HP Insight Control Server Provisioning 7.2 Administrator Guide

HP Part Number: 5900-3055
Published: February 2013
Edition: 1

Acknowledgments

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

For access to applicable source code for the open source software used by HP Insight Control server provisioning, see the *HP Insight Management 7.2 Installation and Upgrade Release Notes*, available at http://www.hp.com/go/insightmanagement/docs.

Contents

1 Introduction/overview

What is Insight Control server provisioning?

Insight Control server provisioning is a virtual appliance used to install and configure HP ProLiant servers. Insight Control server provisioning uses resources such as OS Build Plans and scripts to run deployment jobs.
IC server provisioning allows you to:

- Install Windows, Linux, and ESXi on ProLiant servers
- Update drivers, utilities, and firmware on ProLiant servers using the HP Service Packs for ProLiant (SPPs)
- Configure ProLiant system hardware, iLOs, BIOS, and HP Smart Array
- Deploy to target servers without using PXE (HP ProLiant Gen8 and later)
- Run deployment jobs on multiple servers simultaneously
- Customize your ProLiant deployments via an easy to use browser-based interface
- Migrate from HP Insight Control server deployment (RDP) to Insight Control server provisioning

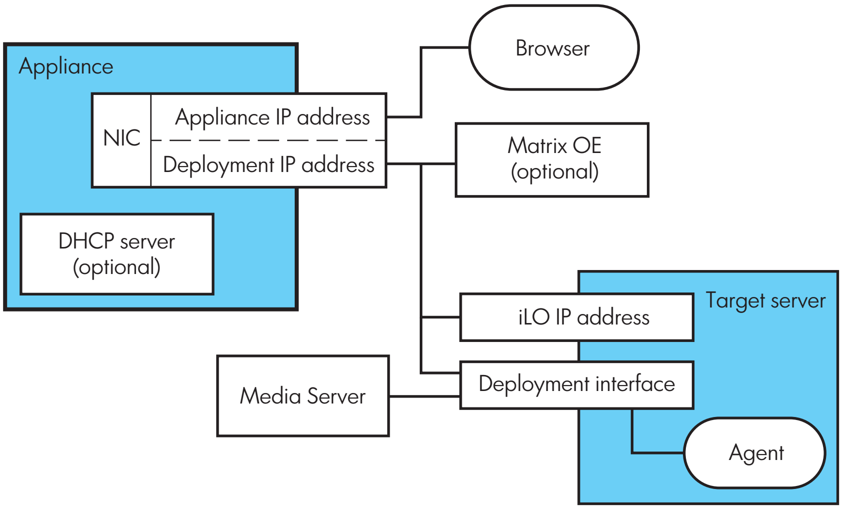
Table 1 Where can I find information on ...?

Topic	Where to find the information
Release notes	See the Insight Control server provisioning section of the *HP Insight Control Release Notes* available at http://www.hp.com/go/insightcontrol/docs.
Support Matrix	See the Insight Control server provisioning section of the *HP Insight Management Support Matrix* available at http://www.hp.com/go/insightcontrol/docs.
How to download and set up the appliance for the first time	See the *HP Insight Control Server Provisioning Installation Guide* available at http://www.hp.com/go/insightcontrol/docs.
Online help in PDF form	The online help content is available in PDF format at http://www.hp.com/go/insightcontrol/docs.
Deep dive	See the *HP Insight Control Server Provisioning Administrator Guide* available at http://www.hp.com/go/insightcontrol/docs for in-depth strategy and usage.
Getting started	The Quick Start section in the online help will walk you through using Insight Control server provisioning to accomplish real tasks. See the How Do I...? section in the online help section for introductory information and instructions on accomplishing tasks.
Terms	See the Insight Control server provisioning glossary: "Glossary " (page 48).
Troubleshooting plus known issues and restrictions	The Troubleshooting index in the online help is a repository for all problem/recommendation information provided by IC server provisioning developers. See the Insight Control server provisioning section of the *HP Insight Control Release Notes* available at http://www.hp.com/go/insightcontrol/docs. See the Insight Control server provisioning section of the *HP Insight Management Support Matrix* available at http://www.hp.com/go/insightcontrol/docs.
User interface	In the general How do I ...? section of the online help see the topic: Navigate the user interface.
Migrating from HP Insight Control server deployment	See the *Data Migration from Insight Control server deployment to Insight Control server provisioning* white paper, available at http://www.hp.com/go/insightcontrol/docs.
White papers	White papers on various topics are available at http://www.hp.com/go/insightcontrol/docs.

1.1 Components of Insight Control server provisioning

The following diagram illustrates how the IC server provisioning virtual appliance networking, Media Server, target servers, and an optional HP Matrix Operating Environment work together.

Figure 1 Insight Control server provisioning components



- The **Appliance** is the HP Insight Control server provisioning product, which is delivered as a virtual machine optimized to run the application.
- The Insight Control server provisioning appliance comes with an embedded **DHCP server**. Depending on your environment, you may configure this server for use or disable it via the appliance UI **Settings** screen. See "Deciding whether to use a DHCP server internal or external to the appliance" (page 10) for additional information.
- The **Appliance IP address** is the IP address assigned to the appliance. Use this IP address to browse to the appliance via a supported **Browser**.
- The **Deployment IP address** is the IP address used by the deployment engine within the appliance. It 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 **Appliance IP address**. If you are using IC server provisioning with the HP Matrix Operating Environment, this is the IP address to provide to **Matrix OE**.
- The **Target server** represents a server managed by IC server provisioning. Each managed server runs an **Agent**, which is software used to make changes to the server. The agent is used for software installation and removal, software and hardware configuration, and server status reporting.
- The **Media Server** contains vendor-supplied OS media used during OS provisioning. It may also contain media for other purposes, such as firmware and driver updates, and is also where captured images are stored. The Media Server is a separate server from the Insight Control server provisioning appliance and is not included as part of the appliance backup and restore actions.

1.2 Adding servers

Before you can run a job on a target server, that server must first be added to Insight Control server provisioning. There are multiple ways to add servers to your appliance. The following sections describe those methods and outline their differences. See also "Adding servers that are already running an operating system" (page 41).

1.2.1 Adding a server via its iLO

You can add a bare metal HP ProLiant server to Insight Control server provisioning by providing the server's embedded iLO management processor's access information. This is done by entering the iLO's IP address, user name, and password on the appliance's **Add server** screen. The appliance then contacts the iLO, verifies the connection, and adds the server to your **Servers** list. A REST API is also available to add a server via its iLO (see "REST call to add a server via iLO" (page 37)

By default, when you add a server via its iLO, the appliance uses the iLO to boot the server into the default service OS specified on the appliance **Settings** screen. Booting the server into maintenance mode allows IC server provisioning to do a full discovery; all the server information required to populate the **Server** properties page is collected. This process takes several minutes as the server's power is cycled and it boots.

You may opt to not bring the server into maintenance mode by selecting that option on the **Add server** page. This adds the server to the **Servers** list with the display name **ILOHOST_<*iLO IP address*>** and no server properties are available on the **Servers** properties page. This process takes less time because the server does not have to boot.

A server may have a Build Plan run on it whether it is in maintenance mode or not, because most Build Plans boot the server to maintenance mode if it is not there already.

1.2.2 PXE booting a server into maintenance mode

Another way to add a server to IC server provisioning is by PXE booting that server into a service OS. When the server completes the boot process, the agent in the service OS contacts the appliance and automatically registers it with the appliance, where the server shows up in the **Servers** list. To add a server this way, simply power the server on.

If the target server has no OS installed, it will automatically try to PXE boot. If there is an OS installed on the server, you will need to watch the console and press the appropriate key to trigger a PXE boot.

The server will boot to the default service OS specified on the appliance **Settings** screen.

NOTE: A server added via PXE boot will automatically have a special access account created on the server's iLO with the user name `hp_automatic_integration_user` and a randomly generated password. Do not delete this account or change its password on your iLO.

1.2.3 Deciding which method to use to add a server

Use the following points to help you decide which method to use when adding servers.

Reasons to add servers via iLO

- You have the iLO credentials for your target servers.
- You have Gen8 or newer servers and want to use HP Intelligent Provisioning.
- You don't want to PXE boot your Gen8 or newer servers.
- You don't want a special access account automatically created on your iLOs.

