HP Network Automation Software

For the Linux and Solaris operating systems

Software Version: 9.20

Satellite Guide

Document Release Date: November 2014
Software Release Date: May 2012

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

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

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

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, after product installation see the `<NA_HOME>/server/license` directory on the NA core server.

Acknowledgements

This product includes software developed by the Apache Software Foundation. (http://www.apache.org)

Parts of this software Copyright © 2003-2008 Enterprise Distributed Technologies Ltd. All Rights Reserved. (http://www.enterprisedt.com)

Documentation Updates

This guide's title page contains the following identifying information:

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

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

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

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

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

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Online web site at:

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1 Getting Started

This document contains information on configuring the HP Network Automation Software (NA) Satellite functionality.

Satellite installations are only supported on supported operating systems running in English.

This document is updated as new information becomes available. To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

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

For more information, see Documentation Updates on page 3.

Terminology

The following terms are used throughout this guide:

- **Realm** — A collection of reachable networks with no overlapping IP addresses.
- **IP Space** — One or more Realms that have no overlapping IP addresses.
- **NA Core** — A single NA Management Engine, associated services (Syslog and TFTP), and a single database. An NA Core can manage multiple Partitions.
- **NA Gateway** — A service that tunnels traffic to and from managed devices. The NA Gateway routes IP traffic to other Gateways. The Gateway enables you to manage servers behind NAT'd devices and firewalls. In addition, the Gateway supports bandwidth throttling on tunnels between Realms and can be used anywhere SSL proxying or TCP port forwarding is used. Tunnels can be authenticated and encrypted using SSL.
- **Core Gateway** — A Gateway running in the same Realm as an NA Core. The Core Gateway is the same software as the Satellite Gateway. You simply configure the Core Gateway differently for an NA Core than for a Satellite Gateway. Note that the Core Gateway Realm should be named "Default Realm" if there is only one NA Core.

  When using the NA Admin Settings, the Local Gateway Host is used. Keep in mind that this option refers to the Core Gateway.

- **Satellite Gateway** — A Gateway running in a Realm that does not include an NA Core. A Satellite Gateway includes the NA Gateway service and an NA Remote Agent.
- **NA Remote Agent** — The NA Remote Agent includes:
  - A process that handles SNMP and coordinates with the NA Management Engine on the NA Core.
  - A Syslog process that handles Syslog notifications from local devices.
  - A TFTP process that enables TFTP access to local devices.

- **Tunnel** — A TCP/IP connection between two Gateways that enables the Gateways to communicate.
- **Gateway Mesh** — A collection of two or more Gateways that route traffic among themselves. At a minimum, a gateway mesh consists of one Core Gateway and one Satellite Gateway.
- **Gateway Crypto Data File** — Includes Private and Public keys for SSL Gateway communication.

What Does the Satellite Funtionality Do?

Today's enterprise networks are complex and can include many types of circuits that bridge connections between the corporate headquarters and a remote office. Often, the link between these offices traverses a VPN connection over public networks, a limited bandwidth circuit, or both. Because of these variables, security and efficiency are often paramount concerns.

The Satellite functionality provides a secure means to route packets from the NA Core to remote networks by creating an encrypted tunnel between the NA Core and remote network. When more than one Satellite Gateway is present, the NA Management Engine creates an NA Mesh within the network of tunnels that enables the NA Core to securely reach any Satellite Gateway via the NA Mesh.

It is recommended that the Core Gateway is running on the same host as the NA Core for the following reasons:

- Performance — You can avoid TCP/IP socket overhead.
- Security — Packets are sent internally and cannot be snooped by other hosts on the network. The connection between the NA Core and Core Gateway is not encrypted. As a result, using a local connection on the same host is more secure.

The NA Gateway does not run on the Windows operating system. When the NA application server uses a Windows operating system, the Core Gateway must be on a different host from the NA Core.

The Satellite functionality can simplify communication between the NA Core and remote networks by encrypting packets and limiting the number of firewall ports that need to be opened. This can simplify the initial setup when communications are restricted by firewalls or where communication between networks must be secured.

When you install the NA Remote Agent, NA makes an SSH connection to the Satellite host. This connection is made through the Gateway Mesh. As a result, your firewall does not have to allow access to port 22 for SSH. Only port 2001 (the Gateway tunnel port) must be open.

Currently, the Detect Network Devices and OS Analysis tasks do not work for devices managed by an NA Satellite.

Is the Satellite Functionality Right for You?

You can use a Satellite configuration if you are managing:

- Devices over a fast LAN, with strict firewall rules between the NA Core. The NA Satellite may ease the management of connections between the NA Core and the devices.
- Devices that have overlapping IP addresses. The NA Core cannot directly manage two devices with the same IP address. With the Satellite functionality, it is possible to partition the network into Realms and access all devices directly.
- Devices that restrict TFTP to a local server for speed, but primarily for security. Traffic over a local network is more secure than traffic that must traverse a firewall and possibly enter the Internet.
- Devices with a slow WAN link and subject to network interruption during software upgrades. The Satellite, which is on the same LAN as the remote devices, caches software images so they only have to be copied across the wire, from the NA core to the Satellite, one time.

