HP Server Automation

Standard Edition

Software Version: 10.00

Server Automation Virtual Appliance (SAVA) Installation and Administration

Document Release Date: Edition 2, September, 2013

Software Release Date: June 2013

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

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

UNIX® is a registered trademark of The Open Group.

Support

Visit the HP Software Support Online website at:

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

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

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

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

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

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

To find more information about access levels, go to:

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

Support Matrices

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

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

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

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

Documentation Updates

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

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

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

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

Product Editions

There are two editions of Server Automation:

- Server Automation (SA) is the Enterprise Edition of Server Automation. For information about Server Automation, see the SA Release Notes and the SA documentation set.
- Server Automation Virtual Appliance (SAVA) is the Standard Edition of Server Automation. For more information about what SAVA includes, see the SAVA Release Notes, the *SAVA Installation and Administration Guide* and the *SAVA at a Glance Guide*.

Documentation Change Notes

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

Date	Changes
06/2013	Original document release
09/13/2013	Updates from field feedback

Contents

1 Server Automation Virtual Appliance (SAVA) Installation Overview

HP Server Automation Virtual Appliance (SAVA), the Server Automation Standard edition, is a single SA Core, single Slice Component bundle version of enterprise-level SA running within a VMware virtual appliance. SAVA supports a slightly limited set of SA server management capabilities including OS Provisioning, Server Patching, Software Management, Application Configuration, Audit and Compliance, Virtualization Management and more.

For a list of differences between SAVA and SA Enterprise edition, see the *SAVA at a Glance Guide*.

Intended Audience

This documentation describes installing the SA virtual appliance and initial SA set up tasks including logging into the SA Client, the SA user interface. It is intended for experienced system administrators who are familiar with configuring and managing the VMware vSphere ESXi hypervisor and using the VMware vSphere Client.

This document does not provide complete instructions for using SA. Information about using the SA Client to manage servers in your facility is provided in the SA 10.0 Enterprise Edition documentation set which you can download from:

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

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

SA 10.00 Documentation

The following documents describe using SA after the virtual appliance is installed and the SA Client has been configured. You can access the document you are interested in directly by clicking the link:

- *SA Overview and Architecture*
- *SA Network Architecture Diagrams*
- *SA Support and Compatibility Matrix*
- *SA Administration Guide*
- *SA User Guide: Application Configuration*
- *SA User Guide: Application Deployment*
- *SA User Guide: Audit and Compliance*
- *SA User Guide: OS Provisioning*
- *SA Reports Guide*

- *SA User Guide: Server Automation*
- *SA User Guide: Service Automation Visualizer*
- *SA User Guide: Software Management*
- *SA User Guide: Server Patching*
- *SA User Guide: Virtualization*
- *SA Integration Guide*
- *SA Content Utilities Guide*

For your convenience, you can download the entire Server Automation Documentation Library from this link:

http://support.openview.hp.com/selfsolve/document/KM00417676/binary/SA_10.x_ALL_Manuals.html

SAVA 10.00 at a Glance Guide

The *SAVA at a Glance Guide* provides information about SA Core Components and architecture as implemented in SAVA and how SAVA functionally differs from the full SA Enterprise Edition.

Performing Tasks in the SA Client

The following are typical tasks you will perform after SAVA is installed and the SA Client is configured:

Table 1

Task	Summary	Documentation Reference
Administration		
Creating SA users and user groups	SA provides a role-based security model that allows only authorized users to perform specific operations on specific servers. For example, users can have privileges to perform OS Provisioning but not Audits or a user can be authorized to do software patching but not authorized to perform application deployment. SA provides a baseline set of users that you can use or modify to your facilities' requirements.	See the *SA Administration Guide*, Chapter 1: *User and User Group Setup and Security*
Creating SA Customers	Assigning SA customers provides a way to group your servers and provide access control boundaries.	See the *SA User Guide: Server Automation*, Chapter 2: *Creating and Managing Customers*

Table 1

Task	Summary	Documentation Reference
Setting user and user group permissions	SA provides a full set of permissions based on function, user role and user group role.	See the *SA Administration Guide*, Appendix A: *Permissions Reference*
Setting up SA Notifications	SA can send e-mail to specified addresses upon the completion or failures of jobs.	See the *SA Administration Guide*, Chapter 10: *SA Notification Configuration*
Using the SA Client		
Installing the SA Client	The SA Client is a powerful Java client for viewing managed and unmanaged servers in your facility and provides centralized access to all SA features with the look-and-feel of a Microsoft Windows desktop application.	See About the SA Client Launcher on page 21and Chapter 1: Getting Started with the SA Client in the *SA User Guide: Server Automation*.
Exploring the SA Library	The SA Library allows you to organize your server resources (packa ages, scripts, software policies, OS build plans, and many other server objects) in a folder hierarchy.	See the *SA User Guide: Server Automation,* Chapter 2: *Exploring the SA Library*
Server Discovery and Management		
Finding managed and unmanaged 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.	See the *SA User Guide: Server Automation*, Chapter 3: *Exploring Servers and Device Groups in the SA Client*
Bringing an unmanaged server under SA management	SA can scan your network to discover servers it both manages and does not manage. Once discovered, you can bring an unmanaged server under SA management by installing an SA Agent. The agent is not required for virtual servers. When an SA Agent is installed on a physical server, the agent registers the server with the SA Core which then adds that server to its pool of Managed Servers. The SA Agent receives user initiated commands from the Core and takes the appropriate action on the server it is installed on, such as software installation and removal, software and hardware configuration, server status reporting, auditing, and so on.	See the *SA User Guide: Server Automation*, Chapter 4: *Installing and Managing Server Agents*

Table 1

Task	Summary	Documentation Reference
Bringing virtual servers under SA management	SA virtualization management provides visibility into your datacenter and all your physical and virtual machines (VMs), compliance with all your regulatory and enterprise policies and Control over your entire virtual environment.	See the *SA User Guide: Virtualization*
Audit and Compliance		
Performing a server audit and checking compliance	SA audit and remediation allows you to define audit policies, which servers to audit and schedule audits.	See the *SA User Guide: Audit and Compliance*
Using Custom Attributes		
Using Custom Attributes	The SA Client provides a data management function by allowing users to set custom attributes for servers. These custom attributes include setting miscellaneous parameters and named data values. Users can write scripts that use these parameters and data values when performing a variety of functions, including network and server configuration, notifications, and CRON script configuration.	See the *SA User Guide: OS Provisioning*, Chapter 4: *Defining Custom Attributes*
OS Provisioning		
Introduction to OS Provisioning	SA OS Provisioning allows you to provision operating systems to bare metal servers and bring them under SA management.	See the *SA User Guide: OS Provisioning*
Setting up an OS Provisioning Media Server	You must set up an external OS Provisioning media server.	See The SAVA OS Media Server for OS Provisioning on page 31

Table 1

Task	Summary	Documentation Reference
Creating OS Build Plans (OSBPs)	OS Build Plans (OSBPs) allow you to specify the operating system to install and how a server is configured. OSBPs also allow you to specify custom server attributes, reboots, and more.	See the *SA User Guide: OS Provisioning*, Chapter 4: *Creating OS Build Plans* See also the OS Build Plan `README.html` file available in the SA Client online help: `Help > Online Help > OS Provisioning > Defining Installation Profiles, Build Plans and OS Sequences > Creating OS Build Plans > Sample OS Build Plan Usage Instructions` **Note**: The readme file provides information about the baseline OSBPs that are provided with SAVA and also contains instructions about copying and modifying the baseline OSBPs for your environment.
SA-supplied Boot Images	SA provides many supported boot images for OS Provisioning. These images are found in the SA Client Library.	See the *SA User Guide: OS Provisioning*, Chapter 5: *SA OS Provisioning-supplied CD Boot Images*
Network Booting A Remote Server	You can remotely boot new servers over a network in both DHCP and non-DHCP environments. OGFS, PXE and OGFS boot are supported in certain cases.	See the *SA User Guide: OS Provisioning*, Chapter 5: *Booting Servers Remotely*
Running OS Build Plans	After the OS Build Plan is configured, it can be run against a server.	See the *SA User Guide: OS Provisioning*, Chapter 5: *Using an OS Build Plan for OS Provisioning*
Software Management		
Performing Software Management	With SA policy-based software management you can automate software installation and application configuration, and ensure that managed servers are compliant with software policies.	See the *SA User Guide: Software Management*

Table 1

Task	Summary	Documentation Reference
Application Deployment		
Performing Application Deployment	SA Application Deployment reduces the complex communications necessary to deploy applications by providing a single point of access where everyone involved can view or enter data that is relevant to them and to their role. Application Deployment also integrates with other HP Software technologies to ensure that applications are successfully moved into Production.	See the *SA User Guide: Application Deployment*
Application Configuration		
Performing application configuration	SA allows you to manage configuration files, including XML configuration files, from a central location and easily propagate changes and updates across multiple servers in your data center. You can manage a single configuration file such as the `/etc/hosts` file on UNIX systems, or multiple complex configuration files associated with an application, such as the configuration files associated with a large business application such as WebLogic or Websphere.	See the *SA User Guide: Application Configuration*

SAVA and SA Video Tutorials

After you have logged into and launched the SA Client, you can access a number of video tutorials that walk you through typical task you will perform in SA. Click on Help in the SA Client and select the Getting Started link.

You can also download a local copy of the tutorials at this link:

http://support.openview.hp.com/selfsolve/document/KM00417668/binary/SA_10_QuickStart.html

2 Initial SA Virtual Appliance Installation

Overview of Initial Installation Steps

1. Ensure your host server meets the system requirements: System Requirements on page 15.
2. Installation: Installing SAVA on page 17
3. Start your appliance: Starting your Appliance for the First Time on page 18.
4. Initial appliance login: Initial Login and Appliance Networking on page 18.
5. Access from browser: Accessing SAVA from a Browser for the First Time on page 20.
6. Set up your Media Server: The SAVA OS Media Server for OS Provisioning on page 31.
7. Install the SA Client: About the SA Client Launcher on page 21

After you complete the initial installation of the SAVA virtual appliance described in this chapter, you must also complete the tasks in Chapter 3, “Post-Installation Setup Tasks”.

System Requirements

Your host server must have the following environment to install and run the SA virtual appliance:

- VMware ESXi version 5.0, 5.0 UI, or 5.1.

Ensure that your host server meets the VMware requirements for running 64-bit guest VMs on the ESXi host.

- VMware vSphere Client with VMware Tools installed.

Ensure that your host system is sized, installed, and configured per the vSphere Installation and Setup guide, which can be found on the VMware vSphere Documentation website.

- A minimum of 4 CPUs to accommodate the VM and at least 16 GB memory allocated for the VM.

These are minimum CPU and memory requirements. If you will be doing multiple concurrent deployments (more than 8 at a time), or will be managing a large numbers of servers (over 1000) then the recommended optimal configuration is 8 CPUs and 30 GB of memory.

- 504 GB of disk space allocated for the VM. HP recommends thin provisioning for the virtual disk. There should be room for the virtual disk to grow up to the provisioned (i.e. reserved) size of 500GB + any hypervisor overhead. See:

  http://www.vmware.com/files/pdf/VMware-DynamicStorageProv-WP-EN.pdf

  The standard VM virtual disk configuration is thin-provisioned. This means you must allow for appliance growth up to 504 GB depending on usage and content.

- One network adapter

The SAVA template comes configured with a single network interface. After you configure your appliance, the appliance network interface must be able to access the target servers' network.