Reasons to boot to maintenance mode when using iLO

- You want to discover all the server information so you can see it and use it for search in the UI.
- You want to verify the server network connection before running a Build Plan.
- You will be running a Build Plan with network personalization, so you must establish the server's deployment NIC. (Network personalization cannot be used unless the server has been booted to maintenance at least once.)
- The Build Plan you want to run requires the default service OS, so this will save time later.

- You want to see the server listed by its default DNS name.

Reasons to not boot to maintenance mode when using iLO

- You want to run a Build Plan immediately and do not want to wait for the server to boot.
- You want to leave the server powered off until you are ready to install it.
- All your servers are of the same type so you do not need the full properties information.

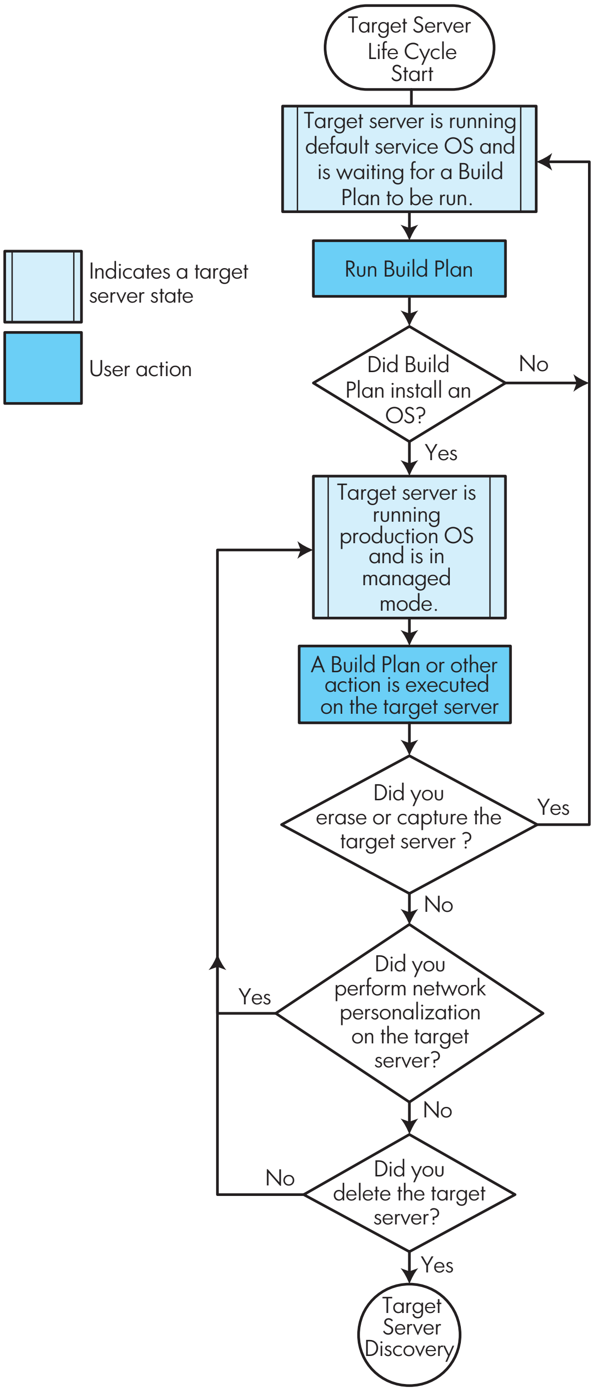
Reasons to PXE boot

- You do not have iLO credentials for your target servers.
- You prefer PXE for all your needs.
- You do not want to use Intelligent Provisioning on your Gen8 or newer servers.
- You prefer the simplicity of a power-on discovery because your servers automatically PXE boot.
- You have a large number of servers, making manual entry of iLO credentials impractical.

1.3 Server life cycle

The following diagram illustrates the typical life cycle for a target server managed by Insight Control server provisioning.

Figure 2 Insight Control server provisioning target server life cycle


Target Server Life Cycle Start
Target server is running default service OS and is waiting for a Build Plan to be run.
Indicates a target server state
User action
Run Build Plan
Did Build Plan install an OS?
No
Yes
Target server is running production OS and is in managed mode.
A Build Plan or other action is executed on the target server
Did you erase or capture the target server ?
Yes
No
Did you perform network personalization on the target server?
Yes
No
Did you delete the target server?
No
Yes
Target Server Discovery

2 Configuring appliance settings

2.1 Network configuration

2.1.1 Deciding whether to use a DHCP server internal or external to the appliance

HP Insight Control server provisioning requires a DHCP server to provide IP addresses to target servers during the provisioning process. Insight Control server provisioning has a DHCP server internal to the appliance you may use, or you can set up your own DHCP server external to the appliance. This section is meant to help you decide which is better for your facility.

1. You should first consider your DHCP requirements when provisioning servers: IP address only or extended DHCP options.

   IP address only

   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
   - Your target servers are all HP ProLiant Gen8 series or newer
   - You will use the embedded HP Intelligent Provisioning features of your 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

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

   The DHCP server internal to the appliance

   Your Insight Control server provisioning 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 subnet your appliance is in
   - 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

NOTE: The appliance 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.

2.1.2 Setting up a DHCP server external to the appliance

The Insight Control server provisioning appliance can support either using the DHCP server internal to the appliance, 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" (page 10) for details.

Below are instructions for configuring an external Windows DHCP server or an external Linux ISC DHCP server.

NOTE: HP recommends setting the lease time on your DHCP server to at least one day to prevent issues caused by time synchronization.

NOTE: 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 your DHCP server is necessary beyond the ability to provide an IP address to target servers and possibly extending the lease time.

NOTE: If you decide to use an external DHCP server, make sure **Service provided by appliance** is set to `None` on the appliance **Settings DHCP** page.

NOTE: You can find the deployment IP address on the **Settings Appliance** page under **Deployment IP**.

Procedure 1 To set 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 your DHCP server IPv4 global settings:

   Table 2 Windows DHCP IPv4 global settings

Code	Option name	Data type
186	`buildmgr_ip`	IP Address
187	`buildmgr_port`	Word

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

   Table 3 Windows DHCP options

Option number	Option name	Option value
66	Boot server	*<Deployment IP address of appliance>*
67	Boot filename	pxelinux.0
186	buildmgr_ip	*<Deployment IP address of appliance>*
187	buildmgr_port	0x1F51

Procedure 2 To set 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. Be sure to set the lease time to at least one day. Here is an example:

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

2. The following lines must be included in 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 your appliance to PXE boot servers.

3 Backing up and restoring your appliance

3.1 Overview

Insight Control server provisioning provides services to back up and restore an appliance. If an appliance is lost or corrupted, it might be necessary to restore the appliance from a backup.

A backup contains configuration settings and management data and is stored in a file of proprietary format.

REST APIs and sample scripts are provided to perform backup and restore operations. Sample scripts are available on the Insight Control server provisioning media and in the product download zip file.

A backup can be restored on the same appliance or on a different appliance than the one from which the backup was created. If an appliance fails and cannot be repaired, a backup can be restored on a replacement appliance.

To successfully restore a backup, the appliance must be running a version of the firmware that is compatible with the backup. Versions are compatible if the first two components of the version number are the same.

During a restore, the appliance firmware reconciles the data in the backup with the current state of the managed environment. There are some discrepancies that restore cannot resolve automatically. After a restore completes, the appliance administrator manually resolves any remaining inconsistencies, which are presented as alerts.

△ **CAUTION:** Restoring a backup replaces all management data and most configuration settings on the appliance. The appliance is not operational during a restore. It can take several hours to perform a restore. A restore cannot be cancelled or undone once it has started. If a nonrecoverable error occurs during a restore, you will have to download a new appliance template as described in the *HP Insight Control Server Provisioning Installation Guide*, available at http://www.hp.com/go/insightcontrol/docs. Restore should only be used to recover from catastrophic failures; it should not be used for minor problems that can be resolved in other ways.

3.2 Creating and downloading an appliance backup

3.2.1 Recommended backup procedures

HP recommends regular backups, preferably once a day. Backups are taken while the appliance is in use and normal activity is taking place. It is not necessary to wait for tasks to stop before creating a backup. A backup is restored by uploading it onto the appliance and then requesting the appliance restore from the backup.

A backup should be performed before and after updating the appliance firmware.

HP recommends using an enterprise backup/restore product such as HP Data Protector to archive backup files. REST APIs are provided for integration with enterprise backup/restore products.

After a backup is taken, the backup file must be downloaded from the appliance and stored in a safe place. The backup file must be downloaded before the next backup is performed to prevent it being overwritten by the next backup.

Only one backup can run at a time.

The backup file name has the format:

`<appliance host name>_backup_<yyyy-mm-dd_hhmmss>.bkp`

For example: `myhost_backup_2012-10-01_092700.bkp`. In this example the backup was created for the appliance host name `myhost` on October 1, 2012 at 9:27 a.m.

Only users with roles of Infrastructure or Backup Administrator have permission to create a backup. Only an Infrastructure Administrator may restore a backup.

3.2.2 Backup REST API overview

The backup REST API provides REST calls to:

- request a backup
- check the backup status
- download the completed backup
- cancel a backup

These calls are summarized in the table below. The backup REST API calls require a session ID for authorization you obtain by issuing the REST request to log in to the appliance as a user with the role of Backup or Infrastructure Administrator.

REST call	Request headers	Request body	Response headers	Response body	Description
POST https://{appl}/rest/backups/	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A task resource which contains a URI for checking the backup status and an associatedResourceUri for getting detailed information about the backup	Request the appliance to take a backup
GET https://{appl}/{uri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A task resource which contains the current backup status	Get backup status
GET https://{appl}/{associatedResourceUri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A backup resource which contains detailed information about a backup including the downloadUri for downloading the backup	Get detailed information about the requested backup including the download URI
GET https://{appl}/{downloadUri}	auth: session ID, accept-language: locale, accept-content: application/octet-stream; q=0.8, application/json, X-API-Version: 1	N.A.	content-disposition: the backup file name	The backup file content	Download a backup
GET https://{appl}/rest/backups	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A SimplePaginatedCollection which contains the last backup resource	Get detailed information about the last backup
DELETE https://{appl}/{associatedResourceUri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A task resource which contains a URI for checking the backup status	Cancel a backup

3.2.3 Sample backup script

An example PowerShell script is provided for creating and downloading a backup. The sample script is available on the Insight Control server provisioning media and in the product download zip file.This script uses PowerShell version 3.0. It makes REST calls to create and download a backup. The sample script can be scheduled to run automatically on a regular basis.

3.2.3.1 How to use the sample backup script

You can copy and paste the sample script into a file on a Windows system that runs PowerShell version 3.0.

HP highly recommends you install `cURL` to improve performance. The sample script works without `cURL`, but it might take several hours to download a large backup. You can download `cURL` at http://curl.haxx.se/download.html. You might also need to install the Microsoft Visual C++ Redistributable, `MSVCR100.dll`, which can be downloaded at http://www.microsoft.com/download/en/details.aspx?id=14632 (64 bit) or http://www.microsoft.com/download/en/details.aspx?id=5555 (32 bit). Make sure the path environment variable includes the path for `cURL`.

You can run this script interactively or in batch mode. To run the script interactively, run it without any parameters. The script will prompt you to enter the appliance host name, appliance user name and password, and the name of a file for storing these parameters for batch mode executions. Enter the name and password of a user with the Backup Administrator or Infrastructure Administrator role. The user name and password will be stored encrypted. To run the script in batch mode, specify the name of the file containing the parameters on the command line.

HP recommends you run the script interactively the first time. Then you can schedule the script to run automatically in the background using the parameter file created by the first run.

You can edit the sample script to customize it for your environment.

3.2.3.2 Example output

```
Enter Appliance name (https://ipaddress)
https://10.10.10.10
Enter Username
*************
Enter password
********
Would you like to save these credentials to a file? (username and password encrypted)
y
Enter file path and file name to save credentials  (example: C:\users\bob\machine1.txt)
C:\users\jerry\jerry-vm.txt
The file 'C:\users\jerry\jerry-vm.txt' already exists.
Overwrite existing credentials for this machine?
y
run backup?
y
Login completed successfully.
Backup initiated.
Checking for backup completion, this may take a while.
 Backup progress: [====================]  100 %

Obtained backup file URI, now downloading
Backup download complete!
Backup can be found at C:\Users\jerry\Documents
If you wish to automate this script in the future and re-use login settings currently entered,
then provide the file path to the saved credentials file when running the script.
ie:  C:\Users\jerry\backup.ps1  filepath
```

3.2.3.3 Sample backup script main processing and functions

The sample script does the following to create and download a backup:

1. Calls `queryfor-credentials()` to get the appliance host name, user name, and password by either prompting the user or reading the values from a file.
2. Calls `login-appliance()` to issue a REST request to obtain a session ID used to authorize backup REST calls.

3. Calls `backup-appliance()` to issue a REST request to start a backup.
4. Calls `waitFor-completion()` to issue REST requests to poll for backup status until the backup completes.
5. Calls `get-backupResource()` to issue a REST request to get the download URI.
6. Calls `download-backup()` to issue a REST request to download the backup.

The following table provides an overview of the functions in the sample script.

Function	Description	Parameters	Output
`queryfor-credentials`	Gathers information from user if in manual entry mode (script ran with zero arguments) or runs silently and gathers info from specified path (script ran with argument).	N.A.	A Json-formatted object that contains the values needed to login.
`login-appliance`	Sends a web request to the appliance to obtain a authorized sessionID.	'username': The username to log into the remote appliance. 'password': the password associated with the username. 'hostname': the appliance to log in to.	A hash table containing the sessionID
`backup-appliance`	Sends a request to start a backup.	'authValue': The authorized sessionID given by login-appliance. 'hostname': The appliance address to connect to.	Outputs a hash table containing the response body from the backup request.
`waitFor-completion`	Checks the status of the backup every five seconds and stops when status changes from running to a different status.	'taskManager': The response body from the backup-appliance function. 'authValue': The authorized session ID from login-appliance. 'hostname': The appliance to send the request to.	Outputs a hash table containing the task resource which contains the backup status and a URI to get detailed information about the backup.
`get-backupResource`	Gets the backup resource which contains detailed information about the backup including the URI to download the backup.	'taskResource': The task resource that contains the backup resource URI. 'authValue': The authorized session ID. 'hostname': the appliance to send the request to.	Outputs a hash table containing the backup resource which contains the URI to download the backup file.
`download-backup`	Downloads the backup file from the appliance to the local system.	'backupResource': the backup resource that contains the URI to download the backup. 'authValue': The authorized session ID. 'hostname': The appliance to send the request to.	Outputs a string containing the absolute path of the backup file on the local system.

3.2.3.4 Troubleshooting tips

The following table contains REST API error codes and resolutions.

HTTP error	Response Body Error Code	Description	Resolution
401 Unauthorized	AUTHORIZATION	An incorrect user name or password was specified.	Specify the correct user name and password.
404 Not Found	RESOURCE_NOT_FOUND	The incorrect URI was specified.	Specify the correct URI. You may need to wait for the appliance software to start. It may help to issue the REST request to get the last backup resource or take another backup to find out the correct URI.
409 Conflict	BACKUP_IN_PROGRESS	The requested operation cannot be performed because a backup is in progress. Only one backup can run at a time.	Wait until the backup finishes or cancel the backup and then retry the operation.
409 Conflict	BACKUP_DOWNLOAD_IN_PROGRESS	The requested operation cannot be performed because a backup is being downloaded. A backup cannot be taken while a download is in progress.	Wait until the download finishes and then retry the operation.
409 Conflict	BACKUP_UPLOAD_IN_PROGRESS	The requested operation cannot be performed because a backup is being uploaded in preparation for a restore.	Wait until the upload and restore finish and then retry the operation.
409 Conflict	BACKUP_RESTORE_IN_PROGRESS	The requested operation cannot be performed because a restore is in progress.	Wait until the restore finishes and then retry the operation.
500 Internal Server Error	Various	An internal error occurred.	Create a support dump. Then reboot the appliance and retry the operation.

3.3 Uploading and restoring a backup

3.3.1 Recommended restore procedures

A backup can be restored on the same appliance or a different appliance than the one from which the backup was created. If an appliance fails and cannot be repaired, a backup can be restored on a replacement appliance.

