HP Network Automation Software

For the Windows®, Linux, and Solaris operating systems

Software Version: 9.20

Administration Guide

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

Oracle Technology — Notice of Restricted Rights

Acknowledgements

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   About This Guide

This guide contains a collection of information and best practices for administering HP Network Automation Software (NA). This guide is for an expert system administrator, network engineer, or HP support engineer with experience deploying and managing networks in large installations.

This guide assumes that you have already installed NA and that you are familiar with start-up configuration tasks. To learn more about these tasks, see the *NA Installation and Upgrade Guide* and the NA help.

HP updates this guide between product releases as new information becomes available. For information about retrieving an updated version of this document, see Documentation Updates on page 3.

Revision History

Table 1 lists the major changes for each new release of this document.

Table 1   Document Changes

Document Release Date	Description of Major Changes
May 2012 (9.20)	First publication for NA version 9.20.

2   HP Network Automation Software Architecture

The NA architecture diagram in Figure 1 illustrates the NA Core components and their logical connections. The diagram also includes external products and components with which NA integrates.

An NA Core is comprised of both an NA server and a database server. The center of the diagram shows the NA server, identified as both the Multimaster Core (MM) #1 and Horizontal Scalability (HS) App #1. Just above the NA server is the database server that is part of Multimaster (MM) Core #1 or the Horizontal Scalability configuration.

NA Cores can be meshed together to provide data replication, high availability, and disaster recovery. In the upper left of the diagram are a second NA server and a second database server, both identified as MM Core #2, along with the required connections between the database servers of MM Core #1 and MM Core #2 to create the mesh.

Included in the NA server are the NA Management Engine, the Core Gateway, the TFTP server, the FTP server, the Syslog server, and the SWIM server processes. The SSH/SCP/SFTP server and the Event System shown inside the NA Management Engine are embedded within the NA Management Engine process.

Around the perimeter of the diagram are the external entities with which the NA Core server integrates. Each connection from the NA Management Engine to an external entitiy identifies the service name, protocol, port number, and direction (bidirectional, inbound, or outbound) with respect to the NA Management Engine.

Figure 1   NA Architecture
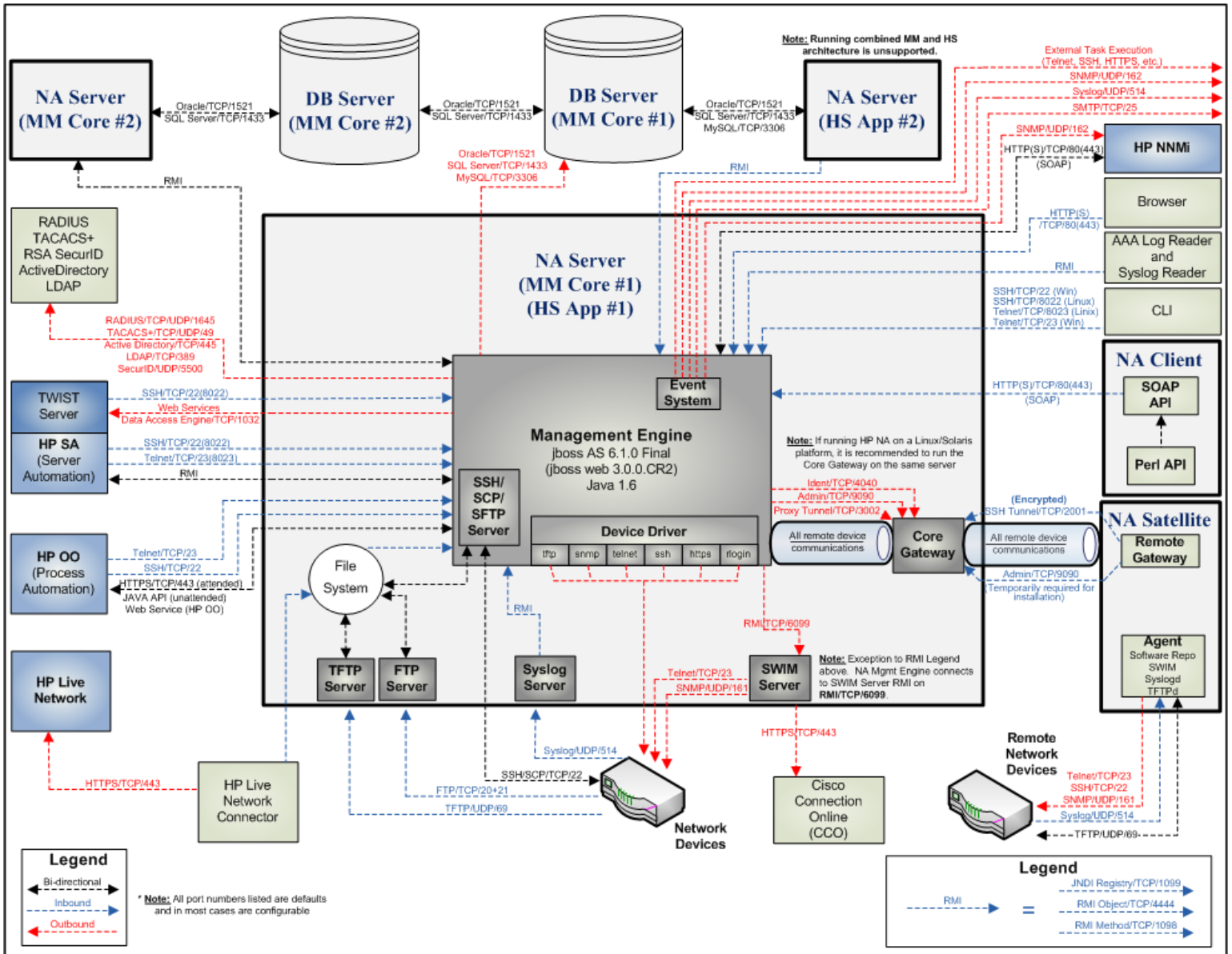
3   IPv6 Readiness

HP Network Automation (NA) is a robust network element management and automation tool. NA communicates with network elements via numerous protocols and authentication methods to gather information. NA then parses the information, normalizing it in a searchable and presentable format.

NA supports IPv6, both as transport and as parsed searchable and presentable bits of IPv6 specific information. NA supports IPv6 connections to DBMS. This includes Microsoft SQL Server 2005.

NA's adoption of IPv6 is focused on providing:

- Transparent access to network elements via IPv4 and/or IPv6
- Information on network element IPv6 configurations
- IPv6 support across NA features

Installation

NA installs and automatically detects network provisioning on the server. The available protocol determines what protocol NA uses for communicating to elements and NA listening servers. This includes:

- IPv4 only
- IPv6 only
- Dual stack environments (whether native or using a transition mechanism)

If NA is installed on a server that is to be updated to support IPv6, the following procedure is recommended:

1   Shut down NA.

2   Add IPv6 support to the server.

3   Restart NA.

4   Check the Admin options for various servers to ensure correct IPv6 address discovery.

Network Services

NA has several network services that will appropriately listen on IPv4-only, IPv6-only, and dual stack environments. These include:

- Web Server (TCP 80 and 443) — Clients using IPv6-enabled OS and browser can access NA via IPv6.

- TFTP Server (UDP 69) — Network elements can upload/download information via TFTP IPv6.

- TELNET Server (TCP 23) — Network elements can upload/download information via TELNET IPv6. Clients accessing the NA CLI can do it via TELNET IPv6.

- SSH/SCP Server (TCP 22) — Network elements can upload/download information via SSH/SCP IPv6. Clients accessing the NA CLI can do it via SSH IPv6.