- Appliance networking requirements

  The appliance requires two static IP addresses. Both of these IP addresses will be assigned to the appliance's single NIC. They must be on the same subnet. The two IP addresses must be able to communicate with all target servers and their iLO management processors. If your iLOs are on a different network from your deployment network, you will need to route traffic from your appliance to the iLO.

  If you host multiple appliances or other VMs on the same host, you must scale the requirements as needed.

Pre-Installation Checklist

You should have the following information and resources available to you before you begin the SAVA installation.

- Access to a number of available IP addresses appropriate for your facility
- An IP address to be assigned as the Appliance IP address
- An IP address to be assigned as the Deployment IP address (the address for the SA instance)
- Access to a VMware vSphere client as administrator with the ability to create VMs
- Access to and IP address for a DHCP server
- Access to and IP address for a DNS server
- A valid subnet mask address
- A valid gateway address
- The latest version of Adobe Flash must be installed on the machine hosting the SA Client

Sample SAVA Installation/Configuration Checklist

To ensure that you have all the information needed for installing/configuring SAVA, you can create an installation checklist of your own. For example:

1	Network					
2	Item	IP	Netmask	Gateway	HW Address	DNS
3	Deployment Server	192.168.100.6		255.255.255.0		
4	SA Standard Server	192.168.100.6		255.255.255.0		
5	ESX1	savavm001.example.net				
6	ESX2					
7	ESX3					
8	Deployment Range					
9						
10	User ID					
11	Administrator	administrator / password1				
12	Admin	opsware_admin				
13	<vCenter>					
14	<HPLN user>					
15						
16	OS media	Mount Point	user/PW	LIC Key		
17	Windows 2003					
18	Windows 2012					
19	Windows 2008R2					
20	RHEL 5					
21	RHEL6					
22	ESXI 5					
23	ESXI5.1					
24						

Installing SAVA

1. Ensure that you have the SAVA multipart installation zip file.

   The SAVA Multipart installation zip file must be concatenated into a single file before it can be extracted. See the SAVA readme file for concatenation instructions on Windows or Linux.

2. Extract the VM template folder from the zip file.
3. Start VMware VSphere.
4. From VMware vSphere, select **File** > **Deploy OVF Template...**, then browse to and select the SAVA `.ovf` file inside the VM template folder.
5. Use the procedure documented in the VMware vSphere documentation to deploy the VM. Do not select Power on for this virtual machine after creation.
6. Select Edit virtual machine settings from the Getting Started vSphere page.

   Verify that your SAVA VM meets the following requirements:

   - At least 16 GB of memory
   - 4 CPUs
   - 504 GB of disk space (HP recommends thin provisioning for the virtual disk. There should be room for the virtual disk to grow up to the provisioned (ie reserved) size of 500GB + any hypervisor overhead.)
   - 1 network adapter configured to have access to the target servers
   - From **Options** > **VMware Tools**, ensure that “Synchronize guest time with host” is checked.

   If your appliance does not meet the requirements listed above, edit the VM appropriately.

7. The SA virtual appliance is now installed and ready for its initial start up.

Starting your Appliance for the First Time

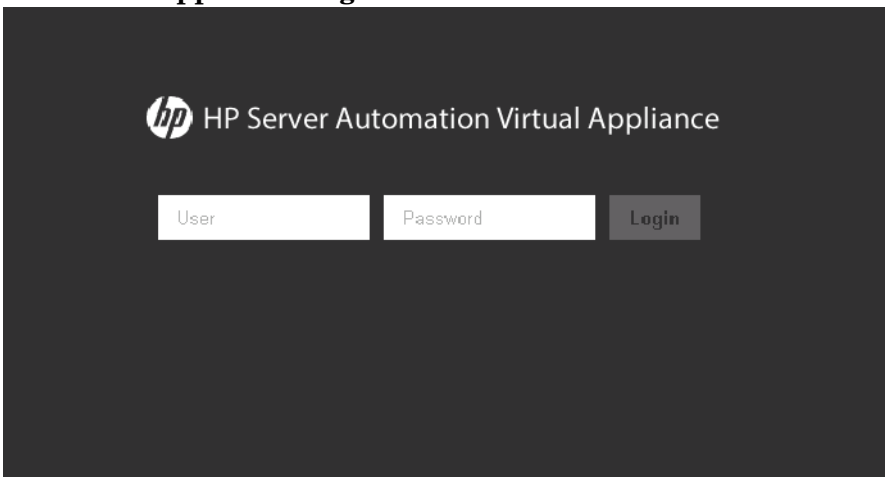
Before powering on your virtual appliance, verify the date and time are set properly on your VM host system. Be sure to maintain an accurate time on the VM host system, for example using NTP, because the VM guest will synchronize with that time.

1. In VMware vSphere, power on your SA virtual appliance by right clicking on the SAVA VM and selecting **Power** > **Power On** or by selecting SAVA from the vSphere Client Getting Started tab.
2. Set the display in vSphere to **Home** | **Inventory** | **VMs and Templates**.
3. Navigate in the tree view on the left to your SAVA VM.
4. Select your SAVA VM and right click. From the context menu, select Open Console. If the VM has not yet been started, when the console opens, click the Play button (green arrow).
5. After a few minutes, the SAVA license agreement appears, click Agree to continue.
6. The HP Support enablement screen appears. The default setting is Enabled. Click OK to continue. If you disable the HP Support console login then HP Support personnel will not be able to log in to your appliance if needed. You can enable/disable support console login through the appliance Settings menu.
7. You now see the appliance login screen. You can now log in to the SA virtual appliance for the first time.

Initial Login and Appliance Networking

1. When you start SAVA for the first time, the SA virtual appliance management login screen will be available from the vSphere Client Console tab. Log in using the user name `administrator` and password `admin`.

Figure 1 SA virtual appliance Login Screen



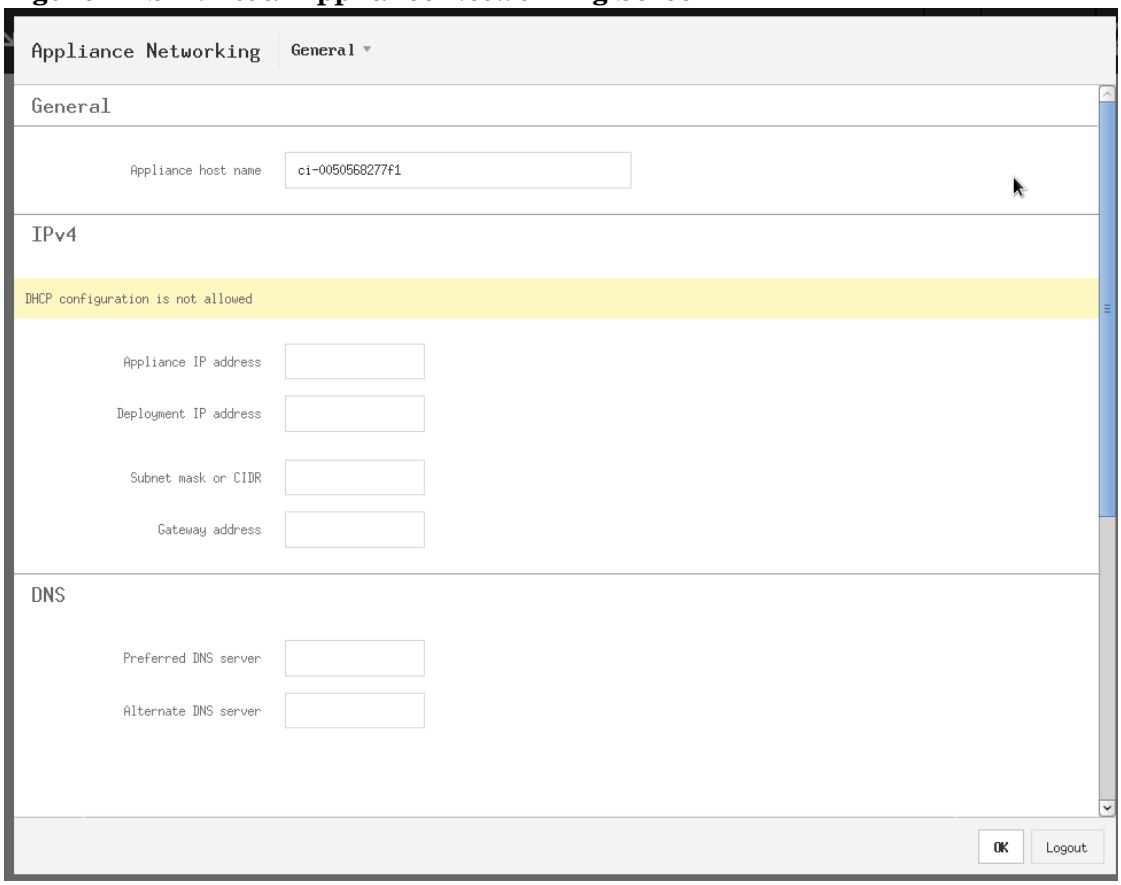
This screen is the login for the SA virtual appliance administration interface; it does not start the SA Core's SA Client interface. See About the SA Client Launcher on page 21 for information about downloading, installing and using the SA Client to access the SA Core.

Tip: If necessary, you can release your cursor from the vSphere Client Console with Ctrl-Alt. You can restart the first time set up in the vSphere Client Console using Ctrl-Alt-Backspace.

2 You are required to specify a new password for the account.

3 Next, you see the SA virtual Appliance Networking Settings screen. You must provide the network settings for the SA virtual appliance.

Figure 2 SA virtual Appliance Networking Screen



4 Enter the appliance networking information as follows:

General

— **Appliance host name**: The name of the SA virtual appliance host. From a supported browser, you can navigate to the SA virtual appliance using this name or by using the appliance IP address.

IPv4

— **Appliance IP address**: The IP address you are assigning to the SA virtual appliance. Use this IP address to browse to the appliance from a supported browser.

— **Deployment IP address**: The IP address used by the deployment engine within SAVA which is used to communicate with a target server's deployment interface IP address and its iLO IP address. This should be on the same network as the SA virtual appliance IP address.

If, after initial set up, you change this IP address from the SA virtual appliance management screen, the appliance will become unavailable for up to 20 minutes while it is reconfigured, followed by an appliance reboot. In addition, all target servers' agents will have to be updated with the new IP address. Ensure that this IP address is set to a valid value.

- **Subnet mask or CIDR**: This field is required if you are specifying a gateway. This is the IPv4 mask representing the bits reserved for network identification (for example, 255.255.255.0), or the Classless Internet Domain Routing (CIDR) mask representing the number of bits reserved for network identification. Valid CIDR values are 1 to 30, inclusive.
- **Gateway address**: This field is not required but HP strongly suggests configuring it to ensure access to SAVA. This is the IP address for the network interface on your router.

DNS

- **Preferred DNS Server**: Enter the IP address of your DNS server.
- **Alternate DNS Server**: If you have an alternate DNS server, enter the IP address here, otherwise you can leave this field blank.

5 Select OK or Logout:

- **OK**: Apply the information you've supplied. There will be a delay of up to 30 minutes while the SA virtual appliance configures.
- **Logout**: Exit the appliance without saving the networking information. The next time you log in you will be taken directly to the SAVA Networking screen.

The password you specified for the account administrator will be applied even if you select Logout.

After your initial login to the SA virtual appliance from the vSphere Console, you can use a browser to access the appliance. Alternatively you can access the appliance from the Console.

When you click OK to apply the networking configuration, the appliance will be unavailable for up to 30 minutes. Do not use or attempt to use the appliance until the Login screen appears again. At that time, you can close the ESXi console window and access the appliance and the embedded SA instance using a web browser or the SA Client.

Accessing SAVA from a Browser for the First Time

SAVA supports the following browsers:

- Google Chrome – latest version
- Windows Internet Explorer version 8 or later
- Mozilla Firefox – latest version

To access the SA virtual appliance Administration screen from a supported browser, enter the host name or IP address you entered for Appliance IP address.

See Chapter 3, "Post-Installation Setup Tasks" for information about installing the SA Client which is used to access Server Automation.

3 Post-Installation Setup Tasks

After you have your SA virtual appliance set up and running, you must perform the following tasks.

- Install the SA Client, see Install the SA Client Launcher on page 22
- Familiarize yourself with the SA Client, see Running the SA Client on page 23
- Configure an OS Media Server, see The SAVA OS Media Server for OS Provisioning on page 31
- Configure a DHCP server, see Configure DHCP on page 38

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 log in to and download the latest version of the SA Client.

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 User Interface on page 24.

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.

The SA Client is supported on the following Microsoft operating systems:

- Windows Server 2003
- Windows 2000
- Windows XP
- Windows Vista

- Windows Server 2008
- Windows 7

The minimum system requirements to run the SA Client are as follows:

- 1 GB of DRAM.
- 0.5 GB of disk space each for the SA Client and the SA Client Launcher.
- If using the SA Client to connect to a core with a residential DSL connection, a minimum 384 Kbps connection is recommended.
- You must be logged in as a user with sufficient permissions to install software on the computer. (You do not need to be an administrator user to install the launcher).
- Ensure that there are no running instances of the Launcher (if necessary, use the Windows Task Manager and kill all instances of `javaw.exe`).

You must download and install the SA Launcher (see the download link on the SAS Web Client Main Page). In order to install the launcher, you must be a Windows user that has permission to install applications on your system.

If you are upgrading, you must uninstall the previous SA Client Launcher version (using the Windows uninstall utility), and install the latest version.

Install 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.

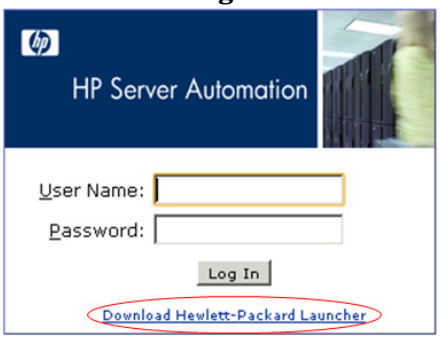
b. Ensure that there are no running instances of the Launcher.

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 IP address you entered for Deployment IP address as the URL. This displays the SA Web Client login page along with a link to download the SA Client launcher, as shown in Figure 3.

Figure 3 Downloading the SA Client Launcher



2 On the SA Web Client login page, click the Download Hewlett-Packard Launcher link.

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 HP 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 log in to the SA Client, at the login window, enter the username `admin` and the password `opsware_admin`, and the Deployment IP address, as shown in Figure 4.

Figure 4 SA Client Login Window

The user name is not case sensitive. If you do not specify a port with the host:port notation, port 80 is used to download the SA Client.

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 would like to differentiate between the core you log in to and the core from which 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 User Interface on page 24.

3 Click **Log In**.

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

If the SA Client does not appear, check your proxy settings and other settings. See SA Client Launcher Advanced Options in Chapter 1 of the *SA User Guide: Server Automation*.

Creating Super Administrators and Super Users

After logging in, the first task you must perform is to create a Super User. After doing so, log back into the SA Client as the Super User. You will see the SA Client as described in SA Client User Interface on page 24. You can then create other users with differing task permissions. based on your facility's needs.

A **Super Administrator** is an SA user who can create users and user groups, specify permissions for user groups, and assign users to user groups. Super administrators can also manage customers and facilities, as well as set folder permissions. The SA installer creates a single default user, the super administrator named `admin`. The password for `admin` is specified during the installation and should be changed immediately afterwards.

To create a Super User, create a default user and add it to the Superusers predefined user group. For more information, see Managing Users - SA Client, Creating a New User, Predefined User Groups and Adding a User to a User Group in Chapter 1 of the *SA Administration Guide*.

A **Super User** is different from a Super Administrator and is not automatically a Super Administrator. A Super User is any user who belongs to the predefined Superusers group. A Super User has full permissions to perform all actions except create and modify users and user groups.

However, a Super User does not automatically have access to any servers. You would need to give access to facilities, customers and device groups as described in Setting Resource Permissions - Facilities, Customers and Device Groups in Chapter 1 of the *SA Administration Guide*.

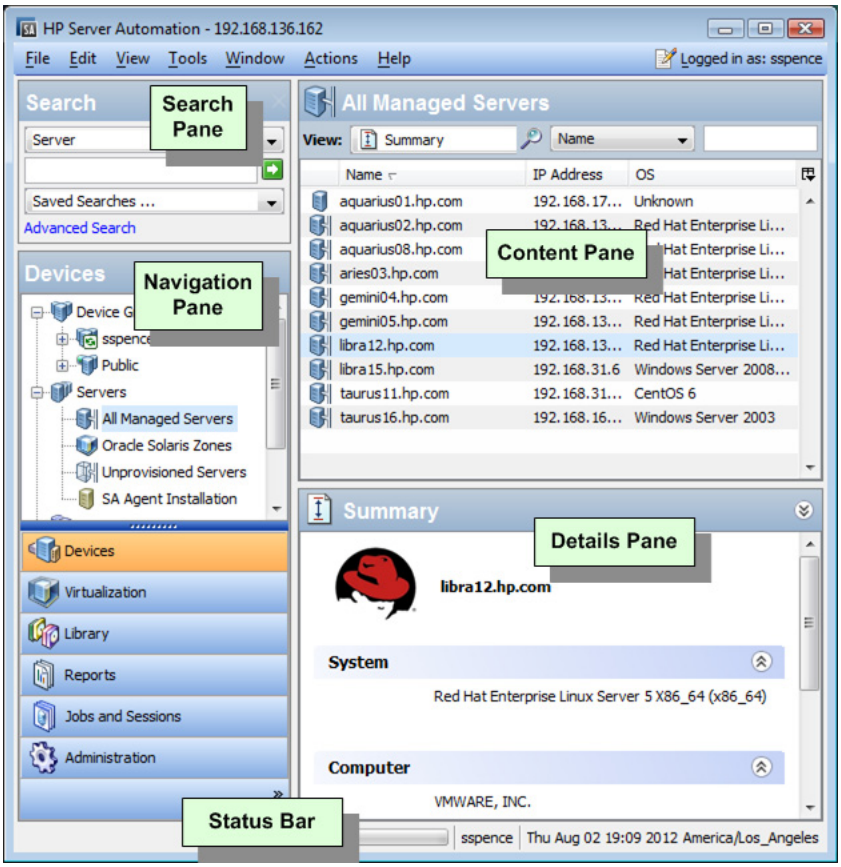
SA Client User Interface

See also Chapter 1: "Getting Started with the SA Client" in the *SA User Guide: Server Automation*.

The SA Client user interface has six main areas as shown in Figure 5.

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

Figure 5 SA Client User Interface



Menus

The SA Client includes the following menus:

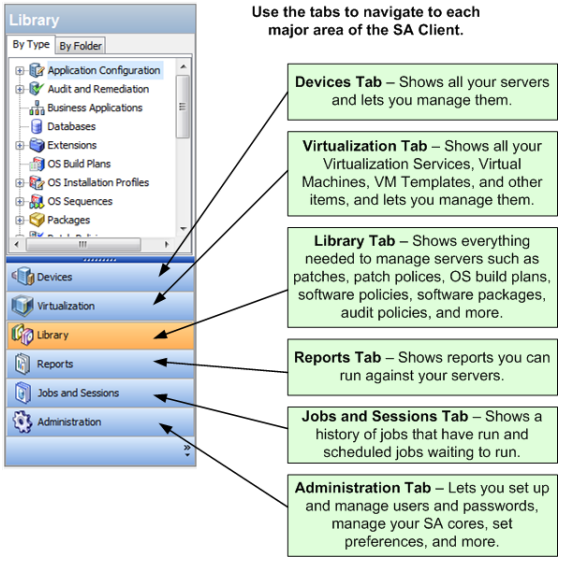
- **File**: This enables you to open a new SA Client window, or close the current window, or exit all open SA Client windows.
- **Edit**: This enables you to cut, copy, paste, delete text, and copy SA Client URLs.
- **View**: This refreshes the current view and shows the latest information from the core 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. (The About SA Client menu provides version and system information.)

Navigation Pane

The Navigation pane shown in Figure 6 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.

Figure 6 Navigation Pane/Search Pane

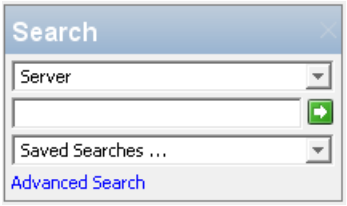


The Search pane allows you to search for any information in HP Server Automation, such as servers, device groups, folders in the SA library, jobs, software and software policies, patches and patch policies, application configurations, database and storage systems, audits, and snapshot results.

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” in the *SA User Guide: Server Automation*.

Figure 7 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

Features Not Supported In SAVA

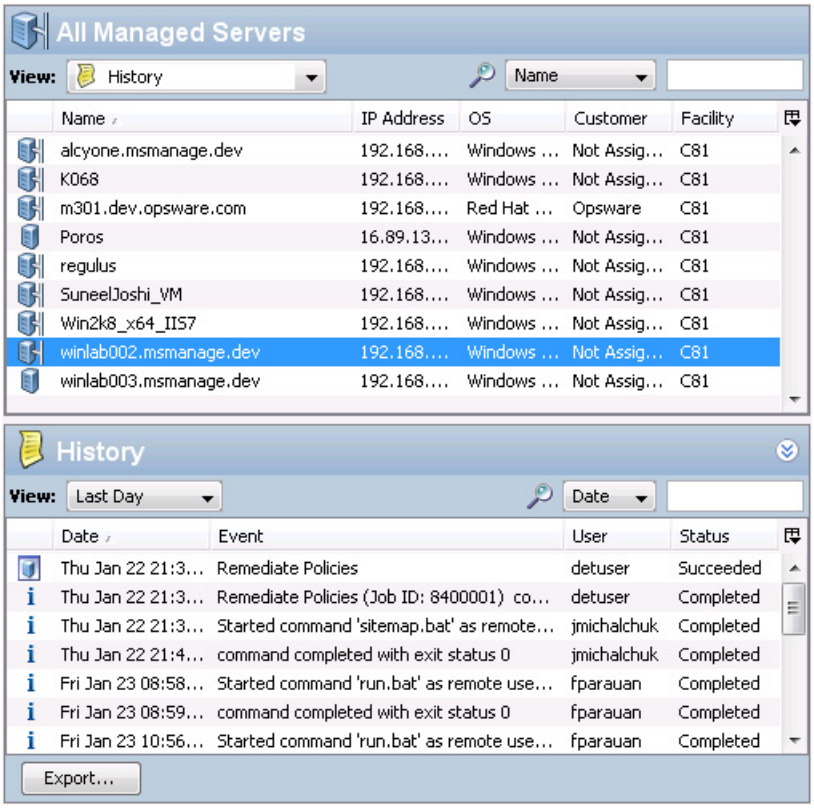
The following SA features are not supported in SAVA and menu selections will be greyed out:

- APX development
- Bandwidth Configuration Management (bandwidth throttling)
- Business Service Automation Essentials (BSAE) reports for SA
- Console access through SSH login
- Deployment automation
- Delegated authentication
- Multi-core mesh
- Network Automation
- SA Client reports
- Software discovery server module
- Server Storage Integration (SSI)

Views in the Content Pane

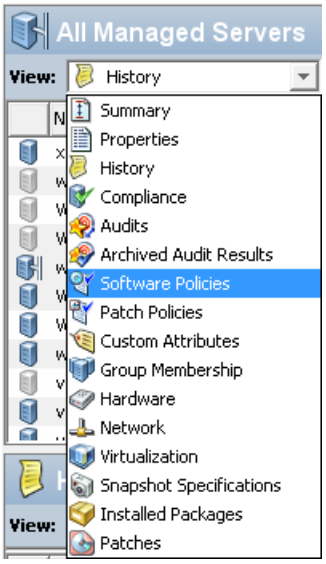
Figure 8 is an example of the Content pane for managed servers. You can perform actions on features in the Content area using the Action Menu, or you can right-click to perform various actions or double-click to open.