Keep in mind that you will need servers on which to run the Gateway Mesh. Each Gateway will need to be installed to properly create the Gateway Mesh.

Installation Prerequisites

Before installing the Satellite functionality, keep the following in mind:

- Satellite installations are only supported on supported operating systems running in English.
- You will need servers on which to run the Gateway Mesh. Each Gateway must be installed to properly create the Gateway Mesh.
- Within a Realm, the IP address space must be unique.
- A Gateway Mesh can be used to add encryption to Telnet-managed devices. Keep in mind, however, encrypting Telnet connections is only an encryption between the Core Gateway and the Remote Gateway. After the packets leave the Gateway, they are in clear text.
- All traffic between Gateways is encrypted using SSL with a private key (stored in the Gateway Crypto Data file), created for each Gateway Mesh.
- Gateways can throttle traffic between Realms. This is useful if NA is using a slow link to manage remote devices in an effort to assure NA does not saturate the link when capturing a device's configuration.
- Multiple Gateways can be installed in the same Realm for redundancy. As a result, a Satellite Gateway has both a Realm name and a Gateway name.
- Install a Core Gateway before installing any Satellite Gateways.
- TCP port 2001 must be open from the Satellite Gateway to the Core Gateway.

- During installation of a Satellite Gateway, port 9090 must also be open from the Satellite Gateway to the Core Gateway. After the Satellite Gateway has been installed, port 9090 is no longer needed.

You do not need to open port 3333 in your firewall. The NA Gateway Installer uses port 3333 to ensure that a Satellite Gateway is not being installed on the same host with a Core Gateway. The NA Gateway Installer listens on port 3333 and then tries to connect to the Core Gateway on port 3333. The connection to port 3333 is supposed to fail. If the connection succeeds, the NA Gateway Installer will exit with an error.

For an example installation, see Appendix A.

Gateway Supported Platforms

- This Satellite functionality supports the HP Network Automation (NA) version 6.1 and later on the following platforms:
- Red Hat-Linux-3AS
- Red Hat-Linux-4AS
- Red Hat-Linux-5SERVER-X86-64
- SuSE-Linux-9ES, 10.x
- SunOS-5.9
- SunOS-5.10

Note that additional steps are required to install Gateways on RH EL 5:

1 Go to <*gateway directory*>/*lib*/.

2 Run *rpm -ivh OPSWgw-ism-37.0.0.0.12.7-1.x86_64.*rp.

Remote Agent Platforms

Table 1 provides information on the supported Remote Agent platforms.

Table 1 NA Satellite-Supported Platforms

	OS	Version	Architecture
Red Hat	RH AS RH EL	3 (32-bit), 4 (32-bit) 5 (64-bit)	i386 i386
Oracle	Solaris	9, 10	Oracle SPARC
Novell	SuSE Enterprise Linux Server	9ES, 10.x	i386

Sharing Satellites between HP Server Automation (SA) and NA is supported in SA 7.50 and NA 9.20. Running Satellites on VMWare is supported in SA 7.50 and NA 9.20.

Hardware Requirements

Table 2 lists the minimum hardware for the Satellite functionality.

Table 2 NA Satellite Minimum Hardware

Category	Minimum
CPU	Two CPUs per 1,500 managed servers per Satellite Core, and 5,000 network nodes.
Memory	4 GB RAM per 1,500 managed servers per Satellite Core, and 5,000 network nodes.
Disk	128 GB

2 Installation

Satellite installation consists of the following processes:

- Installing the Core Gateway on each NA Core as described in Installing a Core Gateway on page 14. Installing the first Core Gateway will create a Gateway Crypto Data File that will be needed to install other Core Gateways, if applicable.
- Installing the Satellite Gateway in each remote Realm as described in Installing a Satellite Gateway on page 15.
- Configuring NA as described in Configuring NA to Communicate with the Core Gateway on page 16. For the Core Gateway Host (referred to as the Local Gateway Host), you will need to know the DNS hostname or IP address for the Core Gateway.
- Deploying the Remote Agent to each remote Satellite Gateway Host as described in Adding a Remote Agent to a Satellite Gateway Host on page 18. You must use the Deploy Remote Agent task in NA for each Satellite Gateway that you installed.

Recommendations

The following recommendations should be used to ensure that the Satellite functionality is installed and running properly.

- Install a Core Gateway for each NA Core.
- Install the Core Gateway on the same host as the NA Core when the NA Core is running on a Solaris or Linux platform. Keep in mind that a Core Gateway must be installed before any Satellite Gateways.
- If there are multiple Core Gateways, each Satellite Gateway should have a tunnel to each Core Gateway.

Security

After installing the NA Core on a Solaris or Linux platform, install the Core Gateways on the same host. This ensures that communication between the NA Core and the Core Gateway is private.

Be sure to keep the Gateway Crypto Data file (the Gateway Installer creates the Gateway Crypto Data file when you install the Core Gateway), in a safe place. The private key in this file controls who can connect to the Gateway Mesh. Each Gateway in the Gateway Mesh has its own encyption keys and they must know the public key for the Core Gateway to join the Gateway Mesh.

Redundancy

For redundancy, you can install multiple Satellite Gateways in the same Realm.

Installing a Core Gateway

To install a Core Gateway in the same Realm with an NA Core:

In an xterm (no $DISPLAY required):

1. Unzip `nas_gw-37.0.0.0.12.7-2.zip`.
2. Type: **`perl install.pl`** and press [Enter].
3. Type the number for your platform and press [Enter].
4. The installer prompts you as to if you are going to config a new Core Mesh, add a new Core Gateway, or add a new Gateway to an existing Mesh.
   a. Type: **`1`** if this is the first Core Gateway.
   b. Type: **`2`** if this is a Core Gateway, but not the first Core Gateway.
   c. Press [Enter].
5. When prompted for a new password for the Gateway Crypto Data file, type a password to secure the Gateway Mesh and press [Enter]. When prompted, re-type the new password for the Gateway Crypto Data file and press [Enter].
6. Type the IP address or hostname for other Gateways to connect to this Gateway and press [Enter].
7. Type the IP address or hostname of the Core NA server and press [Enter].
8. When prompted for a Gateway name, type the Gateway name being installed and press [Enter]. The Gateway name cannot contain any spaces.
9. When prompted for a Realm name, type the Realm name where the Gateway is being installed and press [Enter]. Note: If this is a Core Gateway, type: **`Default Realm`**.
10. Review the Gateway configuration options. If they are correct, type: **`y`**, and press [Enter]

The Gateway Crypto Data file will be needed for Satellite Gateway installs. Keep this data file in a secure location to secure the IP traffic between Gateways. In addition, NA needs a private key for the administration port of the Core Gateway. If the Core Gateway is not on the same host as the NA Core, copy the `saOPSWgw*/certificates/opswgw-mngt-server.pkcs8` file for later use.

To install the first Core Gateway on the same server with an NA Core:

In an xterm (no $DISPLAY required):

1. Unzip `nas_gw-37.0.0.0.12.7-2.zip`.
2. Type: **`perl install.pl`** and press [Enter].
3. Type the number for your platform and press [Enter].
4. The installer prompts you as to if you are going to config a new Core Mesh, add a new Core Gateway, or add a new Gateway to an existing Mesh.
   a. Type **`1`** if this is the first Core Gateway.

b Type **2** if this is a Core Gateway, but not the first Core Gateway.

c Press [Enter].

5 When prompted for a new password for the Gateway Crypto Data file, type a password to secure the Gateway Mesh and press [Enter]. When prompted, re-type the new password for the Gateway Crypto Data file and press [Enter].

6 When prompted if this is a Core Gateway, type **y** and press [Enter].

7 Type the IP address for other Gateways to connect to this Gateway and press [Enter].

8 Type the IP address or Hostname of the Core NA server (usually 127.0.0.1) and press [Enter].

9 When prompted as to whether the Core Application Server is also installed on this host, type: **y** and press [Enter].

10 When prompted for the install location of the Core Application Server, type the NA install directory and press [Enter].

11 When prompted for a Gateway name, type the Gateway name being installed and press [Enter].

12 When prompted for a Realm name, type the Realm name where the Gateway is being installed and press [Enter]. Note: If this is a Core Gateway, type: **Default Realm**.

13 Review the Gateway configuration options. If they are correct, type: **y**, and then press [Enter].

Installing a Satellite Gateway

Install a Satellite Gateway in every Realm that does not have an NA Core.

In an xterm (no $DISPLAY required):

1 Unzip `nas_gw-37.0.0.0.12.7-2.zip`.

2 Type: **`perl install.pl`** and press [Enter].

3 Type the number for your platform and press [Enter].

4 The installer prompts you as to if you are going to config a new Core Mesh, add a new Core Gateway, or add a new Gateway to an existing mesh. Type: **3** and press [Enter].

5 Satellite Gateway installations require the filename of the Gateway Crypto Data file created during the Core Gateway install. If the filename includes a colon (:), SCP is used to copy the file. Type the path to the directory containing the Gateway Crypto Data file and press [Enter]. For example, if the Core Gateway was installed on host 'foo' and the Gateway crypto data file saved in */tmp/gw*, type: `LOGINNAME@foo:/tmp/gw`

6 When prompted for the password for the Gateway Crypto Data file, type the password used when installing the Core Gateway and press [Enter]. When prompted, re-type the new password for the Gateway Crypto Data file and press [Enter].

7 When prompted for the IP address or DNS hostname to connect to a Core Gateway, type the IP or DNS hostname of the Core Gateway to which this Satellite Gateway connects, and then press [Enter].

8 Type the IP address or Hostname of the Core NA Server (usually 127.0.0.1) and press [Enter].

9 When prompted for the Gateway name for the Gateway, type the name the Gateway being installed and press [Enter].

10 When prompted for the Realm name for the Gateway, type the Realm name where the Gateway is being installed and press [Enter]. Note: If this is a Core Gateway, type: Default Realm.

11 Review the Gateway Configuration options. If they are correct, type **`y`** and press [Enter].

Configuring NA to Communicate with the Core Gateway

To configure NA to Communicate with the Core Gateway, do the following:

1 Login to the host where NA is installed.

2 If the Core Gateway is not on the same host as the NA Core, copy the `opswgw-mngt-server.pkcs8` file from the Core Gateway to the root of the NA installation, typically `C:\NA` or `/opt/NA`.

3 Login to NA as an Administrator.

4 On the main menu, click **Admin > Administrative Settings > Device Access**. The Administrative Settings - Device Access page opens.

5 Scroll down to the Gateway Mesh section.

6 For the Core Gateway Host (referred to as the Local Gateway Host), enter the DNS hostname or IP address for the Core Gateway, typically `localhost` if installed on the same system.

7 Click **Save**.

Gateways Page

To test whether NA can communicate with the Core Gateway, on the main menu bar, click **Admin > Gateways**. The Gateway List page opens. The Gateway List page displays the currently configured Gateways and enables you to edit Gateway information. For information, see Edit Gateway Page on page 18.

Table 3 describes the Gateway List page.

Table 3 Gateway List Page Fields

Field	Description/Action
Deploy Remote Agent link	Open the Deploy Remote Agent page, where you can deploy an NA remote agent.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is install and cannot be modified in NA. To change the Realm name, you need to re-install the Gateway.
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA.
Host	Displays the hostname or IP address of the system on which the Gateway is installed. If the Gateway host has multiple IP addresses, this is the IP address that would be used from the Gateway host. The Host IP address is only important if you have more than one Gateway installed in the same Realm. **Note**: You can install multiple Satellite Gateways in the same Realm for redundancy.
Partition	Displays the NA Partition name associated with the Realm name, if applicable.
Core	In a Multimaster Distributed System environment, the Core name is set on the Edit Core page. If the Realm name on the Edit Core page matches the Realm name for a Gateway, the Gateway List page displays the Core name of the Core.
Agent	Displays the name of the NA remote agent for Satellite Gateways. The NA remote agent name can be changed on the Edit Gateway page. Once you have installed the Gateway Mesh, you must install an NA remote agent on each Satellite Gateway host. If there is no NA remote agents installed, the Agent column is empty.
Actions	There is one option: • Edit — Opens the Edit Gateway page.

Edit Gateway Page

NA automatically sets the IP Space name based on the Realm Name. However, if two Realms are in the same IP Space, and you want them diagrammed correctly in L3 diagrams, you can edit the Gateway to set the IP Space name.

To open the Edit Gateway page, on the Gateway List page, click the Edit option in the Actions column. Table 4 describes the Edit Gateway page.

Table 4 Edit Gateway Page Fields

Field	Description/Action
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is install and cannot be modified in NA.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses. Enter a new IP space name.
Host	Displays the hostname or IP address of the system on which the Gateway is installed. Enter a new host name or IP address.
Satellite	Displays the Satellite Gateway running in a Realm that does not have an NA Core. Enter a Satellite Gateway name, if applicable.

Adding a Remote Agent to a Satellite Gateway Host

To add a Remote Agent to a Satellite Gateway Host, you must create a Deploy Remote Agent task in NA. The Deploy Remote Agent task enables you to deploy an NA remote agent on each Gateway host. By installing an NA remote agent on the same LAN with the devices being managed, WAN traffic can be minimized and Syslog and TFTP can be used to manage the devices locally.

To open the Deploy Remote Agent task:

1. Login to NA.
2. On the menu bar click **Tasks > New Task > Deploy Remote Agent**. The Deploy Remote Agent page opens. Be sure to click **Save Task** when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status.

Table 5 describes the Deploy Remote Agent page.

Table 5 Deploy Remote Agent Page Fields

Field	Description/Action
Task Name	Displays Deploy Remote Agent. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks.
Comments	Enter comments about the task.
Task Options	
Action	Select one of the following options: • Install (or Reinstall) — Installs the NA remote agent. If there is already an NA remote agent installed, the existing NA remote agent is removed and a new NA remote agent is installed. • Uninstall — Uninstalls the NA remote agent.
Deploy Agent to Gateway	Select the Gateway name from the drop-down menu where the NA remote agent is to be deployed.
Login	Deploying a remote agent requires root privileges on the Satellite Gateway host. Select one of the following options: • As Root — SSH as username root and enter the root password. • As Non-root — SSH as a non-root user. If you select this option, select either su Password (the root password) or sudo Password (the sudo password, which is typically the same as your username password, but can be different depending on how sudo is configured).

Table 5 Deploy Remote Agent Page Fields

Field	Description/Action
Managing Core	If the Core Gateway is installed on the same host as the NA Core, the Managing Core should be "localhost" (the default). If the Core Gateway is on a different host from the NA Core, the Managing Core should be the hostname or IP Address of the NA Core. (**Note**: If the NA Core host has a different IP address, use the IP address that is appropriate when connecting to the NA Core from the Core Gateway host.)
In Realm	Select the Realm name of the Core Gateway from the drop-down menu.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not availables
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Table 5 Deploy Remote Agent Page Fields

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing.

Handling Multiple NICs on the Satellite Host

If the Satellite gateway host has multiple Network Interface Cards (NICs), you can configure the Satellite to use a particular NIC. After installing the Remote Agent, edit the `/opt/opsware/nassat/jre/nassat.rcx` file and change the value for `tftp/server` to the gateway NIC IP address devices should use to TFTP their configurations to the Satellite.