- SYSLOG Server (UDP 514) — Network elements reporting change can do it via SYSLOG IPv6.

NA functions that instruct network elements to access these services will correctly determine which protocol to use based on a number of factors.

Clients

NA uses numerous protocols for intra-communication and communicating with network elements. These include:

- HTTP (TCP 80) — Access network elements

- HTTP (TCP 443) — Access network elements

- FTP (TCP 21) — Access network elements

- SNMP (UDP 161) — Access network elements

- Telnet (TCP 23) — Access network elements

- SSH/SCP (TCP 22) — Access network elements

- SYSLOG (UDP 514) — Send logging message

- SMTP (TCP 25) — Send email

IPv6 Presentation

The NA user interface supports IPv6 notation. This includes correct understanding, parsing, input, and display of IPv6 addresses. NA provides unique searching features for searching for IPv6 addresses within the system.

NA Features Supporting IPv6

The following NA features support IPv6:

- Detect Network Device
- Discover Driver
- Device Reservation
- Take Snapshot
- Configure Syslog
- Deploy Passwords
- Reboot Device
- Run Command Script
- Run Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Import
- Deduplication
- Check Policy Compliance
- Resolve FQDN
- Searching
- Reporting
- Real time change management
- Work Flow
- CLI and API

Drivers

NA architecture is such that a driver layer exists between the NA Core and the managed network elements. This layer abstracts information from network elements, interprets it, and then forwards the information to NA. NA has IPv6 driver dependencies. As a result, not all drivers support all features of IPv6. Primary adoption includes the Cisco family of network elements.

Currently, the following NA components do not support IPv6:

- Overlapping IPs — Satellite Gateways do not support IPv6.

- Dynamic IPv6 addresses — NA does not gather or track information on device elements or dynamically assigned IPv6 addresses (for example, link local and multicast).

- IPv6 ACLs — The ACL specific feature does not parse/process IPv6 ACLs, though functionality to search, add, delete, and edit IPv6 ACLs exists.

- NMAP — Using NMAP with the NA Detect Network Device feature do not work.

- Multimaster Distributed System and Horizontal Scalability — Dual stack is supported, however with the replication/RMI using IPv4-only.

- Topology Diagramming — Topology diagramming does not support IPv6.

- SA/NA integration — HP Server Automaton does not support IPv6.

- OO/NA integration — HP Operations Orchestration does not support IPv6.

- NNMi/NA integration- HP Network Node Manager with dual stack is supported, but not with IPv6-only.

- BSAE/NA integration — Business Service Automaton Essentials does not support IPv6.

- DDS integration — The Driver Delivery System does not support IPv6.

4 Working with .rcx Files

The HP Network Automation Software (NA) property files use the `.rcx` extension. NA reads `.rcx` files in reverse alphabetical order. If a given setting is in multiple `.rcx` files, NA uses the last-read value. Thus, the settings in the `adjustable_options.rcx` file take precedence over the settings in the other `.rcx` files installed with NA.

> At startup, NA reads *all* files in the `jre` directory and interprets their contents for NA configuration options. For this reason, save all backup copies of `.rcx` files outside the root NA directory.

In Horizontal Scalability environments, NA shares the actual values of most settings, not the `.rcx` files, across the NA cores. When a setting is modified on one NA core, that setting is replicated to the other NA cores. If an NA core is not operational during the change replication, that NA core does not receive the change. In that case, at a later time, use the Admin > Distributed > Renew Configuration Options page to push changes to other NA cores.

> The distributed system options section of the `appserver.rcx` file lists the settings that are specific to one NA core and are not shared across the NA cores.

Some configuration changes require `.rcx` file modifications. The `.rcx` files are located in the following directory:

- *Windows*: `%NA_HOME%\jre\`
- *Unix*: `$NA_HOME/jre/`

> ⚠ Always edit `.rcx` files with care. These files use XML format. If a `.rcx` file change results in invalid XML, the NA console might not start correctly.

> It is recommended to make all configuration changes in the `adjustable_options.rcx` file. NA patch installations and product upgrades might overwrite any of the other NA-installed `.rcx` files.

The general procedure for changing `.rcx` files is as follows:

1. Back up the `.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

   (NA reads all `.rcx` files within the NA directory structure.)

2. Add new content or update existing content as described in the instructions.

3. Save the `.rcx` file.

4 Reload the `.rcx` settings by doing *one* of the following:

- In the NA console, on the Admin > Administrative Settings > User Interface page, click **Save**.

- Run the `reload server options` command from the NA proxy.

- Restart the NA services.

Some changes do not take effect until the NA services have been restarted.

5 Using Certificates with NA

A certificate identifies the web server to the browser or one server to another. This certificate can be self-signed or signed by a certificate authority (CA). HP Network Automation Software (NA) uses the following certificate files:

- The Truecontrol key store file stores private keys and certificates with their corresponding public keys. It is located as follows:

  — *Windows*:
    `%NA_HOME%\server\ext\jboss\server\default\conf\truecontrol.keystore`

  — *UNIX*:
    `$NA_HOME/server/ext/jboss/server/default/conf/truecontrol.keystore`

- The Truecontrol trust store file contains certificates from other parties that you expect to communicate with, or from certificate authorities that you trust to identify other parties. It is located as follows:

  — *Windows*:
    `%NA_HOME%\server\ext\jboss\server\default\conf\truecontrol.truststore`

  — *UNIX*:
    `$NA_HOME/server/ext/jboss/server/default/conf/truecontrol.truststore`

  The `truecontrol.truststore` file is new as of NA version 9.20.

- The CAcerts key store file also stores private keys and certificates with their corresponding public keys. It is part of the Java Development Kit (JDK) installed with NA and is located as follows:

  — *Windows*: `%NA_HOME%\jre\lib\security\cacerts`

  — *UNIX*: `$NA_HOME/jre/lib/security/cacerts`

This chapter contains the following topics:

- Default NA Certificates on page 18
- Adding a Self-Signed Certificate to NA on page 20
- Adding a CA-Signed Certificate to NA on page 23

Default NA Certificates

At installation, NA includes self-signed certificates in the Truecontrol key store, Truecontrol trust store, and the CAcerts key store. The NA-provided certificates are the same on all NA servers. For that reason, it is recommended to replace the default self-signed certificates with a new self-signed or CA-signed certificate. For information, see Adding a Self-Signed Certificate to NA on page 20 or Adding a CA-Signed Certificate to NA on page 23.

Truecontrol Key Store

The `truecontrol.keystore` file contains the certificate that the web browser uses to identify the NA server. Table 2 lists the key properties of the NA-provided self-signed certificate. Property labels and value formats vary across web browsers.

Table 2   Properties of the Default Certificate for Accessing the NA Console

Property	Default Value
Issued to and by	localhost, Hewlett Packard Company • CN = localhost • OU = Hewlett Packard Company • O = Hewlett Packard Company • L = Palo Alto • S = CA • C = US
Serial number	48 4e 9d 84
Valid date range	June 10, 2008 to June 08, 2018
SHA1 fingerprint	05 de dc 68 58 45 ca ea 88 ff 16 05 e7 65 a9 5b 23 29 d7 65
MD5 fingerprint	65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8

By default, web browsers do not trust self-signed certificates. Therefore, NA console users see an unknown certificate warning before the NA console logon page appears.