Figure 8 Content Pane Showing the Server History View



Using 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 Figure 9.

Figure 9 View Drop-down List

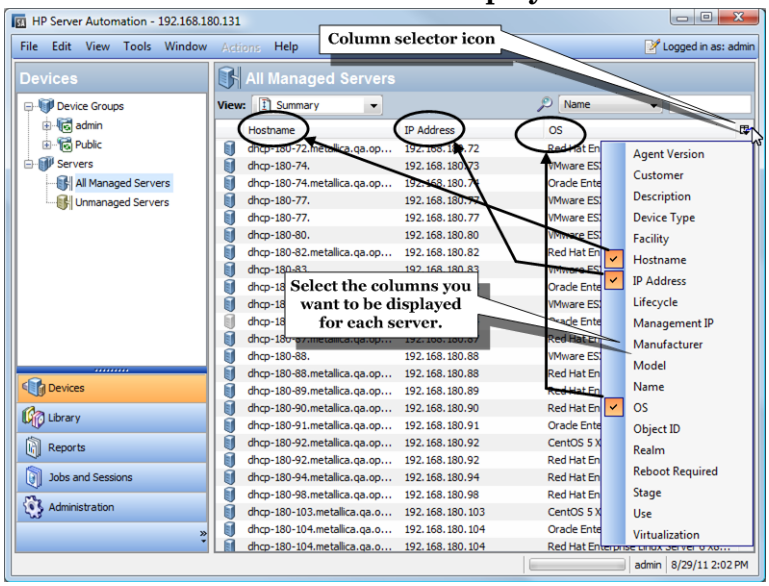


Columns in the Content Pane

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 Figure 10 below.

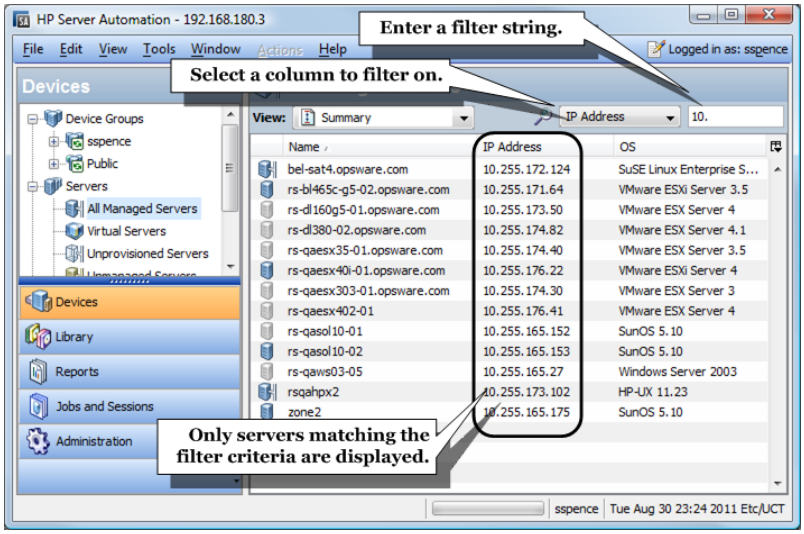
Figure 10 Column Selector - Columns Displayed for Each Server



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 Figure 11 below.

Figure 11 Filter Tool



Details Pane

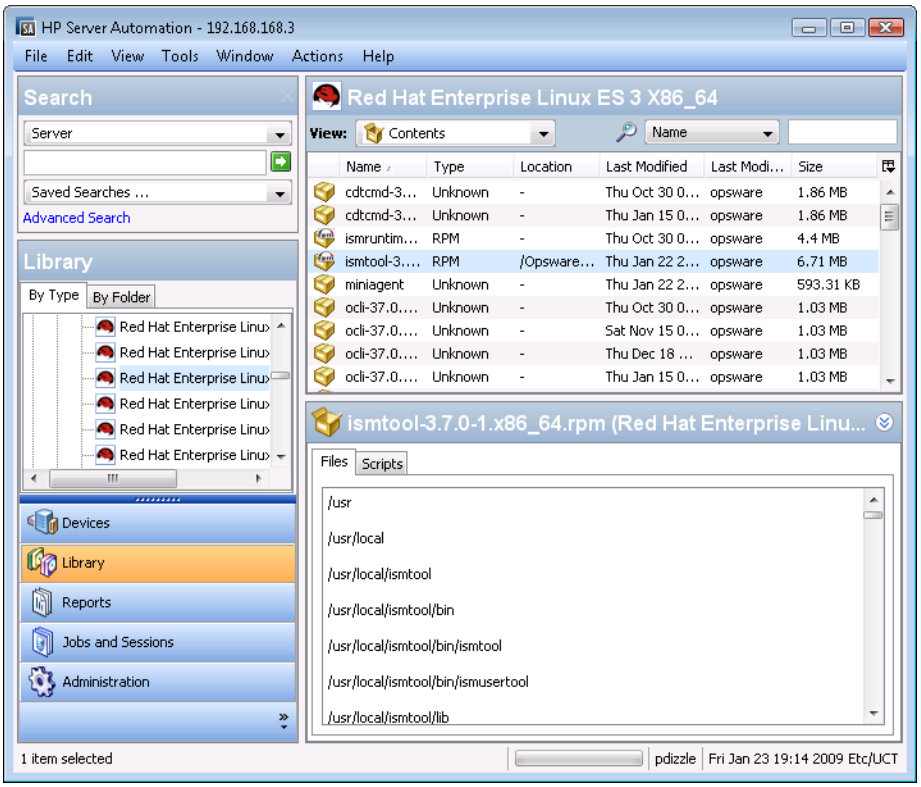
The Details pane allows you to preview information about servers, device groups, patches, and patch policies selected in the Content pane without having to open a new window.

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 Figure 12.

Figure 12 SA Client Showing Package Contents View in the Details Pane



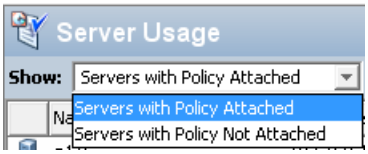
To view other types of information about the selected patch, from the View drop-down list, choose a view.

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 Figure 13.

Figure 13 Details Pane Show Drop-down List

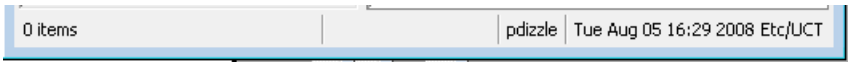


Status Bar

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



The SAVA OS Media Server for OS Provisioning

You must set up a Media Server in order to perform SA OS Provisioning.

Because SAVA is hosted on a virtual appliance optimized to run HP Server Automation, 250 GB of disk space is reserved for non-OS Provisioning content such as software management, compliance and patching content. For this reason, a separate OS Media Server is required to hold operating system images.

Because the Media Server is separate from SAVA, its contents are not included when you backup the virtual appliance. It is your responsibility to ensure the OS Media Server's contents are backed up.

About the Media Server

The Media Server stores and serves the operating system distribution files, SPPs and captured images using the protocol required by an OS Build Plan (OSBP) or installation tool. By default, SA OS Provisioning uses two protocols for all of its OSBPs:

- The SMB (Windows file share) protocol, used for:
  - All Windows operating system installations
  - All operating system image capture and deploy operations
  - SPP Installations
  - Firmware updates
  - Any other operations that require the mounting of a drive

- The HTTP protocol, used for:
  - All Linux and ESXi operating system installations

You can use NFS for Linux and ESXi operating system installations, SPP installations, firmware updates, and other functions requiring a mounted drive. Using NFS requires the additional manual step of setting up a Linux media server and additional manual changes to the OSBPs.

How the Media Server Works with OS Build Plans

For any OSBP that installs an operating system, you must specify the location on the Media Server of the OS installation media by using the Set Media Source step, which takes as its parameter, a URI representing the location of the media to be used in that OSBP. The URI looks something like this:

```
protocol://username:password@host/path#local-mount-point
```

where:

- `protocol` is the protocol to use to access the media, SMB, HTTP, or NFS
- `username:password` are the optional username and password to access the share – used for SMB only
- `host` is the ip address or hostname of the server
- `path` is the path on the media server to the data
- `local-mount-point` is the local drive or path to mount the share to (not used for HTTP)

Some examples of Set Media Source parameters:

```
smb://myuser:mypass@myhost/deployment#z
http://myhostname/deployment/rhel63-x64
nfs://myhostname/deployment#/mnt/mymedia
```

The OSBPs use two custom attributes called `MediaServer` (and optionally `MediaPath`) to point to the media server and the path where the OS media are located.

Set the `MediaServer` (and optionally `MediaPath`) custom attributes on the OSBP (or any other supported carrier such as Facility, Server, Device Group) and define their values appropriately.

For example, if your media server IP is 192.168.1.1 and the path to your media for a Windows 2008 R2 build plan is `/PUB/win2008r2`, then set the values as follows:

```
MediaServer: 192.168.1.1
MediaPath: PUB/win2008r2
```

Check the OSBP Set Media Source step to see whether `MediaServer` or, optionally `MediaPath`, are used.

An example of a Set Media Source step is:

```
"smb://@MediaServer:osprovmedia.acme.com@/@MediaPath:PUB/2008-r2-SP1@"
```

In the above example, if `MediaServer` and `MediaPath` are not defined, then the run-time value will equate to:

```
"smb://osprovmedia.acme.com/PUB/2008-r2-SP1"
```

If `MediaServer` is set to 192.168.1.1 and `MediaPath` is left undefined, then the run-time value will equate to:

```
"smb://192.168.1.1/PUB/2008-r2-SP1"
```

If both `MediaServer` and `MediaPath` are defined to 192.168.1.1 and `PUB/2012-noSP` respectively, then the run-time value will equate to:

```
"smb://192.168.1.1/PUB/2012-noSP"
```

As long as the host, path, username, and password specified in the Set Media Source step match the names and paths used when creating the media server, the OSBPs should work without problem.

Manually Creating a Windows-based Media Server

SAVA requires two types of access to the Media Server:

- Windows file share access to read operating system distribution files and HP SPP, and to store the Windows images created using the provided Windows OS Build Plans (OSBPs).
- HTTP access to read operating system distribution files for Linux and ESXi scripted installations.

This section assumes that the reader is familiar with using a Windows operating system.

Creating a Windows-based Media Server

To create a Windows-based Media server:

1. On a server already running Windows, create a top level directory under which the Media Server files will be stored. The example used will be:

   `c:\MediaServer`

2. Under this top level directory, create two subdirectories: Images and Media. For example:

   `c:\MediaServer\Images`

   `c:\MediaServer\Media`

   The Media folder is where all of the vendor supplied media will be stored, and the Images folder is where all captured images will be written.

3. For each operating system distribution, create a subdirectory under Media and copy the appropriate operating system distributions, including hidden or system files, and SPP.

Setting Up a Windows File Share for Windows Deployments

To setup the Window s file share:

1. Right-click the top level Media Server directory created in Step 1, for example: select c:\MediaServer, and select **Properties** > **Sharing Tab** > **Share**
2. Enter the user(s) authorized to access this share

Only local Windows user accounts should be given authorization to access the file share. Authorizing Domain user accounts to access the file share is not supported.

3 Set the Permission Level to Read/Write and click Share.

If a user is not given write access then all Image capture build plans will fail while trying to store the captured image to this share.

4 Apply the following Microsoft patch to enable use of `ntlmv2` authentication for access validation on the file share. The hotfix can be found at:

http://support.microsoft.com/kb/957441

The hotfix creates/updates the following registry entry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\
AllowLegacySrvCall with value 1 (DWORD)
```

5 To test that the share was created successfully, access the file share from another Windows server.

Setup HTTP Access for Linux and ESXi Deployments

To set up sharing operating system files via HTTP, HP recommends that you use Microsoft Internet Information Services (IIS 7 or above) since it is available as an installable feature on Windows servers.

To configure IIS to share operating system distribution files via HTTP:

1 Launch the IIS Manager from the Media Server. If IIS is not installed, go to Server Manager and select Install Web Server (IIS) feature and enable the IIS Management Console, Static Content, Directory Browsing role services.

2 After launching the IIS Manager, select Sites, right-click Default Web Site and click Add Virtual Directory.

3 Provide the name for this Virtual directory, for example, Deployment, and configure the Physical Path to point to the Media subdirectory created under the top level Media Server directory. For example, `c:\MediaServer\Media`. A new Virtual Directory is created under Default Web Site.

4 Select the newly created Virtual Directory and right-click Directory Browsing in the Features View. Select Open Feature and Enable Directory Browsing feature.

5 Add any required exceptions into IIS to allow serving files without extension, unknown extensions or files with special characters.

By default IIS 7 does not serve these files. Since some of the Linux distribution files fall into this category, it is necessary to add required exceptions into IIS to allow serving these files over HTTP. For more information refer to the following articles:

— *http://support.microsoft.com/kb/326965 http://blogs.iis.net/thomad/archive/2007/12/17/iis7-rejecting-urls-containing.aspx*

— *http://technet.microsoft.com/en-es/library/cc754791%28v=ws.10%29.aspx*

To add the required exceptions into IIS:

a Return to the Features view and select MIME Types feature and select Add. In the Add MIME Type box, enter an asterisk (*) for File name extension and enter application/octet-stream. Select OK.

b Select Add again, and this time type a dot (.) for File name extension and type application/octet-stream in MIME type box. Select OK.

6 Return to the Features view and select Request Filtering. From the Actions menu, select click Edit Feature Settings. Under General section, check options Allow unlisted file name extensions, Allow unlisted verbs, Allow high-bit characters, and Allow double escaping. Select OK.

7 To validate the HTTP connection, return to the Features view and select Browse to open the virtual directory under a browser. The subdirectories created under the example, c:\MediaServer\Media, should be visible in a directory listing format.

If you receive an HTTP error while browsing (HTTP Error 500.19) with the message `Cannot read configuration file due to insufficient permissions`, the IIS service does not have sufficient privilege to access the folder. To fix this:

1 Open Windows Explorer, access the top level Media Server folder and right click, selecting Properties.

2 Select the Security tab and select the Edit button. Select Add.

3 In Select Users or Groups window, enter `IUSR ; IIS_IUSRS`. Select Check Names to verify both users are present and select OK. Note that IUSR and IIS_IUSRS are the default users under which IIS services are launched and file system access is requested only on behalf of these users (not as Administrator). So these users should have Read permissions to the operating system distribution files to allow IIS to serve the files.

4 Ensure that the accounts have Read, List folder, Read and Execute permissions set. Select OK. Retry the virtual directory from browser test.

Manually Creating a Linux-based Media Server

This section assumes that the reader is familiar with executing Linux commands, installing RPMs, and checking services.

Creating a Linux-based Media Server

These instructions are optimized for Red Hat and SUSE Linux operating systems. However, since the Linux Media Server is based on NFS, HTTPD, and SAMBA functionality, any type of Linux could be used providing that these services are configured comparably to what is described in this document.

1 On a server that is already running Linux, create a top level directory under which the Media server files will be stored. The example used is:

```
/usr/MediaServer
```

2 Under this top level directory, create two subdirectories: Images and Media. For example:

```
/usr/MediaServer/Images
```

```
/usr/MediaServer/Media
```

3 For each operating system distribution, create a subdirectory under the Media directory and copy the appropriate operating system distributions, including hidden or system files, and SPP.

Setup NFS Access for the Linux Media Server

NFS can be used for Linux and ESXi operating system installations, SPP installations, firmware updates, and other functions requiring a mounted drive. Using NFS requires manual setup of a Linux media server and manual changes to the OSBPs.

The Set Media Source step parameter in the OSBP requires manual modification. Optionally, a new facility level custom attribute that will contain that URI can be created and used with the Set Media Source step instead of the Linux URI.

To setup the Linux File Share:

1. On the Media Server, install the following NFS RPMs:
   - For Red Hat Linux versions: `rpcbind` and `nfs-utils`
   - For SUSE Linux versions: n`fs-kernel-server`
2. Verify services are running.
   - For Red Hat Linux versions, ensure the `rpcbind`, `nfs` and `nfslock` services are running.
   - For SUSE Linux versions, ensure the `nfsserver` service is running.
3. Under `/usr`, create a directory under which the Media server files will be stored. For example:

   `/usr/MediaServer`
4. Under this directory, create two subdirectories: Images and Media. For example

   `/usr/MediaServer/Images`

   `/usr/MediaServer/Media`

   The Media folder is where all of the vendor supplied media will be stored, and the Images folder is where all captured images will be written.
5. For each operating system distribution, create a subdirectory under Media and copy the appropriate operating system distributions, including hidden or system files, and SPP. Using these directory names will ensure the baseline OSBPs will run without modification.
6. Edit /etc/exports to add the top level Media Server directory and permissions:

   `/usr/MediaServer *(rw)`
7. Force the NFS server daemons to reread `/etc/exports` by executing:

   `exportfs –ra`
8. To test that the share was created successfully, access the file share from another Linux client using the following steps:
   a. Create a mount point.
   b. Mount the NFS export to that mount point.
   c. Once mounted, the remote file system should be accessible

Modify the Operating System Installation OS Build Plans for NFS

To use the HP-provided baseline Linux and ESXi OSBPs with a Linux File Share, the OSBPs require modification. The procedures for copying a baseline OSBP and editing it are found in the *SA User Guide: OS Provisioning*.

Once a new OSBP is saved, edit the Set Media Source step parameter field to the following format:

```
nfs://IP_of_LinuxMediaServer/usr/MediaServer/Media/distributionname
```

where

- `IP_of_LinuxMediaServer` is the IP address of the Linux Media Server
- `distributionname` is the directory name under Media directory where the operating system distribution is located

Modify the Update Firmware OS Build Plan for NFS

The ProLiant SW – Firmware Update OSBP also requires modification. Save the OSBP to a new name and edit the Set Media Source step parameter field to the following format:

Once a new OSBP is copied and saved, edit the Set Media Source step parameter field to the following format:

```
nfs://IP_of_LinuxMediaServer /usr/MediaServer#/mnt/ms
```

where

- `IP_of_LinuxMediaServer` is the IP address of the Linux Media Server
- `/mnt/ms` is the location where the directory will be mounted

Modify the Install SPP OS Build Plans for NFS

To use the HP-provided baseline OSBP to install SPP on any Linux target server with a Linux File Share ensure that the target machine meets the following requirements:

- For SUSE Linux versions: the `nfs-client` RPM must be installed.
- For Red Hat Linux versions: the `rpcbind` and `nfs-utils` RPMs must be installed.
- For Red Hat Linux versions: the `rpcbind`, `nfs` and `nfslock` services must be running.

The ProLiant SW - Install Linux SPP OSBP requires modification. Copy and save the OSBP to a new name and edit the Set Media Source step parameter field to the following format:

```
nfs://IP_of_LinuxMediaServer /usr/MediaServer#/mnt/ms
```

where

- `IP_of_LinuxMediaServer` is the IP address of the Linux Media Server
- `/mnt/ms` is the location where the directory will be mounted

If you receive an error from the OSBPs about "`mount.nfs: requested NFS version or transport protocol is not supported`", add NFS version to the Set Media Source step parameter field. For example:

```
nfs://IP_of_LinuxMediaServer /usr/MediaServer#/mnt/ms?vers=4
```

where `vers=4` is the NFS version.

Configure DHCP

On the SAVA screen, navigate to the **Settings Edit DHCP** page where you can configure your DHCP settings

A DHCP server is required in order to provision servers. You may use the internal DHCP server supplied with the appliance or an external DHCP server. Details on deciding whether to use a DHCP server internal or external to the appliance and instructions for setting up an external DHCP server are found below.

Deciding Whether to Use a DHCP Server Internal or External to the Appliance

SAVA requires a DHCP server to provide IP addresses to target servers during the provisioning process. SAVA has an internal DHCP server that you can use, or you can set up an external DHCP server. This section will help you decide which is best for your facility.

You should first consider what your DHCP requirements will be when you are provisioning servers: *IP address only* or *extended DHCP options*.

IP Address Only Configuration

In this configuration, your DHCP server need only provide standard networking information (IP address, net mask, etc.) to the target servers. This simple configuration can be used if your environment meets all the following conditions:

- You will not PXE boot any servers
- The target servers are all HP ProLiant Gen8 series or newer
- You will use the embedded HP Intelligent Provisioning features of ProLiant servers (no PXE)
- You will use iLO IP addresses and credentials to add servers to the appliance

Extended DHCP Options

In this configuration your DHCP server must provide standard networking information, plus additional options so the target servers can PXE boot from the appliance into the required service OS. The extended DHCP configuration is required if your environment meets any of the following conditions:

- You will PXE boot servers (this includes PXE booting to add servers to the appliance)
- You have target servers earlier than Gen8 series

- You have Gen8 series target servers but will not use Intelligent Provisioning
- You do not want to use iLO to add servers to the appliance

Next, consider whether to use the DHCP server internal to the appliance or if you should configure an external DHCP server.

The Built-in Internal DHCP Server

The SA virtual appliance comes with a built-in DHCP server that is easy to configure and use, and provides all the extended information required for PXE booting.

- Configures easily via the appliance Settings page
- Provides addresses only for the appliance's subnet
- Supports optional information, such as DNS and gateway
- Will always provide extended information required for PXE booting target servers

An External DHCP Server

An external DHCP server might make sense in the following cases:

- You already have a DHCP server on your network
- You require more advanced features than you can configure using the appliance UI

The built-in TFTP server required to allow target servers to PXE boot from the appliance will always run regardless of whether the DHCP server you use is internal or external to the appliance.

Setting up an External DHCP Server

SAVA supports either using the built-in DHCP server or using an external DHCP server set up at your facility.

If you require more control or more features from your DHCP server than are available via the appliance UI, you should disable the DHCP server on the appliance and configure your own server.

See Deciding Whether to Use a DHCP Server Internal or External to the Appliance on page 38 for more information.

Notes

- HP recommends setting the lease time on the DHCP server to at least one day to prevent issues caused by time synchronization.
- These instructions are for configuring the extended DHCP options required for PXE booting target servers from the appliance. If you do not require extended options, no special configuration of the DHCP server is necessary beyond the ability to provide an IP address to target servers and possibly extending the lease time.
- If you decide to use an external DHCP server, ensure that the Service provided by the appliance is set to None on the appliance Settings DHCP page.

- You can find the deployment IP address on the Settings Appliance page under Deployment IP.

To configure an external Windows DHCP server or an external Linux ISC DHCP server, perform the following tasks:

Setting up an External Windows DHCP Server

1 Add a DHCP server role on your Windows system.

2 Set up your scope and start the server. Be sure to set the lease time to one day or greater.

3 Add the following options to the DHCP server IPv4 global settings:

Table 2 Windows DHCP IPv4 global settings

Code	Option Name	Datatype
186	`buildmgr_ip`	IP Address
187	`buildmgr_port`	Word

4 In the DHCP scope, assign the following values to the DHCP options:

Table 3 Windows DHCP options

Code	Option Name	Option Value
66	boot server	`<Deployment IP address of appliance>`
67	boot file name	`pxelinux.0`
186	`buildmgr_ip`	`<Deployment IP address of appliance>`
187	`buildmgr_port`	`0x1F51`

Setting Up an External Linux DHCP Server

If you are using a standard ISC Linux DHCP server, set the following options in order to PXE boot servers from the appliance.

1 Set the lease time to at least one day. For example:

```
default-lease-time 86400;
max-lease-time 129600;
```

2 Included the following lines in the global options declarations:

```
option buildmgr_ip code 186 = ip-address;
option buildmgr_port code 187 = unsigned integer 16;
```

3 The following options and values must be set in either the global or scope area, depending on your needs:

```
next-server <Deployment-IP-Address-of-appliance>;
filename "pxelinux.0";
option buildmgr_ip <Deployment-IP-Address-of-appliance>;
option buildmgr_port 8017;
option dhcp-parameter-request-list =
concat(dhcp-parameter-request-list,ba,bb,fc);
```

Example:

```
next-server 172.1.3.10;
filename "pxelinux.0";
option buildmgr_ip 172.1.3.10;
option buildmgr_port 8017;
option dhcp-parameter-request-list =
concat(dhcp-parameter-request-list,ba,bb,fc);
```

Once these options are set properly, you should be able to use the appliance to PXE boot servers.

Additional Documentation for SA Features

SA features are covered in depth in the Server Automation documentation suite. For information on locating specific information relating to common SAVA tasks, see Performing Tasks in the SA Client on page 10.

4 SA Virtual Appliance Administration

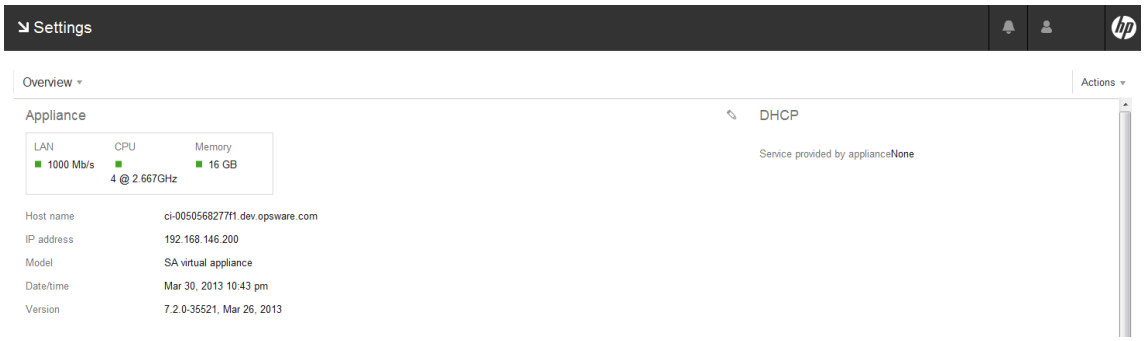
Upgrading the SA virtual appliance and the SA Application

Upgrades to the SA virtual appliance and the SA application itself use the same procedure and often upgrades to both occur in a single upgrade. This section describes how to upgrade the SA virtual appliance and the SA application.

HP strongly recommends that you create a snapshot of the SA virtual appliance before performing any upgrade patch or hotfix so you can roll back to that snapshot should any problems with the upgrade, patch or hotfix occur.

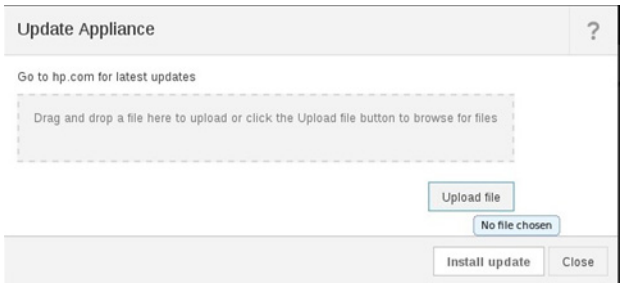
1. You should have already downloaded the upgrade file as directed in SAVA upgrade notice.
2. From the SA virtual appliance administration Settings screen, select **Action** > **Upgrade Appliance**.

Figure 14



3. On the Update Appliance screen, drag and drop the update file or browse to it to select it. Press Upload File to begin the upload to the appliance. An upload progress bar displays.

Figure 15



4 After the upload completes, a screen with information about the update file displays. Confirm that you have uploaded the correct update file. When you are ready, click the Install Update button.

5 You may be asked to accept the HP EULA. Accept the EULA to proceed.

The installation can take up to three hours and may require that the appliance reboot.

Permissions Reference

SA permissions are listed in Appendix A of the *SA Administration Guide*, however there are certain differences between the assigned permissions in SAVA and an enterprise-level SA installation:

- Read permission to the `Opsware` customer is allowed. Read&Write permission is disallowed.
- Global File System (OGFS) permissions for `Facility=any`, `DG=any`, and `Customer=OPSWARE` are disallowed.
- Manage Extensions action permission is disallowed.

Backing Up and Restoring the SA Virtual Appliance

HP recommends that you use the native hypervisor backup procedures provided by VMware vSphere. See your VMware documentation for information about virtual machine backup and restore procedures.

HP recommends regular backups, preferably once a day.

Security

SAVA is delivered as a security-hardened virtual appliance. The number of open ports and protocols supported has been limited to the minimum necessary for operation.

Assumptions

The SAVA appliance should be on a deployment network, separate from the production network (see Security Best Practices on page 53). Additionally, access to the virtual appliance console should be restricted to authorized users (see Restricting Console Access on page 52).

The appliance needs access to the iLOs on target servers as well as their deployment NICs. A network configuration includes a separate management network that connects to target iLOs and a deployment network with DHCP and PXE that connects to target deployment NICs. This type of configuration will require routing between the management and deployment networks to provide access to the target iLOs via the deployment network.

SAVA lands an agent in the production operating system and this agent must be able to communicate back to the appliance. The assumption is that the deployment NIC will be active in the production OS or that there will be a route back to the deployment network for this communication.

Hypervisor and Virtual Machine Security Considerations

As a virtual appliance, the security of the appliance relies on the security of the host hypervisor, in the same way that a physical server relies on the physical security of the datacenter. Administrative access to the host hypervisor needs to be controlled to ensure the security of the appliance. The appliance software image on the VM has been hardened but the hypervisor must be configured to limit access to the virtual appliance console and virtual hard drive (VMware `vmxd` file) to secure the appliance.

Authentication

Access to the appliance requires authentication using a username and password. These user accounts are configured on the appliance. All access through the browser interface occurs over SSL, including authentication, which protects the credentials during transmission over the network.

Session

A session is created when a user logs in to the appliance through the browser or some other client (for example, using the REST API). A session ID is then used for additional requests to the appliance, and it must be protected because it represents the authenticated user.

A session remains valid until the user logs out or the session times out. When using the REST API, you should set the session idle time to a shorter duration or use the default duration of 24 hours and be sure to logout and end the session when done. The screen saver/system lock mechanism of the operating system will provide some protection but the UI should not be left open and unprotected. If the browser UI is closed without logging out, the session token will time out and be invalid after 20 minutes. The browser session is stored in a session cookie stored in memory and will not be retained after the browser closes. It is a best practice to always log off before closing the browser.

Auditing

The audit log contains a record of important actions performed on the appliance. User actions will have a logging ID associated with them so that you can follow the user's trail in the audit log. Some actions are performed by the appliance; those may not have a logging ID.

This is a breakdown of an audit entry:

- DATE TIME,
- Internal component ID,
- <reserved>
- User domain,
- User name/ID,
- Logging ID,
- Task ID,
- Source host/IP,
- Result,
- Action,
- Severity,
- Object Type,
- Object Descriptor,
- Message

Sample audit entries showing a user login and logout:

```
2012-11-16 14:55:20.706 CST,Authentication,,,administrator,jrWI9ych,,,
SUCCESS,LOGIN,INFO,CREDENTIAL,,Authentication SUCCESS

2012-11-16 14:58:15.201 CST,Authentication,,,MISSING_UID,jrWI9ych,,,
SUCCESS,LOGOUT,INFO,CREDENTIAL,,TERMINATING SESSION
```

The audit logs are periodically rolled over to prevent them from growing too large, so you may wish to monitor them and periodically download them to maintain a long-term audit history.

Operations performed via the appliance UI or REST interface are included in the audit log, operations performed as part of the Matrix Operating Environment go through a different interface.

The file containing the additional audit information inside the `audit-logs-<date>.zip` file is `deployment-audit-logs.zip`. Inside that file are zipped a set of system logs under the path `var/opt/opsware/ogfs/mnt/audit/event/<system name>/audit.log.0`. In those audit logs, actions performed via the appliance UI will be recorded as being performed by user `applianceserviceaccount`, while those performed via the Matrix Operating Environment will be recorded as being performed by user `matrixuser` (unless you have designated a different user). There may be additional actions recorded against internal users using regular SA user accounts including SA `detuser`, SA integration, and SA `buildmgr` accounts.

Communication protocols

SSL

All access to the appliance using the browser interface uses HTTPS (HTTP over SSL). This encrypts data over the network and helps to ensure data integrity. Refer to “Algorithms” (page 30) for a list of supported cipher suites.

Certificate management

A certificate is used to authenticate the appliance over SSL. The certificate contains a public key, and the appliance maintains the corresponding private key which is uniquely tied to the public key. The name of the appliance is also contained in the certificate and is used by the browser to identify the appliance.

There are two name fields in the certificate.

- The Common Name (CN) is a required field; by default the fully-qualified name is used.
- The Alternative Name field is optional, but recommended as it allows for multiple names (including IP addresses) to minimize name mismatch warnings from the browser. By default, this field is populated with the fully-qualified name, a short name, and the system’s IP address.

These fields can be changed when you manually create a self-signed certificate or certificate signing request.

If you do use the Alternative Name field, the name from the Common Name field must be included.

The default certificate generated by the appliance is self-signed, meaning it is generated entirely by itself. By default, browsers do not trust self-signed certificates as they have no prior knowledge of them. The browser will display a warning to allow the user to verify the content of the self-signed certificate before accepting it.

A Certificate Authority (CA) can be used to simplify certificate trust management, where the trusted CA is used to issue certificates. If the browser is already configured to trust the CA, certificates signed by the CA are also trusted. A CA can be internal, operated and maintained within your organization, or it can be an external third-party. The appliance supports importing a certificate signed by a CA and using that instead of the self-signed certificate.

To obtain a CA-signed certificate, you first need to generate a Certificate Signing Request (CSR). Under Settings, choose **Actions** > **Create certificate signing request**, then take the response and submit that to your CA in accordance with the CA’s instructions. When the CA signs and issues the certificate, import the response back into the appliance. Under Settings, choose **Actions** > **Import certificate**, cut and paste the content of the issued certificate into the text field, and press the OK button.

Download

To download the appliance certificate for manual import into a browser you can use the browser as described below:

- Firefox – during the Add Exception process, you can View the certificate and verify it. Then from the Details tab you can Export the certificate as X.509 Certificate (PEM).
- Internet Explorer – click in the Certificate error area, View certificate, then the Details tab.

  From here you can verify the certificate, then select Copy to File. Save the certificate as Base-64 encoded X.509.

Browser

General

- SSL/TLS: SSL v3 and TLS should be enabled; SSL v2 is considered insecure and should not be enabled in the browser unless there is some specific need for it.
- Cookies must be enabled; a cookie is used to store the authenticated user's session ID.
- Certificates in Firefox or Internet Explorer are described more below; because the default appliance certificate is self-signed, you will initially get a warning from the browser.

Firefox

When you get the certificate warning "This Connection is Untrusted" and you choose the "Add Exception" option under "I Understand the Risks", an exception will be added, but only for the specific name. So if you browse by another name to the same system, you will again get the warning from Firefox. You can either add another exception for that name, or browse to the original name.

You can manually import the certificate into Firefox outside of this warning and it will wildcard the name, but you must also enable trust for that certificate. In the Advanced section under Options, choose the Encryption tab, then the View Certificates button. An Import button allows you to import a certificate. After that, select the certificate then the Edit Trust button and enable Trust the authenticity of this certificate.

Internet Explorer

This certificate warning does not allow you to view or import the certificate, only to bypass it and continue on. You can manually import a certificate from Internet Options. In the Content tab, choose Certificates, then Import. When prompted for the certificate store, choose the Place…option and select the Trusted Root Certification Authorities store.

Browser Best Practices

- Logout before closing the browser. In the browser, a cookie is used to store the authenticated user's session ID. A memory-based cookie is used so it is deleted upon closing the browser; however this does not affect the session on the appliance. Logging out ensures the session on the appliance is invalidated.
- Avoid links from outside the appliance GUI. Avoid clicking links, for example from email or IM, while logged in to the appliance. The links may be malicious and take advantage of your logged in session. For the same reason, avoid browsing to other sites using the same browser instance, for example separate tabs in the same browser. Use a different browser to ensure a separate browsing process, for example use Firefox for the appliance, and Internet Explorer for non-appliance browsing.

Credentials

Local user account passwords are stored in a salted hash. Password fields in the browser are masked so the passwords are not shown, and passwords are protected over the network using SSL between the appliance and the browser. Local user account passwords must be at least eight characters in length. Additional password complexity rules are not enforced by the system. Password strength and expiration must be controlled via the site security policy (see Security Best Practices on page 53).

Non-browser Clients

The appliance supports a limited number of REST APIs. Requests for these may be issued by any client, not just a browser. In this case, it is up to the caller to ensure appropriate security measures are followed regarding the confidentiality of credentials, including the session token, used for data requests and responses beyond the encryption of the credentials on the wire using HTTPS.

Passwords

Passwords are likely displayed and stored in clear text by a client like cURL. Care should be taken to prevent unauthorized users from viewing displayed passwords or having access to saved data. Likewise for session identifiers, though they may be used in a transient fashion, they should not be accessible to unauthorized users.

SSL/Certificate

The client should specify HTTPS as the protocol to ensure SSL is used on the network to protect sensitive data. The appliance certificate may be required by the client to allow the SSL connection to succeed. The certificate can be obtained from a browser pointed at the appliance. See Download on page 48 for information on downloading the certificate.

Appliance Hardening

Port List

The following table lists the ports that must be open for SAVA.

Table 4 Required Open Ports

Port	Description
3001 (tcp)	SA Agent communications
67 (udp)	DHCP
69 (udp	TFTP
123 (udp)	NTP
8017 (tcp/udp)	Agent Gateway
8081 (tcp)	agentcache
111 (tcp/udp)	NFS boot file mount
2049 (tcp/udp)	NFS
892 (tcp/udp)	mountd
8020 (tcp/udp), 9000 (tcp/udp)	Global File System
1004 (tcp), 1032 (tcp), 2222 (tcp)	Data Access Engine and Software Repository
1018 (tcp)	Command Engine
137 (udp), 138 (udp), 139 (tcp), 445 (tcp)	Media Server SMB

Console Access

Console access is provided for three purposes: a UI Kiosk, appliance administrator password reset, and access by an on-site HP Services tech. Access to the local console itself, for example, using the vSphere client, should be restricted to prevent unauthorized users from attempting to login through the console. See Restricting Console Access on page 52. The UI Kiosk is displayed in a graphical console while password reset and HP Services access are available via a non-graphical console.

The instructions for switching from one console to the other are: Open the appliance console from vSphere.

1. Press and hold Ctrl+Alt.
2. Press and release the spacebar.
3. Press F1 to select the non-graphical console or F2 to select the graphical console.
4. Release Ctrl+Alt.

Console UI Kiosk

The kiosk-mode browser is locked down and restricted to prevent any potential misuse or security issues. It is not intended as a full-featured replacement for your own browser, but rather as a means to access the appliance to run first time setup to initially configure the appliance network so it can be accessed remotely.

Appliance Administrator Password Reset

If the Administrator user password is lost, it can be reset from the appliance console. The steps to reset the password are:

1. Open the appliance console from vSphere and display the non-graphical console.
2. Enter the usernamepwreset.
3. The appliance will present a challenge key. For example:

   ```
   <hostname> login: pwreset Challenge = xyaay42a3a Password:
   ```

4. Call HP Support to obtain the one-time password that will reset the administrator password for the Insight Control server provisioning appliance. The challenge will need to be read to the support representative.
5. The HP Support representative will use the challenge code to generate the one-time password.

   It will be an easy to type, space separated set of strings. For example:

   ```
   VET ROME DUE HESS FAR GAS
   ```

6. When this password is entered, the appliance will display a new, randomly generated password. After noting the new password, press Enter.
7. The newly generated password is pre-expired. When using it to login to the appliance as Administrator, you will be required to change it, just as the default password requires immediate change during First-Time Setup.

   The ability to reset the Administrator password cannot be disabled.

Enabling or Disabling HP Support Services Access

When you first start up the appliance, you are given the opportunity to enable or disable HP Support Services access. Access is enabled by default to allow HP Support personnel to access your system through the system console and diagnose serious problems that you have reported.

HP Support Services access is a root-level shell, so the on-site HP Support tech can fully debug any issues on the appliance. The on-site HP Support representative can obtain a one-time password for shell access using a challenge/response mechanism similar to the one for password reset.

After first time setup you can use the UI to enable or disable HP Support access on the Settings page by selecting **Actions** > **Edit HP support access**. A REST API is also available to enable or disable HP Support services access (see REST Call to Enable or Disable Support Access on page 57.

HP recommends leaving services access enabled. If a problem were to occur that requires services access there is no guaranteeing it will be possible to enable it after the fact.

Restricting Console Access

To restrict access to the console you must also restrict access to the virtual hard drive. See *VMware vSphere Security Hardening Guide* sections on “Host Communications between vSphere Client and ESX Server uses SSL with default certificates — these can be updated” and “Describe VM protection”.

Algorithms

The following algorithms are used:

- SSL (see Supported cipher suites table below)
- Local user account passwords: hashed using SHA-256
- Other passwords: encrypted using 128–bit Blowfish
- Backups/Support Dumps
  - Encryption: AES 128–bit
  - Hash: SHA-256
- Support dump: AES key is separately encrypted using 2048–bit RSA
- Updates: not encrypted, digitally signed using SHA-256 and 2048–bit RSA

The following SSL cipher suites are enabled on the SAVA appliance web server. These cipher suites are for the connection between the browser and the IC server provisioning appliance.

Table 5 Supported Cipher Suites

		Kx	Au	Enc	Mac
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES (256)	SHA1
AES256-SHA	SSLv3	RSA	RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168)	SHA1
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES (128)	SHA1
AES128-SHA	SSLv3	RSA	RSA	AES (128)	SHA1

Downloads from the Appliance

These are the data that can be downloaded from the appliance:

- Support dump - all data in the support dump is encrypted and accessible only by HP support.
- Backup - all data in the backup is in a proprietary format and HP recommends the customers encrypt it in a way that meets their organizational requirements.
- Audit logs - session IDs are not logged, only corresponding logging IDs. Passwords and other sensitive data are not logged.
- SSL Certificate - certificates contain public data.

Security Best Practices

Most security policies and practices utilized in a traditional environment are applicable in a virtualized environment. However, in a virtualized environment, these policies might require modifications and additions. Following are numerous security practices recommended by HP in a virtualized environment. This is only a partial list as differing security policies and implementation practices make it difficult to provide a complete and definitive list. However, this list will serve as a good starting point.

- Use a separate deployment network. For security and performance reasons, HP recommends the following:
  - Establishing a private deployment network separate from the production network
  - Granting only administrators access to the deployment network
  - Using a firewall to restrict traffic into the deployment network
- Restrict access to the appliance console to authorized users. See Restricting Console Access on page 52 for more details.
- Eliminate or disable nonessential services in the management environment. Configure all host systems, management systems, and network devices so that nonessential services are either eliminated or disabled, including networking ports when not in use. This can significantly reduce the number of attack vectors in your environment. The appliance is already configured this way.
- Ensure a process is in place to periodically check for and install patches for all components in your environment.
- Security policy and processes must address the use of virtualization in the environment, for example:
  - Educate administrators about changes to their roles and responsibilities in a virtual environment.
  - If an IDS is being utilized in your environment, ensure that the IDS solution has visibility into network traffic in the virtual switch (within a hypervisor).
  - Mitigate potential sniffing of VLAN traffic by turning off promiscuous mode in the hypervisor and by encrypting traffic flowing over the VLAN.

In most cases, if promiscuous mode is disabled in the hypervisor, it cannot be utilized on a VM guest (the guest can enable it, but it will not be functional).

  - Maintain zones of trust (DMZ separate from production machines).
  - Ensure proper access controls on FC devices.
  - Use LUN masking on both storage and compute hosts.
  - Ensure LUNs are defined in the host configuration rather than by discovery.
  - Use Hard Zoning based on port WWN if possible.
  - Ensure communication with the WWNs is enforced at the switch port level.

- Clearly define and utilize administrative roles and responsibilities (host administrator, network administrator, and virtualization administrator).
- Many components that utilize certificates are delivered with certificates signed by the provider.

To achieve a higher level of security for these components, populate them with trusted certificates at deployment time.

- For local accounts on the appliance, periodically change the passwords in accordance with your password policies and consider the following guidelines:
  - Default passwords should be changed immediately to a more relevant and secure password.
  - Administrators should change management device passwords with the same frequency and according to the same guidelines as the server administrative passwords.
  - Passwords should include at least three of these four characteristics: numeric character, special character, lowercase character, and uppercase character.
- Utilize mutual device authentication (to validate endpoints), when available, and user authentication mechanisms.
- Restrict access to iLO remote console port.
  - For iLO 2: Disable telnet access to iLO 2.
  - For first-generation iLO: Require Remote Console data encryption and set Remote Console Port Configuration to Automatic.
  - These changes force remote console sessions to be encrypted and leave the port closed except when attaching the remote console.
- Do not connect management systems, (for example, the appliance, iLO, and OA), directly to the Internet. If you do require access to the Internet, utilize a corporate virtual private network that provides firewall protection.
- For service management, consider using the practices and procedures, such as those defined by ITIL. Visit *http://www.itil-officialsite.com/home/home.aspx*.
- Consider using The Center for Internet Security Benchmarks available at *http://benchmarks.cisecurity.org/*. Benchmarks are included for HP-UX, Windows, Linux, Citrix Xen Server, and VMware Server.

Advanced Topics

Automate Appliance Management Tasks through REST Calls

You can automate enabling/disabling of HP support access through REST calls to the appliance. You can wrap these calls in a script to further increase the level of automation.

Enabling/disabling HP Support services access requires three REST calls. The first call sets up a user session and generates an authentication token and the second REST call enables/disables services access. Finally, the user session must be ended with a REST call to log out.

In this discussion we use the open-source cURL utility to make the REST calls. The cURL open-source project is located at: *http://curl.haxx.se/*. You can invoke cURL from a command line on either Linux or Windows.

Each REST call is an HTTP request and associated response. The request includes the URL, message type, HTTP headers, request body, and response body.

REST Call to Create a User Session and Get an Authentication Token

The REST call to create the user session requires you to pass an appliance administrator user's credentials (<administrator-user>/<administrator-password> as identified below), and the REST call will respond with a user authorization token (<user-authorization-token> as identified below).

A list of the components of the REST call is shown below:

Table 6 REST Calls

REST Component	Description
URL:	*https://<appliance-hostname-or-address>/rest/login-sessions?action=login* where you supply <appliance-hostname-or-address>
Message Type:	POST
HTTP headers:	accept: application/json content-type: application/json accept-language: en-us (optional)
Request body:	{"userName":"<administrator-user>","password":"<administrator-password>"} where you supply appliance administrator username and password
Response body:	{"sessionID":"<user-authorization-token>"} where you retrieve the user authorization token for use in the second REST call

You invoke cURL as follows and will see the associated response shown below.

cURL command on Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -X POST
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
-d '{"userName":"<administrator-user>","password":"<administrator-password>"}'
```

cURL command on Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -X POST
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
-d {\"userName\":\"<administrator-user>\",\"password\":\"<administrator-password>\"}
```

Example response on success:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:44:01 GMT

Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

{"sessionID":"<user-authorization-token>"}
```

If the request fails, an error diagnostics is returned. Common errors are HTTP `error 404 not found` if the URL is not correct or an exception if the user/password is not correct.

REST Call to Logout of a User Session

The REST call to logout of the user session requires you to pass the user-authorization-token.

Table 7 Logout REST Calls

REST Component	Description
URL:	*https://<appliance-hostname-or-address>/rest/login-sessions?action=logout* where you supply `<appliance-hostname-or-address>`
Message type:	DELETE
HTTP headers:	accept: `application/json content-type: application/json accept-language: en-us` (optional) auth: `<user-authorization-token>` where you supply `<user-authorization-token>`
Request body:	None
Response body:	None If logout was successful

You invoke cURL as follows and will see the associated response shown below:

cURL command on Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -H "auth: <user-authorization-token>" -X DELETE
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

cURL command on Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -H "auth: <user-authorization-token>" -X DELETE
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

Response on success:

```
HTTP/1.1 204 No Content
Date: Wed, 20 Feb 2013 15:36:40 GMT
Via: 1.1 cic.dns.hp
cache-control: no-cache
Content-Length: 0
Content-Type: text/plain; charset=UTF-8

Response Body: None
```

If the request fails, an error diagnostics is returned. Common errors are HTTP `error 404 not found` if the URL is not correct.

REST Call to Enable or Disable Support Access

In addition to being able to enable or disable HP Support access to your Insight Control server provisioning appliance via the UI (on the Settings page select **Actions > Edit HP support access**), you can also accomplish this programmatically. This alternate approach is valuable if the appliance user interface is unresponsive and you need to enable HP Support access for diagnosing a problem.

Programmatically, one needs to make three REST calls to the Insight Control server provisioning appliance. The first call sets up a user session, while the second call enables or disables support access to the appliance. Finally, the third call logs out of the session

See REST Call to Create a User Session and Get an Authentication Token on page 55 for details about making the first REST call.

The second REST call is to either enable or disable support access to the appliance. In this REST call you will need to provide the `<user-authentication-token>` you received from the first login REST call, and you will need to pass either true or false to indicate whether you want to enable services access.

Finally, see REST Call to Logout of a User Session on page 56 for details about making the third REST call to logout of the user session.

A list of the components of the REST call is shown below:.

Table 8 Support Access REST Calls

REST Component	Description
URL:	*https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess* where you supply <appliance-hostname-or-address>
Message type:	PUT
HTTP headers:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: <user-authorization-token> where you supply <user-authorization-token>
Request body:	"<true/false>" specifying whether you want support access enabled
Response body:	"true" if services access was successfully enabled or disabled

You invoke cURL as follows and will see the associated response shown below:

cURL command on Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language:en-us"
-H "auth: <user-authorization-token>" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d "true/false"
```

cURL command on Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language:en-us"
-H "auth: <user-authorization-token>" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d \"<true/false>\"
```

Response on success:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:46:13 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

True
```

If the request fails, you will be returned an error diagnostics. Common errors are HTTP `error 404 not found`, if the URL is not correct, or an exception if the associated user is not authorized to enable/disable services access.

Below is an example Linux shell script using cURL that logs into the appliance, enables or disables support access and logs out.

```
#!/bin/sh
# login
AUTH=`curl -k -X POST -H "accept:application/json" -H "content-type: application/json"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
-d '{"userName":"<administrator-name>","password":"<administrator-password>"}' | perl
-e 'while (<>)
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This REST call either enables or disables support access to the appliance.
curl -i -k -H "accept:application/json" -H "content-type:application/json"
-H "accept-language:en-us"
-H "auth: ${AUTH}" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d "<true/false>"
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

REST API to Create and Download a Support Dump

In addition to being able to download a support dump from the SA virtual appliance from the Appliance Management screen, you can also accomplish this programmatically. This alternate approach is valuable if the appliance user interface is unresponsive and you need to retrieve a support dump for diagnosing a problem.

Programmatically, one needs to make two REST calls to the SAVA appliance. The first call creates the support dump and leaves it on the appliance, while the second call downloads it to a specified location.

In this discussion we use the open-source cURL utility to make the REST calls. The cURL open-source project is located at: *http://curl.haxx.se/*. You can invoke cURL from a command line on either Linux or Windows.

A list of the components of the REST call to create the support dump is shown below:

Table 9 Create Server Dump REST Calls

REST Component	Description
URL:	*https://<appliance-hostname-or-address>/rest/appliance/support-dumps* where you supply `<appliance-hostname-or-address>`
Message type:	POST
HTTP headers:	accept: `application/json content-type: application/json`
Request body:	`{"errorCode": "<support-dump-error>”}` where `<support-dump-error>` is used when generating the support dump file name.
Response body:	`{"type":"DumpDataInfoDto", "dumpFileSize":8087, "uri": "<support-dump-filename>", "category":null, "eTag":null, "created":"Tue Jun 19 03:1 :25 MDT 2012", "modified":null }` You will use `<support-dump-filename>` in the subsequent REST call to download the support dump.

You invoke cURL as follows and will see the associated response shown below:

cURL command on Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json" -H
"accept-language:en-us"
-X POST https://<appliance-hostname-or-address>/rest/appliance/support-dumps
-d `{“errorCode”: “<support-dump-error>”}’
```

cURL command on Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json" -H
"accept-language:en-us"
-X POST https://<appliance-hostname-or-address>/rest/appliance/support-dumps
-d “{\“errorCode\”: \“<support-dump-error>\”}”
```

Response on success:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:46:13 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked
```

If the request fails, an error diagnostic is returned. Common errors are HTTP `error 404 not found` if the URL is not correct.

A list of the components of the REST call to download the support dump is shown below:

Table 10 Download Server Dump REST Calls

REST Component	Description
URL:	*https://<appliance-hostname-or-address>/rest/appliance/support-dumps/<support-dump-filename>* where you supply `<appliance-hostname-or-address>` and `<support-dump-filename>` is obtained by the previous call to create the support dump.
Message type:	POST
HTTP headers:	accept: `application/json content-type: application/json`

As the GET message will retrieve the encrypted support dump, you will want to redirect the output to a `<output-support-dump-file>` using the `-o` argument.

cURL common on Linux and Windows:

```
curl -i -k -X GET https://<appliance-hostname-or-address>/rest/appliance/support-dumps/<support-dump-filename> -o <output-support-dump-file>
```

If the request fails, an error diagnostic is returned. Common errors are HTTP `error 404 not found` if the URL is not correct.

5 Support and Other Resources

Contacting HP

Before you contact HP

Be sure to have the following information available before you call contact HP:

- Technical support registration number (if applicable)
- HP Server Automation Virtual Appliance version
- Applicable error message
- Installed third-party hardware or software
- Operating system type and revision level
- You can also create a support dump that you can use during troubleshooting with your HP representative:

  How to create a support dump on page 61

Support Dump

Support dumps can be very useful in identifying and fixing problems. You might want to create a support dump in the following situations:

- An error message displayed by SAVA recommends that you create a support dump of the appliance so it can be sent to HP Support for analysis.
- You experience a problem you think might require analysis of internal appliance data. HP recommends creating a support dump as soon as the problem occurs to better capture significant data.
- HP Support requests that you create a support dump as part of a service engagement.

How to create a support dump

The support dump feature gathers logs, system configuration, and status information, then creates an encrypted, compressed file that can be sent to HP Support for troubleshooting.

1. Log in to the appliance with administrator privileges.
2. Navigate to the Settings page from the main menu.
3. Select **Actions** > **Create support dump**.

   While the support dump is being created, you may continue doing other tasks.

4 When the support dump creation is complete, you will be prompted to save the `tar.gz` file.

   If your browser settings specify a default download folder, that will be the default download location.

5 Contact HP Support to get instructions about how to deliver the support dump.

Support Dump Contents

A support dump collects the following information from your appliance. The support dump is encrypted.

All appliance configuration information, including:

- Revision of the appliance software
- Network configuration
- DNS servers
- NTP servers

Information about the running appliance, including:

- All processes
- Memory
- Disk space
- Network statistics
- Routing
- Hardware information

Log data, including:

- All standard Linux operating system logs
- All appliance logs
- Logs from all jobs run in the past three days
- Installation logs
- The system audit log

Other information:

- A status report of all processes
- Dates of any certificates used

The following types of items might be included in the support dump as a result of collecting the data above:

- IP addresses (of the appliance, target systems, and connected browsers)
- Host names
- System UUIDs
- User names (no passwords are ever collected in a support dump)
- Network configuration information
- WWIDs