⚠ **CAUTION:** The restore must be to an appliance with the same network settings as the original appliance.

During a restore, the appliance firmware reconciles the data in the backup with the current state of the managed environment. There are some discrepancies that restore cannot resolve automatically.

After a restore completes, the appliance administrator must manually resolve any remaining inconsistencies, which are identified with alerts.

△ **CAUTION:** Restoring a backup replaces all management data and most configuration settings on the appliance. The appliance is not operational during a restore. It can take several hours to perform a restore. A restore cannot be cancelled or undone once it has started. If a nonrecoverable error occurs during a restore, you will have to download a new appliance template as described in the *HP Insight Control Server Provisioning Installation Guide*, available at http://www.hp.com/go/insightcontrol/docs. Restore should only be used to recover from catastrophic failures; it should not be used for minor problems that can be resolved in other ways.

3.3.2 Preparing for a restore

Follow these steps to prepare for a restore:

1. If you are performing a restore on a new appliance, install the new appliance as described in the *HP Insight Control Server Provisioning Installation Guide* available at https://www.hp.com/go/insightcontrol/docs.
2. If this is a new appliance, make sure the network settings are the same as the original appliance.
3. Stop all automatically scheduled backups before starting a restore. After the restore completes, restart the automatically scheduled backups.
4. Before starting a restore, you might want to create a support dump. The support dump can be used to diagnose failures that happened before the restore.
5. Before starting a restore, you might want to download the existing audit logs. Restore will replace the audit logs with those that were included in the backup.
6. Before starting a restore, make sure you know the appliance user names and passwords in effect at the time of the backup. Restore resets the user names and passwords to the ones configured when the backup was taken.
7. If you are restoring to a different appliance than the one from which the backup was taken, you must take extra precautions before starting the restore. Decommission the original appliance or reconfigure it to no longer manage the devices it was managing when the backup was performed. Serious errors can occur if multiple appliances attempt to manage the same devices.
8. Before starting a restore, all users logged into the appliance must log out. Otherwise, users will lose their work. Users are automatically logged out as soon as a restore starts. Users will be blocked from logging in during a restore.
9. If the appliance being restored is running a version of the firmware incompatible with the backup, install a compatible version of the firmware on the appliance before uploading the backup. The platform type, hardware model, major number, and minor number must match to restore a backup. The revision and build numbers do not need to match. The format of the appliance firmware version is:

   ```
   <major number>.<minor number>.<revision number>-<build number>
   ```

   If the backup is incompatible with the firmware on the appliance, the upload returns an error. If this happens, update the firmware or select a different backup.
10. Make the backup accessible to the system where you plan to issue the upload request. If you are using an enterprise backup/restore product to archive backup files, take any steps required by your backup/restore product to prepare for the restore.

3.3.3 Performing a restore

Follow these steps to perform a restore.

NOTE: If you attempt to connect to the appliance while a restore is under way, you will not be able to log in. You will see the appliance maintenance page and a message saying that a restore is in progress.

1. Complete the steps in "Preparing for a restore" (page 18) before beginning.
2. Issue the REST request to log in to the appliance as a user with a Infrastructure Administrator role.
3. Issue the REST request to upload the backup file to the appliance. Specify the session ID returned by the login request in the `auth` header.
4. Check the response to the upload request to make sure the upload succeeded. The upload will fail if the backup version is incompatible with the firmware running on the appliance or if the backup is corrupted. If the backup is incompatible with the firmware on the appliance, update the firmware and then retry the upload or upload a different backup. If the backup is corrupt, upload a different backup.
5. Issue the REST request to start the restore.
6. Check the response to the restore request to make sure the restore started successfully. The restore will fail if the backup version is incompatible with the firmware running on the appliance or if the backup is corrupted. If the backup is incompatible with the firmware on the appliance, update the firmware and then retry the restore or upload a different backup. If the backup is corrupt, upload a different backup.
7. Issue REST requests periodically to get restore progress information. A restore can take several hours to complete. The amount of time required depends on the size of the managed environment. The REST API returns the percentage complete and a description of the restore step in progress.
8. Once the restore completes, the REST API returns a message reporting the restore completed successfully.
9. After the restore completes, users can log in to the appliance. A restore resets the user names and passwords to those in effect at the time of the backup.
10. There will be an alert indicating the restore completed successfully.
11. During the restore, the appliance firmware automatically reconciles the data in the backup with the current state of the managed environment. If there are any discrepancies that cannot be resolved automatically, resolve them manually after the restore. After the restore completes, log in to the appliance to check for alerts related to inconsistencies. Follow the instructions in the alert messages to resolve the discrepancies.
12. After resolving any discrepancies detected by the restore, perform a new backup. Restart the regularly scheduled backups.
13. If an unrecoverable error occurs during a restore, the restore REST API calls will fail. An error message will be displayed indicating the restore failed and that it is necessary to deploy a new appliance from the HP-provided template as described in the *HP Insight Control Server Provisioning Installation Guide* available at http://www.hp.com/go/insightcontrol/docs.

3.3.4 Restore REST API overview

The restore REST API provides REST calls to:

- upload a backup to the appliance
- start a restore
- check the restore status

These calls are summarized in the table below. The REST API calls to start a restore require a session ID for authorization. The session ID is obtained by issuing the REST request to log in to the appliance as a user with the role of Infrastructure Administrator. The REST API calls to get restore status information do not require a session ID.

REST call	Request headers	Request body	Response headers	Response body	Description
POST https://{appl}/rest/backups/archive	auth: session ID, content-type: multipart/form-data, accept-language: locale, accept-content: application/json, X-API-Version: 1	Multipart form data containing the backup file	N.A.	A backup resource which contains the upload status, an id for restoring the backup, and other information about the backup	Upload a backup to the appliance
POST https://{appl}/rest/restores	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	A json object that contains 2 elements. These elements are "type" with value "RESTORE" and "backupIdToRestore" set to the ID returned by the upload request	N.A.	A restore resource which contains restore status and a URI for getting restore progress information	Start restoring an uploaded backup
GET https://{appl}/{uri}	accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A restore resource which contains the current restore status and progress information	Get restore progress information
GET https://{appl}/rest/restores	accept-language: locale, accept-content: application/json, X-API-Version: 1	N.A.	N.A.	A SimplePaginatedCollection which contains the last restore resource	Get information about the last restore or a restore under way

3.3.5 Sample restore script

An example PowerShell script is provided for uploading and restoring a backup. This script uses PowerShell version 3.0. It makes REST calls to upload and restore a backup. HP highly recommends installing cURL to improve performance.

3.3.5.1 How to use the sample restore script

You can copy and paste the sample script into a file on a Windows system that runs PowerShell version 3.0.

HP highly recommends you install cURL to improve performance. The sample script works without cURL, but it might take several hours to download a large backup. You can download cURL at http://curl.haxx.se/download.html. You might also need to install the Microsoft Visual C++ Redistributable, MSVCR100.dll, which can be downloaded at http://www.microsoft.com/download/en/details.aspx?id=14632 (64 bit) or http://www.microsoft.com/download/en/details.aspx?id=5555 (32 bit). Make sure the path environment variable includes the path for cURL.

You can run this script interactively to upload and restore a backup or to get status about a restore under way.

To upload and restore a backup, run the script without any parameters. The script will prompt you to enter the appliance host name, appliance user name and password, and the backup file path. Then the script will upload the backup, start the restore, and get restore progress information until the restore completes.

To get status about a restore under way, run the script with the `-status` parameter and the appliance host name in the form `https://{hostname}`.

3.3.5.2 Example output

Example output from running the script to upload and restore a backup:

```
PS C:\Users\Joe> C:\Users\Joe\Documents\restore.ps1
Restoring from backup is a destructive process, continue anyway?
y
Enter directory backup is located in (ie: C:\users\joe\)
C:\users\Joe\Documents
Enter name of backup (ie: appliance_vm1_backup_2012-07-07_555555.bkp
joe_vm_backup_2012-07-07_777777.bkp
Enter appliance IP address (ie: https://10.10.10.10)
https://10.10.10.1
Enter username
*************
Enter password
********
Login completed successfully
Uploading backup file to appliance, this may take a few minutes...
Upload complete.


Restore progress: [====================]  100 %
Restore complete!
```

Example output from running the script to get restore progress information:

```
C:\users\Joe\Documents\restore.ps1 -status https://10.10.10.1
Restore progress: [====================]  100 %
Restore complete!
```

3.3.5.3 Sample restore script main processing and functions

The sample script can be used to either start a restore or get progress information about an ongoing restore.

If no parameters are passed to the script, it uploads and restores a backup. It does the following:

1. Calls `query-user()` to get the appliance host name, user name and password, and backup file path.
2. Calls `login-appliance` to issue a REST request to get a session ID used to authorize restore REST calls.
3. Calls `uploadTo-appliance()` to upload the backup to the appliance.
4. Calls `start-restore()` to start the restore.
5. Calls `restore-status()` to periodically check the restore status until the restore completes.

If the `-status` option is passed to the script, it checks and reports the status of the last or an ongoing restore until the restore completes. It does the following:

1. Calls `recover-restoreID()` to get the URI for checking the status of the last or an ongoing restore.
2. Calls `restore-status()` to periodically check the restore status until the restore completes.

The following table provides an overview of the functions in the sample script.

Function	Description	Parameters	Output
query-user	Obtains information from user needed to interact with appliance.	N.A.	loginVals: a hash table that contains the information obtained from user.
login-appliance	Sends the user name and password to the appliance, and obtains an authorized session ID.	username: the user name obtained from query-user function. password: the password obtained from query-user function. hostname: the address of the appliance to send the login request to.	authInfo: the response body returned by the remote appliance, which includes the sessionID.
uploadTo-appliance	Uploads the designated backup file to the remote appliance.	filePath: The absolute file path to the backup file. authInfo: The session ID from the login response. hostname: The address of the appliance to upload the file to. backupFile: The name of the file being uploaded.	uploadResponse: the response body for the upload request, which contains the backup ID to be restored.
start-restore	Sends the request to restore the appliance from the backup.	authInfo: The session ID from the login response. hostname: The address of the remote appliance to send the request to. uploadResponse: The response body of the upload request.	restoreResponse: The response body from the restore request, which contains the ID of the ongoing restore.
restore-status	Checks the appliance for the status of the ongoing restore. Displays a progress status bar.	authInfo: the session ID obtained from the login request. hostname: the address of the remote appliance to send the request to. restoreResponse: The response body from the restore request. recoveredUri: The full URI needed to get restore status (only used when opening the script with the status flag).	N.A.
recover-restoreID	Used for when the connection is interrupted or the script closed. Sends a request to the server to get the URI of the ongoing restore task, and then passes the information to restore-status.	hostname: The remote appliance to send the request to.	Returns the URI of the last or ongoing restore.

3.3.5.4 Troubleshooting Tips

The following table contains REST API error codes and resolutions.

HTTP error	Response body error code	Description	Resolution
400 Bad Request	INVALID_PARAMETER	An invalid backup ID was specified.	Specify a valid backup ID. It must be in the form `<hostname>_backup_YYYY-MM-dd_HHmmss`
401 Unauthorized	AUTHORIZATION	An incorrect user name or password was specified.	Specify the correct user name and password.
404 Not Found	RESOURCE_NOT_FOUND	The incorrect URI was specified.	Specify the correct URI. You may need to wait for the appliance software to start. You can find out the correct URI using this guide. It may help to issue the REST request to get the last backup resource.
409 Conflict	BACKUP_IN_PROGRESS	The requested operation cannot be performed because a backup is in progress. A backup cannot be uploaded or restored while the appliance is taking a backup.	Wait until the backup finishes or cancel the backup and then retry the operation.
409 Conflict	BACKUP_DOWNLOAD_IN_PROGRESS	The requested operation cannot be performed because a backup is being downloaded. A backup cannot be uploaded or restored while a download is in progress.	Wait until the download finishes and then retry the operation.
409 Conflict	BACKUP_UPLOAD_IN_PROGRESS	The requested operation cannot be performed because a backup is being uploaded.	Wait until the upload finishes and then retry the operation.
409 Conflict	BACKUP_RESTORE_IN_PROGRESS	The requested operation cannot be performed because a restore is in progress.	Wait until the restore finishes and then retry the operation.
500 Internal Server Error	Various	An internal error occurred.	Create a support dump. Try to restore a different backup.

4 Security considerations

Insight Control server provisioning is delivered as a security-hardened virtual appliance. The number of open ports and the protocols supported on them have been limited to the minimum necessary for the operation of Insight Control server provisioning.

4.1 Assumptions

The appliance should be on a deployment network, separate from the production network (see "Security best practices" (page 31) for more information). Additionally, access to the virtual appliance console should be restricted to authorized users (see "Restricting console access" (page 30) for more information).

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 a router between the management and deployment networks to provide access to the target iLOs via the deployment network.

Insight Control server provisioning 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.

4.2 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 appliance 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.

4.3 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.

4.4 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.

4.5 Authorization

Access to the appliance is restricted by roles, which describe what an authenticated user can do in the appliance. Each user must be associated with at least one role.

4.5.1 User accounts and roles

User login accounts on the Insight Control server provisioning appliance must be assigned a role. The role determines what the user account has permission to view and do. For instance, a Server Administrator cannot edit an OS Build Plan.

The following are the roles provided with IC server provisioning:

Infrastructure Administrator

- all privileges are granted so this role can perform any action on the appliance including management of deployment content (OS build plans, scripts and so on)

Server Administrator

- run OS Build Plans
- manage servers including add, delete, and modify servers
- cannot modify deployment content (OS Build Plans, scripts, configuration files, or packages)
- cannot manage users
- cannot change appliance settings

Backup Administrator

- can only perform backup and restore operations
- provided for use with backup scripting so Infrastructure Administrator credentials do not have to be saved in a script
- you cannot log into the appliance with these accounts

Read Only

- may only view appliance information

For information on how to add, delete, and edit user accounts, see the Insight Control server provisioning online help.

4.6 Auditing

The audit log contains a record of important actions performed on the appliance. The audit log can be downloaded by users in either the Infrastructure Administrator or Server Administrator roles; from **Settings**, select **Actions**→**Download audit log**. 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.

Additional detailed audit information for deployment targets is included in the audit log zip file. While all 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. While those operations are logged in the Matrix Operating Environment audit logs they are also logged on the Insight Control server provisioning appliance so the operations performed via that interface can be reconciled with those performed in the Matrix Operating Environment and those performed via the appliance UI.

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`. There may be additional actions recorded against internal users including `detuser`, `integration`, and `buildmgr`.

4.7 Communication protocols

4.7.1 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.

4.8 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.

NOTE: 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.

4.8.1 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.

4.9 Browser

4.9.1 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.

4.9.2 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 being browsed to. 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**.

4.9.3 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.

4.9.4 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.

4.10 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" (page 31)).

The `matrixuser` account is not a local user account that can access the UI. It is used through a different channel to drive the underlying SA Foundation from the Matrix Operating Environment. The password may be set through the UI and is never displayed. It can be reentered as often as needed in case the value is lost. This password is not stored in clear text and is not retrievable.

iLO credentials entered in the UI are stored in a recoverable form as they must be passed to iLO.

Media server credentials are stored in a recoverable form as they must be used to connect to the Media Server share.

The default passwords for OS installations can be stored in encrypted form. Please refer to the Insight Control server provisioning online help for more information on the default passwords for OSBPs.

4.11 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.

4.11.1 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.

The primary use of a REST connection is for scripted automated backup. A limited rights role for that purpose, the backup administrator, is provided so that the credentials stored with an automated backup script have only the rights necessary to perform the backup.

4.11.2 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" (page 27) for information on downloading the certificate.

4.12 Appliance hardening

4.12.1 Port list

The following table lists the ports that must be open for Insight Control server provisioning.

Port	Description
22 (tcp)	ssh
80 (tcp)	http
443 (tcp)	https
3001 (tcp)	SA agent communications
67 (udp)	DHCP
69 (udp)	TFTP
8017 (tcp, udp)	Agent gateway
8081 (tcp)	Agent cache
111 (tcp, udp)	RPC – for boot file NFS
2049 (tcp, udp)	NFS – for boot files only
892 (tcp, udp)	mountd
123 (udp)	ntp

4.12.2 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" (page 30). 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**.

4.12.3 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.

4.12.4 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 username**pwreset**.
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.

4.12.5 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" (page 35).

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.

4.12.6 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".

4.12.7 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 Insight Control server provisioning appliance web server. These cipher suites are for the connection between the browser and the IC server provisioning appliance.

Table 4 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

4.13 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.
- Media Server setup tool – no data included.
- WinPE generation tool – no data included.

4.14 Media Server security

Insight Control server provisioning requires a Media Server for hosting OS distributions, captured OS images, and HP SPPs separate from the appliance. This is either a Windows or Linux server and access to it should be controlled using standard operating system mechanisms.

The Windows Media Server setup utility enables NTLMv2 for better security. It creates a CIFS share on the specified directory and creates media and images subdirectories. The utility requests a user name to give access to the share and gives the user read/write access to the share. The utility also creates an IIS virtual directory on the media subdirectory with read-only access. The CIFS share is used for Windows deployment and image capture. The HTTP virtual directory is used for Linux and ESX deployment.

The credentials for the share user are stored in a recoverable format on the appliance and used in OS Build Plans to attach to the Media Server. The user provided for the share should have limited rights. The user needs to be able to read and write to the share but not login to the Media Server. A different user should be used for managing the Media Server system and OS distributions.

If Windows image capture is not going to be used, the share can be created read-only. When Windows image capture is being used, the media subtree can be made read-only for the share user via the Media Server operating system.

A white paper describes the steps necessary to manually set up a Linux Media Server – no utility is provided. The same limitations on the share user account and web-based access apply.

4.15 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" (page 30) 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.

    NOTE: 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.

5 Advanced topics

5.1 REST APIs to enable HP Support access or add a server via iLO

REST (Representational State Transfer) calls to enable/disable HP Support services access or to add a server via iLO require 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 or adds a server via iLO. Finally, the user session needs to be ended with a REST call for logging 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.

5.1.1 REST call to create the user session and get the 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:

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 userNname 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>\"}
```

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, 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 user/password is not correct.

5.1.2 REST call to logout of the user session

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

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, you will be returned an error diagnostics. Common errors are HTTP error 404 not found, if the URL is not correct.

5.1.3 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 the user session and get the authentication token" (page 34) for details on 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 the user session" (page 35) for details on making the third REST call to logout of the user session.

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

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
```

5.1.4 REST call to add a server via iLO

You can use REST calls to add a server via its iLO.

Programmatically, one will need to make three REST calls to the Insight Control server provisioning appliance. The first call is used to obtain an authentication token or session ID, then using this session ID, you make the REST call to perform the actual registration. Finally, the third call logs out of the session.

See "REST call to create the user session and get the authentication token" (page 34) for details on making the first REST call to create the user session.

The second REST call is to add a server via iLO. In this REST call you will need to provide the *<user-authentication-token>* you received from the login REST call, and you will need to pass the IP address of the iLO as well as the iLO administrator user/password.

Finally, see "REST call to logout of the user session" (page 35) for details on making the third REST call to logout of the user session.

There are two REST calls that can be used to add a server via its iLO: one is used to add the server and boot it into a maintenance mode, the other is used to add the server and not boot into a maintenance mode. If optional request parameter "addstyle" is specified, the server will be added without putting the server into a maintenance mode. If this parameter is not present, the server will be booted into a maintenance mode.

REST call to add a server via iLO and server will boot into a maintenance mode:

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

REST component	Description
URL:	https://<appliance-hostname-or-address>/rest/os-deployment-ilos where you supply <appliance-hostname-or-address>
Message Type:	POST
HTTP Headers:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: <user-authorization-token> where you supply <user-authorization-token>

REST component	Description
Request Body:	{"type":"OSDIlo","username":"<iLO-administrator-user>","password": "<iLO-administrator-password>","port":<port>,"ipAddress":"<iLO-IP-address>"} Type is the resource name. You supply the <iLO-administrator-user>, <iLO-administrator-password>, the port to use in connecting to iLO and the IPv4 <iLO-IP-address>
Response Body:	{"uri":"/rest/os-deployment-jobs/JobID"} will return URI with Job ID.

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

cURL command on Linux:

```
curl -i -k -X POST -H "auth: <user-authorization-token>" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d '{"type":"OSDIlo","username":"<iLO-administrator-user>",
"password":"<iLO-administrator-password>",
"port":443,"ipAddress":"<iLO-IP-address>"}'
```

cURL command on Windows:

```
curl -i -k -X POST -H "auth: <user-authorization-token>" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d {\"type\":\"OSDIlo\",\"username\":\"<iLO-administrator-use>r\",
\"password\":\"<iLO-administrator-password>\",
\"port\":443,\"ipAddress\":\"<iLO-IP-address>\"}
```

Response on success:

```
HTTP/1.1 202 Accepted
Date: Wed, 20 Feb 2013 17:33:30 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

This response is accompanied by returned job URI.
```

Below is an example script that logs into the appliance, adds the server via iLO and logs out. This script uses cURL.

```
#!/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=login
-d '{"userName":"<administrator-name>","password":"<administrator-password>"}' | perl -e 'while (<>)
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This script invokes a job to add iLO-managed server.
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json" -H "accept:application/json"
-H "accept-language:en-us"  https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d '{"type":"OSDIlo","username":"<administrator-name>","password":"<administrator-password>",
"port":443,"ipAddress":"<iLO-IP-address>"}'
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

REST call to add a server via iLO and server will not boot into a maintenance mode:

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

REST component	Description
URL:	https://<appliance-hostname-or-address>/rest/os-deployment-ilos/?addstyle=old where you supply <appliance-hostname-or-address>
Message Type:	POST

REST component	Description
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:	{"type":"OSDIlo","username":"<iLO-administrator-user>","password": "<iLO-administrator-password>","port":<port>,"ipAddress":"<iLO-IP-address>"} Type is the resource name. You supply the <iLO-administrator-user>, <iLO-administrator-password>, the port to use in connecting to iLO and the IPv4 <iLO-IP-address>
Response Body:	{"uri":"/rest/os-deployment-jobs/JobID"} will return URI with Job ID.

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

cURL command on Linux:

```
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos?addstyle=old
-d ‘{"type":"OSDIlo","username":"<iLO-administrator-user>”,
”password”:”<iLO-administrator-password>”,
”port”:443,”ipAddress”:”<iLO-IP-address>”}’
```

cURL command on Windows:

```
curl -i -k -X POST -H "auth: <user-authorization-toke>n" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos?addstyle=old
-d {\"type\":\"OSDIlo\",\"username\":\"<iLO-administrator-user>\”,
\”password\”:\”<iLO-administrator-password>\”,
\”port\”:443,\”ipAddress\”:\”<iLO-IP-address>\”}
```

Response on success:

```
HTTP/1.1 202 Accepted
Date: Wed, 20 Feb 2013 17:33:30 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

This response is accompanied by returned job URI.
```

Below is an example script that logs into the appliance, adds the server via iLO and logs out. This script uses cURL.

```
#!/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=login
-d '{"userName":"<administrator-name>","password":<administrator-password>"}' ' | perl -e 'while (<>)
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This script invokes a  job to add iLO-managed server.
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos/?addstyle=old
-d '{"type":"OSDIlo","username":"<iLO-administrator-user>","password":"<iLOadministrator-password>",
"port":443,"ipaddress":"<iLO-IP-address>"}'
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

Once the registration process starts, a user will see two iLO related jobs in the left hand side column of the **Jobs** page. First job — "Registers IloManagerService" will contain the job details of adding a server through iLO. Second job — "Add iLO-managed Server" will contain job details booting a server into default service OS, usually Linux PE.

Common errors from registering a server via its iLO:

500 — Internal Server Error

Resolution: Create a support dump

403 — Request Forbidden

Cause: Failed to login a user with provided credentials

Resolution: Try logging in again with valid credentials

409 — Conflict

Cause: iLO IP Address that user provided was already used to register and iLO

Resolution: Delete the server with duplicate iLO and try again or use different iLO address

404 — Not Found

Cause: The server cannot be found

Resolution: Verify that server exists, or not deleted

400 — Bad Request

Cause: When making a REST call one of the supplied parameters could be missing, malformed or invalid.

Resolution: Verify that parameters are in correct form.

5.2 REST API to create and download a support dump

In addition to being able to download a support dump from your Insight Control server provisioning appliance via the UI, 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 Insight Control server provisioning appliance. The first call creates the support dump and leaves it on the appliance, while the second call downloads it.

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:

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 03:11:25 MDT 2012", "modified":null }

REST component	Description
	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, you will be returned an error diagnostic. 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:

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:	GET
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” option.

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, you will be returned an error diagnostic. Common errors are HTTP error 404 not found if the URL is not correct.

5.3 Adding servers that are already running an operating system

Servers currently running a production operating system can be added to IC server provisioning without rebooting by adding the HP Server Automation (SA) agent to the target server, and then registering the server’s iLO.

To add the HP Server Automation agent to a managed server:

1. Determine the SA agent filename from `http://`*`xxx.xxx.xxx.xxx`*`:8081` where *`xxx.xxx.xxx.xxx`* is the Deployment IP address or DNS name of the IC server provisioning

virtual appliance. Look for the files with `.current` extension. There are different agent files depending on the operating system version and architecture type.

The SA Agent files are listed below:

Operating System	SA Agent to download
Windows 2008 x64	opsware-agent-NT-6.0-X64.current
Windows 2008 R2 x64	opsware-agent-NT-6.1-X64.current
Windows 2012 x64	opsware-agent-NT-6.2-X64.current
Red Hat EL 5.x	opsware-agent-LINUX-5SERVER-X86_64.current
Red Hat EL 6.x	opsware-agent-LINUX-6SERVER-X86_64.current
SLES 11	opsware-agent-LINUX-SLES-11-X86_64.current

NOTE: There is no SA agent that runs on VMware ESXi.

2. Download the SA agent using the exact filename in the url without the `.current` extension, `http://`*`xxx.xxx.xxx.xxx`*`:8081/<`*`filename`*`>` where `<`*`filename`*`>` is name of the SA agent file.

IMPORTANT: Do not download the file by listing all the agent files and then using the right-click **Save** link to save it. The file will contain only HTML content and not work with IC server provisioning.

3. Once a Windows agent file is downloaded, rename the filename with a `.exe` extension. For Linux, the filename without an extension is appropriate.
4. Install the SA agent on the target server with the parameters, `-s --opsw_gw_list coreip:3001` where `coreip` is the IP address of the IC server provisioning virtual appliance. Be sure to use the Deployment IP address, not the Appliance IP address.
5. Verify the target server shows up in IC server provisioning.
6. Before an OSBP can be run on this target server, the server's iLO must also be registered with IC server provisioning. This can be done by either of the following ways:
   a. You can add each target server's iLO information manually. From the IC server provisioning **Servers** page, choose **Actions**→**Add Servers**, enter the iLO IP address and credentials of a target server, and be sure to check the box that says **Do not boot to maintenance**. Choose **Add** to initiate the iLO registration or **Add+** to enter more IP addresses.
   b. You can add each server's iLO information using the programmatic REST (see"REST call to add a server via iLO" (page 37)). Be sure to use the option that does not boot the server into maintenance.
7. You can verify that the iLO has been properly registered with the server by going to the **Servers** page and seeing if the iLO IP address is listed there.

6 Support and other resources

6.1 Contacting HP

6.1.1 Before you contact HP

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

- Technical support registration number (if applicable)
- Insight Control server provisioning version
- Applicable error message
- Third-party hardware or software
- Operating system type and revision level
- Support dump (optional): "Creating a support dump" (page 43)

6.1.2 Creating a support dump

6.1.2.1 When you might want to create a support dump

- Some error messages displayed by Insight Control server provisioning recommend you create a support dump of the appliance so it can be sent to HP Support for analysis.
- If 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.
- In some cases HP Support might request you create a support dump as part of a service engagement.

6.1.2.2 How to create a support dump

This 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. The following procedure uses the UI. You can also use a REST API if the UI is not available (see "REST API to create and download a support dump" (page 40)

1. Log in to the appliance with administrator privileges.
2. Navigate to the **Settings** page via 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 on delivering the support dump.

6.1.2.3 Support dump contents

A support dump collects the following information from your appliance.

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

NOTE: 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

6.1.3 HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

For HP technical support:

- In the United States,for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html)

6.1.4 Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website: http://www.hp.com/country/us/en/contact_us.html. After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

6.2 Related information

6.2.1 Documents

The following documents are available at http://www.hp.com/go/insightcontrol/docs.

- *HP Insight Control Server Provisioning Online Help* (in PDF form)
- *HP Insight Control Server Provisioning Administrator Guide*
- The white paper *Data Migration from HP Insight Control server deployment to HP Insight Control server provisioning*

6.2.2 Websites

- Software download website: http://www.hp.com/go/insightupdates
- HP Insight Control server provisioning documentation website: http://www.hp.com/go/insightcontrol/docs

6.3 Typographic conventions

This document uses the following typographical conventions:

`%`, `$`, or `#`	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells. A number sign represents the superuser prompt.
audit(5)	A manpage. The manpage name is *audit*, and it is located in Section 5.
`Command`	A command name or qualified command phrase.
`Computer output`	Text displayed by the computer.
Ctrl+x	A key sequence. A sequence such as **Ctrl+x** indicates that you must hold down the key labeled **Ctrl** while you press another key or mouse button.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
ERROR NAME	The name of an error, usually returned in the `errno` variable.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	The defined use of an important word or phrase.
`User input`	Commands and other text that you type.
`Variable`	The name of a placeholder in a command, function, or other syntax display that you replace with an actual value.
[]	The contents are optional in syntax. If the contents are a list separated by |, you must choose one of the items.
{}	The contents are required in syntax. If the contents are a list separated by |, you must choose one of the items.
...	The preceding element can be repeated an arbitrary number of times.
□	Indicates the continuation of a code example.
|	Separates items in a list of choices.
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.

CAUTION A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.

IMPORTANT This alert provides essential information to explain a concept or to complete a task

NOTE A note contains additional information to emphasize or supplement important points of the main text.

6.4 Customer self repair

HP products are designed with many Customer Self Repair parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period HP (or HP service providers or service partners) identifies that the repair can be accomplished by the use of a Customer Self Repair part, HP will ship that part directly to you for replacement. There are two categories of Customer Self Repair parts:

- Mandatory—Parts for which Customer Self Repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service.
- Optional—Parts for which Customer Self Repair is optional. These parts are also designed for customer self repair. If, however, you require that HP replace them for you, there may or may not be additional charges, depending on the type of warranty service designated for your product.

NOTE: Some HP parts are not designed for Customer Self Repair. In order to satisfy the customer warranty, HP requires that an authorized service provider replace the part. These parts are identified as *No* in the Illustrated Parts Catalog.

Based on availability and where geography permits, Customer Self Repair parts will be shipped for next business day delivery. Same day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the telephone. HP specifies in the materials shipped with a replacement Customer Self Repair part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a Customer Self Repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.

For more information about the HP Customer Self Repair program, contact your local service provider. For the North American program, visit the HP website (http://www.hp.com/go/selfrepair).

7 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hp.com**). Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

agent Software on managed servers used to make changes to the servers. Functions supported include software installation and removal, software and hardware configuration, and server status reporting.

answer file See configuration file.

appliance See virtual appliance.

AutoYaST file The specific term to use when referring to a SUSE Linux Enterprise Server (SLES) configuration file.

bare metal Describes a server that does not have a production operating system installed. This could be a brand new server with no OS installed on it. A bare metal server is typically one that is not yet known to the management software or has just been added but does not have a production OS deployed.

bare metal discovery The process for making a bare metal server known to the provisioning software. In order to discover a bare metal system, that system is usually booted into a special service OS. The service OS has just enough software on it to report various details about the server back to the management software and deploy a production operating system. Bare metal discovery can sometimes be done using the server's iLO, in which case the service OS is not necessary.

blob store A region of memory that is accessible by both the iLO and the embedded software environment. Management software can communicate with the embedded environment through the iLO by reading and writing files to the blob store. This eliminates the need to communicate through the server's production network interfaces.

captured image A data store containing all the information from a target server including the files, disk partition information, and anything else needed to completely recreate the target server back to the same server, or perhaps a different one. The captured image does not include partitions, only file system data. See also image installation.

configuration file The generic term for Windows and Linux unattended installation files. These files provide all the information required to install the operating system without user intervention. Also applies to hardware configuration utilities such as BIOS configuration and Array Controller configuration. Customers may create new configurations for their own purposes. See also AutoYaST file and kickstart file.

custom attribute A simple user-defined name/value pair that is used as a form of variable substitution in scripts and other appliance functions. When referenced, the custom attribute name is replaced by the value of that custom attribute. Custom attributes do not stand alone; they are always associated with an object in the management database, such as servers, groups, or OS Build Plans. Custom attributes can be inherited from a containing object. For example, a server in a group will inherit the custom attributes from that group.

deploy image See image installation.

deployment See provisioning.

deployment job See job.

distribution files See OS distribution files.

embedded deployment See embedded deployment features.

embedded deployment features A set of deployment tools and service OS's that are built in to HP ProLiant servers beginning with the Gen8 series. These embedded tools make it possible to deploy, configure, and troubleshoot a ProLiant server without network booting (PXE) or removable boot media.

enclosure A chassis that contains multiple blade servers and interconnect devices.

facility The collection of servers that a single HP Insight Control server provisioning appliance manages. Usually, these servers are on the same network, or on connected networks. A facility can be all or part of a data center, server room, or computer lab.

file repository See Media Server.

HP Scripting Toolkit (STK) A server deployment product for unattended server provisioning.

HPSUM HP Smart Update Manager, a common tool for firmware and driver updates.

iLO See Integrated Lights-Out (iLO).

iLO Virtual Media An HP Integrated Lights-Out (iLO) feature that allows you to attach a removable storage device or image file from a client machine to the server, and have that appear to the server as a local device. The server can boot from that virtual device or use it with a running operating system.

image installation The process of installing a server using a previously captured image of the disk to make a duplicate of the original server. This is in contrast to a scripted installation.

Integrated Lights-Out (iLO) An independent microprocessor built into ProLiant servers that provides multiple ways to configure, update, and operate servers remotely. iLO can remotely perform most functions that otherwise require a visit to servers at the data center, computer room, or remote location. See http://www.hp.com/go/ilo.

intelligent provisioning A single server deployment using the HP ProLiant Gen8 iLO Management Engine. See also embedded deployment features.

interconnect module An Ethernet, FC, or FCoE interconnect module designed to work in a blade enclosure.

job A task that runs on the Insight Control server provisioning appliance. Jobs typically affect the state of a target server and include running an OS Build Plan.

kickstart file The specific term to use when referring to a Red Hat Enterprise Linux or VMware ESXi installation file. Use configuration file for generic use.

LinuxPE The service OS for the Linux operating system.

maintenance mode A server status where a server has booted to a service OS and is running a maintenance version of the SA OGFS agent. Servers in maintenance mode are typically waiting to be provisioned.

managed server A provisioned server that has an SA agent installed on it and is under the control of the Insight Control server provisioning appliance.

media Software on the Media Server which can include vendor-supplied OS distribution files, HP-provided OS distribution files, captured images, and firmware and driver updates such as HP Service Packs for Proliant (HP SPP).

Media Server A server containing the vendor-supplied OS media used during OS provisioning. The OS media on the Media Server is accessed over the network using HTTP for Linux and ESXi, and SMB for Windows. The Media Server may also contain media for other purposes such as firmware and driver updates, and is also where captured images are stored. The Media Server is a separate server from the Insight Control server provisioning appliance.

Microsoft WAIK Windows Automated Installation Kit. A set of tools, including WinPE, produced by Microsoft for provisioning the Windows operating system. WAIK became available first for Windows Vista.

offline firmware update A method of updating system firmware that requires the server to be taken offline and rebooted as part of the process. In an offline update, the system is shut down and booted into a service OS where the firmware update occurs. Upon completion of the update, the system can be brought back online.

OGFS script A script that executes inside the Opsware Global File System. OGFS scripts execute on the Insight Control server provisioning appliance and are typically written in shell or Python.

Opsware Global File System (OGFS) The OGFS represents the SA data model as a hierarchical structure of file directories and text files. For example, in the OGFS the `/opsw/Server` directory has information about target servers. There are also subdirectories that reflect the contents (such as file systems and registries) of the target servers. If you have the required permissions, you can view and even modify the file systems of target servers in the Global Shell.

OS Build Plan A sequence of OS Build Plan steps that execute in a specific order to perform a task on a target server. OS Build Plans are typically used for provisioning operating systems, but can be used for almost any task that can be automated.

OS Build Plan step An autonomous operation, such as "run script" or "install package", assigned as part of an OS Build Plan.

OS distribution files
The files that make up an operating system before that operating system is installed on a server. These files are provided to consumers via ISO images or physical CD/DVDS from OS companies such as Microsoft, Red Hat, VMware, and Novell.

OS personalization
The process of giving a running server the characteristics that make it unique, including IP configuration, host name, and domain. A server can be personalized during the initial OS deployment or after the OS is already installed.

package
A single compressed (zipped) file that can contain executables, configuration information, and script files. An example of a package is a `.zip` file of Windows drivers to be used during unattended installations.

preboot environment
See service OS.

provisioned
A server in this state has an operating system installed.

provisioning
Installing an operating system on a target server using either scripted installation or captured image deployment.

PXE-free
See embedded deployment features.

script
The types of scripts supported by Insight Control server provisioning are:

- UNIX – Bourne shell (sh), C shell (csh), and KornShell (ksh)
- OGFS – Opsware Global File System
- Windows .BAT – Windows batch file
- Windows VBScript – Visual Basic scripting
- Python – Python programming language

scripted installation
The OS provisioning method that uses configuration files and OS distribution files to deploy an OS to a target server as an unattended installation. This is the native way the operating system is intended to be installed by the OS vendor but with the interactive installation process automated. This is in contrast to an image installation.

Server Automation (SA)
HP Server Automation software. See http://www.hp.com/go/serverautomation.

server discovery
The process where a server becomes known to the Insight Control server provisioning appliance. For bare metal, the server boots to a service OS with an agent installed that registers with the appliance. For servers already running an OS, the agent is installed onto the running OS and then registers with the appliance. Once a server has registered with Insight Control server provisioning, it can be selected for provisioning.

server status

Table 5 Server statuses

☑	Server is provisioned and OK.
⟳☑	Job is running on a provisioned server.
◆	This is an unprovisioned server ready to be provisioned.
⟳◆	Provisioning is in progress on either an unprovisioned or provisioned server.
	Reboot stage of a job running on a provisioned server.
⚠	Provisioning failed on this server. It is available for provisioning.

Table 5 Server statuses *(continued)*

⛔	The server is unreachable. This means HP Insight Control server provisioning is not able to communicate with the server.
❓	Server status is unknown to Insight Control server provisioning.

See also maintenance mode, provisioned, and unreachable.

service OS A special purpose operating system that runs entirely in system memory and is used to perform various maintenance functions on a server, including preparing a system for operating system installation. Insight Control server provisioning has service OS's based on Linux and Windows. See also LinuxPE and WinPE.

SLES Stands for SUSE Linux Enterprise Server. A Linux-based operating system developed by SUSE.

software package See package.

software repository See Media Server.

SPP HP Service Pack for ProLiant. See http://www.hp.com/go/spp.

status See server status and job status.

step See OS Build Plan step.

STK See HP Scripting Toolkit (STK).

target server The intended server for an Insight Control server provisioning operation. A target server has an SA agent running on it.

unattend file The specific term to use when referring to a Windows installation file. Use configuration file for generic use.

unattended installation An automatic Windows or Linux OS installation that does not require user intervention.

unprovisioned A server with an SA agent installed, under the control of Insight Control server provisioning, and waiting to have an operating system installed. See maintenance mode.

unreachable A server status where the server cannot be contacted by the Insight Control server provisioning appliance.

upgrade See virtual appliance upgrade.

virtual appliance A virtual machine with a preinstalled software application that is optimized to run the application.

virtual appliance upgrade Downloading and installing an update release of the HP Insight Control server provisioning appliance to incorporate software updates and new content for OS provisioning.

WAIK See Microsoft WAIK.

WIM install An installation using the Windows Imaging Format. See image installation.

WinPE The Windows Preinstallation Environment is the service OS for the Windows operating system.

Index