You should also change the `syslog/server` value in the `nassat.rcx` file. This is the logging address that is configured on a device when the Configure Syslog task is run in NA.

When you re-deploy the Satellite Agent, you will have to modify the `nassat.rcx` file again.

Enabling SCP Transfers from a Satellite

By default, NA supports TFTP only for backing up device software and configurations through the satellite gateway. To enable SCP transfers from remotely-managed devices to the satellite, follow these steps:

1. Identify an SCP account to use. Navigate to the FTP and SSH Device Access section of the Administrative Settings - Device Access page (**Admin > Administrative Settings > Device Access**).
   - If values are specified for the FTP/SSH User and FTP/SSH Password fields, you must use this information for the SCP account.
   - If no values are specified for the FTP/SSH User and FTP/SSH Password fields, determine a user name and password to use for the SCP account. Configure that account.

     The FTP/SSH user name must be different from the NA user names for accessing the NA console.
2. On the satellite system, configure the identified SCP account. For example, the following commands configure an account with username `nascp` and password `napass`:

   ```
   chmod -R o+rx /opt/opsware/nassat/server/ext/tftp
   useradd -d /opt/opsware/nassat/server/ext/tftp/tftpdroot nascp
   passwd napass
   ```

   The home directory for this user must be `/opt/opsware/nassat/server/ext/tftp/tftpdroot`.
3. On the NA application server, add the `DeviceAccess/scp/allow_satellite` option to the `adjustable_options.rcx` file:
   a. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
   b. In the `adjustable_options.rcx` file, add the following line:

      ```
      <option name="DeviceAccess/scp/allow_satellite">true</option>
      ```

   c. Save the `adjustable_options.rcx` file.
   d. Reload the .rcx settings by doing one of the following:
      — Run the `reload server options` command from the NA proxy.
      — Restart the NA services.

Removing the Remote Agent from the Satellite Gateway Host

The Remote Agent must be removed before uninstalling the Satellite Gateway. To remove the Remote Agent from the Gateway, do the following:

1. Login to NA.
2. On the menu bar, click **Tasks > New Task > Deploy Remote Agent**. The Deploy Remote Agent page opens. (You can also navigate to this page by clicking the Deploy Remote Agent link on the Gateway List page.)
3. Under Task Options in the Action field, click **Uninstall**.
4. Click **Save Task**.

Uninstalling a Gateway

To uninstall a Gateway, do the following:

1. Change to the directory where you unzipped the `gateway.zip` file to install the Gateway.
2. Enter the following command:

```
./saOPSWgw*/uninstall --removeall
```

If you do not specify the `--removeall` option, some of the configuration and log files will not be removed.

Removing the NA Satellite

To remove an NA Satellite, do the following:

1. Remove the Remote Agent from the Satellite Gateway host as described in Removing the Remote Agent from the Satellite Gateway Host on page 23.
2. Uninstall the Gateway as described in Uninstalling a Gateway on page 23.

Upgrading the Satellite

To upgrade the Satellite from NA 7.5x to NA 9.20, do the following:

1. Uninstall all the old Gateways in the Gateway Mesh as described in Removing the Remote Agent from the Satellite Gateway Host on page 23.
2. Re-install new Gateways with the NA 9.20 Gateway installer as described in Installing a Core Gateway on page 14. This step ensures the Gateway security is set up correctly for NA 9.20.
3. Run the Deploy Remote Agent task for each Satellite Gateway as described in Adding a Remote Agent to a Satellite Gateway Host on page 18.

To upgrade from NA 7.6x, NA 9.00, or NA 9.10 to NA 9.20, do the following:

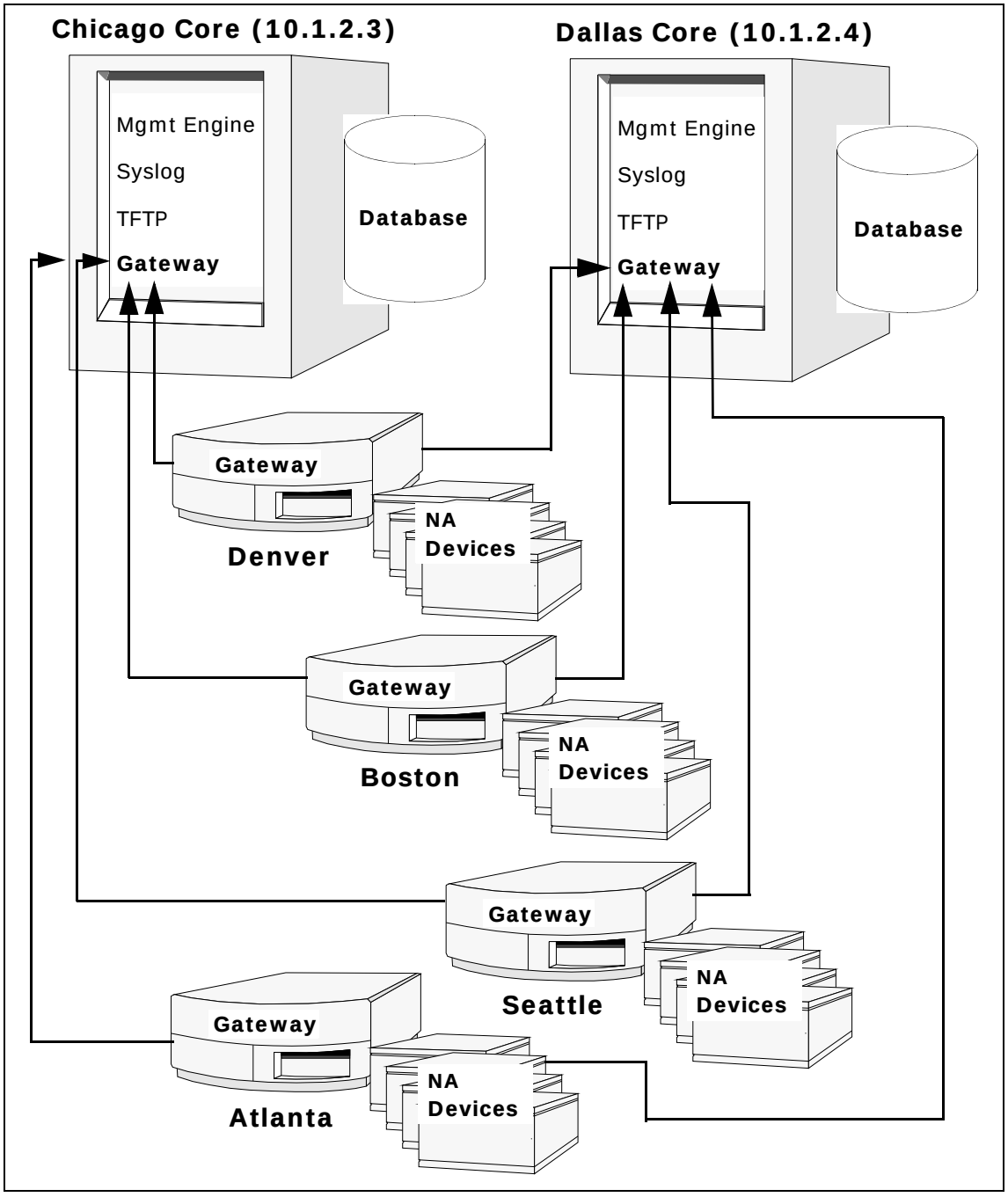
1. Where Gateways are used, after upgrading NA on the NA application server, run the Deploy Remote Agent task to re-install the upgraded Satellite agent on all of the remote Gateways. See Adding a Remote Agent to a Satellite Gateway Host on page 18.
2. On the Deploy Remote Agent page, scroll down to the Task Options section.
3. In the Action field, select the **Install (or Reinstall)** option.
4. Click **Save Task**.

A Installation Example

In the following example, there are two large offices (NA Cores), one in Chicago and one in Dallas, and several smaller offices in Boston, Atlanta, Seattle, and Denver (Realms). One way to setup a Satellite configuration would be to configure:

- A Realm for each city.
- An NA Core in Chicago and Dallas.
- A Satellite Gateway in Boston, Atlanta, Seattle, and Denver.

The following figure illustrates the example. Keep in mind that an NA Core includes both an NA Application server and a Database server, typically on separate hosts. The Core Realms show the Core Gateway on the same host as the NA Application server. The Remote Realms show a Satellite Gateway on a host by itself. Each Satellite Gateway has two tunnels, one to each Core Gateway.



Assuming the two NA Cores are installed on a Solaris platform:

1 Install the Chicago Gateway first:

   a First Gateway: **`y`**

   b Core Gateway: **`y`**

   c Gateway Name: **`Chicago1`**

   d Realm Name: **`Chicago`**

e IP address of NA Core: **127.0.0.1**

Using the loopback interface keeps the traffic between the NA Cores from going out on the Ethernet segment. As a result, the connection is more secure.

f IP address for other gateways to connect: **10.1.2.3**

This must be an external IP address so other Gateways can connect to this Gateway. 10.1.2.3 is an example. Be sure to use the correct IP address for your host.

2 Install the Dallas Core:

a First Gateway: **n**

b Core Gateway: **y**

c Gateway Name: **Dallas1**

d Realm Name: **Dallas**

e IP address of NA Core: **127.0.0.1**

f IP address for other gateways to connect: **10.1.2.4**

To make the second Core Gateway work, modify the Gateway Property file, `/etc/opt/opsware/opswgw-<gateway name>/opswgw-properties`, and change the value of `opswgw.EgressFilter` to:

```
opswgw.EgressFilter=tcp:*:443:127.0.0.1:*,tcp:*:22:NAS:,tcp:*:23:NAS:,
tcp:*:513:NAS:,tcp:*:443:NAS:,tcp:*:80:NAS:
```

3 Install the Satellite Gateways. For Boston:

a First Gateway: **n**

b Core Gateway: **n**

c Gateway Name: **Boston1**

d Realm Name: **Boston**

e IP Address of the Core Gateway: **10.1.2.3**

4 Edit the `opswgw.properties` file on Boston1. The `opswgw.properties` file should have:

```
opswgw.TunnelSrc=10.1.2.3:2001:100:0:/var/opt/opsware/crypto/
opswgw-Boston1/opswgw.pem
opswgw.TunnelSrc=10.1.2.4:2001:200:0:/var/opt/opsware/crypto/
opswgw-Boston1/opswgw.pem
```

5 Install the other Satellite Gateways in a similar manner.

6 For redundancy, install a second Gateway in Boston.

a First Gateway: **n**

b Core Gateway: **n**

c Gateway Name: **Boston2**

d Realm Name: **Boston**

e IP Address of the Core Gateway: **10.1.2.3**

7 Assume there is only a T1 link to the Boston office and you do not want NA to monopolize the link. A T1 link is about 1.5Mbit/s, so limit NA to half of that (or 750Kbit/s). Edit the `opswgw.properties` file and set the bandwidth throttle to 750. The `opswgw.properties` file should look like the following:

```
opswgw.TunnelSrc=10.1.2.3:2001:100:750:/var/opt/opsware/crypto/
opswgw-Boston1/opswgw.pem
opswgw.TunnelSrc=10.1.2.4:2001:200:750:/var/opt/opsware/crypto/
opswgw-Boston1/opswgw.pem
```

Set the bandwidth throttle for both tunnels so that if you fail-over to Dallas (10.1.2.4), the bandwidth is still throttled.

B Troubleshooting

The NA Satellite has two levels of security to ensure that unauthorized processes cannot access the Satellite. Failures in the NA Satellite are usually the result of a configuration error that causes these security checks to deny connections. The following sections describe how to check these security levels if NA Satellite operations are failing.

Security in the Gateway Mesh

The first security level is in the Gateway Mesh. Only the NA Core host is allowed to connect to the Core Gateway. If the Core Gateway is installed with the incorrect IP address of the NA Core, connections will fail.

To check if the Gateway Mesh security is denying a connection, look for the word “disallow” in the Core Gateway log file by executing the following command at a shell prompt on the Core Gateway host:

```
grep disallow /var/log/opsware/opswgw-*/opswgw.log
```

If there is a line that states a connection is disallowed from a certain IP address, the security on the Core Gateway is the issue. The solution is to make sure the NA Admin Setting for Local Gateway and Gateway IngressMap are in sync.

If the Core Gateway is on the same host as the NA Core, the IP address in the IngressMap should be 127.0.0.1. The Local Gateway Admin Setting should be localhost or 127.0.0.1.

If the Core Gateway is on a separate host, the Local Gateway Admin Setting must have the correct IP address of the Core Gateway. The IngressMap must have the correct IP address of the NA Core host.

To modify the IngressMap line in the `properties` file, edit the `/etc/opt/opswgw-*/opswgw.properties` file. If there is more than one Gateway installed, replace the asterisk (*) with the name of the Gateway. Find the IngressMap line that looks like the following:

```
opswgw.IngressMap=127.0.0.1:NA
```

Security in the NA Core and Satellite

The second security level is in the NA Core and NA Satellite. They only accept connections from known hosts.

On the NA Core, the known host is the Local Gateway Admin Setting. On the Satellite, the known host is always localhost. To check for this, look for “Rejected” in the NA Core jboss wrapper log. Enter:

```
grep Rejected $NA/server/log/jboss_wrapper.log
```

(where `$NA` is the root of your NA Core installation).

If the Deploy Remote Agent task was run with an incorrect hostname for the NA Core host, the Satellite will not be able to connect back to the NA Core. To check for this, enter the above 'grep' command on the NA Satellite host. For information, see Removing the Remote Agent from the Satellite Gateway Host on page 23.

In addition, check to ensure that the EgressFilter on the Core Gateway has the correct IP address for the NA Satellite by editing the Gateway *properties* file on the Satellite host. Locate the line that looks like the following:

```
opswgw.EgressFilter=tcp:*:443:XXX.XXX.XXX.XXX:*,tcp:*:22:NA:,tcp:*:23:NA:
,tcp:*:513:NA:
```

(where `XXX.XXX.XXX.XXX` is 127.0.0.1).

Redundant Core Gateways are not supported by the Gateway installer. However, if you want to have redundant Core Gateways (not recommended), edit the `adjustable_options.rcx` file and add the other Core Gateway IP addresses by adding the following lines to the file:

```
<array name="rpc/allowed_ips">
<value>10.255.52.10</value>
<value>10.255.54.22</value>
</array>
```

The IP addresses above should be replaced with the correct IP addresses for your NA Core Gateways.

C Sharing the Gateway Mesh

This appendix includes information on how to setup HP Network Automation (NA) and HP Server Automation (SA) to share the same Gateway Mesh.

Overview

Keep the following in mind when sharing the Gateway Mesh:

- NA can only use the Gateway Mesh that is installed by SA.
- You can modify SA Core Gateways that NA Cores use to identify the NA hosts to the Gateway Mesh.
- You can modify the SA Satellites to enable egress to the ports that NA uses to manage devices.

Installation Steps

For each NA Core, identify the SA Core Gateway that will be used by that NA Core.

1. On the SA host, edit (or create) the `/etc/opt/opsware/opswgw-cgws`*`N-core`*`/opswgw.custom` file where *`N`* is the Core number and *`core`* is the Core name (for example: `/etc/opt/opsware/opswgw-cgws1-VMCORE1/opswgw.custom`).
2. Add the following lines to the end of the file:
   ```
   opswgw.EgressFilter=tcp:*:443:127.0.0.1:*
   opswgw.IngressMap=192.168.99.1:NA
   ```
3. Change `192.168.99.1` to the correct IP address for the NA Core. Note that `cgw` stands for Core GateWay. If there multiple cgw slices, add IngressMap for NA to all of them. NA can only use one cgw, but future versions may be able to failover to other slices.
4. Restart the Core Gateway:
   ```
   /etc/init.d/opswgw-sas restart opswgw-cgws
   ```

   Note that if there is more than one NA Core using the same SA Core Gateway, add multiple lines to each file, one for each NA Core's IP Address.

For each Satellite Gateway NA uses:

1. Edit the `/etc/opt/opsware/opswgw-`*`gateway`*`/opswgw.properties` file, where *`gateway`* is the name of the gateway specified at SA Satellite install time.
2. Add the following lines:
   ```
   opswgw.EgressFilter=tcp:*:22:NA:,tcp:*:23:NA:,tcp:*:513:NA:,tcp:*:80:
   NA:,tcp:*:443:NA:
   opswgw.EgressFilter=tcp:127.0.0.1:8443:NA:
   ```

```
opswgw.ProxyPort=3002
```

Note that the first line enables NA to use all of the ports that are needed to manage different types of devices (SSH, Telnet, rlogin, http, and https). The second line enables the NA Core to communicate with the NA Remote Agent that listens for RPC calls on port 8443. The third line adds a second ProxyPort that matches the ProxyPort that NA expects (3002).

3 Restart the Satellite Gateway:
`/etc/init.d/opswgw-sas restart opswgw`

4 Copy the `spog.pkcs8` file from the `/var/opt/opsware/crypto/twist/spog.pkcs8` on the SA host to *`NARoot`*`/spog.pkcs8` on the NA host, where *`NARoot`* is the directory where NA is installed.

5 Configure NA to use the SA Core Gateway on the Admin Settings page in NA using the Device Access tab in the Gateway Mesh section. For information, see the *NA User Guide*.

```
Local Gateway Host: IP Address of SAS (Core Gateway) host
Local Gateway Proxy Port: 3002
Local Gateway Admin Port: 8085
Gateway Admin Private Key Filename: spog.pkcs8
```

6 Run the Deploy Remote Agent task in NA for each Satellite Gateway host. Note that if a SA Satellite is running the OS Provisioning Media Server, the NA Remote Agent on that host must be reconfigured to use the TFTP server used by the OS Provisioning Media Server.

7 Edit the `/opt/opsware/nassat/nassat.rcx` file and the value for `TFTP/Server` to `/opt/opsware/boot/tftpboot` (the path to the TFTP root directory used by the OS Provisioning Media Server).

8 Edit the `/etc/xinetd.d/tftp` file and change `server_args = -s /tftpboot` to `server_args = -c -s /tftpboot`

The `-c` flag enables NA to create files in the TFTP root directory that is needed to capture network device configurations. SA uses TFTP to push files out to servers. As a result, the create ability is not needed for SA.

9 Make sure the `/opt/opsware/boot/tftpboot` directory is owned by the same user specified in the `/etc/xinetd.d/tftp` file.

10 Restart the TFTP daemon (in.tftpd) by sending the HANGUP signal to the xinetd process:

```
kill -1 `ps ax | grep xinetd | grep -v grep | awk '{print $1}'`
```

11 Edit the `/etc/init.d/nassat` file and comment out the StartTFTP line by putting a pound sign (#) at the front of the line, for example:

```
#  StartTFTP
```

12 Restart the NA Agent:

```
/etc/init.d/nassat restart
```

Uninstalling the Gateway Mesh

To uninstall the Gateway Mesh:

1. Run the Deploy Remote Agent task in NA with the “uninstall” radio button selected. Run the task once for each Satellite Gateway Host.
2. For each Satellite Gateway NA is using:
   a. Edit the `/etc/opt/opsware/opswgw-`*`gateway`*`/opswgw.properties` file, where *`gateway`* is the name of the Gateway specified at SA Satellite install time.
   b. Remove the following lines from the file:

```
opswgw.EgressFilter=tcp:*:22:NA:,tcp:*:23:NA:,tcp:*:513:NA:,tcp:*:8
0:NA:,tcp:*:443:NA:
opswgw.EgressFilter=tcp:127.0.0.1:8443:NA:
```

3. Restart the Satellite Gateway:

```
/etc/init.d/opswgw-sas restart opswgw
```

4. Configure NA to not use any Gateways in the Admin Settings page of NA on the Device Access tab in the Gateway Mesh section. For information, see the *NA User Guide*.
5. Set the Local Gateway Host option to the empty string.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NA 9.20

Document title: *NA Satellite Guide, November 2014*

Feedback: