripts in the Global Shell using the SA Client.

Script Execution Features

The Script Execution feature in the SA Client enables you to perform the following functions:

- Organize your scripts into folders and define security permissions to control access of their contents across different users and user groups.
- Create or upload scripts in the SA Client.
- Run scripts across multiple UNIX or Windows servers or server groups.
- Execute scripts in the Global Shell.
- Schedule one time or recurring script execution jobs.
- Notify the status of the script execution job via email.
- Approve script execution jobs.
- View the script output against multiple servers in a tabular format.
- Export the script execution results.
- Search for scripts and script execution jobs.

Script Execution Process

The script execution process involves defining permissions, managing scripts, and executing scripts.

Defining Permissions

In this phase, an SA Administrator assigns Folder permissions, Client feature permissions, and Customer constraints to define the security boundaries across various user groups. The permissions determines the actions the users in a user group can perform with the SA Client.

See the SA Administration Guide for more information about defining security permissions.

Managing Scripts

In this phase, a policy setter or an advanced system administrator performs script management tasks such as creating or importing scripts, editing script properties, exporting scripts, and deleting scripts. See Managing Scripts for more information.

Executing Scripts

In this phase, a system administrator executes server scripts directly on servers or server groups and OGFS scripts in the Global Shell. A system administrator can also execute scripts by adding the scripts to a software policy and then remediating the servers against the software policy. See Executing Scripts and the SA User Guide: Software Management for more information.

Types of Scripts

In the SA Client, the Script Execution feature supports two main types of scripts: server scripts and OGFS scripts.

- The Server script allows you to execute scripts on UNIX and Windows servers managed by SA. The SA Client supports the following types of Server scripts for UNIX and Windows operating systems: UNIX/Linux shell, Windows batch (.BAT), Windows Visual Basic (VBScript), Windows PowerShell and Python (.py). Python scripts can be executed on both Unix and Windows.
- The OGFS scripts allows you to execute scripts in the Global Shell from the SA Client. You can specify the directory path in the OGFS to execute the scripts.

The server scripts are further classified to Saved Scripts, and Ad-hoc Scripts.

- Saved scripts are accessible to all the users, if they have the appropriate permissions. You are required to have the appropriate permissions to create, view, edit, and execute saved scripts.
- Ad-Hoc scripts are created or uploaded for one-time use and are not stored in Server Automation. Ad- Hoc scripts are created or uploaded and then immediately executed by a user and during this process, only this user has access to the scripts.

After you create a script and save it as a specific type of script in Server Automation, you cannot convert the script to the other type of script.

In the SA Client, you can specify to run a Sever script as a Super User or as a specified user.

- A Super User script allows you to execute the script as root on UNIX or Local System on Windows servers without entering a password. This applies to any user who has permission to execute the script, including users that do not have "Run Ad hoc & Saved Scripts As Super User" permission.
- If the script is not designated as a Super User Script, then you need to enter a user name and password to run the script unless you have the "Run Ad hoc & Saved Scripts As Super User" permission. You also require the appropriate permissions to manage and run Super User Server Scripts.

See the *SA Administration Guide* for information on the permissions required to run the Super User Server Scripts. All the OGFS scripts can only be executed as an SA User.

Managing Scripts

The script management tasks include:

Creating a Script

Opening a Script in the SA Client

Editing Script Properties

Locating Scripts in Folders

Exporting a Script

Renaming a Script

Deleting a Script

Note: You must have a set of permissions to create and manage a script. To obtain these permissions, contact your SA Administrator. See the SA Administration Guide for more information.

Creating a Script

In the SA Client, you can create a script from either the By Type or the By Folder view in the Library.

Script Creation Guidelines

Server Automation supports the following types of Server scripts for UNIX and Windows operating systems: UNIX/Linux shell, Windows batch (.BAT), Windows Visual Basic (VBScript), Windows PowerShell and Python (.py). Python scripts can be executed on both Unix and Windows .

When creating scripts you must adhere to the following guidelines:

4 MB is the maximum size allowable for a script.

When you create a UNIX shell script with a language other than the Bourne (sh) shell, use the sh-bang (#!) format at the top of the script to specify the correct command interpreter. The command interpreter needs to be present on the managed server.

For example, if you are using Perl, the beginning of the script would contain the following line:

```
#!/usr/bin/perl
```

The following example shows a short Perl script (it displays “hello world”):

```
#!/usr/bin/perl
print “hello world\n”
```

VBScripts are executed by the VBScript interpreter on the Windows server.

To access command line parameters with UNIX shell commands, use the following convention: `$1 $2...`

To access command line parameters with Windows .BAT, use: `%1 %2...`

Script lines do not need to be terminated in a specific way. But with Windows scripts, Server Automation converts all `\n` to `\r\n`. With UNIX scripts, all `\r\n` are converted to `\n`.

Scripts should be written to send error output to standard error.

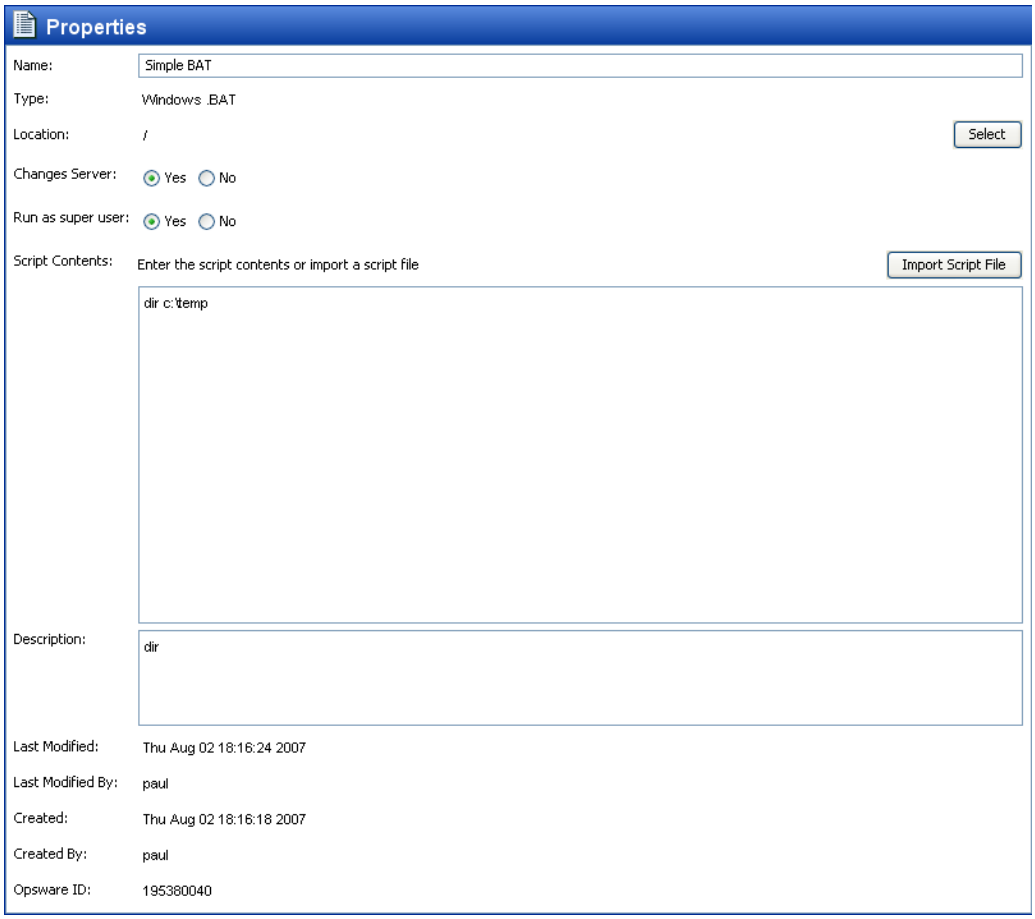
Scripts should use the standard convention of returning a zero code to indicate success. For other return codes, there is no standard code system to follow. Create unique non-zero return codes to handle each type of error.

Creating a Script from the By Type View in the Library

To create a script perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. Select the script type and from the **Actions** menu, select **New**. The Script window appears as shown in Figure 80.

   Figure 80. Script Window



3. In the Name field, enter the name of the script.
4. (Windows only) Select the script type from the Type drop-down list.
5. Click **Select** to specify the location for the script in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the script and then click **Select**.
6. In the Changes Server field, select Yes, if the script causes a change in the server configuration when executed.
7. In the Run as Super User field, select Yes if the script can be run as a Super User when executed. Selecting yes, allows you to run the script as a Super User without providing a password for the script.

8. This option is enabled only if you have to appropriate permission. See the SA Administration Guide for more information about script execution permissions.
9. In the Script Contents field, enter the contents of the script or click **Import Script File** to import a script.

   Note: If you import a script that uses Unicode (UTF8) encoding and your computer's regional language settings are set to English, and then you export the script and attempt to execute it, you may encounter errors because Unicode (UTF8) encoding may add a "." or other special character at the beginning of the script. If this occurs, simply edit the script to remove the extraneous characters.
10. In the Description field, enter text that describes the purpose or contents of the script.
11. To save the changes, select **Save** from the **File** menu.

Creating a Script from the By Folder View in the Library

To create a script perform the following steps:

1. From the Navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the Content pane.
2. Select the folder that should contain the script.
3. From the **Actions** menu, select **New** > **Script**. The Script window appears.
4. In the Name field, enter the name of the script.
5. Select the script type from the Type drop-down list.
6. Click **Select** to change the location for the script in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the script and then click **Select**.
7. In the Changes Server field, select Yes, if the script causes a change in the server configuration when executed.
8. In the Run as Super User field, select yes if the script can be run as a Super user when executed. OGFS Scripts can only be executed as an SA User.

   This option is enabled only if you have to appropriate permission. See the SA Administration Guide for more information about script execution permissions.
9. In the Script Contents filed, enter the contents of the script or click **Import Script File** to import a script. In the Open window, select the script to import and then click **Open**.

   Note: If you import a script that uses Unicode (UTF8) encoding and your computer's regional language settings are set to English, and then you export the script and attempt to execute it, you may encounter errors because Unicode (UTF8) encoding may add a "." or other special character at the beginning of the script. If this occurs, simply edit the script to remove the extraneous characters.
10. In the Description field, enter text that describes the purpose or contents of the script.
11. To save the changes, select **Save** from the **File** menu.

Note: The Library in the SA Client contains a Home directory and each user has a folder in the Home directory. You can save private scripts in this folder and later execute the script on managed servers.

Opening a Script in the SA Client

In the SA Client, there are several ways to open a script. You can open a script from:

- The Search option in the Navigation pane
- The By Type view in the Library
- The By Folder view in the Library
- The Device list in the Navigation pane

Opening a Script from Search

1. From the Navigation pane, select **Search**.
2. Select Server Script or OGFS Script from the drop-down list and then enter the name of the script in the text field.
3. Select  . The search results appear in the Content pane.
4. From the Content pane, select the script and then select **Open** from the **Actions** menu. The Script window appears.

Opening a Script from the By Type View in the Library

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**. The scripts appear in the Content pane.
2. From the Content pane, select the script and then select **Open** from the **Actions** menu. The Script window appears.

Opening a Script from the By Folder View in the Library

1. From the Navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the Content pane.
2. From the Content pane, select the script in a folder and then select **Open** from the **Actions** menu. The Script window appears.

Opening a Script from Devices

1. From the Navigation pane, select **Devices** > **Servers** > **All Managed Servers**. The server list appears in the Content pane.

   Or

2. From the Navigation pane, select **Devices** > **Device Groups**. The device groups list appears in the Content pane.
3. From the Content pane, select a server and then from the **Actions** menu, select **Open**. The Server Explorer window opens.
4. From the Views drop down list, select **Management Policies** > **Software Polices**. The software policies attached to the server appear in the Content pane.

5. From the Content pane, select the software policy and then select **Open** from the **Actions** menu. The Software Policy window appears.
6. From the Views drop down list, select Policy Items. The policy items appear in the Content pane.
7. From the Content pane, select the script and then select **Open** from the **Actions** menu. The Script window appears.

Editing Script Properties

After you create a script, you can view and modify its properties. You can view properties such as the SA user who created the script, the date when it was created, and the Object ID of the script. You can also modify the name, description, contents, the Library folder location of the script and the script options.

To view and edit script properties, perform the following steps:

1. Open a script in the SA Client. See Opening a Script in the SA Client for ways to open a script. The Script window appears.
2. In the Name field, edit the name of the script.
3. Click **Select** to change the location for the script in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the script and then click **Select**.
4. In the Changes Server field, select Yes, if the script causes a change in the server configuration when executed.
5. In the Run as Super User field, select yes if the script can be run as a Super User when executed. Selecting yes, allows you to run the script as a Super User without providing a password for the script.

   This option is enabled only if you have the appropriate permission. See the SA Administration Guide for more information about script execution permissions.
6. In the Script Contents field, edit the contents of the script or click **Import Script File** to import another script. In the Open window, select the script to import and then click **Open**.

Note: If you import a script that uses Unicode (UTF8) encoding and your computer's regional language settings are set to English, and then you export the script and attempt to execute it, you may encounter errors because Unicode (UTF8) encoding may add a . or other special character at the beginning of the script. If this occurs, simply edit the script to remove the extraneous characters.

7. In the Description field, edit the text that describes the purpose or contents of the script.
8. To save the changes, select **Save** from the **File** menu.

Viewing All the Software Policies Associated with a Script

In the SA Client, Server scripts can be added to a software policy. In the Scripts window, you can view all the software policies that contain the selected Server script. You cannot add OGFS script to a software policy.

To view the policy usage for a script, perform the following steps:

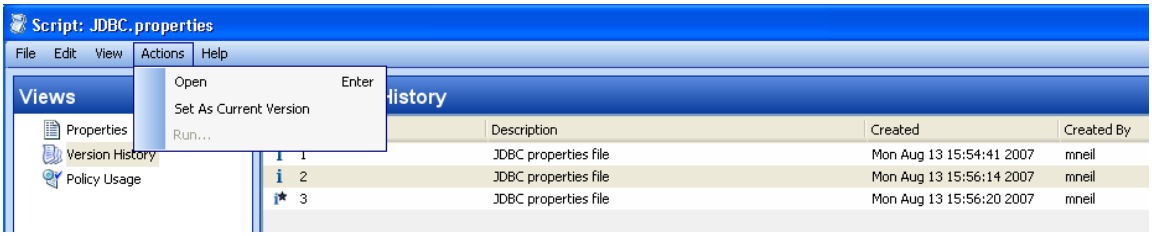
1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. From the Content pane, select the script and open it. The Scripts window appears.
3. From the Views drop down list, select Policy Usage. The list of software policies associated with the scripts appears in the Content pane.

Viewing Script Version History

To view the version history of a script perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. From the Content pane, select the script and open it. The Scripts window appears.
3. From the Views drop down list select Version History. The events associated with the script will display in the Content pane. You can view the script content from different versions of a script. The indicates the current version of the script. You can view the script content from different versions of a script. See the History of Server Changes for more information on server history.
4. To make any of the previous version of script current, select the script version and from the **Actions menu**, select **Set as Current Version** as shown in Figure 81.

   Figure 81. Script Version History



Locating Scripts in Folders

To locate a script in the folder hierarchy, perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. From the Content pane, select the script and then select **Locate in Folders** from the **Actions** menu. The folder hierarchy for the script appears in the Content pane.

Exporting a Script

To download a script, perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**. The scripts appear in the Content pane.

   Or
2. From the Navigation pane, select **Library** > **By Folder** and then select the folder which contains the script.

3. From the Content pane, select a script to export.
4. From the **Actions** menu, select **Export Script**. The Export Software window appears.
5. In the Browse window, specify the location for the script to be exported to.
6. Click **Export**.

Renaming a Script

To rename a script perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. From the Content pane select the script, and then from the **Actions** menu select **Rename**.
3. Enter the new name for the script in the Content pane.

Deleting a Script

To delete a script perform the following steps:

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**.
2. From the Content pane select the script, and then from the **Actions** menu select **Delete.** The Confirmation window appears.
3. Click **Delete** to delete the script.

Executing Scripts

In the SA Client, you can execute scripts in the following ways:

Execute a server script directly on servers or server groups and execute scripts in the Global Shell. See Running a Server Script (Saved Script or Ad-Hoc Script) and Running an OGFS Script for more information.

Add a script to a software policy and execute the script by attaching the software policy to the server and then remediating the server against the software policy. See the SA User Guide: Software Management for more information.

A software policy allows you to execute multiple scripts on a servers or server groups simultaneously, and execute a sequence of scripts on a server by specifying an install order in the software policy. See the SA User Guide: Software Management for information about software policies.

Note: You must have a set of permissions to execute a script. To obtain these permissions, contact your SA Administrator. See the SA Administration Guide for more information. For security purposes, several permission-based scenarios can be experienced to run or copy scripts in folders, run super user scripts, run non-super user scripts, etc.

Ways to Open the Run Script Window

The Run Script window allows to you execute a script on managed servers. In the SA Client you can launch the Run Script window in the following ways:

- From the Device List
- From the Device Explorer
- From the Library

From the Device List

1. From the Navigation pane, select **Devices** > **Servers** > **All Managed Servers**. The server list appears in the Content pane.

   Or
2. From the Navigation pane, select **Devices** > **Device Groups**. The device group list appears in the Content pane.
3. From the Content pane, select a server or device group.
4. From the **Actions** menu, select **Run Script**. The Run Script window appears.

From the Device Explorer

1. From the Navigation pane, select **Devices** > **Servers** > **All Managed Servers**. The server list appears in the Content pane.
2. From the Content pane, select a server.
3. From the Action menu, select **Open**. The Device Explorer appears.
4. From the **Actions** menu, select **Run Script**. The Run Script window appears.

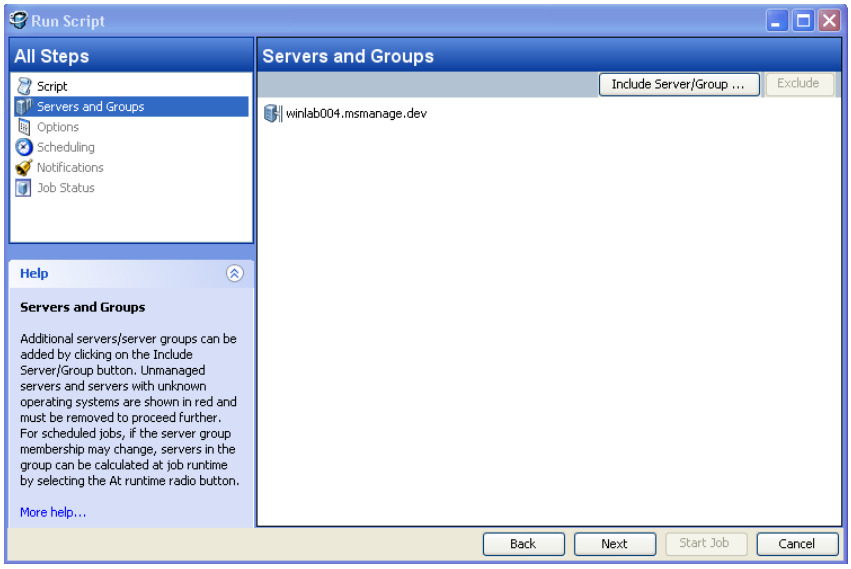
From the Library

1. From the Navigation pane, select **Library** > **By Type** > **Scripts**. The scripts list appears in the Content pane.
2. From the Content pane, select a script.
3. From the **Actions** menu, select **Run**. The Run Script window appears.

Running a Server Script (Saved Script or Ad-Hoc Script)

The Run Script, as shown in Figure 82, allows you to run a script on managed servers and consists of the following steps:

Figure 82. Run Server Script Window



Servers and Groups

Script

Options

Scheduling

Notification

Job Status

Note: You can now execute server scripts that do not change the server (Change Server option is set to No) in parallel with other scripts. This functionality is governed by the following configuration parameters:
* `way.server_script.run_read_only_scripts_in_parallel` (Administration >System Configuration> Command Engine): if set to 1, allows scripts that are marked does not change server to run in parallel with other scripts.
* `batchbot.max_concurrent_scripts` (Administration > System Configuration > Agent): when set to a non-zero value, determines the maximum number of scripts (including pre/post package scripts) that will be run in parallel by the agent. This parameter needs a 10.21 or latest SA Agent.

See Ways to Open the Run Script Window on how to access the Run Script window. If you access the Run Script window from the Device list or Device Explorer, the first step in the window is Script. If you access the Run Script window from the Library, the first step in the Run Script window is Servers and Groups.

Servers and Groups

This step allows you to specify the servers or server groups for executing the script. In this step, you can add and remove servers or server groups from the list.

If you choose the option Now, then the membership is determined based on the time when you made the selection. As a result the script is executed on the servers that were in the group when you selected the option. Changes to the group membership does not affect the list of servers on which the script will be executed.

If you choose the option Runtime, then the membership is determined when the script execution job is run. The script is executed on the servers present in the server group when the job is run. Changes to group membership is reflected in the list of servers when is script is executed.

Note: To be able to select the Runtime option, the "Allow Run Refresh Jobs" permission is required. See the SA Administration Guide for more information on permissions.

To select servers and groups perform the following steps:

1. Open the Run Script window from one of the methods described in Ways to Open the Run Script Window.
2. In the Run Script window, select the step Servers and Groups.
3. (Optional) Click **Include Server/Group** to add servers or server groups to the list or select a server or server group and click **Exclude** to remove servers from the list.
4. For a server group, in the Server Group Calculation field, select the option Now to execute the script on the servers that were in the group when you made the selection. Select the option Runtime to execute the script on the servers when the job is run.
5. Click **Next** to proceed to the Script step.

Script

This step allows to select a saved script or define an ad-hoc script to be executed on managed servers. See Types of Scriptsfor information on the script types.

Saved Script

To select a saved script perform the following steps:

To select a saved script, select the option Select Saved Script.

1. From the Name drop-down list select the script or click **Select Script** to open the Select Script window. Select the script from the Select Script window.
2. The script properties such as version, type, location are displayed in the content pane. To view the contents on the script, click **View Script**. The contents of the script are displayed in the Run Script window.
3. Click **Next** to proceed to the Options step.

Ad-Hoc Script

To define an ad-hoc script perform the following steps:

1. To select an ad-hoc script, select the option Define Ad-hoc Script.
2. From the Type drop-down list, select the script type.
3. Enter the contents of the script in the Script Contents field or click **Import Script File** to import a script.

Note: If you import a script that uses Unicode (UTF8) encoding and your computer's regional language settings are set to English, and then you export the script and attempt to execute it, you may encounter errors because Unicode (UTF8) encoding may add a "." or other special character at the beginning of the script. If this occurs, simply edit the script to remove the extraneous characters.

4. Click **Next** to proceed to the Options step.

Options

This step allows you to specify the runtime options and output options for executing a script. In this step you can specify whether to execute the script as root or Local System or as a specified user. You can also specify the script time-out value, any additional parameters for executing the script, and the output options for the script.

To specify the runtime and output options for a script perform the following steps:

In the Runtime User field select root (for UNIX) , Local System (for Windows) or Super User (for Unix and Windows) to execute the script as root or Local System.If the list of servers includes both Unix and Windows and you select Super User, the script will be executed as root on the Unix servers and as Local System on the Windows servers. To execute a script on both Unix and Windows, the script type must be supported on both platforms. To execute the script as root or Local System, you require the appropriate permissions. See the SA Administration Guide for information about the permissions required for executing scripts.

Or

Select Name and enter user name and password to execute the script as a specified user. To execute the script simultaneously across multiple servers or server groups, you must use the same user name and password across all the servers.

(Windows only) Enter the domain name in the domain field.

In the Script timeout field enter the script timeout value in minutes. The time out value is the amount of time required for a script to complete execution activities on a server. If the script is not executed when the timeout value is reached, then the script is stopped by SA and a script error occurs. Select a timeout value greater than the time required for execution to complete.

In the Specify any needed parameters for this script execution field, enter any parameters if required.

In the Output Options, select Discard all script output to discard script output or else select Retain script output.

Select the output size of the script from the Size of the output to retain drop-down list.

Click **Next** to proceed to the Scheduling step.

Scheduling

This step allows you to schedule the script execution job. You can choose to run the script execution job immediately, or on a specified date and time, or on a recurring basis.

To schedule a script execution job, perform the following steps:

In the Schedule Frequency section, choose to run the script once, daily, weekly, monthly, or on a custom schedule. Select any one of the following options:

Once: Choose this option to run the job immediately or only once at a specified date and time.

Daily: Choose this option to run the job on a daily basis at a specified time.

Weekly: Choose this option to specify the day or days of the week to run the job.

Monthly: Choose this option to specify the months to run the job, and the days of the month.

Custom: In the Custom Crontab string field, enter a string the indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values.

In the Time and Duration section, for each type of schedule, specify the start time for the job. You must also specify the start date and end date for the job.

In the Time Zone section, choose a time zone or accept the default, which is set according to the time zone settings in your user profile.

Click **Next** to proceed to the Notifications step.

Notifications

This step allows you to set email notifications to alert users on the success or failure of a job. You can also associate a Ticket ID with the job. This setting is optional.

To set email notifications, perform the following steps:

Click **Add Notifier**.

Enter the addresses in the Email Address of Recipient field.

For each recipient, select the check box for when to send an email notification:

On Success: sends email to recipient if the job succeeds.

On Failure: sends email to recipient if the job fails.

On Termination: sends email to recipient if the job is terminated.

Termination occurs when you stop an actively running job via the End Job action.

This notification does *not* apply to jobs that are cancelled before they are run.

Enter an ID to be associated with this job in the Ticket ID field.

Click **Next** to proceed to the Job Status step.

Job Status

This step allows you to start the job, view the job progress, the job results, the script output for a managed server, and export the script output from all the servers.

SA supports the following file formats for exporting script output results:

- A Zip file with folders for each managed server
- A Zip file containing no folders
- Consolidated raw text file

- Consolidated formatted text file
- Consolidated CSV file

You can also view jobs in the Jobs Log window of the SA Client. See Browsing Job Logs for information about job logs.

To start a job, perform the following steps:

1. To start the job, click **Start Job**.

   If you selected Immediately in the Scheduling step, the job will begin now. If you scheduled the job for a later time, the job will run later. You can then view the job in the Jobs Log window of the SA Client.
2. The job's progress information appears in the Job Status window. You can view the server on which the script was executed, the job status, and the exit code. If the exit code is zero, then it indicates that the script is executed successfully. If the exit code is non-zero, then it indicates an error during script execution.

   If the job status is displayed as Pending Approval, then the job is blocked until it is approved by a process that is external to SA. See Browsing Job Logs for information about job status.
3. (Optional) To view the script output from a managed server, select the managed server and script output appears below the table.
4. (Optional) To view the script output from all the managed servers, select the option Show output in table. The output for each server appears in the Output column in the table.
5. (Optional) To view the output for all the servers in separate columns, select the option Show output in table and enter the delimiter character in the Delimiter checkbox. The output for each server appears in separate columns in the table.
6. (Optional) To export the script output results, click **Export All Results**. In the Browse window specify the location and the file type and click **Export**.
7. Click **Close** to exit the Run Script window.

Terminating an Active Script Execution Job

You can stop a script job that is actively running. For example, you may need to stop a job that is producing erroneous results or will run beyond an allotted maintenance window. It should be noted that the termination process does not stop the script on a server or device where it is already running; it prevents the script from running on subsequent servers or devices.

You can terminate a script execution job from the Run Server Script window or from the SA Client Jobs and Sessions window.

Terminating an active script execution job has the following results:

After the cancellation request is received, work is not started on any additional servers.

If a script has already started on a server, it will be completed; however, it will not be started on additional servers.

The Job Status view of the Run Server Script window will indicate the job status for each server on which the script was run:

Server Status	Explanation
Cancelled	The script did not run on the listed device.
Succeeded	The script completed running on the listed device.

The Job Logs view of the SA Client Jobs and Sessions window will indicate the job status of the script:

Job Status	Explanation
Terminating	The termination request has been received and the job is in the process of ending.
Terminated	The termination process has completed.

Permissions for Terminating Active Jobs:

In general, users with the permission to start a job will be able also be able to terminate that job. In addition, users having *Edit or Cancel Any Job* permission are able to soft-cancel any running job.

See the *SA Administration Guide* for SA permissions details.

To terminate an active script execution job from the Run Server Script window:

Access the Run Server Script window and start the job.

See the following instructions for details:

Ways to Open the Run Script Window

Running a Server Script (Saved Script or Ad-Hoc Script)

Running an OGFS Script

From the Run Server Script window, click **End Job**. (This option only appears if the job is in progress.)

The End Job warning dialog will be displayed advising you that the job will complete the scripts that have been started on a server, but will not start any scripts on remaining servers.

Click **OK** to confirm that you wish to terminate the job. The Job Status window displays the progress of the termination.

If the job termination was successful on a particular device, it will be indicated by Cancelled status. Servers where the script completed will be indicated by Succeeded status. To see details about the server's status, select the server. Details will be displayed in the lower pane.

When the termination is complete, you can also view the job in the SA Client Job Log.

From the SA Client navigation pane, click **Jobs and Sessions**. The Job Logs view appears with your job listed with Terminated status.

To terminate an active script execution job from the SA Client Jobs and Sessions window:

From the SA Client navigation pane, click **Jobs and Sessions**. The Job Logs view appears.

From the Status filter, select In Progress to find running jobs.

Select **View** > **Refresh** from the menu to refresh the list. The content pane displays jobs with In Progress status.

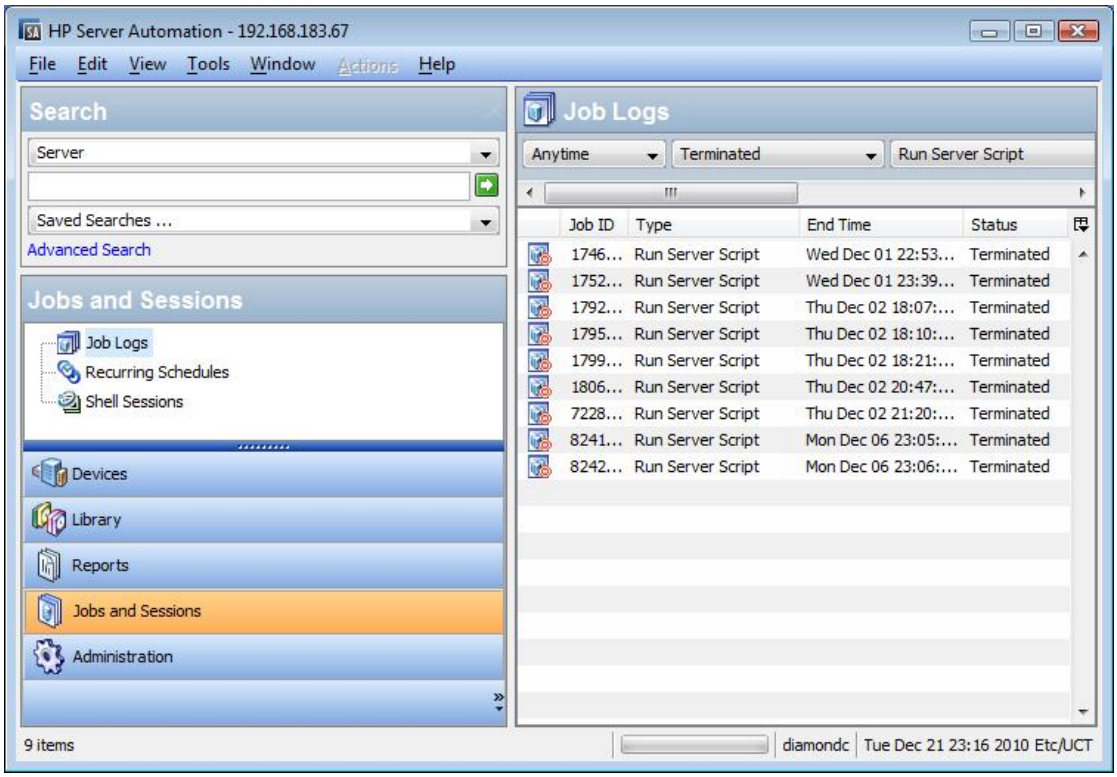
You can additionally filter the list by the type of job (such as Run Server Script) from the Type filter.

In the content pane, select the job that you want to terminate.

Select **Action** > **End Job**. (This option only appears if the selected job is in progress.)

When the termination process is complete, the job will have Terminated status, as shown in Figure 83.

Figure 83. Terminated Jobs from Job Log



Cancelling a Scheduled Script Execution Job

You can cancel scheduled jobs that are not in progress from the SA Client Jobs and Sessions window. When you cancel a scheduled script execution job, the entire job is cancelled and it appears in the Job Log queue with Cancelled status.

To cancel a schedule job:

From the SA Client navigation pane, select **Jobs and Sessions**. The Job Logs window appears in the content pane.

In the Status filter, select: Scheduled.

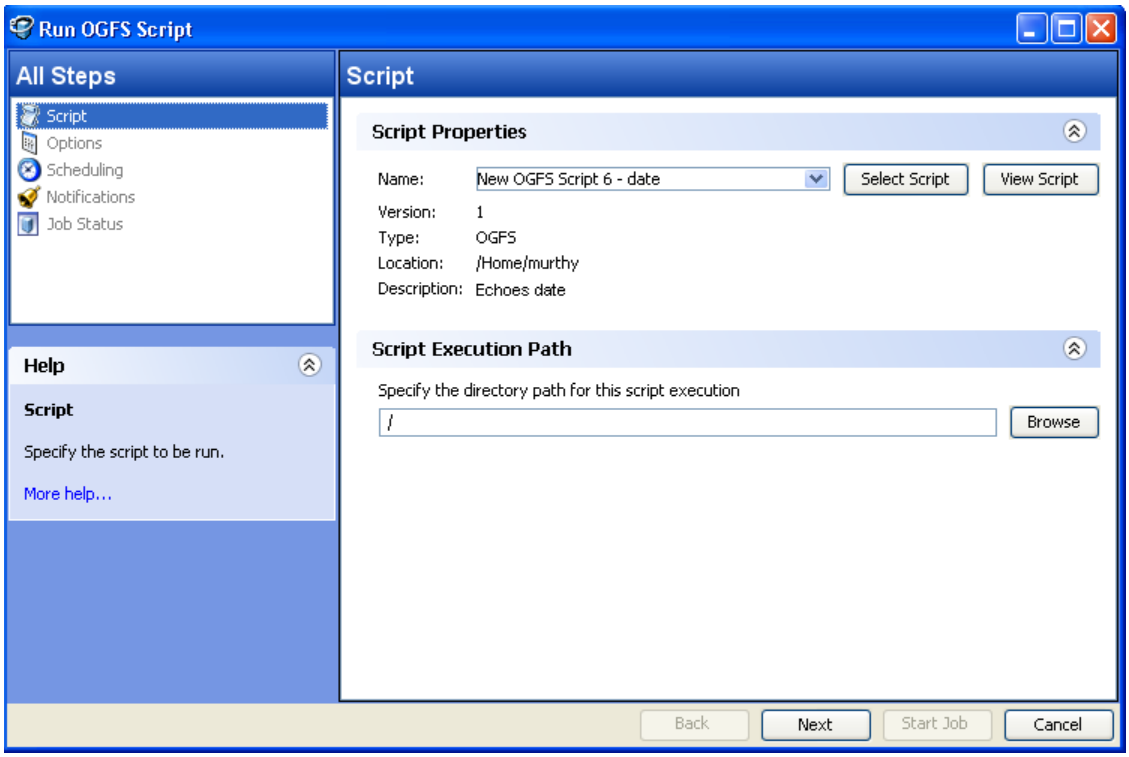
Select the scheduled job that you want to cancel.

From the menu, select **Action** > **Cancel**. The job appears in the Job Log with Cancelled status.

Running an OGFS Script

The Run OGFS Script, as shown in Figure 84, allows you to run an OGFS script and consists of the following steps:

Figure 84. Run OGFS Script Window



Script

Options

Scheduling

Notification

Job Status

Script

This step allows to specify an OGFS script for execution.

To select an OGFS script perform the following steps:

From the Navigation pane, select **Library** > **By Type** > **Scripts**. The scripts list appears in the Content pane.

Or

From the Navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the Content pane.

From the Content pane, select an OGFS script.

From the **Actions** menu, select **Run**. The Run OGFS Script window appears.

In the Script Properties section, select script from the Name drop-down list or click **Select Script** to open the Select Script window. Select the script from the Select Script window.

The script properties such as version, type, location, description are displayed in the content pane. To view the contents on the script, click **View Script**. The contents of the script are displayed in the Run OGFS Script window.

In the Script Execution Path section, enter the OGFS directory path for executing the script or click **Browse** to specify the directory path in the OGFS.

Click **Next** to proceed to the Options step.

Options

This step allows you to specify the runtime options and output options for executing a script. In this step you can specify the script time-out value, any additional parameters for executing the script, and the output options for the script.

To specify the runtime and output options for a script perform the following steps:

In the Script timeout field enter the script timeout value in minutes. The time out value is the amount of time required for a script to complete execution activities. If the script is not executed when the timeout value is reached, then the script is stopped by SA and a script error occurs. Select a timeout value greater than the time required for execution to complete.

In the Specify any needed parameters for this script execution field, enter any parameters if required.

In the Output Options, select Discard all script output to discard script output or else select Retain script output.

Select the output size of the script from the Size of the output to retain drop-down list.

Click **Next** to proceed to the Scheduling step.

Scheduling

This step allows you to schedule the script execution job. You can choose to run the script execution job immediately, or on a specified date and time, or on a recurring basis.

To schedule a script execution job, perform the following steps:

In the Schedule Frequency section, choose to run the script once, daily, weekly, monthly, or on a custom schedule. Select any one of the following options:

Once: Choose this option to run the job immediately or only once at a specified date and time.

Daily: Choose this option to run the job on a daily basis at a specified time.

Weekly: Choose this option to specify the day or days of the week to run the job.

Monthly: Choose this option to specify the months to run the job, and the days of the month.

Custom: In the Custom Crontab string field, enter a string the indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values.

In the Time and Duration section, for each type of schedule, specify the start time for the job. You must also specify the start date and end date for the job. The Time Zone is set according to the time zone set in your user profile.

Click **Next** to proceed to the Notifications step.

Notifications

This step allows you to set email notifications to alert users on the success or failure of a job. You can also associate a Ticket ID with the job. This setting is optional.

To set email notifications, perform the following steps:

Click **Add Notifier**.

Enter the addresses in the Email Address of Recipient field.

To send email to the address if the job succeeds, select the checkbox On Success.

To send email if the job fails, select the select the checkbox On Failure.

Enter an ID to be associated with this job in the Ticket ID field.

Click **Next** to proceed to the Job Status step.

Job Status

This step allows you to start the job, view the job progress, view the job results, view the script output for a managed server, and export the script output from all the servers.

SA supports the following file formats for exporting script output results:

- A Zip file with folders for each managed server
- A Zip file containing no folders
- Consolidated raw text file
- Consolidated formatted text file
- Consolidated CSV file

You can also view jobs in the Jobs Log window of the SA Client. See Browsing Job Logs for information about job logs.

To start a job, perform the following steps:

1. To start the job, click **Start Job**.

   If you selected Immediately in the Scheduling step, the job will begin now. If you scheduled the job for a later time, the job will run later. You can then view the job in the Jobs Log window of the SA Client.
2. The job's progress information appears in the Job Status window. You can view the server on which the script was executed, the job status, and the exit code. If the job status is displayed

as Pending Approval, then the job is blocked until it is approved by a process that is external to SA. See Browsing Job Logs for information about job logs.

3. (Optional) To view the script output from all the managed servers, select the option Show output in table. The output for each server appears in the Output column in the table.
4. (Optional) To view the output for all the servers in separate columns, select the option Show output in table and enter the delimiter character in the Delimiter checkbox. The output for each server appears in separate columns in the table.
5. (Optional) To export the script output results, click **Export All Results**. In the Browse window specify the location and the file type and click **Export**.
6. Click **Close** to exit the Run OGFS Script window.

Chapter 8 SA Global Shell

The Global Shell is a command-line interface to the Global File System (OGFS). The command-line interface is a UNIX shell such as `bash` that runs in a terminal window. The OGFS unifies the SA data model and the contents of managed servers, including files, into a single, virtual file system. You open a Global Shell session from within the SA Client or from a direct `ssh` connection in a terminal client on your desktop. With the Global Shell, you can automate repetitive system administration tasks by running scripts across multiple servers in a secure environment.

SA Global File System (OGFS)

The OGFS represents the SA data model as a hierarchical structure of file directories and text files. For example, in the OGFS, the `/opsw/Customer` directory contains details about SA customers and the `/opsw/Server` directory has information about managed servers. The `/opsw/Server` directory also contains subdirectories that reflect the contents (such as file systems and registries) of the managed servers. If you have the required permissions, in the Global Shell, you can view and even modify the file systems of managed servers.

Remote SA Shell (rosh) Utility

The Remote SA Shell (`rosh`) utility enables you to log on to managed servers 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`.

Benefits of the Global Shell

The Global Shell, OGFS, and `rosh` utility, offer the following benefits:

- **Security**: Logging on to managed servers is controlled by the Server Automation security framework.
- **Auditing**: Logins and commands on managed servers are recorded in audit log files.
- **Re-use of existing scripts**: Existing native scripts can run on managed servers with the `rosh` utility. For example, you can run .BAT, .vbs, and .sh scripts on managed servers. Scripts written in UNIX shells will run within the Global Shell, which supports `bash`, `csh`, and other common shells.
- **Routine maintenance tasks on multiple servers**: By accessing the global view of the OGFS, system administration scripts can run iteratively on groups of servers.
- **Access to the** Server Automation **data model**: Global shell scripts can access information about managed servers, including custom attributes.

Commands Available in the Global Shell

The Global Shell offers the following types of UNIX shells:

bash *(default)*

csh

ksh

sh

tcsh

Many common UNIX commands (too numerous to list here) are available within the Global Shell. To display these commands, in a Global Shell session, list (`ls`) the contents of the following directories:

/bin /usr/bin

/opsw/bin

The `/opsw/bin` directory contains utilities (such as `rosh`) which are specific to SA. For more information, see Global Shell Utilities Syntax.

Differences Between the Global Shell and UNIX Shells

The Global Shell is different from native UNIX shells in the following ways:

- **Restricted command set**: Some UNIX commands (such as `cron`) are unavailable in the Global Shell. To find out if a command is available, use the `which` command.
- **Limited recursion**: Commands cannot use recursion with the file systems of managed servers. Examples of recursive commands are `find`, `ls -r`, and `rm -r`.
- SA **user**: You log on to the Global Shell as an SA user, not as a UNIX user.
- SA **permissions**: The operations that you can perform and the servers that you can access are limited by the SA permissions of your SA user group.
- **Private directories**: The following directories are accessible only by your SA user:

/tmp
/var/tmp
/usr/tmp

  For example, the `/tmp` directory seen by the `jdoe` SA user is different than the `/tmp` seen by `tjones`.

- SA **data model in the OGFS**: Stored in the Model Repository, the data model consists of objects such as customers, facilities, and servers. End users manipulate these objects with the SA Client. The OGFS represents the data model in a file system that resembles a UNIX file system. Changes to the data model appear as changes in the OGFS, and vice versa.
- **Axis (@) symbol in directory names**: In the OGFS, for example, this symbol appears in the following directories:

/opsw/Server/@

/opsw/Server/@Group

/opsw/Group/Public/group-name/@

  The axis (@) symbol represents the end of the filtering criteria for managed servers.

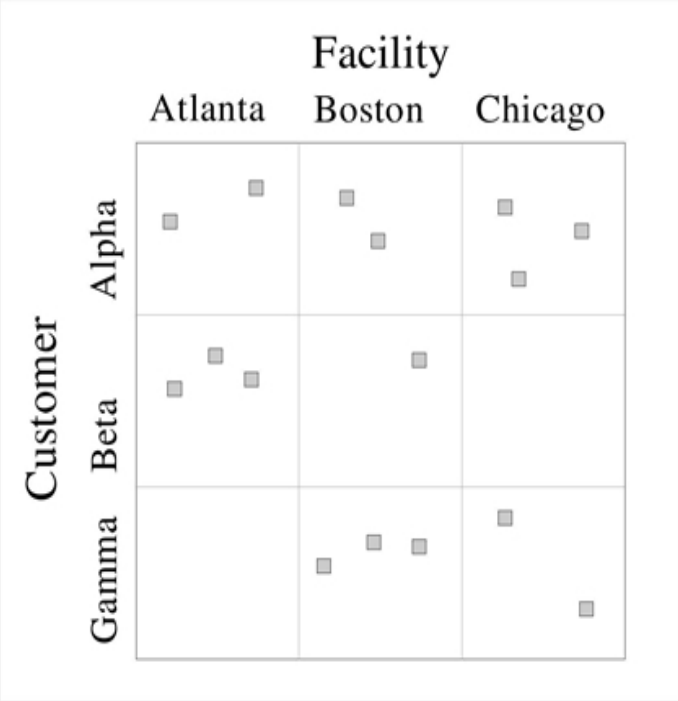
Server Filtering in the OGFS

As you navigate down the OGFS tree, the path grows longer and more specific as fewer servers are visible in the `Server` directory. In the OGFS, the `/opsw` directory contains subdirectories for several types of objects in the SA model space, such as `Server`, `Group`, `Facility`, `OS`, `Application`, `Customer`, and so on.

In the Global Shell interface, you can filter your view of these object types in the `Server` directory by specifying an axis (`@`) in the path. A path in the SA model space can be a list of filtering criteria that selects objects of a given type. This path begins with the desired object type, such as `/Server`, and each filtering criteria begins with an `@`, such as `@Customer`. An ending `@` denotes the end of the filtering criteria.

Filtering in the Server Directory is graphical representation of related objects (customers and facilities) in a hierarchical `Server` directory. The small boxes represent managed servers. Examples of ways that you can filter this directory immediately follow the diagram.

Filtering in the Server Directory



Based on Filtering in the Server Directory , the following examples illustrate ways to narrow your search for servers:

- To find all 16 servers, specify the following path:

ls /opsw/Server/@

- To find servers in the Atlanta facility, specify the following path:

ls /opsw/Server/@Facility/Atlanta/@

- To find servers that belong to customer Alpha, specify the following path:

$ ls /opsw/Server/@Customer/Alpha/@

- To find servers in the Atlanta facility that belong to customer Alpha, specify either of the following paths:

ls /opsw/Server/@Facility/Atlanta/@Customer/Alpha/@

ls /opsw/Server/@Customer/Alpha/@Facility/Atlanta/@

The following paths are filtered away by the OGFS, because they would yield a dead-end. There are no servers belonging to customer Gamma in the Atlanta facility.

ls /opsw/Server/@Facility/Atlanta/@Customer/Gamma/@

ls /opsw/Server/@Customer/Gamma/@Facility/Atlanta/@

Note: This same filtering logic can be applied to `@Realm`, `@Group`, and `@Application`.

Global Shell Tutorial

This tutorial covers just a few of the highlights of the OGFS and the Global Shell. After completing this tutorial, you will know how to navigate the directories of the OGFS and how to run commands on managed servers from within the Global Shell. Although the tutorial is organized into steps, after performing step 1, you can perform the remaining steps in any order.

Before starting the tutorial, you need the following capabilities:

- You can log on to the SA Client. As you work through this tutorial, you might find it helpful to compare the stdout of the Global Shell with information displayed by the SA Client.
- Your SA user has Read & Write permissions on at least one managed server. Typically assigned by a security administrator, permissions are discussed in the SA Administration Guide.
- Your SA user has all Global Shell permissions on the same managed server. For information on these permissions, see aaa Utility.

The example commands in this tutorial operate on a Windows server named `abc.opsware.com`. This server belongs to a device group named All Windows Servers. When trying out these commands, substitute `abc.opsware.com` with the host name of the managed server you have permission to access. Also, replace `jdoe` with your SA user name. If you wish to run the commands on a UNIX managed server, replace `ipconfig` with `ifconfig`; and replace `Administrator` with `root`.

Now, let's get started with the tutorial:

1. Open a Global Shell session.

   You can open a Global Shell session from within the SA Client. From the **Tools** menu, select **Global Shell**. You can also open a Global Shell session from a terminal client running on your desk top. For instructions, see Opening a Global Shell Session.

2. Check your session.

   First, enter the `whoami` command, which displays the SA user name for this session:

$ **whoami**

jdoe

You can enter the ps command to view the process status of your Global Shell session. The following `ps` command shows the session is running the default `bash` shell:

$ **ps**

PID TTY TIME CMD

7033 ? 00:00:00 bash

13712 ? 00:00:00 ps

Enter the `uname` command, which displays information about the server running the OGFS component of SA:

$ **uname -a**

Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15 21:17:59 EDT 20 05 i686 GNU/Linux

If you log on to a UNIX managed server with `rosh`, `uname` displays information about that managed server, not the server running the OGFS component. Run the `uname` command when you are not sure if you are interacting with the Global Shell or with the shell of a managed server accessed with `rosh`.

3 Confirm your home directory.

Every SA user has a home directory in the OGFS. The home directory has a `public/bin` subdirectory where you can store scripts to be executed by other users running Global Shell sessions. Each SA user also has a personal `/tmp` directory for temporary files. You cannot view or modify the `/tmp` directories of other users.

The following commands show some information about the directories of the `jdoe` user:

$ **cd**

$ **pwd**

/home/jdoe

$ **ls -ld /home/jdoe/public/bin**

drwxr-xr-x 2 jdoe jdoe 4096 2006-05-17 17:12 /home/jdoe/

public/bin

$ **ls -ld /tmp**

drwxrwxrwx 3 root root 4096 2006-06-09 23:37 /tmp

4 List all managed servers.

The `/opsw/Server` directory of the OGFS contains information about the servers managed by SA. This directory is an example of how the OGFS represents objects (in this case servers) of the SAdata model. Behind the scenes, SA stores this information in a database referred to as the Model Repository.

To view the names of the servers managed by SA, enter the following command:

$ **ls /opsw/Server/@**

abc.ospware.com m33.opsware.com gist.opsware.com pal.opsware.com hare.opsware.-com qv55.opsware.com

. . .

5 Examine server information.

Each managed server has a directory structure containing information about that server. The `attr` subdirectory contains text files that describe the server's attributes. The attribute name matches the file name and the attribute value is the file contents. The following `cat` command lists the OS version of the managed server named `abc.opsware.com`:

$ **cd /opsw/Server/@/abc.opsware.com**

$ **cat attr/osVersion**

Microsoft Windows 2000 Advanced Server Service Pack 4 Build 2195 (05-02-2006

The `Interface` subdirectory has information about the server's network interfaces. Here's an example:

$ **cat "Interface/Local Area Connection/info"**

AdminEnabledFlg: no

CardIndex:

CardSerialNum:

CircuitId:

Collisions:

ConfiguredDuplex: AUTO

ConfiguredSpeed: AUTO

. . .

6 List the files of a managed server.

In addition to information about managed servers, `/opsw/Server` contains directories that correspond to the file systems of those servers. If you have the necessary permissions, in a Global Shell session you can access multiple servers from a single virtual file system, the OGFS.

The following command navigates to file system of the `abc.opsware.com` server:

$ **cd /opsw/Server/@/abc.opsware.com/files**

The next `ls` command displays OGFS subdirectories that correspond to native users of the managed server. Your security administrator specified these users (login names) when adding OGFS permissions. These are not SA users.

$ **ls**

Administrator LocalSystem

Native users might have different views of the managed server's file system. Therefore, under each user, the OGFS presents different file systems for each user. The following `cd` command

drills down to the `Program Files` directory as seen by the `Administrator` user on the Windows server.

$ **cd "Administrator/C/Program Files"**

$ **pwd**

/opsw/Server/@/abc.opsware.com/files/Administrator/C/Program Files

Next, list the files in the `Program Files` directory:

$ **ls -1**

Accessories

Common Files

ComPlus Applications

Internet Explorer

Messenger

. . .

Although these files reside in a directory on the managed server's file system, you are in the OGFS, as shown by the preceding `pwd` command. To verify that you are in a Global Shell session (and not in a session running on the managed server), enter the following commands:

$ **whoami jdoe**

$ **uname -a**

Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15 21:17:59 EDT 2005 i686 GNU/Linux

7 Copy a file from the OGFS to a managed server.

By entering the `cd` command, go to your home directory in the OGFS, for example:

$ **cd**

$ **pwd**

/home/jdoe

Next, create a simple text file in your home directory:

$ **echo "this is text" > myfile.txt**

$ **cat myfile.txt**

this is text

Copy the file that you just created to a directory in the file system of a managed server. The following command copies `myfile.txt` to the `C:\temp` directory of the `abc.opsware.com` server:

$ **cp myfile.txt **

/opsw/Server/@/abc.opsware.com

/files/Administrator/C/temp/afile.txt

Do not copy large files between the OGFS and managed servers. Copy only small files, such as configuration files.

8 Log on to a managed server with `rosh`.

In the preceding steps, you accessed the file system of a managed server from within a Global Shell session. In this step, from the Global Shell you log on to a managed server with `rosh`. After you log in, you interact with the command-line environment (MSDOS or UNIX shell) of the managed server.

The following `rosh` command logs in as Administrator to a Windows managed server named `abc.opwsare.com`:

$ **cd /opsw/Server/@/abc.opsware.com**

$ **rosh -l Administrator**

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

The prompt indicates that you are now in the command-line environment of the managed server. Enter the `ipconfig` and `hostname` commands:

C:\WINNT\system32>**ipconfig**

ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : opsware.com

IP Address. . . . . : 192.168.8.217

Subnet Mask . . . . . : 255.255.254.0

Default Gateway . . . . . : 192.168.8.1

C:\WINNT\system32>**hostname**

hostname

abc

Terminate the remote login with the `exit` command:

C:\WINNT\system32>**exit**

Enter the `uname` command to verify that you have returned to the Global Shell session:

$ **uname -a**

Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15 21:17:59 EDT 2005 i686 GNU/Linux

9 Create a script that runs across servers.

A Global Shell script can iterate within the OGFS and run the `rosh` command to execute native commands on multiple servers. The example script shown in this step iterates through the servers of the public device group named All Windows Servers. On each server, the script runs the `ipconfig` command with the `rosh` command. In this example, substitute your SA user name for `jdoe`.

First, return to your home directory in the OGFS:

$ **cd**

$ **cd public/bin**

$ **pwd**

/home/jdoe/public/bin

Next, run the `vi` editor:

$ **vi**

In `vi`, insert the following lines to create a `bash` script:

```
#!/bin/bash
# This is simple_iterate.sh.
# Change jdoe to your user name.

OUTFILE="/home/jdoe/public/bin/ipconfig_all.txt"
rm -f $OUTFILE

cd "/opsw/Group/Public/All Windows Servers/@/Server"

for SERVER_NAME in *
do
 echo ---- $SERVER_NAME
 echo ---- $SERVER_NAME >> $OUTFILE
 rosh -n $SERVER_NAME -l Administrator \
        "ipconfig" >> $OUTFILE
done
# Last line in simple_iterate.sh.
```

Save the file in `vi`, naming it `simple_iterate.sh`. Quit `vi`.

Change the permissions of `simple_iterate.sh` with `chmod`, and then run it:

$ **chmod 755 simple_iterate.sh**

$ **./simple_iterate.sh**

---- abc.ospware.com

---- gist.opsware.com

---- hare.opsware.com

---- m33.opsware.com

. . .

As the script runs, it echoes the name of each server to `stdout`, and redirects the output of the `ipconfig` command to the `ipconfig_all.txt` file. Enter the `more` command to view the contents of `ipconfig_all.txt`:

$ **more ipconfig_all.txt**

---- abc.ospware.com

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection: . . .

10 Learn more.

Here are a few suggested tasks for learning more about the OGFS and the Global Shell:

- Explore the folders and contents under `/opsw/Library`, comparing them with the Library windows of the SA Client.
- If you have NA installed, navigate to the `/opsw/Net*` (network) directories. For descriptions of these directories, see Network Directories.
- On Windows servers, examine the `registry` and `complus` directories under `/opsw/Server/@/`*server-name*.
- List the files in the `method` directory, also under `/opsw/Server/@/`*server-name*. These files are the executables of the SA Command-Line Interface (OCLI), which enables you to perform SA functions from within the Global Shell. To learn how to run the CLI methods, see the SA Platform Developer Guide.

Global Shell Examples

The examples in this section use `bash`, the default shell of a Global Shell session. These are relatively simple examples. For more complex examples, including those with method invocations and search filters, see the SA Platform Developer Guide.

Opening a Global Shell Session

You can open a Global Shell session with an `ssh` client or from within the SA Client. When you open a session, the working directory is `/home/`*user-name*.

To open a Global Shell session with an `ssh` client, perform the following steps:

1 On a host that is not an SA core server or a managed server, open a terminal window.

2 In the terminal window, enter an `ssh` command with the following syntax:

ssh -p 2222 *user-name*@*ogfs-host*

To use this command, port 2222 must be open on the firewall that protects the OGFS server. The *user-name* is your SA user (login) and the *ogfs-host* is the host name (or IP address) of the core server running the OGFS. The SA user name is not case sensitive. After you enter the `ssh` command, the OGFS prompts for the password of the SA user.

To open a Global Shell session from within the SA Client, from the **Actions** menu, select **Global Shell**.

Finding Servers in the OGFS

List the names of all servers that you can manage with SA:

ls /opsw/Server/@

List the IDs of the servers:

ls -a /opsw/.Server.ID

Find all servers in the `.opsware.com` domain by specifying the wildcard character (*):

ls -d /opsw/Server/@/*.opsware.com

List all servers in the Atlanta facility:

ls /opsw/Server/@Facility/Atlanta/@

List the servers in the public device group named Alpha:

ls /opsw/Group/Public/Alpha/@/Server

List the servers in the All Windows Servers group, first with backlashes to escape the spaces in the group name, then by enclosing the option in single quotes:

ls /opsw/Group/Public/All\ Windows\ Servers/@/Server

ls '/opsw/Group/Public/All Windows Servers/@/Server'

List the servers of the Widget customer:

ls /opsw/Customer/Widget@/Server

The following two commands display the same output, the servers in the Atlanta facility that belong to the Green customer:

ls /opsw/Server/@Facility/Atlanta/@Customer/Green/@

ls /opsw/Server/@Customer/Green/@Facility/Atlanta/@

Getting Server Information from the OGFS

List the Object ID and of the server named `m256.opsware.com`:

cd /opsw/Server/@/m256.opsware.com

cat self:i ; echo

(The preceding `echo` command is optional. It generates a new line character, which makes the output easier to read. The semicolon separates `bash` statements entered on the same line.)

List the name of the server with an Object ID of `340039`:

cat /opsw/.Server.ID/340039/self

By iterating through the server names with a `for` loop in `bash`, display the platform (operating system) name for each server:

```
cd /opsw/Server/@
for SERVER_NAME in *
do
  cat $SERVER_NAME/attr/platform
done
```

Display the amount of RAM in the server named `abc.opsware.com`:

```
cd /opsw/Server/@/abc.opsware.com
grep Quantity Memory/RAM/info
```

Display the network interfaces of a the server named `blizzard.opsware.com`:

```
cd /opsw/Server/@/glengarriff.snv1.dev.opsware.com/Interface
for INTERFACE_NAME in *
do
echo ..... $INTERFACE_NAME .....
grep Interface "$INTERFACE_NAME/info"
echo ""
done
```

Browsing a Server's File System or Registry

List all of the files the `C:\ Program Files` directory of the Windows server named `abc.opsware.com`:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
ls C/Program\ Files
```

List the registry keys of the `abc.opsware.com` server:

```
cd /opsw/Server/@/abc.opsware.com/registry/\ Administrator/
ls *
```

List the contents of the `/var` directory on the UNIX server named `m256.opsware.com`:

```
/opsw/Server/@/m256.opsware.com/files/root
```

ls var

Managing Custom Attributes

On the server `abc.opsware.com`, create a custom attribute named `MyGreeting` with the value `hello there`:

cd /opsw/Server/@/abc.opsware.com/CustAttr

echo -n "hello there" > MyGreeting

cat MyGreeting

Execute `runit.bat` on the `abc.opsware.com` server, passing the value of the `My Test` custom attribute as a command-line parameter for `runit.bat`:

cd /opsw/Server/@/abc.opsware.com

TESTPARAM=`cat CustAttr/"My Test"`

rosh -l Administrator "C:\temp\runit.bat $TESTPARAM"

When you create or edit custom attributes within the OGFS, Server Automation preserves leading and trailing white space characters in custom attribute values.

Copying Files Within the OGFS

Do not use the techniques in this section to copy large files. The OGFS is not designed distribute large amounts of data. However, you can use these techniques for copying small files (such as configuration files) to and from managed servers.

Copy `myfile.txt` from the home directory in the OGFS of the `jdoe` user to the `C:\temp` directory of the Windows server named `abc.opsware.com`:

cp /home/jdoe/myfile.txt \

/opsw/Server/@/abc.opsware.com/files/Administrator/C/temp

Copy `myfile.txt` from the home directory in the OGFS of the `jdoe` user to the `/tmp` directory of the UNIX server named `m25.opsware.com6`:

cp /home/jdoe/myfile.txt \

/opsw/Server/@/m256.opsware.com/files/root/tmp

Copy the `C:\temp\myfile.txt` file from the `abc.opsware.com` server to the `m344.opsware.com` server:

cp /opsw/Server/@/abc.opsware.com/files/\

Administrator/C/temp/myfile.txt \

/opsw/Server/@/m344.opsware.com/files/\

Administrator/C/temp/myfile.txt

Copying Files Between the OGFS and a Development Server

You can securely copy files between the OGFS and a server that is not part of Server Automation. To copy the files, perform the following steps:

1. On a host that is not an SA core server or a managed server, open a terminal window.
2. In the terminal window, enter either the `scp`, `sftp`, or `rsync` command and specify port 2222, your SA user name, and the host running the OGFS.

The following three `scp` examples perform the same operation: They copy the file `myscript.sh` from the local machine to the file `/home/jdoe/myscript.sh` in the OGFS. The SA user is `jdoe` and the host running the OGFS is 192.168.166.178.

scp -P 2222 myscript.sh jdoe@192.168.166.178:myscript.sh

scp -P 2222 myscript.sh jdoe@192.168.166.178:/home/jdoe

scp -P 2222 myscript.sh jdoe@192.168.166.178:

The following example copies `myscript.sh` from the home directory of `jdoe` in the OGFS to the local machine:

scp -P 2222 jdoe@192.168.166.178:myscript.sh myscript.sh

The following `sftp` example copies `myscript.sh` from the local machine to the OGFS:

sftp -oPort=2222 jdoe@192.168.166.178

Connecting to 192.168.166.178...

Global Shell

jdoe@opsware's password:

sftp> put myscript.sh

. . . .

The following `rsync` example transfers files from `/path` on the local machine to `/other/path` in the OGFS:

rsync -av -e "ssh -p 2222" /path \
jdoe@192.168.166.178:/other/path

Logging on to a Managed Server With rosh

The next three `rosh` commands perform the same operation: logging on to the Windows server named `abc.opsware.com` as the `Administrator` user. After logging on, the current working directory on the remote shell is the default working directory of the Administrator Windows user. These `rosh` commands require different options, depending on the current working directory in the OGFS. For example, the first `rosh` command does not require the `-n` (server name) and `-l` (user) options because the option values can be inferred from the current working

directory of OGFS. The options of the following three `rosh` commands differ because of the current working directory:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
rosh
. . .
exit
. . .
cd /opsw/Server/@/abc.opsware.com
rosh -l Administrator
...
exit
. . .
cd /home/jdoe
rosh -n abc.opsware.com -l Administrator
...
exit
```

The next `rosh` command logs into the UNIX server named `m256.opsware.com` as the `root` user with the current working directory of `/tmp`:

```
rosh -n m256.opsware.com -l root -d /tmp
```

Running OGFS Scripts on Managed Servers With rosh

The next sequence of commands create a .BAT script in the OGFS and then run the script on a Windows managed server. Created with `echo` statements, the `myfile.bat` script resides in the OGFS under `/home/jdoe/public/bin`. (Note that `myfile.bat` does not reside in the file system of the managed server.) The `myfile.bat` script contains three commands: `ipconfig`, `cd`, and `dir`. The `rosh` command runs `myfile.bat` on the server named `abc.opsware.com` as the `Administrator` Windows user. The following commands create a local .BAT script and run it remotely with `rosh`:

```
cd /home/jdoe/public/bin

echo ipconfig > myfile.bat
echo "cd c:\temp" >> myfile.bat
echo dir >> myfile.bat

rosh -n abc.opsware.com -l Administrator -s ./myfile.bat
```

Create a script named `who.sh` in the `/home/jdoe/public/bin` directory of the OGFS and then run `who.sh` on the server named `m256.opsware.com`:

```
cd /home/jdoe/public/bin

echo \#\!\/bin\/sh > who.sh
echo "uname -n" >> who.sh
echo id >> who.sh
echo pwd >> who.sh

rosh -n m256.opsware.com -l root -s ./who.sh
```

Running Native Programs on Managed Servers With rosh

The next two `rosh` commands run the `dir` and `ipconfig` MSDOS commands on the Windows server named `abc.opsware.com`. Note that the native MSDOS commands are enclosed in quotes. Because the server name and user (login) can be inferred from the current working directory, the first `rosh` command omits the `-n` and `-l` options, as shown in the following code:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
rosh "dir & ipconfig"
. . .
cd /home/jdoe
rosh -n abc.opsware.com -l Administrator "dir & ipconfig"
```

Run the `ipconfig` command on `abc.opsware.com` and redirect the output to a file in home directory of `jdoe` in the OGFS:

```
rosh -n abc.opsware.com -l Administrator "ipconfig" \
> /home/jdoe/ipconfig_ouptput.txt
```

On the UNIX server named `m256.opsware.com`, run the `uname` and `ls` commands as `root`:

```
rosh -n m256.opsware.com -l root "uname -a; ls /tmp"
```

Within a `for` loop in `bash`, run the MSDOS `ipconfig` command on each server in the All Windows device group:

```
cd /opsw/Group/Public/All\ Windows\ Servers/@/Server

for SERVER_NAME in *
do
echo ..... $SERVER_NAME .....
```

```
rosh -n $SERVER_NAME -l Administrator "ipconfig"

echo ""

done
```

Character Encoding for the OGFS

To support international environments, the OGFS can display information in different character encodings such as Shift-JIS (Japanese) and EUC-KR (Korean). You can control the encoding of Global Sessions in the following ways:

- To specify the encoding of your Global Shell sessions, in the Terminal and Shell Preferences of the SA Client, select an item from the Encoding drop-down list.
- To change the encoding of an active Global Shell session, run the `swenc` command with the `-e` option.

If you change the encoding of an active session, you must also change the encoding of the terminal application for that session. This procedure varies according to the terminal application.

Terminal Application Configuration

The terminal application that is hosting a Global Shell or Remote Terminal session must be configured to use the same encoding expected by the session. If the encodings do not match, the data might be displayed incorrectly.

When the SA Client launches the terminal application, it composes the command specified by the Terminal Client field in the Terminal and Shell Preferences. If the Terminal Client field includes the `%e` substitution variable, the SA Client replaces `%e` with an encoding name. For Global Shell sessions, this encoding name is specified by the Encoding field of the Terminal and Shell Preferences. For Remote Terminal sessions, this encoding name is the value of the Encoding field in the Properties section of the Device Explorer. If the terminal application does not support the encoding that replaces the `%e` variable, or if the `%e` variable is not specified, you must change the encoding manually in the terminal application after it starts.

Data that Cannot Be Displayed

Data that cannot be displayed might be from a managed server (such as the contents of files) or it might be the name of an object in the SA model. If the session's encoding does not support the data to be displayed, the data often appears as question marks. (However, it might appear as other characters such as exclamation points.) The session attempts to display this data with the current encoding. Usually, this data cannot be accessed. To access this data, select a compatible encoding for the session.

Objects in the SA model, such as Facility and Server, appear as file names in the OGFS. If these file names contain characters that cannot be represented by the encoding of the session, they are displayed as question marks, appended by the Object ID of the object. In the following example, the IDs are 10002 and 11002:

New York

Paris

Montr?al~10002

??~11002

If the model object does not have an ID, such as a custom attribute, then the session attempts to display the name with the current encoding.

LANG and LC_CTYPE Environment Variables

Many UNIX commands (such as `ls`) rely on the character encoding, which is determined by the `LANG` or `LC_CTYPE` environment variables. In a Global Session, if the encoding is changed with the `swenc` command, the system attempts to reset these variables.

Server Automation determines the new value of the `LANG` variable with the following process:

1. The value of `LANG` is generated by combining the language of the user's profile in the SA Client with the current session encoding. For example, if the language is English and the session encoding is UTF-8, `LANG` is set to en_US.utf8.
2. The value determined by the preceding step is compared with the set of valid locales on the OGFS server (according to the output of `locale -a`). If the value is a valid locale, `LANG` is set to this value.
3. If the value is not a valid locale, the system attempts to find a valid locale that specifies the user's language without the encoding. For example, if the user's language is English and the session encoding is EUC-JP, and this combination does not form a valid locale, `LANG` is set to en_US. If no matching locale is found, `LANG` is left unspecified.

The new value of the `LC_CTYPE` variable is determined in the following order:

1. Server Automation attempts to find a valid locale that matches the session encoding, regardless of the language.
2. If a valid locale is found, `LC_CTYPE` is set to this locale. For example, if the session encoding is EUC-JP, the `LC_CTYPE` variable is set to ja_JP.eucjp.
3. If no matching locale is found, `LC_CTYPE` is left unspecified.
4. If Server Automation cannot set the `LANG` or `LC_CTYPE` variables with the preceding process, you should set them manually.

Transcoded Data in a Managed Server

Transcoding is the conversion of data from one character encoding to another. Server Automation automatically transcodes some of the data between Global Shell sessions and other sources of data. For example, the file names of managed servers are transcoded, but the contents of the files are not. To see which data is transcoded, see Data Transcoded for Global Shell Sessions. To display the transcoding mode of the current Global Shell session, enter the `swenc` command with no options.

Table: Data Transcoded for Global Shell Sessions

Data	Transcoding
Objects in the SA model space, such as `Facility`, `Customer`, and `Server`. These objects are stored in the SA Model Repository (database) in UTF-8.	Between UTF-8 and the session encoding.
File and directory names of managed servers.	Between the managed server encoding and the session encoding.
Metadata of managed servers, such as user names and registry key names.	Between the managed server encoding and the session encoding.
File contents of managed servers.	None
Contents of Windows registries, services, COM objects, and IIS metabases.	None
`rosh`: Contents of saved scripts executed on managed servers (a `rosh` push operation).	None
`rosh`: Ad-hoc scripts executed on managed servers.	None
`rosh`: Command-line arguments to programs executed on managed servers.	None
`rosh`: Data streams (such as stdin and stdout) of programs executed on managed servers.	None
`rosh`: Data streams of `rosh` jump operations.	None
OGFS `home`, `tmp`, and `var/tmp` directories.	None

Disabling the Transcoding of Managed Server Data

On UNIX servers, file and directory names can contain characters in arbitrary encodings. When accessed through the OGFS, file and directory names are transcoded by Server Automation. If the encoding of the names does not match the default encoding of the managed server, the transcoded data might be unusable.

You can disable transcoding with the `swenc` command. To turn transcoding on or off, use the `–T` option:

swenc -T {on | off}

If transcoding is disabled, file and directory names are passed unmodified from the managed servers. Therefore, you must manually configure the encoding of the terminal application to display the names correctly.

Windows servers store their file system data internally in the UTF-16 encoding. Because the encoding is known, transcoding is performed correctly and does not need to be disabled. There-

fore, the `-T` option of the `swenc` command has no effect on Windows servers. For more information, see swenc Syntax.

Global Shell Error Messages

The Global Shell feature provides the file system error messages that are described in Global Shell Errors.

Table: Global Shell Errors

Error	Description	Action
Input/output error	Your session has exceeded the time-out limit or the Agent is not running.	Start a new session or check the status of the Agent.
Operation not permitted.	No password was found.	Verify that you have a valid password.
Permission denied.	You are not allowed to view a directory. This does not mean that the directory does not exist on a given server. See the SA Administration Guide for more information.	Verify that you have `readFileSystem` permissions.
RFS Specific error	You do not have permissions on the managed server. For example, this error will occur if you are trying to perform an operation on a managed server and you do not belong to the Administrators group that has the required permissions assigned to it.	You must have a set of permissions to perform operations on managed servers. To obtain these permissions, contact your SA administrator. See the SA Administration Guide for more information.

Remote Terminal

With Server Automation, you can log on to a managed server in a terminal window in two ways:

- Using the Remote Terminal, as described here.
- The `rosh` command entered in a Global Shell session.

The remote terminal opens a terminal window for UNIX servers or an RDP client window for Windows servers. Unlike a Global Shell session, a remote terminal session does not provide access to the OGFS.

You can specify your terminal and RDP client preferences for remote terminal and Global Shell sessions in the Set Preferences window. See Terminal and Shell Options for more information.

Prerequisite for a Remote Terminal

Logging into a remote server requires that you have SA login permissions on the managed server. See the SA Administration Guide for more information. You cannot log into a remote terminal with a user name or password that contains multi-byte characters.

To open a remote terminal session on a Windows managed server running Windows Firewall, you must set an exception that is not enabled by default. On the managed server, run Windows Security Center, then select Windows Firewall > Exceptions > Remote Desktop.

This feature must be able to establish a loopback connection on the machine running the SA Client. Some firewall and VPN utilities have settings that prevent loopback connections.

Opening a Remote Terminal

In the Device Explorer of the SA Client, perform the following steps:

1. Select a managed server.
2. Open the managed server.
3. From the **Actions** menu, select **Remote Terminal**.

Chapter 9

SA Command Line Interface (OCLI)

Overview of OCLI

The SA Command Line Interface (OCLI) consists of two tools:

- `oupload` – Uploads files into the Software Repository
- `odownload` – Downloads files from the Software Repository

These commands help to automate the setup tasks for package management in Server Automation. For a list of supported package types, see the SA User Guide: Software Management.

OCLI runs on a server managed by SA. The operating system of this server can be one of the following: Oracle Sun Solaris, Linux, IBM AIX, HP-UX, and Microsoft Windows.

Upload Verification

After you upload a package with OCLI, verify that the upload has been successful by locating the package with the SA Client. Typically, you add the uploaded package to a folder or a policy.

Encoding Options for OCLI

The `oupload` and `odownload` commands include options for specifying the encoding scheme of packages or customer display names. These options are required only when you want to override the default setting in the LANG environment variable of your shell.

RPM Uploads

For RPM packages, always remember to upload the source files after uploading a package. Uploading the source files is important from a maintenance perspective because it allows users to modify packages at a later date.

Passwords and Environment Variables

The `oupload` and `odownload` commands prompt for the SA user name and password when needed. Alternatively, you can set the `ISMTOOLUSERNAME` and `ISMTOOLPASSWORD` environment variables.

The 'ocli.conf' configuration file located at the root of the OCLI installation can be edited to set a OCLI username and password for connecting to SA. If you provide username and password in the

ocli.conf file, then the password will be encrypted in the file after the first run of the `ouplo ad` or `odownload` command.

Upload Examples

To upload `mytoolkit.rpm` into the `/Kit Apps/Services` folder, enter the following command on a single line:

$ oupload --pkgtype RPM --os "Red Hat Enterprise Linux AS 3"
--folder "/Kit Apps/Services" mytoolkit.rpm

To upload `iPlanet_Web_Server-4.1sp19-LC~0.sparc64.rpm` for the customer Opsware and the operating system Solaris 5.11, enter the following command on a single line:

```
$ <installation_directory>/bin/oupload --pkgtype RPM --old --
customer Opsware
--os "SunOS 5.11" iPlanet_Web_Server-4.1sp19-LC~0.sparc64.rpm
```

Be sure to enclose values containing spaces, such as `SunOS 5.11`, in quotes.

Installing the SA Command-line Interface (OCLI)

The SA Command-line Interface (OCLI) is shipped as a zip file in the SA Software Repository. You can install and use the OCLI on Windows and Unix machines.

After you install OCLI, you can use the new `oupload` and `odownload` commands available to move software between a managed server and the Software Repository.

Note: You must install an SA Agent and OCLI on the host on which you will run OCLI.

Installing OCLI

Verify that you have the required permissions and install a Server Agent on the managed server where you will run OCLI.

1. Log into the SA Client and search for the software policy "Ocli" and open it.
2. Go to the "Server Usage" tab and select Actions > Attach Server.
3. Select the servers on which you want to run OCLI.
4. Ensure that the Remediate Servers Immediately check box is selected.
5. Click "Attach".

Running OCLI

Unix

For the shells csh, tcsh, and similar variants, enter the following command:

```
source <installation_directory>/ocli/login.csh
```

For the shells sh, bash, ksh, and similar variants, enter the following command at the command line:

```
source <installation_directory>/ocli/login.sh
```

Note: You may also use some embedded sh scripts directly by running:

```
<installation_directory>/ocli/bin/oupload.sh

<installation_directory>/ocli/bin/odownload.sh
```

Windows

1. Log in to the managed server
2. Launch a command window and enter the following command at the prompt:

   ```
   set PATH=%PATH%;<installation.dir>\ocli\scripts
   ```
3. In the command window, enter the following command on a single line:

   ```
   set PATH=%PATH%;%SYSTEMDRIVE%\Program Files\Opsware\HPSApython
   ```

OCLI Command Syntax

The `oupload` and `odownload` commands have the following syntax. The *filenames* and *localpath* can contain a relative or absolute local file or directory path. If an option value contains spaces, enclose the value in quotes.

`oupload [`*options*`]` *filenames*

`odownload [`*options*`]` *filenames localpath*

Note: When using the SA Command-line Interface (OCLI) on a UNIX server, the `oupload` and `odownload` scripts are invoked from the `/bin` directory:

```
<ocli_installation_directory>/bin/oupload.sh
<ocli_installation_directory>/bin/odownload.sh
```

Options Common to oupload and odownload

Table: Options Common to Both Commands

Arguments	Values	Description
`--customer (-C) <value>`	String (customer name, wildcards accepted) or integer (customer ID)	Specifies the customer of the file. Do not use the `--customer option` with the `--folder option`. To use `--customer`, the `--old option` is also required. If you specify `--old`, specifying `--customer` is required unless you are using `--patchtype in` oupload. When you upload an AIX LPP file, or an HP-UX Depot that contains patches, it is associated with "Customer Independent" and this option is ignored. When you upload an AIX Maintenance Level set of LPPs, you must associate them with "Customer Independent" so that all base filesets and update filesets contained in it are associated with the same customer
`--feedback (-Q)`	N/A	Displays feedback while the command runs. By default, this option is enabled. Cannot specify this option with `–q`
`--forcenooverwrite`	N/A	This option prevents like files from being overwritten. When used for oupload, if the file already exists in SA, the upload operation will be cancelled and the file will not be overwritten. When used for odownload, if the file already exists locally, the download operation will be cancelled and the file will not be overwritten. In both cases, no input is required.

Arguments	Values	Description
		Note: If there are multiple files for upload/download and the for-cenooverwrite option is given, the files that already exist will be skipped. the operation itself will not be can-celed.
`--forceoverwrite`	N/A	This option forces like files to be overwritten. When used for oupload, if the file already exists in SA, it will be overwritten by the file being uploaded. When used for odownload, if the file already exists locally, it will be overwritten by the file being downloaded. In both cases, no input is required.
`--fr (-f) <value>`	• Alphanumeric • Period • Hyphen • Default = theword	Specifies the host name or IP address of the Software Repository.
`--frport (-F) <port>`	Integer Default = 1003	Specifies the port of the Software Repository.
`--fullhelp (-H)`	N/A	Displays full help information. Cannot specify this option with `-h` or `–V`
`--help (-h)`	N/A	Displays abbreviated help information. Cannot specify this option with `-H` or `–V`
`--nofeedback (-q)`	N/A	Does not display feedback while the command runs. Cannot specify this option with `–Q`
`--old (-o)`	N/A	Specifies that the operation behaves as in Server Automation 5.x. The file is not uploaded into a folder. The `--old` option is required if you specify `--`

Arguments	Values	Description
		`customer`. Using this option will make use of the agent certificates, and the user will not be prompted for any password
`--os (-O) <type>`	String (OS name, wildcards accepted) Valid Strings and Integer Values for the --os Option	Specifies the operating system of the package. Specifying this option is required. If a value has a space in the name, enclose the entire name in quotes. For Fujitsu Solaris 2.8, use the value for Solaris 8. For Fujitsu Solaris 2.9, use the value for Solaris 9.
`--timeout (-z) <value>`	Integer Default = 60	Sets the timeout to the server in seconds.
`--truthgw (-g) <value>`	• Alphanumeric • Period • Hyphen • Default = spin	Specifies the host name or IP address of the Data Access Engine.
`--truthgwport (-G) <port>`	Integer Default = 1004	Specifies the port of the Data Access Engine.
`--verbose (-v)`	N/A	Displays debug information.
`--version (-V)`	N/A	Displays version information for the OCLI. Cannot specify this option with `-h` or `–H`.

Valid Strings and Integer Values for the --os Option

Note: Use either the '-O' or the '--os' option when specifying the platform id or string. For example:

```
--os <string>
-O <integer>
```

Table: Allowable OS Name Strings and Integer Values for --os Option

OS Name (String)	Internal ID (Integer)
AIX 6.1	120076
AIX 7.1	120077
CentOS 5	20076
CentOS 5 X86_64	50076
CentOS 6	50200
CentOS 6 X86_64	50201
CentOS 7 X86_64	50202
Citrix XenServer 5	100035
Citrix XenServer 6	100036
HP-UX 11.11	1080007
HP-UX 11.23	40774
HP-UX 11.31	40039
Oracle Enterprise Linux 5	180076
Oracle Enterprise Linux 5 X86_64	190076
Oracle Linux 6	180077
Oracle Linux 6 X86_64	190077
Oracle Linux 7 X86_64	170098
Red Hat Enterprise Linux Client 6	170095
Red Hat Enterprise Linux Client 6 X86_64	170096
Red Hat Enterprise Linux Desktop 5	20056

OS Name (String)	Internal ID (Integer)
Red Hat Enterprise Linux Desktop 5 X86_64	30056
Red Hat Enterprise Linux Server 5	10028
Red Hat Enterprise Linux Server 5 IA64	140076
Red Hat Enterprise Linux Server 5 PPC64	230076
Red Hat Enterprise Linux Server 5 S390X	230078
Red Hat Enterprise Linux Server 5 X86_64	20028
Red Hat Enterprise Linux Server 6	10029
Red Hat Enterprise Linux Server 6 PPC64	70029
Red Hat Enterprise Linux Server 6 S390X	80029
Red Hat Enterprise Linux Server 6 X86_64	60029
Red Hat Enterprise Linux Server 7 X86_64	61100
Red Hat Enterprise Linux Workstation 6	170094
Red Hat Enterprise Linux Workstation 6 X86_64	170093
SunOS 5.10	30007
SunOS 5.10 X86	10044
SunOS 5.11	427453
SunOS 5.11 X86	427452
SuSE Linux Enterprise Server 10	20100
SuSE Linux Enterprise Server 10 PPC64	90200
SuSE Linux Enterprise Server 10 S390X	90600
SuSE Linux Enterprise Server 10 X86_64	70100
SuSE Linux Enterprise Server 11	80100
SuSE Linux Enterprise Server 11 PPC64	90300
SuSE Linux Enterprise Server 11 S390X	90800
SuSE Linux Enterprise Server 11 X86_64	90100
Ubuntu Server 12.04	60001

OS Name (String)	Internal ID (Integer)
Ubuntu Server 12.04 X86_64	60002
VMware ESX Server 4	10096
VMware ESX Server 4.1	20096
Windows 7 x64	170101
Windows 8.1 x64	170301
Windows 2003 *(deprecated)*	10007
Windows 2003 x64 *(deprecated)*	60100
Windows 2008	160076
Windows 2008 R2 IA64	100200
Windows 2008 R2 x64	170092
Windows 2008 x64	170076
Windows 2012 R2 x64	95000
Windows 2012 x64	170099
Windows XP *(deprecated)*	10008

Table: Allowable Platform Family Name Strings and Integer Values for --os Option

Platform Family Name (String)	Internal ID (Integer)
OS Independent	1
UNIX	N/A
WINDOWS	N/A

Note: Most of the package types in SA are not OS-agnostic (including ZIP packages). This is due to their path-like structures, such as the install path. As a result, using “OS Independent” as their platform is not recommended and might not be supported in future versions.

Options Only for the oupload Command

The following table lists options that apply only to the `oupload` command.

Table: Options Only for the ouplоad Command

arguments	values	description
`--filename-encoding (-e) <encoding>`	String	Specifies the character set of the file name. See also Encoding Options for OCLI. When specifying non-ASCII characters in the value for the --customer argument, include the -e argument on the command line to tell Server Automation which character set to use when communicating with the Model Repository.
`--folder (-d) <folder-path>`	String	Specifies the folder ID or folder path into which the package is uploaded. wildcards in a folder path are allowed. For example, if the destination folder is `myfolder4pkgs`, you can specify `myfolder4*`. Do not specify `--folder` with `--customer`.
`--metainfo-encoding (-E) <encoding>`	String	Specifies the character set of the meta-information in the package.
`--patchtype (-a) <type>`	• AIX LPP • HP-UX Depot • Windows Hotfix • Windows OS Service Pack • Windows Update Rollup • Solaris Patch • Solaris Patch Cluster	Cannot specify this option with -C, use the --old option. Before uploading a unit of type "Windows Service Pack", "Windows Hotfix" or "Windows Update Rollup, " prior metadata needs to exist. This is done by importing the Microsoft Metadata Catalog file, described in "Configuring and Importing the Microsoft Patch Database Metadata" in the SA User Guide: Server Patching.

arguments	values	description
		If importing from a managed server, assign the server to SA Customer Opsware .
`--pkgtype (-t) <type>`	• AIX LPP • HP-UX Depot • Microsoft Patch Database • Build Customization Scripts • RPM • Solaris Package • Solaris Patch • Solaris Patch Cluster • DEB • Windows MSI • ZIP • EXE • IPS • Chef cookbook	Specifies the type of file. **Specifying either this option** or the `-patchtype` option **is required.** Wildcards are accepted. The OCLI does *not* support uploading response files for the Solaris Package package type. Use SA Client to associate a response file with a Solaris Package. If a value contains spaces, you must enclose the value in quotation marks.
`--R <unit_id>`	Integer	If a package with the same name already exists in the upload location, but it has different platforms assigned, you can use this option to replace the package specified by the <unit_id> along with the assigned platforms.

Note: Before uploading a unit of type **Windows Service Pack**, **Windows Hotfix** or **Windows Update Rollup**, prior metadata needs to exist. This is done by importing the **Microsoft metadata catalof** file.

Options Only for the odownload Command

The following table lists options that apply only to the `odownload` command.

Table: Options Only for the odownload Command

argument	value	description
`--filename-encoding (-e)` <*encoding*>	String	Specifies the character set encoding in which to save the file name. See also Encoding Options for OCLI.

Chapter 10

Troubleshooting Server Communication Tests

This section describes the server communication tests in detail. For an overview, see Running Server Communication Tests.

The server communication test performs the following diagnostic tests to determine if a server is reachable:

- Command Engine to Agent (AGT) Test: Determines if the SA Command Engine can communicate with the agent. The Command Engine is the Server Automation core component that enables distributed programs to run across many servers. The Command Engine handles the storage and versioning of scripts into the SA Model Repository. SA stores scripts in the Model Repository.
- Crypto Match (CRP) Test: Checks that the SSL encryption files that the agent uses are valid.
- Agent to Command Engine (CE) Test: Verifies that the agent can connect to the Command Engine and retrieve a command for execution.
- Agent to Data Access Engine (DAE) Test: Checks whether or not the agent can connect to the Data Access Engine and retrieve its device record. The Data Access Engine provides an XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the SA Client, system data collection, and monitoring agents on servers.
- Agent to Software Repository (SWR) Test: Determines if the agent can establish an SSL connection to the Software Repository. SA stores software in the Software Repository, including software packages for operating systems, applications, databases, customer code and software configuration information.
- Machine ID Match (MID) Test: Checks that the Machine ID (MID) on the server matches the MID registered in the Model Repository.

When the test run finishes, it returns results that show either success or failure for each test run on each server. For each failed test, the nature of failure is listed by error type in the error details column of the Communication Test window. In some cases, the failure of one test might prevent other tests from being executed.

See Running Server Communication Tests for information about how to run a Communication Test.

Command Engine to Agent (AGT) Test

The Command Engine to Agent (AGT) communications test system checks that the Command Engine can initiate an SSL connection to the Agent and execute an XML/RPC request.

The thirteen possible results are:

— AGT – OK

- AGT – Untested
- AGT – Unexpected error
- AGT – Connection refused
- AGT – Connection time-out
- AGT – Request time-out
- AGT – Server never registered
- AGT – Realm is unreachable
- AGT — Tunnel setup error
- AGT — Gateway denied access
- AGT — Internal Gateway error
- AGT — Gateway could not connect to server
- AGT — Gateway time-out

AGT – OK

No troubleshooting necessary.

AGT – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Command Engine cannot contact the Agent, then no other tests are possible.

What Can I Do If a Test Is Not Run During an AGT Test?

First resolve all tests that failed, and then run the Communication Test again.

AGT – Unexpected error

This result indicates that the test encountered an unexpected error.

What Can I Do If I Get an Unexpected Error?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

AGT – Connection refused

This result indicates that the Command Engine is receiving a TCP reset packet when it attempts to connect to the Agent on port 1002. The likely cause is that the Agent is not running. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During an AGT Test?

1 Log into the server and confirm that the Agent is running. Verifying that an Agent is Running.

2. If the Agent is not running, restart the Agent. Restarting a Server Agent.
3. From the managed server, use netstat to confirm that a socket is in listen mode on port 1002. If not, stop and restart the Agent.
4. From the server itself, use SSH to connect to the IP address of the server where the Agent is installed and port (1002) that the Agent is listening on. If this does not succeed, stop and restart the Agent.
5. Verify that the Management IP address that Server Automation is using to reach the server is the correct address. Checking Management IP of a Managed Server. If the IP addresses do not match, stop and restart the Agent, then rerun the test.
6. If the previous steps are performed and the test still fails, the problem is likely caused by either a software-based firewall on the server itself or an external firewall blocking the connection.

AGT – Connection time-out

This result indicates that the Command Engine is not receiving any reply packets when it attempts to initiate a TCP connection to the Agent on port 1002. The likely cause is that the server is not running, or that the IP address that Server Automation is using to reach the Agent is incorrect. (A firewall might also be blocking the connection.) To check the IP address that Server Automation is using to reach the Agent, see Checking Management IP of a Managed Server.

What Can I Do If the Connection Times Out During an AGT Test?

Follow the same steps used to resolve this issue specified in What Can I Do If the Connection is Refused During an AGT Test?.

AGT – Request time-out

This result indicates that the Command Engine is able to successfully complete a TCP connection to the Agent on port 1002, but no response is received from the Agent in response to the XML-RPC request. The likely cause is that the Agent is hung.

What Can I Do If the Request Times Out During an AGT Test?

1. Log into the server and restart the Agent. Restarting a Server Agent.
2. Check to see whether or not some other process is consistently utilizing an excessive amount of the CPU on the server where the Agent is installed. Also check to see if the system is performing slowly due to a lack of available memory and/or excessive file IO. In any of these cases, the system might be performing too slowly to permit the Agent to respond to the test in a timely manner.

AGT – Server never registered

This test indicates that the server being tested has neither been registered with the Command Engine, nor can it communicate with the Command Engine. The cause of this could be any number of reasons similar to those in the Agent to Command Engine (CE) Test test. It is also possible (but unlikely) that the Agent was installed but never started.

What Can I Do If the Server Has Not Been Registered with the Command Engine During an AGT Test?

To troubleshoot this error, use the following procedures:

1. Ensure that the Agent is running. For these instructions, Verifying that an Agent is Running.
2. Ensure that the Agent can contact the Command Engine.
3. If the Agent is in a Satellite facility, ensure that its Gateways are properly configured and that it is properly configured to use those Gateways. Checking Network Gateway Configuration.
4. If the Agent is not in a Satellite:
   - Ensure the host name “way” (no quotes) resolves to its valid IP address. Resolving Host Name.
   - Verify that a connection can be established to port 1018 of way.

One (or more) of the above checks will fail. To solve that failure, refer to the corresponding error code for the Agent to Command Engine (CE) Test test on Agent to Command Engine (CE) Test, or to the realm connectivity and configuration test.

AGT – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This means that a path of tunnels between the Gateways in the SA core and the realm of the managed server cannot be established.

What Can I Do If the Realm Is Unreachable During an AGT Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact Hewlett Packard Customer Support for assistance in troubleshooting the Gateway network.

AGT — Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway mis-configuration.

What Can I Do If I Get a Tunnel Setup Error During an AGT Test?

Contact your SA administrator.

AGT — Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Command Engine access to the Agent.

What Can I Do If the Gateway is Denied Access During an AGT Test?

Contact your SA administrator.

AGT — Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do If There is an Internal Gateway Error During an AGT Test?

Contact your SA administrator.

AGT — Gateway could not connect to server

The Gateway could not establish a connection to the Agent. This might be because the Agent is not running, or because a firewall might be blocking the connection.

What Can I Do If the Gateway Couldn't Connect to the Server During an AGT Test?

If you suspect the Agent is not running, see Verifying that an Agent is Running. To make sure that the Gateway can establish a connection to the IP address of the server where the Agent is installed, try to ping the IP address of the server where the Agent is installed.

AGT — Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do If the Gateway Times Out During an AGT Test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

Crypto Match (CRP) Test

This test checks that the SSL cryptographic files that the Agent uses are valid.

The five possible results are:

- CRP – OK
- CRP – OK
- CRP – Unexpected error
- CRP – Agent certificate mismatch
- CRP – SSL negotiation failure

CRP – OK

No troubleshooting necessary.

CRP – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot be reached, then no other tests are possible.

What Can I Do If a Test Is Not Run During a CRP Test?

First resolve all tests that failed, and then run the Communication Test again.

CRP – Unexpected error

This result indicates that the test encountered an unexpected error.

What Can I Do If I Get an Unexpected Error During a CRP Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

CRP – Agent certificate mismatch

This result indicates that the SSL certificate that the Agent is using (`cogbot.srv`) does not match the SSL certificate that is registered with Server Automation for that Agent. Also, a server hosting a Slice Component bundle with the wrong time zone specified could cause a large number of servers with a CRP error during a communications test.

What Can I Do If I Get a Certificate CN Mismatch During a CRP Test?

If the mismatch is determined to be due to a time zone mismatch, synchronize the time zone specifications for the servers. If the error is due to a certificate mismatch, use the Recert Agent Custom Extension to issue a new certificate to the Agent.

CRP – SSL negotiation failure

This result indicates that the Agent is not accepting SSL connections for the SA core. (The SA core is the entire collection of servers and services that provide Server Automation services.) The likely cause of this error is that one or more files in the Agent crypto directory are missing or are invalid.

What Can I Do If I Get an SSL Negotiation Failure During an CRP Test?

Run the Server Recert custom extension in the “set allow recert flag only” mode on the server, and then Run the Server Agent Installer with the “-c” switch.

Reinstalling the Agent with the “-c” option (“c” stands for “clean”) removes all certs on the server and also removes the MID file, which forces the Agent to retrieve a new MID from the Data Access Engine.

- See Running Server Communication Tests for more information about how to install an Server Agent using the “-c” switch.

After you reinstall the Agent, run the test again to check if the Agent is now reachable.

Agent to Command Engine (CE) Test

This test checks that the Agent can connect to the Command Engine and retrieve a command for execution.

The sixteen possible results are:

- CE – OK
- CE – Untested
- CE – Unexpected error
- CE – Connection refused
- CE – Connection time-out
- CE – DNS does not resolve
- CE – Old Agent version
- CE – Realm is unreachable
- CE – No Gateway defined
- CE – Tunnel setup error
- CE – Gateway denied access
- CE – Gateway name resolution error
- CE – Internal Gateway error
- CE – Gateway could not connect to server
- CE – Gateway time-out
- CE – No callback from Agent

CE – OK

No troubleshooting necessary.

CE – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Command Engine, then no other tests are possible.

What Can I Do If a Test Is Not Run During a CE Test?

First resolve all tests that failed, and then run the Communication Test again.

CE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a CE Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

CE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. It is also possible that a firewall might be blocking the connection.

What Can I Do If the Connection is Refused During a CE Test?

1. Check that the name “way” resolves to its correct IP address. For instructions on how to do this, see Resolving Host Name.
2. Check to make sure there isn't a firewall refusing the connection to this IP address.

CE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the “wrong” IP address. In other words, the Agent doesn’t know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During a CE Test?

Follow the same steps specified in What Can I Do If the Connection is Refused During a CE Test? .

CE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “way” to a valid IP address. In other words, the Agent does not know the correct IP address of the Command Engine.

What Can I Do If the Command Engine Name Does Not Resolve During a CE Test?

Log into the server and confirm that the host name “way” can resolve. If not, check the DNS configuration of the server to make sure that the host name “way” is configured to its correct IP address. Resolving Host Name.

CE – Old Agent version

This result indicates that the Agent was unable to contact the Command Engine, but the test was unable to determine the exact cause because the Agent is out of date.

What Can I Do If the Agent is Out of Date During a CE Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Command Engine (“way”) did not resolve, or the connection was refused.

- If you believe that the host name of the Command Engine (“way”) did not resolve, then CE – DNS does not resolve.
- If you determine that the connection was refused, CE – Connection refused.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Customer Support) and re-run the test. See Running Server Communication Tests for more information about how to install an agent.

CE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the Gateways in the SA core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a CE Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network.

CE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a CE Test?

To troubleshoot this error, try the following:

1. Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:
   - **UNIX/Linux**: /etc/opt/opsware/agent
   - **Windows**: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent
2. Make sure that this file contains a single line as shown:

   ```
   opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
   ```

CE – Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do If A Tunnel Setup Occurs Error During a CE Test?

Contact your SA administrator.

CE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Command Engine.

What Can I Do if the Gateway is Denied Access During a CE Test?

Contact your SA administrator.

CE – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “way”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if a Name Resolution Error Occurs on the Gateway During a CE Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “way” can be resolved (for example: “host way”).

If you cannot connect, contact your SA administrator so that you can check the DNS configuration of the core Gateway server.

CE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a CE Test?

Contact your SA administrator.

CE – Gateway could not connect to server

The Gateway could not establish a connection to the Command Engine. The situation might be because the Command Engine is not running, or because the Gateway is resolving the Command Engine host name (“way”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can’t Connect to Server During a CE Test?

Check that the name “way” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. See Resolving Host Name and Verifying that a Port is Open on a Managed Server in this appendix.

CE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a CE Test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

CE – No callback from Agent

The Command Engine was able to contact the Agent, but the Agent did not call back to retrieve its command. However, the Agent reports that it can connect to a Command Engine.

What Can I Do if There is No Callback from Agent?

Ensure network connectivity between the agent and the nearest agent gateway. For example, make sure no firewalls are preventing access. The default port for the agent gateway is 3001. For more information on gateway monitoring, see the SA Administration Guide. For information on configuring the agent gateway, see the SA Installation Guide.

Agent to Data Access Engine (DAE) Test

This test checks that the Agent can retrieve its device record from Data Access Engine. The fifteen possible results are:

- DAE – OK
- DAE – Untested
- DAE – Unexpected error
- DAE – Connection refused
- DAE – Connection time-out
- DAE – DNS does not resolve
- DAE – Old Agent version
- DAE – Realm is unreachable
- DAE – No Gateway defined
- DAE – Tunnel setup error
- DAE – Gateway denied access
- DAE – Gateway name resolution error
- DAE – Internal Gateway error
- DAE – Gateway could not connect to server
- DAE – Gateway time-out

DAE – OK

No troubleshooting necessary.

DAE – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Data Access Engine then no other tests are possible.

What Can I Do If a Test Is Not Run During a DAE Test?

First resolve all tests that failed, and then run the Communication Test again.

DAE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a DAE Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

DAE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During a DAE Test?

1. Check that the name “spin” resolves to its correct IP address. Resolving Host Name.
2. Check to make sure that a firewall is not refusing the connection to this IP address.

DAE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During a DAE Test?

Follow the same steps specified in What Can I Do If the Connection is Refused During a DAE Test?.

DAE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “spin” to a valid IP address. In other words, the Agent does not know the correct IP address of the Data Access Engine.

What Can I Do If the Data Access Engine Name Does Not Resolve During a DAE Test?

Log into the server and confirm that the host name “spin” can be resolved. If not, check the DNS configuration of the server to make sure that the host name “spin” is configured to its correct IP

address. Resolving Host Name.

DAE – Old Agent version

This result indicates that the Agent was unable to contact the Data Access Engine, and the test is unable to determine the exact cause, because the Agent is out of date.

What Can I Do If the Agent is Out of Date During an DAE Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Data Access Engine ("spin") did not resolve, or the connection was refused.

- If you believe that the host name of the Data Access Engine ("way") did not resolve, then see DAE – DNS does not resolve.
- If you determine that the connection was refused, see DAE – Connection refused.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Customer Support) and re-run the test. See Running Server Communication Tests for information about how to install an agent.

DAE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the SA core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a DAE Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network

DAE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a DAE Test?

To troubleshoot this error, try the following:

1. Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:
   - **UNIX/Linux**: /etc/opt/opsware/agent
   - **Windows**: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent
2. Make sure this file contains a single line as shown:

   ```
   opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
   ```

DAE – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway mis-configuration.

What Can I Do if a Tunnel Setup Error Occurs During a DAE Test?

Contact your SA administrator.

DAE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Data Access Engine.

What Can I Do if the Gateway is Denied Access During a DAE Test?

Contact your SA administrator.

DAE – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “spin”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if There is a Name Resolution Error on the Gateway During a DAE Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “spin” can be resolved (for example: “host spin”).

If you cannot connect, contact your SA administrator so that you can check the DNS con-figuration of the core Gateway server.

DAE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a DAE Test?

Contact your SA administrator.

DAE – Gateway could not connect to server

The Gateway could not establish a connection to the Data Access Engine. This might be because the Data Access Engine is not running, or because the Gateway is resolving the Data Access Engine host name (“spin”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can't Connect to Server During a DAE Test?

Check that the name "spin" resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. Resolving Host Name and Verifying that a Port is Open on a Managed Server.

DAE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a DAE Test?

Ensure that network connectivity is available between the Gateways in the path between the managed server's realm and the SA core.

Agent to Software Repository (SWR) Test

This test checks that the Agent can establish an SSL connection to the Software Repository.

There 16 possible results are:

- SWR – OK
- SWR – Untested
- SWR – Unexpected error
- SWR – Connection refused
- SWR – Connection time-out
- SWR – DNS does not resolve
- SWR – Old Agent version
- SWR - Server identification error
- SWR – Realm is unreachable
- SWR – No Gateway defined
- SWR – Tunnel setup error
- SWR – Gateway denied access
- SWR – Gateway name resolution error
- SWR – Internal Gateway error
- SWR – Gateway Could not connect to server
- SWR – Gateway time-out

SWR – OK

No troubleshooting necessary.

SWR – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Software Repository, then no other tests are possible.

What Can I Do If a Test Is Not Run During a SWR Test?

First resolve all tests that failed, and then run the Communication Test again.

SWR – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a SWR Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

SWR – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is trying to connect to the wrong IP address. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During an SWR Test?

1. Check that the name “theword” resolves to the correct IP address. For this information, see Resolving Host Name.
2. Check to make sure that a firewall isn’t refusing the connection to this IP address.

SWR – Connection time-out

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Software Repository. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During an SWR Test?

Follow the same steps specified in What Can I Do If the Connection is Refused During an SWR Test? .

SWR – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “theword” to a valid IP address. In other words, the Agent does not know the correct IP address of the Software Repository.

What Can I Do If the Software Repository Name (“theword”) Does Not Resolve During an SWR Test?

Log into the server and confirm that the host name “theword” can be resolved. If not, contact your SA administrator so that you can check the DNS configuration of the server.

SWR – Old Agent version

This result indicates that the Agent was unable to contact the Software Repository, and the test is unable to determine the exact cause because the Agent is out of date.

What Can I Do If the Agent is Out of Date During an SWR Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Software Repository (“theword”) did not resolve, or the connection was refused.

- If you think that the host name of the Software Repository (“theword”) did not resolve, then see SWR – DNS does not resolve.
- If you determine that the connection was refused, see SWR – Connection refused.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Customer Support) and re-run the test. See Server Agent Management for information how to install a server agent.

SWR - Server identification error

Whenever an Agent makes a request of the Software Repository, the identity of the server is validated to confirm that the server should be allowed access to the information requested. This error indicates that the Software Repository was unable to identify the server being tested, or incorrectly identified that server.

What Can I Do If I Get a Server Identification Error?

The Software Repository identifies servers based on the incoming IP address of the request. To troubleshoot this error, try the following:

1. Check the Network Settings tab for the server in the SA Client to see if Network Address Translation (NAT) is in use. If it is, make sure that NAT is statically configured, and that only one server is using the NAT address. If multiple servers are using the same IP address, you will need to reconfigure the NAT device. See See "Network Address Translation (NAT) for Managed Servers" for more information.
2. If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the SA core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the “primary” interface through the Network Settings tab for the server in the SA Client. See See "Network Address Translation (NAT) for Managed Servers" for more information.
3. The server's IP address might have changed recently. If this is the case, stop and restart the Agent. For instructions on how to stop and start an Agent, see Restarting a Server Agent.

SWR – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the SA core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a SWR Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network.

SWR – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a SWR Test?

To troubleshoot this error, try the following:

1. Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:
   - **UNIX/Linux**: /etc/opt/opsware/agent
   - **Windows**: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent
2. Make sure that this file contains a single line as shown:

   ```
   opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
   ```

SWR – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do If a Tunnel Setup Error Occurs During a SWR Test?

Contact your SA administrator.

SWR – Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Software Repository.

What Can I Do if the Gateway is Denied Access During a SWR Test?

Contact your SA administrator.

SWR – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “theword”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if a Name Resolution Error Occurs on the Gateway During a SWR Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “theword” can be resolved (for example: “host theword”).

If you cannot connect, contact your SA administrator so that you can check the DNS configuration of the core Gateway server.

SWR – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a SWR Test?

Contact your SA administrator.

SWR – Gateway Could not connect to server

The Gateway couldn't establish a connection to the Software Repository. This error might be because the Software Repository is not running, or because the Gateway is resolving the Software Repository host name (“theword”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can’t Connect to Server During a SWR Test?

Check that the name “theword” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP address. For more information, see Resolving Host Name and Verifying that a Port is Open on a Managed Server.

SWR – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a SWR Test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

Machine ID Match (MID) Test

This test checks whether the MID that the Agent reported matches that recorded in the Model Repository (SA data repository).

You can receive four possible errors from the Machine ID (MID) Communication Test:

- MID – OK
- MID – Untested
- MID – Unexpected error
- MID – MID mismatch

MID – OK

No troubleshooting necessary.

MID – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Model Repository, then no other tests are possible.

What Can I Do If a Test Is Not Run During an MID Test?

First resolve all tests that failed, and then run the Communication Test again.

MID – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During an MID Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Customer Support.

MID – MID mismatch

This result indicates that the MID that the Agent reported does not match the recorded MID in the Model Repository for that Agent. The likely cause is that the Command Engine is running the test against the wrong Agent.

What Can I Do If the MID is Mismatched During an MID Test?

To troubleshoot this error, try the following:

1. Check the Network Settings tab for the server in the SA Client to see if NAT is in use for this server. If it is, make sure that static, 1-to-1 NAT is being used. Server Automation requires that all managed servers be reachable on a distinct, consistent IP address, so configurations that assign addresses dynamically or use port-based translation are not supported.
2. If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the SA core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the “primary” interface through the Network Settings tab for the server in the SA Client.

3 The IP address might have changed recently. If this is the case, stop and restart the Agent. For these instructions, see Restarting a Server Agent.

Common Troubleshooting Tasks

The following list of troubleshooting tasks are common to more than one Communication Test error:

- Verifying that an Agent is Running
- Verifying that a Port is Open on a Managed Server
- Restarting a Server Agent
- Checking Management IP of a Managed Server
- Checking Network Gateway Configuration
- Resolving Host Name

Verifying that an Agent is Running

To verify that an Agent is running on a server, perform the following steps:

1 On Solaris, HP-UX, or AIX, enter this command:

```
/usr/ucb/ps auxwww | grep opsware
```

You should get this result if the Agent is running:

```
/opt/opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args
```

2 On Linux, enter this command:

```
ps auxwww | grep opsware
```

You should get the same result as the preceding step.

3 On Windows, from the Administrative Tools | Services, check to make sure that the `opswareagent` service is running.

Verifying that a Port is Open on a Managed Server

For some errors, you will need to verify that the port is open on the server where the Agent is installed. To do this, perform the following steps:

1 Check if the port is open.

2 On Solaris, HP-UX, AIX, or Linux enter:

```
netstat -an | grep 1002 | grep LISTEN
```

If the port is open on the box, you should get back the following:

```
*.1002    *.*    0 0 24576 0 LISTEN
```

3 On Windows, at the command prompt enter:

```
netstat -an | find "1002" | find "LISTEN"
```

If the port is open on the box, you should get back the following result:

```
TCP 0.0.0.0:1002 0.0.0.0:0 LISTENING
```

4. Confirm that the port is actually open. To do this, from the computer where the Agent is installed, connect to port 1002 by using both localhost and the external IP address of the server. Performing the connection will help you confirm that a connection refused message is being caused by the lack of an open port on the managed server rather than a problem with networking hardware between the core and the managed server.

Restarting a Server Agent

To restart a Server Agent, log onto the managed server and enter the following commands:

UNIX:

/etc/init.d/opsware-agent restart

HP-UX:

/sbin/init.d/opsware-agent restart

AIX:

/etc/rc.d/init.d/opsware-agent restart

Windows:

net stop opswareagent

net start opswareagent

Checking Management IP of a Managed Server

To check the Management IP of a managed server, perform the following steps:

1. To view the management IP of the managed server, log into the SA Client.
2. From the Navigation panel, click **Devices** > **All Managed Servers**.
3. From the All Managed Servers list, open the server for which you want to check the Management IP.
4. Select the Inventory panel and then the Network tab of the server's properties.
5. Check to make sure that the Management IP address matches the IP address of the managed server.

Checking Network Gateway Configuration

To check the network Gateway configuration, perform the following steps:

1. On Solaris, enter this command to check routing table:

   ```
   netstat -rn
   ```

   Your results should look like this:

   ```
   default 192.168.8.1 UG 1 5904
   ```

   where `192.168.8.1` is the IP of the Gateway.

2 On Linux, enter this command to check routing table:

```
route -n
```

Your results should look like this:

```
0.0.0.0 192.168.8.1 0.0.0.0 UG 0 0 0 eth0
```

where `192.168.8.1` is the IP of the Gateway.

3 On Windows, enter this command to check routing table:

```
route print
```

Your results should look something like this:

```
0.0.0.0 0.0.0.0 192.168.8.1 192.168.8.120 20
```

where `192.168.8.1` is the IP of the Gateway.

4 In each case, you should also ping 192.168.8.1 (IP) to confirm that you can actually reach the Gateway.

Resolving Host Name

All managed servers (those with agents) must be able to resolve unqualified Server Automation service names for the following components:

- spin (Data Access Engine)
- way (Command Engine)
- theword (Software Repository)

If you need to ensure that one of these host names resolves correctly, contact your SA administrator to find out what qualified host name or IP address these service names should resolve to.

1 Try to ping the host. For example, execute the following command if you wanted to resolve the host name, way:

```
ping way
```

2 If the host name cannot resolve, you will get the following errors:

Linux/Solaris/AIX/HP-UX:

```
ping: unknown host way
```

Windows:

```
Ping request could not find host way. Please check the name
and try again.
```

3 If the host name can resolve, you might get back various permutations of these types of messages (OS independent):

```
way is alive
```

or

```
pinging way (ip) with 32 bytes of data
```

Chapter 11

Agent Installation and Upgrade Utilities

Agent Install Command

This section provides information on Agent installation using the Agent Installer CLI (Command Line Interface) and contains the following topics:

Overview of Agent Installation Using the CLI

Requirement: When you install Agents on existing servers, you should synchronize the local time on the servers with an external time-server that uses a network time protocol (NTP).

The Agent Installer can be invoked from the command line or within a script and can be operated unattended because user interaction is not required. The Agent Installer also retrieves cryptographic material, retrieves configuration information, and writes a configuration file and a log file.

The Agent installer installs the SA agent on your servers and makes them known to Server Automation so that they can be managed.

Installing an Agent on a server with a pre-built OS into Server Automation enables:

- Baseline discovery of the operating system on the server.

- Managing the baseline operating system, including patch management, when the operating system is defined in Server Automation with the Prepare Operating System Wizard.
- Full provisioning and management capabilities for any new applications deployed on the server.

When installed, the Agent registers the server with the Model Repository. Server Automation assigns the server to a generic operating system that corresponds to the operating system that the Agent discovered during the installation. The server is assigned to a placeholder OS node. For each operating system, the SA Client contains a node <*operating_system_version*>/Not Assigned.

Note: The Agent Installer can install Agents when a core is not available to a server. If a newly-installed Agent cannot contact a core, the Agent runs in a dormant mode. While dormant, it periodically attempts to contact the core. When the core becomes available, the Agent performs the initialization tasks, such as hardware and software registration, that usually take place when the Agent is first installed.

The server is tracked in the SA Client. However, the server operating system *cannot* be managed while the server is assigned to the generic operating system node. You must reassign the server to the operating system that was defined with the OS Provisioning feature.

The server is associated with the default facility for the local instance of Server Automation.

If the managed server's IP address does not fall within a specified IP range, the server is associated with the default IP range group (Default). The default group is associated with the customer Not Assigned.

See Assigning a Server to a Customer - SA Client for information about how servers are associated with customers.

The Agent Installer Command

The Agent Installer command is available on any SA core server in the directory `/var/-opt/opsware/agent_installers`. A different Agent Installer is provided for each different operating system version.

Preparation for Agent Installation

It is recommended that you set up a Windows file share to make the Agent Installer for various operating systems available from one place. Setting up a file share allows you to install Agents on servers quickly and easily. If this is not possible, the Agent Installer needs to be moved by using an alternate file transfer mechanism, such as SFTP.

At the completion of the Agent installation process, a server becomes a managed server and the hardware and software data that the Agent discovered are stored in the Model Repository.

Checklist Before Installing the SA Agent

Before installing the agent, perform the following tasks on the server where it is to be installed. Performing these tasks is vital to installing the Agent quickly within maintenance windows.

1. Because the Agent runs on port 1002, verify that no other applications are using this port.
   - On a UNIX server, enter this command from a terminal window:

     ```
     netstat -an | grep 1002 | grep LISTEN
     ```

   - On a Windows server, enter this command from a terminal window:

     ```
     netstat -an | find "1002" | find "LISTEN"
     ```

2. Check for sufficient disk space for Agent installation on the server.

   The installer checks for the following amounts of free disk space in these directories:
   - 100MB in `/opt/opsware` (UNIX)
   - 100MB in `/var/opt/opsware` (UNIX)
   - 30MB in `%SystemDrive%\\Program Files\Opsware` (Windows)
   - 100MB in `%SystemDrive%\Program Files\Common Files\Opsware` (Windows)

   These default directories can be overridden with parameters at installation time.

   These space requirements might not be enough. The `vardir` directory is used for dynamic content like logs and downloaded packages. If there is not enough disk space for the packages during remediation, it will fail.
3. On the Solaris operating system, check for legacy sun4m architecture. Currently, the Agent works only for sun4u architecture.
4. For Windows verify that the Windows Registry has the correct settings:
   a. Start regedit and locate the following registry key:

      ```
      HKEY_LOCAL_
      MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
      ```

   b. Select the `NtfsDisable8dot3NameCreation` entry.
   c. On the Edit menu, click DWORD and verify that the value is set to 0. The value *must* be set to 0. If necessary (because the value is set to 1), change the value by following your organization's IT policies and reboot the server.
5. To install an Agent on a server running Solaris, you must also install the following Solaris packages:

   For Python:

```
SUNWtoo

SUNWtoox
```

   For showrev:

```
SUNCadm

SUNWlibC

SUNWlibCx

SUNWadmfw
```

6 Before you install an Agent on a server, the server must meet certain package and patch requirements that vary by operating system. See the *SA Support and Compatibility Matrix* for agent package and patch requirements.

Installing an Agent

Perform the following tasks to install an Agent on an unmanaged server.

Obtaining the Agent Installer Package

The Agent needs administrator-level privileges (root on UNIX servers and Local System on Windows servers) to manage a server. Therefore, Agent installation needs to be performed as root on UNIX operating systems and as administrator on Windows operating systems.

You can install an agent on any server listed in the SA Support and Compatibility Matrix.

Perform the following steps to download an Agent Installer for an unmanaged server.

From the Command Line

1 Log into the unmanaged server using a remote shell. On UNIX, log in as root. On Windows, log in as administrator.

2 Locate the appropriate Agent Installer on a core server

From the command line: in the directory `/var/opt/opsware/agent_installers`. Each operating system version has a different package for the Agent Installer.

UNIX:

```
opsware-agent-<version>-<system_name>-<system_version>
```

Red Hat Linux:

```
opsware-agent-<version>-<system_name>-5CLIENT-<system_version>
```

Note that Red Hat may use the terms *Client* and *Desktop* interchangeably.

Windows:

```
opsware-agent-<version>-<system_name>-<system_version>.exe
```

3 From the directory where the Agent Installer was copied, run the Installer by entering the correct executable and options for the installation environment. The options are listed under Agent Installer Options.

From the SA Client

If you do not have remote shell access to the SA Core from an unmanaged server, you may need to manually export the Agent Installer package locally on SA Core machine and copy it to the unmanaged server. To export the Agent Installer package, perform the following tasks.

1 Launch the SA Client.

2 From the Navigation pane, select **Library** > **Packages.**

3 Select the appropriate operating system from those listed under packages as shown in Selecting an Agent Installer Package.

Select the SA Agent. The filename will be in the format:

UNIX:

opsware-agent-<version>-<system_name>-<system_version>

Red Hat Linux:

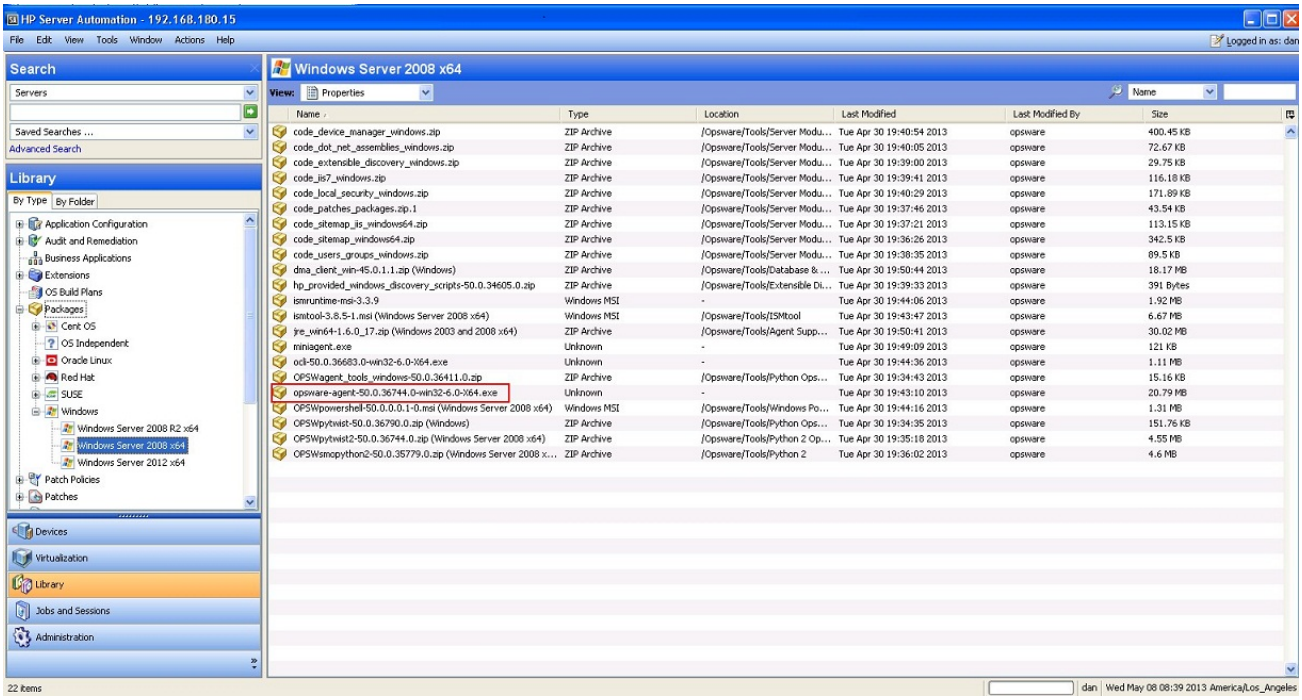
opsware-agent-<version>-<system_name>-5CLIENT-<system_version>

Note that Red Hat may use the terms Client and Desktop interchangeably.

Windows:

opsware-agent-<version>-<system_name>-<system_version>.exe

Selecting an Agent Installer Package



4. Click the package name for the Agent Installer that you want to export. From the Actions menu, select Export Software. The Browse window appears.
5. In the Browse window, specify the download location for the package and Click Export. The package is exported to the specified location.
6. Copy the Agent Installer to the target server.

Example: Agent Installer Command and Options

The following example command installs the server agent on a Solaris 5.10 server in the default directories, connects to the gateway on the server core2.hp.com using port 2010, and logs the results of the installation in the log file named agent.log:

```
% opsware-agent-45.0.0.0.98-solaris-5.10 --logfile agent.log --
loglevel info
```

--opsw_gw_addr core2.hp.com:2010

Agent Installer Options

Use the options listed below with the Agent Installer command. You must use either the `--opsw_gw_addr` option or the `--no_opsw_gw` option. All others are optional.

Table: Agent Installer Options

Option	Description
--auth_path	Specifies the complete path to the file that contains the trusted authorities in PEM format.
--coreinstall	Install initialization scripts in the proper location for the core server.
--customer_id <*customer*>	Assigns the managed server to the specified customer. This option requires the `--username` and `--password` options. For more information about customers see Creating and Managing Customers.
--del_opsw_gw_addr_list	Deletes the list of gateway addresses.
`-f`	Forces the Agent to be installed even if environment check errors occur. This option is useful when the server is not connected to an SA core. When using the `-f` option, you must run the Agent installer as root on Unix operating systems and as the administrator on Windows operating systems.

--fingerprint	Specifies the fingerprint of the core certificate.
	If you specify a value for this option, the Agent installer will verify that the Certificate Authority certificate used to sign the core's SSL certificate matches the value you provided. Specifying a value for this option increases security during the Agent installation process by ensuring that the Agent attaches itself to the correct core.
	To obtain the correct value for the core certificate fingerprint option, log on to the core as root (you may need to have an SA System Administrator perform this task for you) and run the following command:
	`/opt/opsware/bin/openssl x509 -in /var/-opt/opsware/crypto/agent/opsware-ca.crt -fingerprint -noout`
	The output looks like the following:
	`SHA1 Fingerprint=D2:3B:F8:72:B9:55:0D:DE:97:04:D5:C2:A5:6B:B2:09:5C:0A:0D:7F`
	The fingerprint is the string of hexadecimal numbers following the equal sign:
	`D2:3B:F8:72:B9:55:0D:DE:97:04:D5:C2:A5:6B:B2:09:5C:0A:0D:7F`

--force_full_hw_	Causes a full hardware registration to be performed on the server after the

Option	Description
reg	Agent is installed. The default is for a minimal hardware registration to be performed. For more information, see Software and Hardware Inventory.
--force_sw_reg	Causes a software registration to be performed on the server after the Agent is installed. By default, the software registration is not performed until the regularly scheduled time. For more information, see Software and Hardware Inventory.
--force_virt_reg	Force full virtualization registration (default is no registration).
-h	Displays all the options available with the Agent installer command.
`--logfile` <*path*>	Specifies the path and file name of the Agent installer log file. By default, the current directory is set as the path. By default, the log file is: `opsware-agent-installer-`<*date*>`.log`
`--loglevel` <*level*>	Sets the log level for log messages. <*level*> must be one of the following: `trace`, `info`, `warn`, or `error`. The level `error` logs the least detail. The level `trace` logs all messages. By default, the log level is set to `info`.
--no_anonym-ous_ssl	Disables anonymous SSL. This option configures the Agent so that browsers cannot connect to its web interface without a valid certificate. This option applies to dormant Agents only. If specified, the dormant Agent will require clients that connect to its web interface to have a valid certificate.
--no_check_ reachability	Suppresses a reachability check. The default is to perform a reachability check during fresh installs, and not to perform this check during upgrades.
--no_open_fw	Does not open the Windows firewall to communicate with the SA core. By default, the Agent installer will modify the Windows firewall con-figuration on Windows 2003 (r2) or Windows 2008 servers to allow the core to contact the managed server on port 1002. If you specify this option, the firewall configuration will not be modified and the server may not be manageable by SA.
--no_opsw_gw	Specifies that no gateway is needed. Either this option or the `--opsw_ gw_addr` option must be specified.
--no_start_ agent	Prevents the Agent from starting after installation. By default, the Agent is started immediately after installation. See also Starting an Agent After Installation.
--opsw_gw_addr <*host:port*>	Specifies the host and port number of the gateways used during Agent installation. Either this option or `--no_opsw_gw` must be specified.

Option	Description
--password <*password*>	Specifies the password for the user specified in the `--username` option. This option is only used by the `--customer_id` option.
`--reboot`	Causes the server to be rebooted after the Agent is installed, but only if required. During Agent installation on a Windows server, the Agent installer copies the file ogshcap.dll to the following location: `%SystemRoot%\system32\ogshcap.dll` If the file is open or is in use, the Agent installer is unable to copy this file. The Agent installer then asks the user whether to restart the machine and copies the file after restart. You can also specify `--reboot` on the command line to initiate the reboot at the end of the Agent installation.
--remediate	Remediates the server against any software policies attached to the server, including all software policies specified in the `--software_policy` option. For more information, see the SA User Guide: Software Management.
--resetconf -r	Resets the Agent configuration file to the default settings.
`--rpmbin` <*path*>	Specifies the path to the RPM handler to use for RPM operations. Use this option, when an RPM handler is already installed on the server. If an RPM handler is not already installed on the server, use the `--withrpm` option instead to install one. It is not necessary to use this option with the `--withrpm` option.
--settime -t	Sets the time on the server to that of the core. If the managed server's clock is significantly ahead of the clock on the SA Core, the clock on the managed server will be set back. Since this can cause problems, do not use the `--settime` option unless you are sure that this scenario is not a problem in your environment. If a managed server's clock is significantly behind the clock on the core, the Agent installation might fail. To install an Agent successfully, use the `--settime` option or manually set the time and date on the managed server before retrying the Agent installation.
`--software_policy` <*ID*>	Attaches the software policy *<ID>* to the server. <ID> must be the name of a software policy in the SA Library. If you want to remediate the software policy immediately, specify the `--remediate` option. For more information, see the SA User Guide: Software Management.

Option	Description
--spin_host	Specify the host name or IP address of the Data Access Engine component. If you specify this option, you must also specify the `--no_opsw_gw option`.
--username <*name*>	Specifies an SA user name. This option requires the `--password` option. This option is only used by the `--customer_id` option.
`--withmsi`	Installs Windows MSI 2.0 along with the Agent. If Windows MSI 2.0 is already installed, this option has no effect. Works with Windows 2000 and Windows 2003 or later.
`--withrpm`	Installs the RPM handler with the Agent. By default, an Agent is not installed. It is recommended that you always include the `--withrpm` option when you install Agents on Solaris servers. Use this option only with the Agent installers for Solaris 5.8, 5.9 and 5.10. On Solaris 5.8 and 5.9, RPM 3.0.6 is installed in the directory `/opt/opsware/rpm`. On Solaris 5.10 x86, RPM 4.4.4 is installed in the directory `/opt/opsware/rpm`. The RPM database is installed in the directory `/opt/opsware/rpm`. On AIX, RPM 3.0.5 is installed in the directory `/opt/freeware` and the RPM database is installed in the directory `/var/opt/freeware/lib/rpm`. If an RPM handler is already installed, you can use the `--rpmbin` option.
`--workdir` <*path*>	Specifies the path to the Agent installer temporary working directory. Use this option if the default working directory causes problems with installation.

Starting an Agent After Installation

You can manually start the Agent on a server as follows.

UNIX:

```
/etc/init.d/opsware-agent start
```

HP-UX:

/sbin/init.d/opsware-agent start

AIX:

/etc/rc.d/init.d/opsware-agent start

Windows:

```
net start opswareagent
```

Verifying Agent Functionality

Perform the following steps to verify Agent functionality:

1. From the navigation panel in the SA Client, select **Devices** > **All Managed Server**s. The All Managed Servers list appears. Browse the list to find the server whose Agent installation you want to verify. If necessary, open the server and select the correct customer and facility for the server and then click **File** > **Save**.

   Or

   Search for the server whose agent installation you want to verify.
2. Verify that the server appears in the All Managed Servers list and has the correct properties.

   See Searching for Servers Based on Agent Information and for more information.
3. If you want to discover reasons why a server is unreachable, you can run a Communication Test. See Running Server Communication Tests - SA Client for more information.

Augmenting the Information for a Managed Server

Caution: Use caution when you augment the discovery process for a managed server that is functioning in the operational environment. You might inadvertently install or uninstall software from the server. During the test remediate, verify what software will be uninstalled from the server before you perform the actual remediate operation.

Perform the following steps to augment the information for a managed server:

1. Model the OS and other applications running on the server in Server Automation by defining the OS with the Prepare Operating System Wizard and by creating nodes and templates for applications running on the managed server.

   See the SA User Guide: Provisioning for more information about operating system definitions.
2. Move the server to the appropriate nodes for the OS and installed applications.

   The server is tracked in the SA Client; however, the server operating system *cannot* be managed while the server is assigned to the generic operating system node. You must reassign the server to the operating system that was defined with the OS Provisioning feature.
3. Remediate the server.
4. If an IP range group was set up, servers are automatically associated with customers when users install an Agent on the servers. Otherwise, the servers are associated with the Not Assigned customer. To change the customer associated with a server, see Editing the Properties of a Server.
5. To specify the server's use, stage, and state, edit the server's properties. See Editing the Properties of a Server for more information.

Discovery is complete. Server Automation assumes that the server should always be running the specific OS build it has been associated with. Any changes to the OS outside of Server Automation are not captured in the model.

Users can deploy and manage new applications on the server, just as if Server Automation initially provisioned the server. Users can also deploy OS level patches on the server, or rebuild the OS by using the OS build with which the server was associated.

Uninstalling an Agent on UNIX and Windows

Requirement: To uninstall Agents on Windows NT, Windows Scripting Host 5.1 or Internet Explorer 5.5 must be installed on Windows NT.

Perform the following steps to uninstall an Agent on UNIX or Windows:

1. Log into UNIX as root user. Log into Windows as Administrator.
2. Change directories to any directory other than the Agent's installation directory.
3. *On UNIX*, enter the following command:

   ```
   <installation_directory>/bin/agent_uninstall.sh
   ```

   By default, for Solaris and AIX, the Agent Uninstaller will not remove the SA RPM package. For command line options for the agent uninstaller, including how to activate removal of the SA RPM package, Agent Uninstaller Options.
4. *On Windows*, enter the following command:

   ```
   msiexec /x <installation_directory>\bin\agent_uninstall.msi
   ```

   You can also use the Windows Control Panel's Add or Remove Programs option to remove the Agent.
5. As the uninstall proceeds, the *UNIX* platform `stdout` shows the uninstallation progress. The *Windows* uninstall does not show uninstallation progress.

Agent Uninstaller Options

When you use the Agent Uninstaller, you can include the options that Agent Uninstallation UNIX Options and Agent Uninstallation Windows Options show.

Table: Agent Uninstallation UNIX Options

Option	Description
`--unin-stallerVersion`	Show the uninstaller version.
`--help`	Show this help.
`--no_deactivate`	Do not deactivate the server; by default, the server is deac-tivated.
`--force`	Do not prompt for confirmation before deactivating the server.
`--delete_opsw_rpm`	Remove the OPSW RPM package (AIX, Solaris only). Use the fol-

Option	Description
	lowing commands to remove the RPM package: Solaris: `pkgrm -n OPSWrpm` AIX: `installp -u rpm.rte`

Table: Agent Uninstallation Windows Options

Option	Description
`NO_DEACTIVATE="1"`	Do not deactivate the server; by default the server is deactivated.
`FORCE="1"`	Do not prompt for confirmation before deactivating the server.

During Agent Uninstallation on a Windows server, the Agent Installer removes the ogshcap.dll file from the following location:

```
%SystemRoot%\system32\ogshcap.dll
```

If the file is open or is in use, the Agent Installer is unable to remove the ogshcap.dll file. The Agent Installer then prompts the user to restart the machine and removes the file after restart.

Uninstalling Earlier Versions of Agents on UNIX

Perform the following steps to uninstall Agents versions 5.1 and earlier:

1. Stop the Agent on the server by running the following command as root:

Linux:

```
/etc/rc.d/init.d/cogbot stop
```

Solaris:

```
/etc/init.d/cogbot stop
```

HP-UX:

```
/sbin/init.d/cogbot stop
```

AIX:

```
/etc/rc.d/init.d/cogbot stop
```

2. Deactivate or delete the server by using the SA Client Server menu.
3. For Linux servers only, run `chkconfig` to de-register the Agent initialization script:

```
% /sbin/chkconfig -del cogbot
```

4. As root, delete the following files and directories to remove the Agent files from the server:

Linux:

```
/etc/rc.d/init.d/cogbot
```

Solaris:

```
/etc/init.d/cogbot
/etc/rc2.d/S79cogbot
/etc/rc0.d/K44cogbot
```

HP-UX:

```
/sbin/init.d/cogbot
/sbin/rc2.d/cogbot
```

AIX:

```
/etc/rc2.d/init.d/cogbot
/etc/rc.d/S79cogbot
```

All UNIX:

```
/opt/OPSW
/var/lc
```

Uninstalling Earlier Versions of Agents on Windows

Perform the following steps to uninstall earlier versions of Agents on Windows:

1. Stop the Agent by running the following command as administrator:

   ```
   C:\> net stop shadowbot
   ```

2. Deactivate or delete the server by using the SA Client Server menu.
3. Deregister the Agent service by running the following command as administrator:

   ```
   C:\> "%SystemDrive%\Program
   Files\Loudcloud\blackshadow\watchdog\watchdog.exe" -x
   ```

4. As administrator, delete the following directories to remove the Agent:

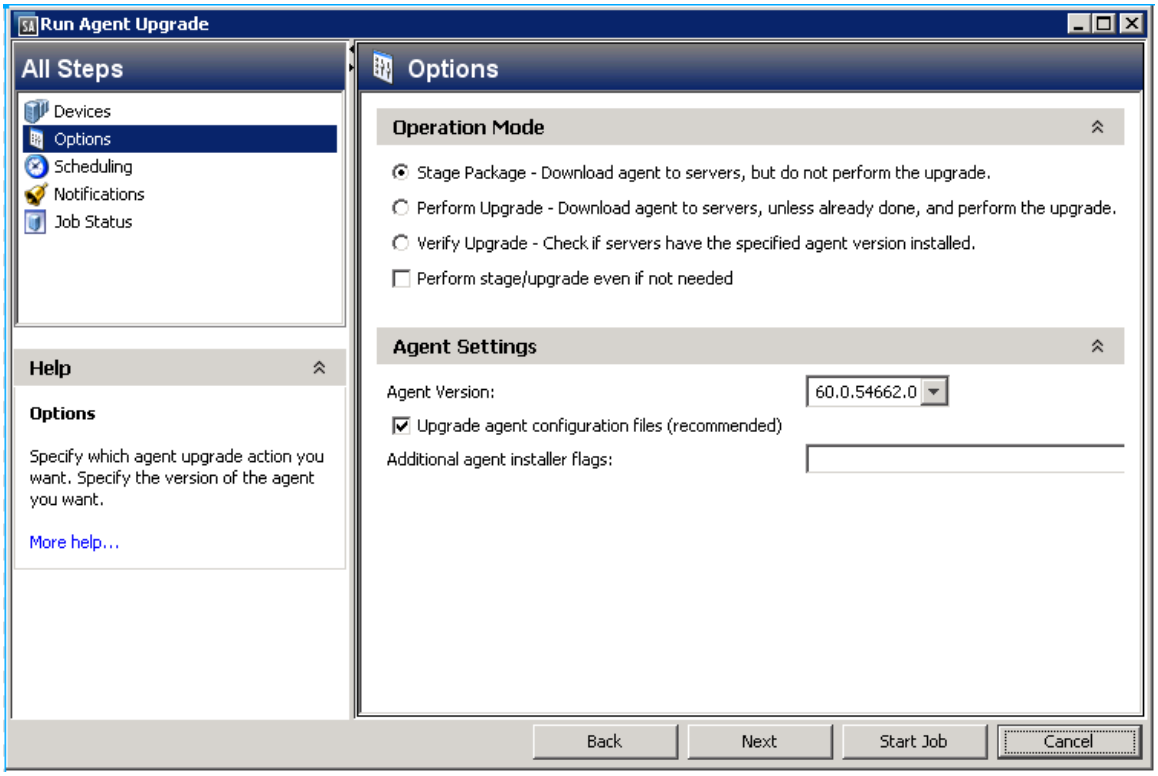
   ```
   "%SystemDrive%\Program Files\Loudcloud"
   "%SystemDrive%\Program Files\Common Files\Loudcloud"
   ```

Agent Upgrade - SA Client

This section describes how to upgrade the SA agent using the SA Client. The SA agent runs on managed servers and enables SA to communicate with and manage your servers.

For more information, see Server Agent Management.

1. From the SA Client navigation pane, select the Devices tab. This displays the Device Groups and Managed Servers nodes.
2. Select either one or more managed servers or one or more device groups.
3. Right click or select the **Actions** menu and select **Run > Agent Upgrade**. This displays the agent upgrade wizard and the servers and device groups you selected.



4. Use the ⊞ and ⊟ buttons to add or remove servers and device groups.
5. If you selected any device groups you can specify when the members of the group are determined. For the Server Group Calculation setting:
   - Select Now to have the device group membership calculated once when the job is created. If you schedule the job to run in the future and the device group membership changes, the servers the job runs on will not change. It will only run on the servers in the device group at the time the job was created.
   - Select At Runtime to recalculate the group membership prior to running the job. If you schedule a recurring job, the job will recalculate the device group members each time the job runs.
6. Select Next to display the Options window.
7. Select the operation you want to perform:
   - Stage Package - Downloads the agent to the specified servers, but does not perform the upgrade.
   - Perform Upgrade - Downloads the agent to the specified servers, unless it was already downloaded, and performs the upgrade.
   - Verify Upgrade - Just checks the agents on the specified servers and reports if the servers have the specified agent version installed.
   - If you want the operation to be performed even if it has already been performed, check the box labeled “Perform stage/upgrade even if not needed.”
8. Select the agent version you want to install. You should typically select the highest version number.
9. Deselect the checkbox for Agent files configuration upgrade if you do not want to upgrade them. However, we recommend that you upgrade the configuration files when upgrading

to a new Agent version.

10. Optionally specify additional parameters to the agent installer. For details, see Agent Installer Options.
11. At any time, select Start Job to accept the remaining defaults and run the job, or select Next to display the Scheduling window.
12. Specify when you want the agent upgrade job to run. Select Next to display the Notifications window.
13. Specify email addresses and conditions to receive notifications when the job finishes. Optionally specify a ticket identifier. Select Next to display the Job Status window.
14. Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.

    When your job finishes, you can select any server to see the job results for that server.
15. To see the version of the agent running on a server, select the server in the SA Client and select the Properties view. Scroll down to the Reported Information to see the agent version. For more information, see Reported Information for Servers.

Note: The server may not immediately display as reachable in the SA Client. You can wait for the server to display or issue a Communication Test which can shorten the time before the server displays as reachable. See Running Server Communication Tests - SA Client for more information.

Agent Upgrade Command

This section contains the following topics:

- Ways to Upgrade Agents
- Prerequisites for Using the Agent Upgrade Tool
- Upgrading the Agent on Managed Servers
- Commands for the Agent Upgrade Tool
- Options for the Agent Upgrade Tool
- Example: Options for the Agent Upgrade Tool
- Example: Commands and Output for Agent Upgrade Tool

Ways to Upgrade Agents

After you upgrade Server Automation running in a facility, you should upgrade the Agents on every managed server to the new version, so that you can use the new features in the newly-upgraded core.

Server Automation features continue to work on a managed server even when it is running an older Agent. However, new features in the new versions might not be available for that server.

Refer to the SA Release Notes for the new version for information about the compatibility of new features with older agents.

You can upgrade the Agents on managed servers in the following ways:

- Use the Agent Installer command to install a new Agent on one server at a time. See Agent Install Command for information on how to use the Agent Installer.
- Use the Agent Upgrade Tool to upgrade Agents on groups of servers. Running the tool upgrades deployed Agents on managed servers. You can run the script simultaneously on many servers to upgrade large groups of Agents.

The Agent Upgrade Tool has the following characteristics:

- It is a command line interface that provides a flexible mechanism for selecting servers to upgrade, and for monitoring and reviewing upgrade operations.
- You can use it to upgrade many Agents on managed servers simultaneously.
- It runs within your preferred UNIX shell, allowing it to leverage the power of standard UNIX shells and text processing tools.
- You can use it to upgrade a server in any facility running Server Automation. You can run it from an OPSH shell attached to any Server Automation in any facility.

The OPSH shell is a program that authenticates users in Server Automation, starts the user's normal UNIX shell (as specified in the standard password database). Use the OPSH shell to run the Agent Upgrade Tool.

Prerequisites for Using the Agent Upgrade Tool

- Locate the appropriate OPSH RPM package in the SA Library for your platform. These packages are named beginning with "OPSWopsh".
- Download the OPSH RPM package to a core server. See "Exporting a Package" in the SA User Guide: Software Management for instructions on downloading a package.
- Install the OPSH RPM on the core server. This places the OPSH shell and the Agent Upgrade Tool in the directory `/opt/opsware/opsh/bin`.
- You need the correct permissions to upgrade Agents. Run the OPSH shell by specifying the SA `admin` user and password to ensure that you have the appropriate permissions. (Contact your SA administrator to obtain the password.)

  When you start an OPSH shell to run the Agent Upgrade Tool, the user name and password are authenticated by Server Automation
- The server where you install the `opsh` RPM must be able to resolve the name `way.<facility-domain>` to the host running the Command Engine in the facility's core. For example, if the Command Engine runs on a host in the `prod.opsware.com` domain, the servers must resolve the name `way.prod.opsware.com`. You specified the `facility-domain` when you installed the core.

Upgrading the Agent on Managed Servers

To upgrade the Agent, perform the following steps:

1. After you install the `opsh` RPM on a core server, enter the following command as root to start the OPSH shell:

`opsh [username@]facility-domain`

For example:

`opsh admin@prod.opsware.com`

See the preceding section for the name resolution requirement for `facility-domain`. See Commands for the Agent Upgrade Tool for more information on `opsh`.

2 (Optional) To obtain information about the current Agents running on the managed servers before you upgrade them, enter any of the following commands and options:

`opsh_agent query` *server-options*

(Enter this command if you want to view a report of the Agent versions running on the servers before you upgrade them.)

`opsh_agent verify` *server-options schedule-options* `\`

agent-version

(Enter this command if you want to verify the versions of the Agents running on the managed servers before you upgrade them.)

3 To upgrade Agents on specified servers, enter the following Agent Upgrade Tool commands and options:

`opsh_agent stage` *server-options schedule-options* `\`

`[--always]` *agent-version*

(Enter this command if you want to download the package for the Agent to the managed server before you run the upgrade.)

`opsh_agent upgrade` *server-options schedule-options* `\`

`[--always]` *agent-version*

4 (Optional) To review the status of the Agent upgrade, enter the following command and option:

`opsh_agent review` *session-id*

Commands for the Agent Upgrade Tool

- `opsh [username@]`*facility-domain*

  This command starts an OPSH shell and authenticates the user name against the SA facility running at the specified domain.

  If you do not specify a user name, the currently logged in user name is used. The OPSH shell prompts for a password.

  A new UNIX shell (which is attached to the specified SA core-domain) is started. (The password database for the user specifies which UNIX shell to use.)

- `opsh_agent query` *server-options*

  This command must be run from an OPSH shell started with the opsh command.

  This command queries the reported version of Agents and any staging status for the specified servers by examining data in the Model Repository.

One line is printed to stdout for each server that shows device ID, IP address, current Agent version, and any staging status.

You can specify the servers by using the `--device, --customer, --facility, and --os` options.

- `opsh_agent stage server-options schedule-options \ [--always] agent-version`

  You must run this command from an OPSH shell started with the opsh command.

  This command contacts the Agent on each specified server and instructs it to download the package for the specified version of the Agent from the Software Repository.

  If the download is successful, the staging status is written to the Model Repository for the server.

  To download the package to the server even when this command was entered previously (recorded in the Model Repository), specify the `--always` option.

  One line is printed to stdout for each server that shows the device ID, IP address, and a success or failure indicator.

  You can specify the servers by using the `--server, --customer, --facility and --os` options.

  A session is started and the session ID displays for later review. After the session ID displays, you can type `CTRL-C` and review the session later using the `opsh_agent review` command.

- `opsh_agent upgrade server-options schedule-options \ [--always] agent-version`

  You must run this command from an OPSH shell started with the opsh command.

  This command contacts the Agent on each specified server and instructs it to upgrade to the specified version. If the necessary package has not been downloaded on the server already (the `opsh_agent stage` command was entered), the package is downloaded from the Software Repository.

  If the upgrade is successful, the package is removed from the server and the staging status is deleted from the Model Repository.

  To upgrade the Agent even when the specified version of the Agent was already installed on the managed servers, enter the --always option. (The Model Repository records when Agents are upgraded on servers.)

  One line is printed to stdout for each server that shows the device ID, IP address, and a success or failure indicator.

  You can specify the servers by using the --server, --customer, --facility, and --os options.

  A session is started and the session ID displays for later review. After the session ID displays, you can type CTRL-C and review the session later by using the opsh_agent `review` command.

- `opsh_agent verify server-options schedule-options \ agent-version`

You must run this command from an OPSH shell started with the opsh command.

This command contacts the Agent on each specified server to verify that it is running the specified version.

One line is printed to stdout for each server that shows the device ID, IP address, the word OLD, NEW, or CURRENT and the actual Agent version running on the server.

You can specify the servers by using the --server, --customer, --facility, and --os options.

A session is started and the session ID displays for later review. After the session ID displays, you can enter CTRL-C and review the session later by using the opsh_agent `review` command.

- `opsh_agent review session-id`

  You must run this command from an OPSH shell started with the opsh command; although, not necessarily the same OPSH shell from which the original command was started.

  This command attaches to a running `opsh_agent stage`, `opsh_agent upgrade` or `opsh_agent verify` session running on the Command Engine. It prints the same output to stdout that the original command would have printed if the user had not typed CTRL-C and terminated the command. If the session is complete, it shows the same results that were shown when the session completed.

Options for the Agent Upgrade Tool

Server-options: `--server|-S <svr-spec> --customer|-C <cust-spec> --facility|-F <fac-spec> --os|-O <os-spec>`

If more than one of the `--customer`, `--facility`, or `--os` options is specified, only servers that match all options are selected. Any servers specified by using the `--server` option are added to (or subtracted from) the list specified by combining the `--customer`, `--facility`, and `--os` options.

Table: Options for the Agent Upgrade Tool

Long Option	Short Option	Value	Meaning
`--server`	`-S`	`<svr-spec>`	Server by device ID, IP address, or system name
`--customer`	`-C`	`<cust-spec>`	All servers associated with the customer specified by the customer ID or name
`--facility`	`-F`	`<fac-spec>`	All servers in the facility specified by the facility ID or name
`--os`	`-O`	`<os-spec>`	All servers running the operating system specified by the OS name

Schedule-options: `--when|-W when-time --until|-U until-time`

Table: Schedule Options

Long Option	Short Option	Value	Meaning
`--when`	`-W`	`<when-time>`	Start time for a stage, upgrade, verify, or test operation in the format: MM/DD/YYY-HH:MM If the `--when` option is used, the operation starts at the specified time, but the command displays a session ID and returns immediately. When you schedule an operation, you use the `review` command to review the results after the operation has run. If the `--when` option is not specified, the operation starts immediately and the command displays the output of the command.
`--until`	`-U`	`<until-time>`	End time for a stage, upgrade, verify or test operation in the format: MM/DD/YYY-HH:MM If the `--until` option is specified, the operation stops processing servers at the specified time. Any servers that are not complete are left in a consistent state; this might require that the session run past the specified time.

Miscellaneous options: `--ip|-I --always|-A --parallel|-P --theword|-T`

Table: Miscellaneous Options

Long Option	Short Option	Value	Meaning
`--ip`	`-I`	(N/A)	Display IP addresses instead of host names.
`--always`	`-A`	(N/A)	Always stage or upgrade servers even if the current version is staged or upgraded.
`--parallel`	`-P`	`<Concurrency>`	The maximum of concurrent commands. (Recommended default = 10)
`--theword`	`-T`	`<hostname>`	The host name or IP address to use

Long Option	Short Option	Value	Meaning
			when contacting the Software Repository from a server.

Example: Options for the Agent Upgrade Tool

The following table provides examples for running the Agent Upgrade Tool.

Table: Examples of Options for the Agent Upgrade Option

Example	Description
`--server 1,2`	Selects servers 1 and 2.
`--facility Y,Z`	Selects all servers (for all customers) in facilities Y and Z.
`--customer -A,-B --facility Z`	Selects all servers in facility Z except those owned by customers A and B.
`--server 1,2,-3,-4 --customer A,B --facility Y,Z`	Select servers 1 and 2 as well as all servers owned by customers A or B which are in facilities Y or Z except servers 3 and 4.
`--server 1,-2 --customer A,B --facility -Y,-Z --os SunOS 5.8`	Select server 1 and all servers owned by customers A or B, except those in facilities Y or Z and which are Solaris 5.8 machines excluding server 2.

Example: Commands and Output for Agent Upgrade Tool

```
# cd /opt/OPSWopsh/bin
# ./opsh admin@prod.opsware.com
admin@prod.opsware.com's password:
#
# ./opsh_agent verify --os "SunOS*" 14a.2.12.18
Session 37802500101L
Device ID Name/IP address Version Result Status Reason
410101L core2-1.prod.opsware.com 14a.2.12.18 CURRENT SUCCESS
^C
Interrupted review of running session 37802500101L
Use review 37802500101L command anytime to review session status
#
```

```
# ./opsh_agent review 37802500101L
Session 37802500101L
Device ID Name/IP address Version Result Status Reason
410101L d033.prod.opsware.com 14a.2.12.18 CURRENT SUCCESS
670101L dhcp-174.prod.opsware.com 14a.2.12.16 OLDER SUCCESS
1460100L emb218-37.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
20100L f001.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
10100L f002.manu.opsware.com 14a.2.12.21 NEWER SUCCESS
210100L m022.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
Session 37802500101L completed.
```

Chapter 12 Global Shell Utilities Syntax

aaa Utility

The `aaa` utility grants and revokes permissions for operations that use the OGFS. For example, the `aaa` utility grants permission for the `readServerFilesystem` operation, allowing you to browse a server's file system in the SA Client. To run the `aaa` utility, you must belong to the Administrators user group.

The permissions granted and revoked by the `aaa` utility are stored in the `/opsw/Permissions` directory of the OGFS. For details on the contents of the directory, see /opsw/Permissions Directory.

aaa Syntax

The `aaa` utility has the following syntax:

aaa shell-perm (grant | revoke) -o *`operation`* [-u *`user-group`*]

[-f *`facility`* | -c *`customer`* | -g *`device-group`* [-s | -l *`login`*]]

AAA Options describes the command options and Global Shell Operations lists the operations that can be granted or revoked the `aaa` utility.

Table: AAA Options

Option	Description
`-o` *operation*	The operation on which to grant or revoke the permission. For a list of allowed values, see the Operation column in Global Shell Operations.
`-u` *user-group*	The SA user group that is assigned the permission. This value is inferred from the current working directory if it corresponds to a user group. If it cannot be inferred, specify a user group.
`-f` *facility*	The name, ID, or path to a facility, such as: `/opsw/Facility/Chicago` Permission will be granted to all servers in this facility.
`-c` *customer*	The name, ID, or path to a customer, such as: `/opsw/Customer/Alpha` Permission will be granted to all servers that belong to this customer.
`-g` *device-group*	The name, ID, or path to a public device group, such as:

Option	Description

	`/opsw/Group/Public/Unix Servers`
	Permission will be granted to all servers that belong to this group. To specify the device group by name, omit the following:
	`/opsw/Group/`

`-l` *login*	A login account on the servers that are specified by the `-f`, `-c`, or `-g` option. On a UNIX server, for example, the *login* is the UNIX user name. Login accounts with multi-byte characters are not supported.
-s	The login account on the servers (specified by `-f`, `-c`, or `-g`) is the same as the SA user name. (Use of `-s` is also referred to as defining a reflexive permission.)

aaa Usage Rules

The following usage rules and recommendations apply to the `aaa` utility:

- For operations that are performed on a server, one of the `-f`, `-c`, or `-g` options is required.
- As a best practice, when you are granting permissions, use care when you select servers so that you do not capture more servers than you intend. This is particularly important when using the `-c` or `-f` option. For example, if you want to grant permission to the `loginToServer` operation for all servers in the `Chicago` facility as `root`, you could use the `-f` option to select all servers in a particular facility. However, this may also select Windows servers, which is probably not desired since the `root` user does not typically exist on Windows servers. In this case, you should define a public device group that only includes servers in the `Chicago` facility which are running a UNIX operating system.
- If you specify the `-f`, `-c`, or `-g` option, you must also specify either the `-s` or `-l` option. The choice of the `-s` or `-l` option depends on the policies of your organization. If users log into managed servers with generic user names (such as `root`), then you should specify the -l option. If users log into managed servers with individual user names, which are the same as their SA user names, they should specify the `-s` option.
- The `-f` and `-c` options are provided as a convenience; however, in general, it is recommended that you define permissions based on device groups instead.
- The `revoke` command can only remove a permission that was previously granted. If the permission was not previously granted, the `revoke` command has no effect.
- The `revoke` command only removes a permission for a specific user group. If a user has overlapping permissions, revoking permissions from a single user group will not prevent the user from performing that operation. For example, suppose a user belongs to two user groups that both have the `launchGlobalShell` permission. If this permission is revoked from only one of those user groups, the user still has the `launchGlobalShell` permission.

aaa Examples

The following example gives all members of the `Advanced Users` group permission to open a Global Shell session:

aaa shell-perm grant -o launchGlobalShell \

-u 'Advanced Users'

The following command allows members of the `Advanced Users` group to view the file systems as `root` of all UNIX servers:

aaa shell-perm grant -o readServerFilesystem \

-u 'Advanced Users' -g 'Public/All Unix Servers' -l root

The next example gives all members of the `Unix Admin` user group permission to log in as `root` to all servers in the `Public/Trading Servers` device group:

aaa shell-perm grant -o loginToServer -u 'Unix Admin'\

-g 'Public/Trading Servers' -l root

The following example allows the `Advanced Users` group to run commands as `root` on servers associated with the `Acme Inc` customer.

aaa shell-perm grant -o runCommandOnServer \

-u 'Advanced Users' -c 'Acme Inc' -l root

The next example removes the permission for the `Unix Admin` user group to log into servers that belong to the device group named `Public/Unix Servers`. The command applies to any login, because the `-l` option is not specified.

aaa shell-perm revoke -o loginToServer -u 'Unix Admin'\

-g 'Public/Unix Servers'

The following example allows the `Oracle Users` group to log into servers that belong to the device group `Oracle Servers` as the login `oracle`. For instance, if the SA user `joe` belongs to the `Oracle Users` group, he can log into the servers as the server user `oracle`.

aaa shell-perm grant -u 'Oracle Administrators' \

-o loginToServer -g '/opsw/Group/Public/Oracle Servers' \

-l oracle

Instead of the `-l` option, the next example has the `-s` option, which allows the `Oracle Users` group to log into servers that belong to the device group `Oracle Servers` as the login that matches the SA user name. For instance, if the SA user `joe` belongs to the `Oracle Users` group, he can log into the servers as the server user `joe`.

aaa shell-perm grant -u 'Oracle Administrators' \

-o loginToServer -g '/opsw/Group/Public/Oracle Servers' -s

Global Shell Operations (Permissions)

The actions that an SA user can perform within the Global Shell are determined by the operations specified by the `aaa` utility. Most of these operations, such as `readServerFilesystem`, can be granted on both managed servers and on a login basis. The login is the user name on the managed server, such as the Administrator user on Windows or root on UNIX.

A login is not specific to a particular platform (operating system). For example, if the permissions specify that a user can read the file system as root, then root will appear under the files subdirectory, regardless of the platform. The Server Explorer of the SA Client displays the login names that you have been authorized to access that server's file system.

The operations are listed in the `/opsw/Permissions` directory of the OGFS.

Global Shell Operations identifies and describes the server operations in Global Shell. In the table, the On Server column identifies which operations can be granted for a set of managed servers, and the On Login column identifies the operations that can be granted for specific logins (users).

Table: Global Shell Operations

Operation (Permission)	Description	On Server	On Login
`launchGlobalShell`	Launches the Global Shell.	No	No
`loginToServer`	Opens a shell session on a UNIX server. In the SA Client, this is the Remote Terminal feature that opens a terminal window for a UNIX server.	Yes	Yes
readServerComplus	Reads COM Plus objects as a specific login. In the SA Client, use the Server Explorer to browse these objects on a Windows server.	Yes	Yes
`readServerFilesystem`	Reads a managed server as a specific login. In the SA Client, use the Server Explorer to browse the file system of a managed server.	Yes	Yes
readServerMetabase	Reads IIS Metabase objects as a specific login. In the SA Client, use the Server Explorer to browse these objects on a Windows server.	Yes	Yes
`readServerRegistry`	Reads registry files as a specific login. In the SA Client, use the Server Explorer to view the Windows Registry.	Yes	Yes

Operation (Permission)	Description	On Server	On Login
relayRdpToServer	Opens an RDP session on a Windows server. In the SA Client, this is the Remote Terminal feature that opens an RDP client window for a Windows server.	Yes	No
runCommandOnServer	Runs a command or script on a managed server using a rosh operation, where that command or script already exist. In the SA Client, this is used for Windows Services when you use the Server Explorer.	Yes	Yes
runTrustedOnServer	Only for internal use by Server Automation. Do not use this operation. Server Automation uses this operation for scripts in /opsw/Script/Shared, which implement certain Server Automation features. These scripts are provided with Server Automation and cannot be created or modified by users.	Yes	Yes
writeServerFilesystem	Modifies files on a managed server as a specific login. In the SA Client, use the Server Explorer to modify the file system of a managed server.	Yes	Yes

rosh Utility

The Remote SA Shell (rosh) command makes a client connection that enables you to remotely run programs on managed servers. You invoke the rosh command from within a Global Shell session.

rosh Syntax

For servers, the rosh command has the following syntax:

rosh (-n *server-name* | -i *server-id*)[-d *dir*] [-l *login-name*]

[-s] [-t | -T] [*command*[*arg* ...]]

For network devices, the rosh command has the following syntax:

rosh (-n *device-name* | -i *device-id*) [-N] [-C *comment*]

[-L] [-P *parameters*] [-s] -[-V *variables*] [*command* [*arg* ...]]

Rosh Options and Commands describes the `rosh` options of the preceding syntax statements.

Table: Rosh Options and Commands

Option	Description
`-3`	
`-C` comment	A comment for the log of a network script invocation.
`-d` *dir*	Sets the working directory (path) on the remote server. The default is the remote user's home directory.
`-D`	
`-h`	
`-i` *server-id*	Specifies the server by its ID, which must already exist in the `/opsw/.Server.ID` directory.
`-l` *login-name*	Specifies the login name of the remote user who performs operations on a remote server, which must already exist in the `/opsw/Server` directory.
`-L`	The network script should be run line-by-line.
`-m`	Network device mode.
`-n` *server-name*	Specifies the server by its name, which must already exist in the `/opsw/Server` directory.
`-N`	The -i or -n option refers to a network device instead of a server.
`-P` *parameters*	Parameters for a network advanced script.
`-r`	Relays RDP data to a managed server (on Windows).
`-s` *script-name*	Treats a command as the name of a saved script that will be sent to and run on the remote server.
`-t`	Forces the remote session to run in a pseudo terminal (for UNIX servers only).
`-T`	Forces the remote session to run without a pseudo terminal (for UNIX servers only).
`-v`	
`-V` *variables*	Variables for a network command or advanced script.
`-w` *seconds*	Inactivity time out.
`-W` *seconds*	Overall time out.

Option	Description
`command [args . . .]`	Runs a program or saved script.

rosh Usage Rules

The following usage rules apply to the `rosh` program:

- Specify either the `-n` or `-i` option to log into or run programs on a managed server. These options are mutually exclusive, but if both are specified the `-i` option has precedence.
- If neither the `-n`, `-i`, and `id` options are specified, the managed server can be inferred if your working directory is at or below:

/opsw/Server/.../server-name/

Or

/opsw/.Server.ID/server-id/

- If `-r` is specified, no other option (excluding `-n` or `-i`) can be specified.
- If `-l` is not specified, the login-name can be inferred if your working directory is at or below:

/opsw/Server/.../server-name/files/login-name/

Or

/opsw/.Server.ID/server-id/files/login-name/

- If `-s` is specified and *command* is a saved shared script with a `setuid` policy, the `login-name` specified by the `-l` option will be overridden. In this case, the `-l` option may be omitted. These scripts are stored in `/opsw/Script/Shared`.
- If your working directory is not below *server*`/files/`*login-name* and `-d` is not specified, the `cwdpath` defaults to the home directory for *login-name*. To default to the home directory, you must specify `-l`.
- For network scripts, if your current working directory is below a network device directory in the OFGS, you do not need to specify the device with `-N`, `-n` or `-i`. The network device is implied by the current working directory.
- For network scripts, if the full path of the script is not specified, `rosh` uses the search path indicated by the `NETWORK_SCRIPT_PATH` environment variable. If this variable is not set, `rosh` searches for the script in these directories:

/opsw/Script/Network/Command/

/opsw/Script/Network/Diagnostic/

/opsw/Script/Network/Advanced/

rosh Operations

The `rosh` command establishes a client connection that enables you to remotely run programs on managed servers. The SA Global Shell feature provides the following modes of operation for

`rosh`:

- **jump**: This operation starts a shell session in a pseudo-terminal on a managed server. This mode operates when you do not use the `-s` option and when you do not specify a command or a script. You must have the `loginToServer` permission on the managed server to jump.
- **reach**: This is a remote execution of commands that are native to the platform (operating system) of the managed server. This mode operates when you specify a command. You must have the `runCommandOnServer` permission on the managed server to reach.
- **push**: This is a remote execution of a script on a managed server. The script is stored in the OGFS and is sent to the managed server by `rosh`. You must have the `runCommandOnServer` permission on the managed server.

rosh Examples

The following examples illustrate what these operations look like for an SA user named `psi` at this path:

/opsw/Server/@/salish.snv1.corp.opsware.com/files/root/etc

[psi@m168 etc](538) $ uname -n; id; pwd

m168.dev.opsware.com

uid=59796(psi) gid=59796(psi) groups=59796(psi)

/opsw/Server/@/salish.snv1.corp.opsware.com/files/root/etc

The `rosh` jump command would display the following information about the managed server:

[psi@m168 etc](539) $ rosh

[root@salish etc]# uname -n; id; pwd

salish.snv1.corp.opsware.com

uid=0(root) gid=0(root)

groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),12(mail),7(lp),4(adm),9(kmem),6(disk),5(tty),3(sys),2(daemon),8(mem)

/etc

[root@salish etc]# logout

The `rosh` reach command displays the following information about the managed server:

[psi@m168 etc](541) $ rosh "uname -n; id; pwd"

salish.snv1.corp.opsware.com

uid=0(root) gid=0(root)

groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),12(mail),7(lp),4(adm),9(kmem),6(disk),5(tty),3(sys),2(daemon),8(mem)

/etc

The `rosh` push command displays the following information about the managed server:

[psi@m168 etc](544) $ cat /tmp/who.sh

#!/bin/sh

uname -n

id

pwd

[psi@m168 etc](543) $ rosh -s /tmp/who.sh

salish.snv1.corp.opsware.com

uid=0(root) gid=0(root)

groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),12(mail),7(lp),4(adm),9(kmem),6(disk),5(tty),3(sys),2(daemon),8(mem)

/etc

The following example runs a script on a network device:

$ cd /opsw/Network/@/sw-ee-1-2b

$ rosh -s -C 'Updating device location' \

-V 'Location=Opsware - Sunnyvale' 'Set Location'

run script task 8725081 completed successfully.

Results:

Script 'Set Location for Cisco IOS configuration (for drivers: Cisco switches, Catalyst 2950, 3550, 3750 & 8500 series, IOS version 12.x)' completed.

swenc Utility

The `swenc` command enables you to switch the character encoding within a Global Shell session.

swenc Syntax

The `swenc` command has the following syntax:

swenc [-e *`encoding`*] [-T {on | off}] [-E] [-x] [-c *`command`*]

Swenc Options describes the `swenc` options.

Table: Swenc Options

Option	Description
`-c` *command*	Executes *command* and exits, reverting the session encoding to its previous state.
-E	Lists the valid character encodings.
`-e` *encoding*	Changes the character encoding of the current session.
`-T {on | off}`	Turns on or off the transcoding of data from the UNIX managed server. (Data from Windows servers does not need to be transcoded.) See Transcoded Data in a Managed Server.
-x	Prevents the launching of a sub-shell.

swenc Usage Rules

The following usage rules apply to the `swenc` utility:

- If you specify no options, `swenc` displays the character encoding and transcoding mode of the current session.
- Unless you specify the `-x` option, `swenc` starts a new sub-shell, which uses the encoding specified with the `-e` option. To leave the sub-shell and revert to the previous encoding, enter `exit`.
- Changing the encoding with `swenc` affects all processes in the current session, including background processes. If you change the encoding while background processes are running, the background processes might encounter errors.
- The `swenc` command affects only the current Global Shell session. For example, if you run the `rosh` command after the `swenc -e` command, the `rosh` command does not inherit the encoding that you changed with the `swenc` command.
- The `swenc` command does not change the working directory of the session, unless the working directory contains path names that cannot be represented in the new encoding. In this case, the working directory is the user's home directory.
- If you change the character encoding, make sure that the encoding of the terminal application that hosts the Global Shell and Remote Terminal sessions is set properly. To view or change the terminal client, go to the Terminal and Shell Preferences of the SA Client.

Chapter 13

OGFS Directories

Directories in the OGFS

The SA Global File System (OGFS) is accessible from within a Global Shell session. Many directories contain similar files. The `id` file contains the Server Automation unique identifier (primary key) for the object represented by the directory. The `attr` directory contains text files that describe the attributes of the managed server. The `info` file is deprecated in Server Automation 6. Instead of the `info` file, use the files in the `attr` directory. The `self` file represents this specific server object (instance). The `method` directory contains executables that invoke the methods in the SA API. For details on the executables in the `method` directory, see the SA Platform Developer Guide.

In the directory listings that follow, the italicized text represents variable paths (specific instances of objects in the data model). For example, *server-1* is the name of a specific managed server. The italicized text in parentheses contains comments.

root (/) Directory

At the `root` level of the OGFS is a directory for each SA user. Each user directory and all files and directories under it are visible only to processes in an authenticated session. Each SA user has the following private directories:

- A home directory which is at `/home/`*user-name* (SA user name)
- Temporary directories located at `/tmp`, `/var/tmp` and `/usr/tmp`

Each user's home directory contains a `public` directory (`/home/`*user-name*`/public`) which is readable by all other SA users and can be used to share files with other SA users. The `root` directory has the following structure:

/. (root)

bin/

dev/

etc/

home/

lc/

lib/

opsw/

opt/

proc/

sys/

tmp/

usr/

var/

/opsw Directory

The `opsw` directory represents the data model of Server Automation. For example, the `/opsw/Customer` directory represents customer objects in the data model. Global Shell scripts and other client applications can navigate within the data model in the OGFS. Except for the `api` and `bin` directories, all of the directories under the `opsw` directory represent objects. The api directory contains executables that invoke methods on the Server Automation API. The `bin` directory contains Global Shell utilities such as `rosh` and `aaa`.

For Server Automation, the top level of the `opsw` directory has the following structure:

/opsw/

  api/

Application/

.Application.ID/

bin/

Customer/

.Customer.ID/

Facility/

.Facility.ID/

Group/

.Group.ID/

Hardware/

.Hardware.ID/

  Library/

  .Library.ID/

NetModel/

NetOS/

NetType/

Network/

.Network.ID/

OS/

.OS.ID/

Realm/

.Realm.ID/

Script/

Server/

.Server.ID/

ServiceLevel/

.ServiceLevel.ID/

The ID directories organize objects by their unique SA identifier. These directories are equivalent to those organized by name. For example, if a server with an ID `10043` is named `m44.opsware.com`, then the following directories contain the same information:

/opsw/.Server.ID/10043

/opsw/Server/@/m44.opsware.com

If the NA is installed, the `/opsw` directory also contains several network directories. See Network Directories.

/opsw/Server Directory

The `Server` directory not only contains information about managed servers, but also organizes the servers by their associated objects. For example, the `/opsw/Server/@Group` directory organizes servers by device group.

At the top level, the /opsw/Server directory has the following structure:

/opsw/Server/

@/

server-1/

server-2/

. . .

@Application/

Application Servers/

Database Servers/

. . .

@Customer/

customer-1/

customer-2/

. . .

@Facility/

facility-1/

facility-2/

...

@Group/

Private/

private-group-1/

private-group-2/

...

Public/

public-group-1/

public-group-2/

...

@Hardware/

@OS/

@ServiceLevel/

The sections that follow list some of the directory structures under `/opsw/Server`.

/opsw/Server/@ Directory

This directory contains all managed servers. The `files` directory reflects the file system of the managed server. When you modify the file system beneath the `files` directory, you do so as a specific user (such as `login-1`) of the managed server.

The `Interface` directory contains information about the network interface of the server. This directory might contain symbolic links to a network device. See /opsw/Network Directory for more information on these links.

The paths in the following directory structure are under `/opsw/Server/@`. For example, the full path name of *server-1* in the following structure is `/opsw/Server/@/`*server-1/*.

server-1/

attr

ChangeLog

complus

CPU/

0

1

...

CustAttr/

custom-attribute-1

custom-attribute-2/

...

files/

login-1/

(file system as seen by login-1)

login-2/

(file system as seen by login-2)

...

info

Interface/

network-interface-1/

...

Memory/

RAM

SWAP

metabase/

login-1/

(metabase as seen by login-1)

login-2/

(metabase as seen by login-2)

...

method/

registry/

login-1/

(registry as seen by login-1)

login-2/

(registry as seen by login-2)

...

self

Storage/

storage-device-1/

...

server-2/

...

server-3/

...

/opsw/Server/@Facility Directory

This directory filters servers according to their facility:

facility-1/

@/*(all servers in facility-1)*

server-1/

server-2/

...

@Group/

group-1/

@/ *(all servers in both facility-1 and group-1)*

server-1/

...

group-2/

...

facility-2/

...

/opsw/Server/@Group Directory

This directory does not contain network devices. This directory filters servers according to their device groups:

group-1/

@/ *(all servers in group-1)*

server-1/

...

child-group-1/

@ *(all servers in child-group-1)*

server-1/

...

child-group-2/

...

@Facility/

facility-1/

@ *(all servers in both group-1 and facility-1)*

server-1/

...

group-2/

@/ *(all servers in group-2)*

...

/opsw/Library Directory

The `Library` directory contains information about folders and the objects within folders: application policies, OS sequences, and packages. This directory has the following structure:

/opsw/*folder-path-1*/@/

AppPolicy/

app-policy-1/

attr/

method/

self

app-policy-2/

...

attr/

method/

OSSequence/

os-sequence-1/

attr/

method/

self

os-sequence-2/

. . .

Package/

package-1/

attr/

method/

self

package-2/

. . .

self

/opsw/*folder-path-2*/

. . .

Other Directories Under /opsw

This section lists, in alphabetical order, the object directories under `/opsw` other than the `Server`, `Library`, and `Net*` (network) directories.

/opsw/Application Directory

This directory is deprecated in Server Automation 6.0.

This directory represents the SA Software Tree, a hierarchical structure for organizing applications:

/opsw/Application/

Application Servers/

application-1/

@/

CustAttr/

custom-attribute-1

custom-attribute-2

. . .

.id

info

child-application-1/

@/

. . .

grandchild-application-1/

@/

...

grandchild-application-2/

...

child-application-2/

...

application-2/

...

Database Servers/

application-1/

...

Operating System Extras/

application-1/

...

Other Applications/

application-1/

...

System Utilities/

application-1/

...

Web Servers/

application-1/

...

/opsw/Facility Directory

Typically, a facility identifies the geographical location of a data center, such as a city or building. This directory contains information about facilities and the servers they manage:

/opsw/Facility/

facility-1/

@/

attr

CustAttr/

custom-attribute-1

custom-attribute-2

...

info

method

self

Server/

server-1/

server-2/

...

facility-2/

...

/opsw/Group Directory

This directory represents device groups. This directory also contains groups for network devices under the following conditions:

- NA is installed.
- The SA group has the NA-associated attribute set.
- The SA and NA group names are the same.

In the following structure, the `child-group` and `grandchild-group` reflect nested device groups:

/opsw/Group/

Public/

group-1/

@/

CustAttr/

custom-attribute-1

custom-attribute-2

...

info

Server

server-1/

server-2/

...

child-group-1/

@/

...

grandchild-group-1/

@/

...

grandchild-group-2/

...

child-group-2/

...

group-2/

...

Private/

group-1/

...

group-2/

...

/opsw/Library

This directory corresponds to the Library of folders displayed by the SA Client.

/opsw/Library/ct

folder-1/

@/

attr

method

OSSequence

self

Software

SoftwarePolicy

subfolder-1/

@/

...

subfolder-2/

...

folder-2/

@/

...

/opsw/OS Directory

This directory contains information about the operating systems defined in SA. It does not contain the actual bits for the operating systems, which are stored in the OS Provisioning Media Server. The `/opsw/OS` directory has the following structure:

/opsw/OS/

os-name-1/

Not Assigned/

@/

CustAttr/

custom-attribute-1

custom-attribute-2

...

info

Server-1/

server-1/

server-2/

...

os-name-2/

...

/opsw/Permissions Directory

This directory contains information about the Global Shell permissions. The `info` directory contains a file for each operation (permission) that can be granted with the `aaa` utility. For each user group, the `operations` subdirectory contains a text file corresponding to an operation (such as `launchGlobalShell`) that have been granted to the group by `aaa`. The contents of these text files summarize the parameters of the permissions for that operation and user group.

For example, the `readServerFilesystem` text file is in the `operations` directory of the `Advanced Users` group:

/opsw/Permissions/UserGroups/Advanced Users/operations/readServerFilesystem

The `readServerFilesystem` text file contains the following information:

Facility: C40(40) Login: sysadmin

Group: Unix Servers (2880040) Login: root

In this example, all members of the `Advanced Users` group can read the file system as user `sysadmin` on servers that belong to `Facility C40` (with ID `40`), and as user `root` on servers that belong to the device group `Unix Servers` (with ID `2880040`).

If a user group directory does not contain a text file for an operation, then the group does not have permission to perform that operation. If the text file is empty, the user group has permission to perform the operation, but the operation has no parameters. The `launchGlobalShell` operation, for example, has no parameters.

The `/opsw/Permissions` directory has the following structure:

/opsw/Permissions/

info/

launchGlobalShell

loginToServer

readServerComplus

readServerFilesystem

readServerMetabase

readServerRegistry

relayRdpToServer

runCommandOnServer

runTrustedOnServer

writeServerFilesystem

UserGroups/

user-group-1/

description

operations/

launchGlobalShell

loginToServer

. . .

user-group-2/

. . .

/opsw/Realm Directory

A realm is a logical name for a group of IP addresses that can be contacted by a particular set of SA Gateways. Typically, each Satellite and Facility has one or more distinct realms. To find out which managed servers belong to a realm, note the server names below the *realm*`/@/Server` subdirectory.

The `Realm` directory has the following structure:

/opsw/Realm/

realm-1/

@/

info

Server/

server-1/

server-2/

...

realm-2/

...

/opsw/Script/Shared Directory

This directory contains utility scripts that are included with Server Automation. These scripts are not the same as the DSE shared scripts that are accessible with the SA Client. The contents of this directory cannot be changed by end users.

/opsw/Script/

Shared/

script-1/

description

policy

source

version

script-2/

...

/opsw/ServiceLevel Directory

This directory is deprecated in Server Automation 6.0.

Service levels are user-defined categories such as Silver, Gold, and Platinum. The `/opsw/ServiceLevel` directory has the following structure:

/opsw/ServiceLevel/

service-level-1/

@/

CustAttr/

custom-attribute-1

custom-attribute-2

...

.id

inf-1/o

...

child-service-level-1/

@/

...

grandchild-service-level-1/

@/

...

child-service-level-2/

...

Server/

@/

...

service-level-2/

Network Directories

For NA, the top level of the `opsw` directory includes the following subdirectories:

/opsw/

...

NetModel/

NetOS/

NetType/

Network/

.Network.ID/

. . .

Script/Network

/opsw/Network Directory

This directory organizes the devices by their model, OS, type, and group. All network devices are in the `/opsw/Network/@` directory. The `Changelog` directory contains time-stamped events for the device. The `Config` directory contains time-stamped configuration files.

At the top level, the `/opsw/Network` directory has the following structure:

/opsw/Network/

@/

device-1/

attr/

ChangeLog/

Config/

info

method/

Module/

Port/

port-1/

.id

info

Link/

port-2/

. . .

self

Vlan/

device-2/

. . .

@Group/

@NetModel/

@NetOS/

@NetType/

The `Port` and `VLAN` directories contain Layer 2 information. Within each subdirectory of the `Port` directory, an `info` file contains duplex information and other data for a specific network port. The `Link` directory contains a symbolic link to a server interface or a port on another network device (if the MAC address to the interface or port is available). In the following example, the `eth0` under `Network` is a symbolic link to `eth0` under `Server`:

/opsw/Network/@/sw-ee-1-2b/Port/FastEthernet0_1/Link/eth0

symbolic link to -->

/opsw/Server/@/m180.mycomp.com/Interface/eth0

Similarly, the `Server` directory can have a symbolic link to the corresponding entry under `Network`:

/opsw/Server/@/x.mycomp.com/Interface/eth0/Link/FastEthernet0_7

symbolic link to -->

/opsw/Network/@/sw-ee-2-4a/Port/FastEthernet0_7/eth0

/opsw/Network/@Group Directory

This directory does not contain groups for managed servers. This directory filters network devices according to their groups:

group-1/

@/ *(all devices in group-1)*

device-1/

...

@NetModel/

@NetOS/

@NetType/

child-group-1/

@ *(all devices in child-group-1)*

device-1/

...

child-group-2/

...

group-2/

@/ *(all devices in group-2)*

...

/opsw/NetModel Directory

This directory contains subdirectories for vendors, for example, `/opsw/NetModel/Cisco`. The `/opsw/NetModel` directory has the following structure:

vendor-1/

model-1/

@/

@Group/

@NetOS/

@NetType/

model-2/

. . .

vendor-2/

. . .

/opsw/NetOS Directory

This directory organizes devices by their operating system. The `/opsw/NetModel` directory has the following structure:

family-1/

os-1/

@/

@Group/

@NetOS/

@NetType/

os-2/

. . .

. . .

family-2/

. .

/opsw/NetType Directory

This directory organizes network devices by the following types:

Firewall

L3Switch

L4to7Switch

Proxy

Router

Switch

unknown

VPN

Wireless Access Point

WirelessAP

The `/opsw/NetType` directory has the following structure:

type-1/

@/

@Group/

@NetOS/

@NetType/

type-2/

. . .

/opsw/Script/Network Directory

This directory contains utility scripts for network devices. For information about these scripts, see the NA documentation.

/opsw/Script/Network/

- Advanced/
- Command/
- Diagnostic/

Index

A

D

E

R

S

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide: Server Automation (Server Automation 10.23)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!