Accepting the Truecontrol Certificate in a Web Browser

When the Truecontrol certificate is not in a web browser's list of trusted certificates, the web browser might display a warning message regarding the validity of the certificate. To resolve this issue, follow these steps:

1   Verify that the certificate values are as expected.

   For the default NA-provided certificate, the values should match the information described in Table 2, though the formatting and display order might be different.

2   Follow the web browser procedure for adding the verified certificate to the list of trusteed certificates.

Viewing the Truecontrol Key Store

To view the contents of the `truecontrol.keystore` file from the command line, follow these steps:

1   Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

   • *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

   • *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

2   Examine the contents of the Truecontrol key store file by entering the following command:

   • *Windows*:
      `%NA_HOME%\jre\bin\keytool.exe -list -keystore truecontrol.keystore`

   • *UNIX*:
      `$NA_HOME/jre/bin/keytool -list -keystore truecontrol.keystore`

When prompted for the key store password, enter: **sentinel**

The key store output is of the following form:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
sentinel, 10-Jun-2008, PrivateKeyEntry,
Certificate fingerprint (MD5): 65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
```

Alternatively, use the `-v` (verbose) option for more output in the following form:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: sentinel
Creation date: 10-Jun-2008
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto,
ST=CA, C=US
Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto,
ST=CA, C=US
Serial number: 484e9d84
Valid from: Tue Jun 10 16:28:04 BST 2008 until: Fri Jun 08 16:28:04 BST 2018
Certificate fingerprints:
        MD5:  65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
        SHA1: 05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65
        Signature algorithm name: SHA1withRSA
        Version: 3
```

Truecontrol Trust Store

At NA installation, the `truecontrol.truststore` file contains one self-signed certificate. You can add other products' certificates to this file to support inter-application communication across secure sockets layer (SSL).

For information about importing the HP Network Node Manager i Software certificate into the `truecontrol.truststore` file, see the *HP Network Node Manager i Software–HP Network Automation Integration Guide*.

Adding a Self-Signed Certificate to NA

You can create a new self-signed certificate that is unique to your environment. Using a new self-signed certificate does not require third-party involvement but could require that each NA console user configure their web browser to trust the new self-signed certificate.

To create a self-signed certificate and add it to NA, follow these steps:

1 Generate a new self-signed certificate as follows:

   a Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      — *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

      — *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

   b Create a backup copy of the `truecontrol.keystore` file.

   c Use the `keytool` command to generate a new certificate in the Truecontrol key store file. For example:

      — *Windows*:
      ```
      %NA_HOME%\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
      -validity 3650 -alias nacert -keystore truecontrol.keystore
      ```

      — *UNIX*:
      ```
      $NA_HOME/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
      -validity 3650 -alias nacert -keystore truecontrol.keystore
      ```

      When prompted for the key store password, enter: **sentinel**

      For more information, run the `keytool` command with no options.

   d Enter the requested information:

      — When prompted for your first and last name, enter the identifier of the NA server, which could be `localhost`, the short hostname, or the IP address.

      Do *not* enter the fully-qualified domain name (FQDN) of the NA server.

      Using a value other than `localhost` adds an additional configuration step that requires restarting the NA services.

      — When prompted to confirm the organization informtion (for example, `Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct? [no]:`), type **yes**, and then press **Enter**.

      — When prompted for a password, press **Enter** to use the key store password.

2 Use the `keytool` command to export the newly-created certificate to a file. For example, from the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

   • *Windows*:
   ```
   %NA_HOME%\jre\bin\keytool.exe -export -alias nacert \
   -file nacert.cer -keystore truecontrol.keystore
   ```

   • *UNIX*:
   ```
   $NA_HOME/jre/bin/keytool -export -alias nacert -file nacert.cer \
   -keystore truecontrol.keystore
   ```

When prompted for the key store password, enter: **sentinel**

Specify the alias used when generating the certificate in step 1 on page 20.

The output file (for example, `nacert.cer`) is created in the location from which the command is run.

The command output is of the following form:

```
Certificate stored in file nacert.cer
```

3   Import the exported certificate into the CAcerts key store as follows:

a   Move the export file from its current location to the directory that contains the `cacerts` file. For example, from the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

— *Windows*: `move nacert.cer %NA_HOME%\jre\lib\security`

— *UNIX*: `mv nacert.cer $NA_HOME/jre/lib/security`

b   Change to the directory that contains the `cacerts` file:

— *Windows*: `%NA_HOME%\jre\lib\security`

— *UNIX*: `$NA_HOME/jre/lib/security`

c   Create a backup copy of the `cacerts` file.

d   Use the `keytool` command to import the new certificate into the CAcerts key store file. For example:

— *Windows*:
```
%NA_HOME%\jre\bin\keytool.exe -import -alias nacert \
-file nacert.cer -keystore cacerts
```

— *UNIX*:
```
$NA_HOME/jre/bin/keytool -import -alias nacert -file nacert.cer \
-keystore cacerts
```

When prompted for the key store password, enter: **changeit**

When prompted to trust the certificate, type **yes**, and then press **Enter**.

Specify the file (for example, `nacert.cer`) created in step 2 on page 20.

The alias is the identifier of the new certificate in the `cacerts` file. It does not need to match the alias in the `truecontrol.keystore` file.

The command output is of the following form:

```
Owner: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Issuer: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
        MD5:  FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
        SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
        Signature algorithm name: SHA1withRSA
        Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4   To force NA to use the new certificate, remove the NA-provided certificate from the Truecontrol key store as follows:

    a   Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

       — *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

       — *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

    b   Use the `keytool` command to export the sentinel certificate to a backup file. For example:

       — *Windows*:
```
%NA_HOME%\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

       — *UNIX*:
```
$NA_HOME/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

    When prompted for the key store password, enter: **sentinel**

    The command output is of the following form:

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

    c   Move the backup file (for example, `sentinel_from_truecontrol_keystore.cer`) to a safe location.

    d   Use the `keytool` command to delete the existing sentinel certificate from the Truecontrol key store. For example:

       — *Windows*:
```
%NA_HOME%\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

       — *UNIX*:
```
$NA_HOME/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

    When prompted for the key store password, enter: **sentinel**

    The command output is of the following form:

```
[Storing truecontrol.keystore]
```

5   *Optional*. In step 1 on page 20, if the identifier of the NA server was *not* `localhost`, update the NA configuration as follows:

    a   Change to the directory that contains the `.rcx` files:

       — *Windows*: `%NA_HOME%\jre`

       — *UNIX*: `$NA_HOME/jre`

    b   Back up the `adjustable_options.rcx` file to a location outside of the `<NA_HOME>` directory.

    c   In the `adjustable_options.rcx` file, add the following line:

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

    d   In the new line, replace `hostname` with the identifier entered for first and last name in step d of step 1 on page 20.

e   Save the `adjustable_options.rcx` file.

Completing this step improves the NA console user experience by removing the wait time for each new page within the NA console.

6   Restart all NA services:

   • *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

      — **TrueControl ManagementEngine**

      — **TrueControl FTP Server**

      — **TrueControl SWIM Server**

      — **TrueControl Syslog Server**

      — **TrueControl TFTP Server**

   • *UNIX*: Run the following command:

      `/etc/init.d/truecontrol restart`

7   Instruct each NA console user to add the new certificate to their web browser's list of trusted certificates.

Adding a CA-Signed Certificate to NA

Using a new CA-signed certificate requires interaction with a third-party but does not require that each NA console user configure their web browser to trust the certificate.

To request a CA-signed certificate and add it to NA, follow these steps:

1   Generate a new local certificate as follows:

   a   Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      — *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

      — *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

   b   Create a backup copy of the `truecontrol.keystore` file.

   c   Use the `keytool` command to generate a new certificate in the Truecontrol key store file. For example:

      — *Windows*:
      `%NA_HOME%\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \`
      `-validity 3650 -alias nacacert -keystore truecontrol.keystore`

      — *UNIX*:
      `$NA_HOME/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \`
      `-validity 3650 -alias nacacert -keystore truecontrol.keystore`

   When prompted for the key store password, enter: **sentinel**

   For more information, run the `keytool` command with no options.

   d Enter the requested information:

     — When prompted for your first and last name, enter the fully-qualified domain name (FQDN) of the NA server.

     — When prompted to confirm the organization informtion (for example, `Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct? [no]:`), type **yes**, and then press **Enter**.

     — When prompted for a password, press **Enter** to use the key store password.

2 Use the `keytool` command to create a certificate signing request (CSR) from the new local certificate. For example, from the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

  • *Windows*:
```
%NA_HOME%\jre\bin\keytool.exe -certreq -alias nacacert \
-file narequest.csr -keystore truecontrol.keystore
```

  • *UNIX*:
```
$NA_HOME/jre/bin/keytool -certreq -alias nacacert -file narequest.csr \
-keystore truecontrol.keystore
```

Specify the alias used when generating the local certificate in .

The output file (for example, `narequest.csr`) is created in the location from which the command is run.

3 Submit the CSR to the CA. If given the option, request that the new certificate be in a Tomcat-compatible or Apache-compatible format.

The CA should return one of the following:

  • One file, a signed certificate, referred to as `server.crt` in this procedure.

    The `server.crt` file contains both the server certificate (the top certificate contained in the file) and one or more CA certificates (the last certificates contained in the file).

    In a text editor such as WordPad or vi, copy the contents of the CA certificate into a new file, the `CA.crt` file.

    Use the `server.crt` file when importing the server certificate into the `truecontrol.keystore` file and the `CA.crt` file when importing the CA certificate into the `truecontrol.truststore` file.

  • Two files, referred to as `server.crt` and `CA.crt` in this procedure.

    In a text editor such as WordPad or vi, add the contents of the `CA.crt` file to the end of the `server.crt` file.

    Use the modified `server.crt` file when importing the server certificate into the `truecontrol.keystore` file and the `CA.crt` file when importing the CA certificate into the `truecontrol.truststore` file.

The following examples show what the CA-provided files might look like:

Combined server and CA certificates in one file:

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
................................................................
................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
................................................................
................................................................
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

Separate server and CA certificate files:

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
................................................................
................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

4   Import the modified (if necessary) `server.crt` and `CA.crt` files into the Truecontrol key store as follows:

    a   Copy the `server.crt` and `CA.crt` files to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      —   *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

      —   *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

    b   Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      —   *Windows*: `%NA_HOME%\server\ext\jboss\server\default\conf`

      —   *UNIX*: `$NA_HOME/server/ext/jboss/server/default/conf`

    c   Create a backup copy of the `truecontrol.keystore` file.

    d   For each of the `server.crt` and `CA.crt` files, use the `keytool` command to import the new certificate into the Truecontrol key store file. For example:

      —   *Windows*:

```
%NA_HOME%\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file server.crt -keystore truecontrol.keystore

%NA_HOME%\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file CA.crt -keystore truecontrol.keystore
```

— *UNIX*:

```
$NA_HOME/jre/bin/keytool -import -trustcacerts -alias nacert \
-file server.crt -keystore truecontrol.keystore

$NA_HOME/jre/bin/keytool -import -trustcacerts -alias nacert \
-file CA.crt -keystore truecontrol.keystore
```

When prompted for the key store password, enter: **sentinel**

When prompted to trust the certificate, type **yes**, and then press **Enter**.

The alias is the identifier of the new certificate in each file. It usually matches the alias used to generate the certificate request in step 2 on page 24.

The command output is of the following form:

```
Owner: CN=NA_server.example.com
Issuer: CN=NA_server.example.com
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
         MD5:  FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
         SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

e   Repeat step d until all CA-provided certificates have been imported into the `truecontrol.keystore` file.

5   To force NA to use the new certificate, remove the NA-provided certificate from the Truecontrol key store as follows:

a   Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

— *Windows*: %NA_HOME%\server\ext\jboss\server\default\conf

— *UNIX*: $NA_HOME/server/ext/jboss/server/default/conf

b   Use the `keytool` command to export the sentinel certificate to a backup file. For example:

— *Windows*:

```
%NA_HOME%\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

— *UNIX*:

```
$NA_HOME/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **sentinel**

The command output is of the following form:

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

c   Move the backup file (for example, `sentinel_from_truecontrol_keystore.cer`) to a safe location.

    d Use the `keytool` command to delete the existing sentinel certificate from the Truecontrol key store. For example:

    — *Windows*:

```
%NA_HOME%\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

    — *UNIX*:

```
$NA_HOME/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

    When prompted for the key store password, enter: **sentinel**

    The command output is of the following form:

```
[Storing truecontrol.keystore]
```

6 Update the NA configuration as follows:

    a Change to the directory that contains the `.rcx` files:

    — *Windows*: `%NA_HOME%\jre`

    — *UNIX*: `$NA_HOME/jre`

    b Back up the `adjustable_options.rcx` file to a location outside of the `<NA_HOME>` directory.

    c In the `adjustable_options.rcx` file, add the following line:

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

    d In the new line, replace `hostname` with the identifier entered for first and last name in step d of step 1 on page 23.

    e Save the `adjustable_options.rcx` file.

    Completing this step improves the NA console user experience by removing the wait time for each new page within the NA console.

7 Restart all NA services:

    • *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

    — **TrueControl ManagementEngine**

    — **TrueControl FTP Server**

    — **TrueControl SWIM Server**

    — **TrueControl Syslog Server**

    — **TrueControl TFTP Server**

    • *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

8 Test the new certificate by logging on to the NA console. If the web browser trusts the CA, it will trust the connection to the NA console with no warning message.

Troubleshooting

This section contains information about errors you might see while working with certificates in NA.

Incorrect Magic

Some operating systems, such as RedHat Linux, include a `keytool` utility. If the version of the keytool provided with the operating system does not match the NA JRE version, you will see an error message similar to the following:

```
keytool error: gnu.javax.crypto.keyring.MalformedKeyringException:
incorrect magic
```

In this case, use the keytool utility provided with NA:

*   *Windows*: `%NA_HOME%\jre\bin\keytool.exe`
*   *UNIX*: `$NA_HOME/jre/bin/keytool`

httpmonitor Errors

If you change the certificate and do not import it into the CAcerts key store, you will see `httpmonitor` errors.

Correct this problem by importing the new certificate into the NA key store as described in Adding a Self-Signed Certificate to NA on page 20.

6   Enabling FIPS Mode

The Federal Information Processing Standardization (FIPS) specifies cryptography requirements for both software and hardware. For NA managed devices, FIPS functionality is only pertinent for SSH/SCP device access or SNMPv3 use. Devices that do not support SSH/SCP or SNMPv3 are not affected.

Enabling FIPS mode affects device access as follows:

- Restricts the encryption algorithms that can be used. For example, AES and 3DES are permitted; however Blowfish and DES are not.

- Replaces implementation of other encryption algorithms with a FIPS-compliant encryption algorithm.

➤ Because enabling FIPS restricts the algorithms NA uses to communicate with devices, NA might not be able to communicate with non-FIPS compliant devices.

To enable FIPS mode, follow these steps:

1   Add the following line to the `adjustable_options.rcx` file:

```
<option name="crypto/fips/enabled">true</option>
```

2   Restart the NA management engine.

In the log file, a message incidates that FIPS mode is enabled. For example:

```
{system/crypto} [main] 75 FIPS140Mode: Loading FIPS JCE Provider
```

3   Log on to the NA console as an administrative user.

4   Navigate to the View Details page (Admin > System Status > BaseServerMonitor > View Details).

Text indicates that FIPS mode is enabled. For example:

```
crypto/fips/cipher_list = [3des-cbc, aes128-cbc, aes128-ctr, aes192-cbc
crypto/fips/mac_list = [hmac-sha1, hmac-sha1-96]
```

To disable FIPS mode, follow these steps:

1   Add the following line to the `adjustable_options.rcx` file:

```
<option name="crypto/fips/enabled">false</option>
```

2   Restart the NA management engine.

7   Configuring the Task Completion Email Content

For each task, you can set NA to send an email message upon task completion. The format of the email content (subject and body) is the same for all tasks.

The default format of the email message subject is as follows:

```
<option name="task/email/subject">Task $TaskName$ completed. Task status: $TaskStatus$
</option>
```

The default format of the email message body is as follows:

```
<option name="task/email/text">
Task          : $TaskName$
originated by : $OriginatorName$
scheduled on  : $TaskScheduleDate$
completed with the following status:
              $TaskStatus$.
The following devices have been processed:
              $TaskDevices$.
View the task information here:
              $AppURL$/task.view.htm?taskID=$TaskID$
</option>
```

This format produces an email message similar to the example shown in Table 3.

Table 3   Example of the Default Task Completion Email Message

Content Type	Example
Subject	Task Import Users completed. Task status: Succeeded

Body	Task : Import Users
	originated by : admin
	scheduled at : 2011-08-16 12:35:45.0
	completed with the following status:
	              Succeeded.
	The following devices have been processed:
	              None.
	View the task information here:
	              https://server.example.com:8443//task.view.htm?taskID=2801

To change the format, language, or both of the email content, follow these steps:

1   Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

2   In the `appserver.rcx` file, locate the following comment line:

```
<!-- task email notification options -->
```

3   Copy the following blocks from the `appserver.rcx` file to the `adjustable_options.rcx` file:

   - `<option name="task/email/subject">`

   - `<option name="task/email/text">`

4   Edit the subject and text values. Table 4 lists the available variables for use in these options.

5   Save the `adjustable_options.rcx` file.

6   Restart the NA management engine.

Table 4   Variables for the Task Completion Email Content

Variable	Description
$ApprovalDate$	Task approval date.
$ApproverEmails$	Comma separated list of email addresses of the task approvers.
$ApprovalPriority$	Task approval priority.
$OriginatorFirstName$	The first name of the task originator.
$OriginatorLastName$	The last name of the task originator.
$OriginatorName$	The name of the task originator.
$TaskName$	The task name.
$TaskComments$	The task comments.
$TaskDevices$	A list of devices affected by the task.
$TaskFrequency$	The frequency of the task.
$TaskID$	The task identifier.
$TaskScheduleDate$	The task scheduled timestamp.
$TaskStatus$	The task status. For example; Succeeded, Failed, or Skipped.

8 Disabling the Use of Adobe Flash

HP Network Automation Software (NA) uses Adobe® Flash for displaying the device selector. If you disable the use of Flash, the NA console uses a pure HTML and JavaScript version of the device selector. Generally speaking, this version is slower than the Flash version because of the underlying protocol for communication between NA and the NA console, especially for large data sets (for example, 10,000 devices).

To disable the use of Adobe Flash in the NA console, follow these steps:

1   Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

2   In the `appserver.rcx` file, locate the following line:

        <option name="flexui/devicechooser">true</option>

3   Copy the line from the `appserver.rcx` file to the `adjustable_options.rcx` file.

4   In the `adjustable_options.rcx` file, change the copied line to:

        <option name="flexui/devicechooser">false</option>

5   In the `adjustable_options.rcx` file, to control how many items the search box should return, add the following line:

        <option name="flexui/devicechooser/return_count">12</option>

Optionally change the default value of 12 in this line.

To reduce the number of search results, narrow the search pattern. For example, "192.168" might yield too many results to be displayed. Use "192.168.5" instead.

6   Save the `adjustable_options.rcx` file.

7   Restart all NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
    — **TrueControl ManagementEngine**
    — **TrueControl FTP Server**
    — **TrueControl SWIM Server**
    — **TrueControl Syslog Server**
    — **TrueControl TFTP Server**
- *UNIX*: Run the following command:

        /etc/init.d/truecontrol restart

9 Configuring the Default Setting of the Force Save Check Box for New Tasks

For many NA device tasks, the Force Save task option specifies whether NA should overwrite the startup configuration with the current running configuration at the completion of the task. The setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type in the `appserver.rcx` file.

For each device task, the `appserver.rcx` file contains an option in the following format:

```
<option name="DeviceInteraction/EnforceConfigurationSave/task_name">setting</option>
```

Possible values for `task_name` are:

- Take Snapshot
- Discover Driver
- Run ICMP Test
- Deploy Passwords
- Deploy Config
- Configure Syslog
- Run Command Script
- Run Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Backup Device Software
- Reboot Device
- Run Device Script
- Delete ACLs
- VLAN Task

Possible values for `setting` are:

- true—The Force Save field is visible for this task type and defaults to selected (overwrite the startup configuration). The user running the task can override the default setting by clearing the Force Save check box.
- false—The Force Save field is visible for this task type and defaults to cleared (do not change the startup configuration). The user running the task can override the default setting by selecting the Force Save check box.
- disabled—The Force Save field is not visible for this task type. The task will never attempt to overwrite the startup configuration with the running configuration.

To change the default setting of the Force Save check box for a specific device task type, follow these steps:

1 Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

2 In the `appserver.rcx` file, locate the following line for the task that you want to change:

```
<option name="DeviceInteraction/EnforceConfigurationSave/task_name">setting</option>
```

3 Copy the line to change from the `appserver.rcx` file to the `adjustable_options.rcx` file.

4 In the `adjustable_options.rcx` file, edit the *setting* value.

5 Save the `adjustable_options.rcx` file.

6 Restart the NA management engine.

▶ The change take effect for new tasks only.

10 Parsing Cisco ACS 5.x Logs for Change Detection

As of version 9.20, HP Network Automation Software (NA) provides a mechanism for parsing Cisco Secure Access Control System (ACS) 5.x logs for change detection when those logs are forwarded by ACS 5.x to the NA Syslog server.

▶ The NA AAA Log Reader Agent cannot be used to process ACS 5.x logs because ACS 5.x uses a format different from that of standard RFC-compliant logs. Also, the NA AAA Log Reader Agent is a Windows application while ACS 5.x is installable on a Cisco Secure ACS appliance or VMware.

To enable the use of ACS 5.x logs for change detection, follow these steps:

1 Configure the ACS 5.x server to forward ACS logs to the NA syslog server:

   a On ACS 5.x, use System Administration > Log Configuration > Remote Log Targets > Create to set the IP address of the NA Syslog server.

   Use Advanced Syslog Options to verify that the Port and Facility Code values match the configuration of the NA Syslog server.

   b On ACS 5.x, use System Administration > Log Configuration > Log Categories > Global (or Per Instance) to set the categories of logs to be forwarded (for example, AAA Audit).

   For the selected categories, use the Remote Log Target tab to add the NA Syslog server configured in the previous step as a target.

   For more information, see:

   http://www.cisco.com/en/US/products/ps9911/products_user_guide_list.html

2 On the NA server, update the syslog configuration

   a Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

   b In the `appserver.rcx` file, locate the following line:

       <option name="syslog/process_other_treatments">false</option>

   c Copy the line from the `appserver.rcx` file to the `adjustable_options.rcx` file.

   d In the `adjustable_options.rcx` file, change the copied line to:

       <option name="syslog/process_other_treatments">true</option>

   e Save the `adjustable_options.rcx` file.

3   Restart all NA services.

    • *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

        — **TrueControl ManagementEngine**

        — **TrueControl FTP Server**

        — **TrueControl SWIM Server**

        — **TrueControl Syslog Server**

        — **TrueControl TFTP Server**

    • *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

4   In the NA console, go to Admin > Administrative Settings > Configuration Mgmt, and then add the pattern "CSCOacs" to the Syslog Detection Patterns list.

11 Extending the Number of Custom Enhanced Fields

In the NA console, you can configure up to 31 custom data fields each for the Device Details page and the Device Interfaces page. These fields are available as follows:

- Six fields can be configured on the Admin > Custom Data Setup page.

- 25 fields can be configured on the Admin > Enhanced Custom Fields Setup page (when the Enable Enhanced Custom Fields check box is selected on the Admin > Administrative Settings > User Interface page).

To extend the available number of enhanced custom fields for the Device Details page, the Device Interfaces page, or both pages, follow these steps:

1 Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

2 In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file as follows:

- To extend the number of enhanced custom fields for the Device Details page, add the following line:

    ```
    <option name=" metadata/field_limit/RN_DEVICE">100</option>
    ```

- To extend the number of enhanced custom fields for the Device Interfaces page, add the following line:

    ```
    <option name=" metadata/field_limit/RN_DEVICE_PORT">100</option>
    ```

To restrict the number of available enhanced custom fields, replace 100 with a smaller value. (Specifying a larger value has the same effect as the leaving the value at 100.)

3 Save the `adjustable_options.rcx` file.

4 Reload the `.rcx` settings by doing *one* of the following:

- Run the `reload server options` command from the NA proxy.

- Restart the NA management engine.

12 Changing NA Credentials When Connecting to a New Database Location

If the NA database has been moved to a different server, use the tc_tools utility to configure NA to connect to the new database location. This location must include a valid NA database. For information about installing the NA database, see the *NA Installation and Upgrade Guide* or consult your database administrator.

The tc_tools utility updates the following information on the NA server:

- Database server name
- Database port
- Database name
- Database username
- Database user password

To connect NA to a different NA database, follow these steps:

1 At a command prompt, run the following command:

    - Windows: `<installdir>\client\tc_tools.bat`
    - UNIX: `<installdir>/client/tc_tools.sh`

2 Type **1** to change the database connection information.

3 At each prompt, do *one* of the following:

    - Type the new value for the prompt.
    - Press **Enter** to retain the value between the brackets ([ ]).

4 At the prompt to choose an operation, type **4** to exit the utility.

5 Restart the NA management engine.

13 Full-Text Search of Configuration Text (Oracle and SQL Server)

HP Network Automation Software (NA) supports a contains (full text) search of Configuration Text. After full-text search is enabled, faster configuration text search is available for the following report options:

- Reports > Search For > Devices > Configuration Text > contains (full text)

- Reports > Search For > Configurations > Configuration Text > contains (full text)

- Reports > Search For > Device Templates > Configuration Text > contains (full text)

- Reports > Advanced Search > Search Criteria > Configuration Text > contains (full text)

Additionally, you can create a dynamic group or a dynamic policy scope based on the results of a Search Criteria > Configuration Text > contains (full text) search.

Similarly, these searches also support searching for configuration text that does not contain (full text). The search is always case insensitive for the contains (full text) and does not contain (full text) operators.

The contains (full text) search is an indexed search and requires that the database is enabled for full-text search.

Because the contains (full text) search is indexed, it returns results faster than does the contains search. However, the contains (full text) search supports fewer options than does the contains search.

> This feature is not supported on MySQL.

This topic contains the following topics:

Enabling Full-Text Search of Configuration Text

Full-text search accesses an index of the text records in the database. The initial index generation requires available time and disk space.

▶   If Oracle Text (for an Oracle database) or the SQL Server Full Text Search service (for a Microsoft SQL Server database) is not yet enabled, also plan for database downtime.

NA maintains the full text index by incrementally indexing new configurations added during snapshot tasks and by removing the index entries of deleted configurations.

▶   Note the following:

- Because index generation is CPU-intensive, NA tasks might run slower than normal during the process of enabling full text search.

- Do not restart the NA management engine while index generation is in progress.

In a Horizontal Scalability environment, enable full-text searching on *one* NA server.

In a Multimaster Distributed System environment, enable full-text searching on *each* NA server. Run the enablement procedures in parallel. That is, complete step 1 on each NA server before initiating step 2 on any NA server, and so forth.

Follow the steps appropriate to the database type:

- Enabling Full-Text Search on Oracle on page 45
- Enabling Full-Text Search on Microsoft SQL Server on page 47

Enabling Full-Text Search on Oracle

To enable full-text search on an Oracle database, follow these steps:

1   Verify that Oracle Text is enabled and has the required privileges and space:

   a   Log on to the NA proxy with the credentials used to install NA.

   b   Run the following command:

```
fulltextsearch -option analyze
```

   c   Examine the output of the analyze command.

   — If Oracle Text is not enabled, engage the Oracle database administrator to change the configuration. For information about enabling Oracle Text, see "Administering Oracle Text" in the *Oracle Text Application Developer's Guide*.

   Another information source is the Oracle MetaLink document collection, for which you must have a MetaLink account with Oracle. Documents of interest include the following:

   –   280713.1: *Manual installation, deinstallation of Oracle Text 10gR1*

   –   979705.1: *Manual installation, deinstallation of Oracle Text 10gR2*

   –   579601.1: *Manual installation, deinstallation and verification of Oracle Text 11gR1*

   –   970473.1: *Manual installation, deinstallation and verification of Oracle Text 11gR2*

   — If Oracle Text is enabled, do the following:

   –   Determine whether data pruning is needed. If the analyze command output recommends database pruning, complete this process before generating the full-text index. For more information, see "Data Pruning" in the *NA Installation and Upgrade Guide*.

   –   Verify that the approximate additional space required for the index generation process is available on the database server.

   The index configuration process requires available disk space of 50% to 200% of the configuration text size. Actual space requirements depend on the database contents.

   The index configuration process is resource-intensive. Actual time depends on database hardware and configuration as well as the volume of text to be indexed.

   For more information, see "Frequently Asked Questions About Indexing Performance" in the *Oracle Text Application Developer's Guide*.

2   In the NA console, delay any Take Snapshot tasks that are scheduled to start before the end of the approximate time required for index generation to complete.

3   Generate the full-text index:

   a   From the NA proxy, run the following command:

```
fulltextsearch -option enable -numthreads T
```

   T is the number of parallel threads. Possible values range from 1 to one less than the number of database server cores.

       b   Examine the output of the enable command.

         — The expected status is COMPLETE & VALID.

         — If the status is IN PROGRESS, wait for index generation to complete.

         — If the status is INVALID, remove the index with the `fulltextsearch -option disable` command, and then repeat step a.

You can close the command prompt window during index generation. In this case, run the following command to determine the status of the index generation:

```
fulltextsearch -option status
```

Alternatively, you can watch the NA logs with the troubleshooting option feature/proxy set to debug.

4   In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

• *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

    — **TrueControl ManagementEngine**

    — **TrueControl FTP Server**

    — **TrueControl SWIM Server**

    — **TrueControl Syslog Server**

    — **TrueControl TFTP Server**

• *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

5   In the NA console, examine the status of recent Take Snapshot tasks. Rerun any that failed.

On an Oracle database, the log file contains an error for any Take Snapshot tasks that were running during the generation of the full text index. You can ignore the following error:

```
java.sql.SQLException: ORA-29861: domain index is marked LOADING/
FAILED/UNUSABLE
```

Enabling Full-Text Search on Microsoft SQL Server

To enable full-text search on a Microsoft SQL Server database, follow these steps:

1   Verify that the SQL Server Full Text Search service is enabled and has the required privileges:

   a   Log on to the NA proxy with the credentials used to install NA.

   b   Run the following command:

```
fulltextsearch -option analyze
```

   c   Examine the output of the analyze command.

      — If the SQL Server Full Text Search service is not enabled, engage the SQL Server database administrator to change the configuration.

      — If the SQL Server Full Text Search service is enabled, determine whether data pruning is needed. If the analyze command output recommends database pruning, complete this process before generating the full-text index. For more information, see "Data Pruning" in the *NA Installation and Upgrade Guide*.

2   On SQL Server 2005, remove the SQL Server noise words as follows:

   a   Change to the `$SQL_Server_Install_Path\Microsoft SQL Server\ MSSQL.1\MSSQL\FTDATA\` directory.

   b   Back up the `noiseENU.txt` file.

   c   Delete all entries in the `noiseENU.txt` file to leave an empty file.

For more information about editing noise words, see the "Noise Words" topic in the MSDN library:

     http://msdn.microsoft.com/en-us/library/ms142551(v=sql.90).aspx

On SQL Server 2008, by default no noise words are enabled.

3   Generate the full-text index:

   a   Log on to the NA proxy with the credentials used to install NA.

   b   Run the following command:

```
fulltextsearch -option enable
```

On SQL Server, this command returns immediately and starts full-text indexing. Wait some time before you start using the new search. In the output, verify that this run did not generate any SQL exceptions.

4   Determine the status of the index generation by running the following command:

```
fulltextsearch -option status
```

•   The expected status is COMPLETE & VALID.

•   If the status is IN PROGRESS, wait for index generation to complete.

•   If the status is INVALID, remove the index with the `fulltextsearch -option disable` command. If necessary, increase the available disk space, and then repeat step 3.

Alternatively, you can watch the NA logs with the troubleshooting option feature/proxy set to debug.

5   In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
    — **TrueControl ManagementEngine**
    — **TrueControl FTP Server**
    — **TrueControl SWIM Server**
    — **TrueControl Syslog Server**
    — **TrueControl TFTP Server**
- *UNIX*: Run the following command:

    ```
    /etc/init.d/truecontrol restart
    ```

Disabling Full-Text Search

In a Horizontal Scalability environment, disable full-text searching on *one* NA server.

In a Multimaster Distributed System environment, disable full-text searching on *each* NA server. Run the disablement procedures in parallel. That is, complete step 1 on each NA server before initiating step 2 on any NA server, and so forth.

To permanently disable the contains (full text) search operator in the NA console and to remove the full-text index from the database, follow these steps:

1   If any dynamic groups are configured to use the contains (full text) or does not contain (full text) operator, edit or delete these dynamic group configurations.

2   If any dynamic policy scopes are configured to use the contains (full text) or does not contain (full text) operator, edit or delete these dynamic policy configurations.

3   Remove the full-text index:

a   Log on to the NA proxy with the credentials used to install NA.

b   Run the following command:

    ```
    fulltextsearch -option disable
    ```

4   Disable the full-text search feature by removing the contains (full text) and does not contain (full text) operators from the NA console:

a   Change to the directory that contains the `.rcx` files:

    — *Windows*: `%NA_HOME%\jre`
    — *UNIX*: `$NA_HOME/jre`

b   Back up the `adjustable_options.rcx` file to a location outside the `$NA_HOME` (`%NA_HOME%` on Windows) directory.

c   In the `adjustable_options.rcx` file, add the following line:

    ```
    <option name="fulltextsearch/enabled">false</option>
    ```

d   Save the `adjustable_options.rcx` file.

e   Reload the `.rcx` settings by doing *one* of the following:

— Run the `reload server options` command from the NA proxy.

— Restart the NA management engine.

5   In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

    — **TrueControl ManagementEngine**

    — **TrueControl FTP Server**

    — **TrueControl SWIM Server**

    — **TrueControl Syslog Server**

    — **TrueControl TFTP Server**

- *UNIX*: Run the following command:

    ```
    /etc/init.d/truecontrol restart
    ```

14 Enabling Case-Insensitive Search (Oracle)

HP Network Automation Software (NA) supports case-insensitive searches of many objects in the NA database on Oracle. (The MySQL and Microsoft SQL Server database searches are already case-insensitive.)

This topic contains the following sections:

Affected Fields

When enabled, case-insensitive search is available for most text fields in the NA console.

Search Box

The IP or Hostname search box follows the case-sensitivity configuration.

Search Criteria

The Search Criteria field is available for the following functions:

- Defining a dynamic device group on the New Group and Edit Group pages.
- Defining a dynamic policy scope on the New Policy and Edit Policy pages.
- Creating a custom search on the Advanced Search page.

With an Oracle database, case-insensitive search is not available for the following fields:

- ACL Application
- ACL Configuration
- Comments
- Configuration Text with the contains and does not contain operators. (The contains (full text) and does not contain (full text) operators are always case-insensitive.)

All other fields follow the case-sensitivity configuration.

Device Selector

For the New Task and Rerun Task pages, the Filter box on the device selector follows the case-sensitivity configuration.

Reports

Table 5 lists the report fields that can be searched on a case-insensitive basis when the case-insensitive search feature is enabled.

Table 5   Case Sensitivity of Report Search Fields

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
Device	• Host Name • Device Vendor • Device Model • FQDN • Access Methods • Device Location • Serial Number • Asset Tag • Device Software Version • Device Firmware Version • Device Description • Password Rule • ACL ID • ACL Handle	• ACL Type • Module Slot • Module Description • Module Model • Module Serial • Module Firmware Version • Module Hardware Revision • ROM Version • Service Type • Custom Service Type • VTP Domain Name • VTP Operating Mode	• Comments • Configuration Text • ACL Configuration • ACL Application
Interface	• Port Name • Port Type • Port Status • Running Port State • Description • Configured Duplex • Configured Speed • Negotiated Duplex	• Negotiated Speed • VLAN Name • Host Name • Module Slot • Module Description • Module Model • Module Serial • Module Firmware Version	
Module	• Host Name • Module Slot • Module Description • Module Model	• Module Serial • Module Firmware Version • Module Hardware Revision	• Comments
Policy	• Policy Name • CVE	• Vendor URL • Solution URL	• Solution
Policy, Rule, and Compliance	• Host Name	• CVE	
Configuration	• Host Name	• Changed By	• Comments • Configuration Text
Diagnostic	• Host Name		• Diagnostic Text
Task	• Task Name • Host Name	• Scheduled By	• Comments • Result

Table 5   Case Sensitivity of Report Search Fields (cont'd)

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
Session	• Host Name	• Created By	• Session Data
Event	• Added By	• Host Name	• Description
User	• First Name • Last Name • User Name	• Email Address • AAA User Name • Comments	
ACL	• Host Name • ACL ID • ACL Handle	• ACL Type • Changed By	• ACL Configuration • ACL Application • Comments
MAC Address	• Host Name • Port Name	• Port Description • VLAN	
IP Address	• Host Name • Port Name • Port Description	• VLAN • Associated MAC	
VLAN	• Host Name • VLAN Name • VLAN Type	• VLAN Description • Private VLAN	
Device Template	• Template Name • Device Vendor	• Device Model • Device Description	• Comments • Configuration Text
Single Search	• Added By • Host Name	• Description	

Enabling Case-Insensitive Search of an Oracle Database

For an Oracle database, case-insensitive search accesses a case-insensitive index of the text records in the database for each field in the query.

In a Horizontal Scalability environment, enable case-insensitive searching on *one* NA server.

In a Multimaster Distributed System environment, enable case-insensitive searching on *each* NA server.

To enable case-insensitive search of NA with an Oracle database, follow these steps to generate the case-insensitive indexes:

1   Connect to the NA proxy with the credentials used to install NA.

2   Run the following command:

```
mod oraclecaseinsensitive -option enable
```

3   In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

  — **TrueControl ManagementEngine**

  — **TrueControl FTP Server**

  — **TrueControl SWIM Server**

  — **TrueControl Syslog Server**

  — **TrueControl TFTP Server**

- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

Disabling Case-Insensitive Search

In a Horizontal Scalability environment, disable case-insensitive searching on *one* NA server.

In a Multimaster Distributed System environment, disable case-insensitive searching on *each* NA server.

To permanently disable case-insensitive search of NA with an Oracle database and to remove the case-insensitive indexes from the database, follow these steps:

1   If any dynamic groups are configured with case-insensitive search criteria, edit or delete these dynamic group configurations.

2   If any policies are configured with case-insensitive search criteria, edit or delete these policy configurations.

3   Remove the case-insensitive indexes:

a   Connect to the NA proxy with the credentials used to install NA.

b   Run the following command:

```
mod oraclecaseinsensitive -option disable
```

4   In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

  — **TrueControl ManagementEngine**

  — **TrueControl FTP Server**

  — **TrueControl SWIM Server**

  — **TrueControl Syslog Server**

  — **TrueControl TFTP Server**

- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

15 Reclaiming Unused Space (Oracle)

Database maintenance often involves deleting data chunks within a database table, which results in free space inside the table. New records added after this maintenance populates the free space inside the table first, so the new records can be spread across several physical locations within the table. This fragmentation degrades database performance by extending data access times.

HP Network Automation Software (NA) pruning tasks can cause database table fragmentation. This section identifies one way to defragment an Oracle database tablespace. This procedure can be performed while the database is online.

⚠ This documentation describes one approach to this database administration task. Read the prerequisites to determine whether this approach applies to your situation. For other approaches and more detailed information, see the documentation for your database type and version.

Tablespace defragmentation can be run against all tables in the NA schema. Table 6 lists the NA database tables and the associated LOB columns that are most frequently affected by fragmentation.

Table 6   NA Database Tables Frequently Affected by Fragmentation

Table Name	Target LOB Columns
RN_DEVICE_ACCESS_LOG	• ChangeEventData • Comments
RN_DEVICE_DATA	• DataBlock • Comments
RN_DEVICE_TOPOLOGY_DATA	
RN_DIAGNOSTIC_DATA	• DataBlock • Comments
RN_EVENT	• EventText • EventData
RN_EVENT_MESSAGE	• MessageBody
RN_SCHEDULE_TASK	• Comments • Result • TaskData

To defragment an Oracle database tablespace, follow these steps:

1 Verify that the tablespace meets the following prerequisites:

   • The tablespace must be set with automatic segment space management (ASSM).

   • The disk space available to the redo log must be sufficiently large relative to the size of the tablespace.

2 Enter the SQL*Plus command-line interface as the SYSDBA user.

3 Use the Oracle Segment Advisor to determine whether defragmentation is needed. Either check the results of the Automatic Segment Advisor or run the Segment Advisor manually.

   For more information, see "Using the Segment Advisor" in the *Oracle Database Administrator's Guide*.

4 For each table that requires defragmentation, do the following:

   a Enable row movement by running the following command:

   ```
   ALTER TABLE <table_name> ROW MOVEMENT;
   ```

   b Reclaim unused rows by running the following command:

   ```
   ALTER TABLE <table_name> SHRINK SPACE;
   ```

   c Reclaim unused LOB columns by running the following command:

   ```
   ALTER TABLE <table_name> MODIFY LOB (<lob_column_name>) (SHRINK SPACE);
   ```

Alternatively, reclaim unused rows and columns with one command as follows:

```
ALTER TABLE <table_name> SHRINK SPACE CASCADE;
```

This CASCADE command replaces step b and step c.

16 Restoring Databases

Oracle

For information on restoring Oracle databases, see your Oracle database administrator.

SQL Server

To restore a Microsoft SQL Server database:

1 Make a backup of the database you are about to restore.

2 Launch SQL Server Management Studio.

3 Connect to the SQL Server database server and navigate to your database.

4 Right-click the database, and then select Tasks > Restore > Database.

5 Click the Restore: From Device button.

6 Click Select Devices.

7 Click Add.

8 Open the file browser under File name and select the filename you want to restore.

9 Click OK three times.

10 Click the Options tab.

11 Select Force restore over existing database.

12 Click OK. The database should be restored.

If you receive an error message, such as "Database is in use," you need to either close the connection to that database (stop the jboss server), or go to the Options tab and change the names of the physical files listed to a different name. If you are not using the "sa" login to connect to the database, you may need to change the database login.

To do this, launch Query Analyzer from SQL Server Management Studio. In the database you just restored, enter the following command:

SQL command "sp_change_users_login 'auto_fix' 'username'

Where: `username` is the username that jboss is using to communicate to the SQL Server.

MySQL

To restore MySQL databases, there are two methods.

To restore using the copied files restores all MySQL databases that were on the server at the time of the backup, not just the NA database. This method should only be used if NA is the only application using the database server.

1   Make a backup of the MySQL.

2   Stop the MySQL service (click My Computer --> Control Panel --> Administrative Tools --> Services).

3   Copy all of the files that were backed up from the `mysql\data` directory originally back into the `mysql\data` directory.

4   Restart the MySQL service.

To restore MySQL databases using the .sql backup file:

1   Make a backup of the MySQL database.

2   Edit the `.sql` file. Add the following line to the top of the file:
    `SET FOREIGN_KEY_CHECKS=0;`

> If you are restoring to a different database name, the foreign key constraints inside the dump file reference '<Database_Name>.RN_DEVICE' ('DeviceID'), including the database name. If you restore this to a different database name, in effect you are referencing the database <Database_Name> for your FOREIGN_KEY checks. This is a bug in mysqldump and how it interacts with the InnoDB table types. The solution is to remove the "<Database_Name>."

3   Navigate to the mysql\bin directory and enter the following command to get to the mysql command interface:
    `mysql -h <hostname> -u <username> -p <password>`

4   Enter the following commands in the mysql command interface. (Note that mysql needs forward slashes '/' in path names.)
    ```
    drop database <DatabaseName>;
    create database <DatabaseName>;
    use <DatabaseName>;
    source <BackupFileName>.sql;
    grant all privileges on <DatabaseName>.* TO <username> identified by
    '<password>';
    ```

    Where: `username` is the username that NA uses to connect to the database and `password` is the user's password.

    ```
    grant all privileges on <DatabaseName>.* TO <username>@localhost
    identified by '<password>';
    ```

    Where: `username` is the username that NA uses to connect to the database and `password` is the user's password.

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 Administration Guide, May 2012*

Feedback: