Network Automation

Software Version: 10.30

Administration guide

Document Release Date: June 2017
Software Release Date: June 2017

Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, and Windows Server® 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

For the full Oracle license text, see the `license-agreements` directory on the NA product DVD.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

Support

Visit the HPE Software Support web site at: https://softwaresupport.hpe.com/.

Most of the support areas require that you register as an HPE Passport user to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

Contents

Introduction

This guide contains a collection of information and best practices for administering Network Automation (NA). This guide is for an expert system administrator, network engineer, or HPE 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 *Install and Upgrade guide* and the NA help.

Network Automation Architecture and Ports

The *NA Architecture* diagram illustrates the NA Core components and their logical connections. The diagram also includes external products and components with which NA integrates.

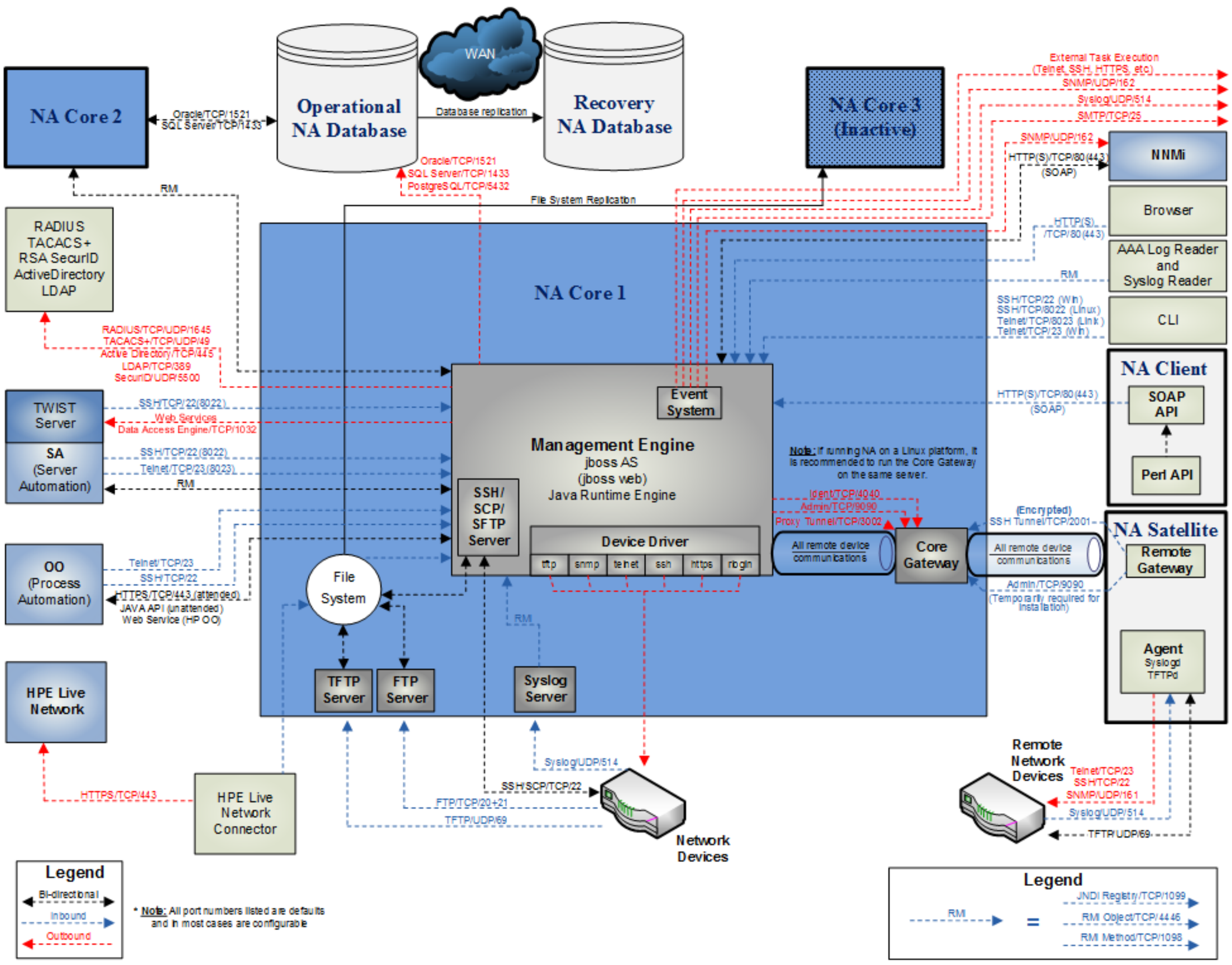
An NA Core is comprised of both an NA server and a database server. The center of the diagram shows the NA server, identified as both the Multimaster Core (MM) #1 and Horizontal Scalability (HS) App #1. Just above the NA server is the database server that is part of Multimaster (MM) Core #1 or the Horizontal 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, and the Syslog 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 entity identifies the service name, protocol, port number, and direction (bidirectional, inbound, or outbound) with respect to the NA Management Engine.

NA Architecture



Note: If running NA on a Linux platform, it is recommended to run the Core Gateway on the same server.

* Note: All port numbers listed are defaults and in most cases are configurable

Ports

The following table shows the ports used by Network Automation (NA Core).

Ports Used by Network Automation (NA Core)

Port	Type	Name	Purpose	Change Configuration
22	TCP	SSH Server Port	SSH port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.

Ports Used by Network Automation (NA Core), continued

Port	Type	Name	Purpose	Change Configuration
23	TCP	Telnet Server Port	Telnet port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.
69	UDP	TFTP Port	Network devices to the NA server	Change not supported
80	TCP	HTTP Port	HTTP port from the NA client to the NA server	Contact your Support representative for assistance.
443	TCP	HTTPS Port	HTTPS port from the NA client to the NA server	Contact your Support representative for assistance.
514	UDP	Syslog Port	Receive syslog messages from network devices on the NA server	See “Configuring the NA Syslog Server” in the NA Installation and Upgrade Guide.
1098	TCP	RMI Activation Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.
1099	TCP	RMI Registration Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA	Contact your Support representative for assistance.

Ports Used by Network Automation (NA Core), continued

Port	Type	Name	Purpose	Change Configuration
			clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	
1433	TCP	Microsoft SQL Server Port	Port on the Microsoft SQL Server that communicates with the NA Core. In a Distributed System configuration, the SQL Server databases communicate with each other on port 1433.	Contact your Support representative for assistance.
1521	TCP	Oracle SQL*Net Port	Port on the Oracle database server that communicates with the NA Core. In a Distributed System configuration, the Oracle processes connect to each other on port 1521.	Contact your Support representative for assistance.
4446	TCP	jboss Remoting Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide	Contact your Support representative for assistance.

Ports Used by Network Automation (NA Core), continued

Port	Type	Name	Purpose	Change Configuration
			and the NA CLI/API Command Reference.)	
4712	TCP	jbossTS Recovery Manager Port	jboss transaction management	Contact your Support representative for assistance.
4713	TCP	jbossTS Transaction Status Manager Port	jboss transaction management	Contact your Support representative for assistance.
4714	TCP	jbossTS Socket Process ID Port	jboss transaction management	Contact your Support representative for assistance.
5432	TCP	PostgreSQL Port	Port on the PostgreSQL database server that communicates with the NA Core	Contact your Support representative for assistance.
5445	TCP	jboss HornetQ netty port	jboss Messaging service	Contact your Support representative for assistance.
5455	TCP	jboss HornetQ netty-batch port	jboss Messaging service	Contact your Support representative for assistance.
6879	TCP	SA port	SA Client	Contact your Support representative for assistance.
8022	TCP	SSH Server Port	SSH port from the NA client to the NA server on the Linux operating system	See "Telnet/SSH Page Fields" in the NA help.
8023	TCP	Telnet Server Port	Telnet port from the NA client to the NA server on the Linux operating system	See "Telnet/SSH Page Fields" in the NA help.
8080	TCP	HTTP Port	HTTP port from the NA client to the NA server. Use instead of 80 when NA	Contact your Support representative for assistance.

Ports Used by Network Automation (NA Core), continued

Port	Type	Name	Purpose	Change Configuration
			coexists with NNMi.	
8443	TCP	HTTPS Port	HTTPS port from the NA client to the NA server. Use instead of 443 when NA coexists with NNMi.	Contact your Support representative for assistance.

The following table shows the ports used by Network Automation (NA Satellite).

Ports Used by Network Automation (NA Satellite)

Port	Type	Name	Purpose	Change Configuration
2001	TCP	Gateway Tunnel Port	TunnelPort from the Satellite to the Core Gateway. The Core Gateway listens for tunnel connections.	Contact your Support representative for assistance.
3002	TCP	Gateway Proxy Port	ProxyPort from the NA Core to the Core Gateway and from the Satellite agent to the Satellite	See "Device Access Page Fields" in the NA help.
4040	TCP	Gateway Ident Port	IdentPort from the NA Core to the Core Gateway	Contact your Support representative for assistance.
8005	TCP	Tomcat Server Port	Port for Tomcat to listen for commands like SHUTDOWN	Contact your Support representative for assistance.
8009	TCP	Tomcat AJP Port	Port for Tomcat to listen for AJP messages	Contact your Support representative for assistance.
8443	TCP	Tomcat HTTPS Port	RpcPort from the Satellite to the management agent (Tomcat), Syslog, TFTP	Contact your Support representative for assistance.
9090	TCP	Gateway Admin Port	AdminPort from the Satellite to the Core Gateway. Note that the Satellite uses all of the	See "Device Access Page Fields" in the NA help.

Ports Used by Network Automation (NA Satellite), continued

Port	Type	Name	Purpose	Change Configuration
			ports that the NA Core uses for managing devices (from the Satellite to the device: 22, 23, 514, 80, and 443).	

IPv6 Readiness

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.

The NA 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
- Deploy Change Plan
- 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
- Satellites

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:

- 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 – Server Automaton does not support IPv6.
- OO/NA integration – Operations Orchestration does not support IPv6.
- NNMi/NA integration – Network Node Manager with dual stack is supported, but not with IPv6-only.
- DDS integration – The Driver Delivery System does not support IPv6.

Tuning NA Performance

This chapter describes several ways to tune the performance of Network Automation (NA). It includes the following topics:

Tuning the NA Management Engine

This section describes recommended tuning of the NA Management Engine. If you update the maximum number of concurrent tasks, also update the maximum data source pool size and the number of connections from NA to the Oracle database.

Task Scheduling

It is recommended that scheduled tasks be planned to run throughout the day to balance the use of NA core server resources.

> **Note:** To prevent a scheduled task running against the entire inventory device group, add the following line to the `adjustable_options.rcx` file:
>
> ```
> <option name="scheduler/stop_inventory_tasks">true</option>
> ```

It is recommend that snapshot tasks occur after the work day ends to capture that day’s changes.

Maximum Concurrent Tasks

The maximum number of concurrent tasks tunes the NA task functionality.

> **Note:** The Maximum Concurrent Tasks and the Maximum Concurrent Group Tasks are specific to the NA Cores and cannot be replicated across the Cores in a Multimaster Distributed System environment.

The recommended value for the maximum number of concurrent tasks depends on the size of the NA deployment. A higher value is not necessarily better.

The following table lists the recommended configuration for maximum concurrent tasks depending on the NA core server size:

NA Core Server Size	Maximum Concurrent Tasks
Small NA Core Server	40
Standard NA Core Server	150 on each NA core
High Powered NA Core Server	360 on each NA core

To set the maximum number of concurrent tasks, follow these steps:

1. Log on to the NA console as an NA administrator.
2. On the Administrative Settings - Server page (**Admin > Administrative Settings > Server**), under Tasks, set Max Concurrent Tasks to the recommended value, and then click **Save**.

> **Tip:** After changing the maximum number of concurrent tasks, see "Maximum Data Source Pool Size" below and "Number of Database Connections from NA" on page 31.

Maximum Data Source Pool Size

If you change the Max Concurrent Tasks setting or the Max Concurrent Group Tasks setting or if the expected maximum number of concurrent users of the NA console changes considerably, update the maximum data source pool size configuration.

The correct maximum data source pool size is the sum of the following factors:

- The Max Concurrent Tasks setting

  This value is listed under Tasks on the Administrative Settings - Server page.
- The Max Concurrent Group Tasks setting

  This value is listed under Tasks on the Administrative Settings - Server page.
- The expected maximum number of concurrent NA users

This number depends on the way your company uses NA.

> **Tip:** The All Users page (**Admin >Users**) lists all user accounts that can connect to NA.

- A buffer of 20

To set the maximum data source pool size configuration, follow these steps:

1. Stop all NA services. See "Start, Stop, or Restart All NA Services" on page 195.
2. To set the maximum data source pool size value, do the following:
   a. Change to the following directory:
      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\deploy`
      - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/deploy`

   b. Back up the `db-ds.xml` file to a location outside the `<NA_HOME>` directory.

   c. In a text editor such as WordPad or vi, open the `db-ds.xml` file.

   d. Search for the string `NASDataSource` to locate the following lines:

   ```
   <attribute name="DataSourceName">NASDataSource</attribute>
   <attribute name="InitialPoolSize">0</attribute>
   <attribute name="MinPoolSize">0</attribute>
   <attribute name="MaxPoolSize">50</attribute>
   ```

   e. Set the `MaxPoolSize` attribute to the calculated value.

   f. Uncomment the following option to set the maximum time for a query to be executed:

   ```
   <attribute name="UnreturnedConnectionTimeout">480</attribute>
   ```

   g. Search for the string `NASReportDataSource` to locate the following lines:

   ```
   <attribute name="DataSourceName">NASReportDataSource</attribute>
   <attribute name="InitialPoolSize">0</attribute>
   <attribute name="MinPoolSize">0</attribute>
   <attribute name="MaxPoolSize">50</attribute>
   ```

   h. Identify, but do *not* change, the value of the `MaxPoolSize` attribute for the NA report data source configuration.

   The values of both maximum pool size attributes factor into the calculation of the number of available database connections.

   i. Save the `db-ds.xml` file.

3. In an NA Horizontal Scalability environment, repeat step 2 on each NA server.
4. On each NA server, start all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

Configuring the NA Cache Size

This topic describes how to tune the NA cache for specific object types. Experience has shown that tuning these values so that NA caches all of the corresponding object types improves NA performance without impacting memory consumption.

To tune the NA cache

1. In the NA console, on the System Status page (**Admin > System Status**), click **Run Now** in the DatabaseMonitor row.
2. On the Monitor Details page, note the count for each of the database objects in the following table.

NA Database Object Description	NA Database Object Name	Current Count	New Value	Configuration Parameter
Identifier of the authentication rule and the protocol used for the last successful access to the device	RN_DEVICE_LASTUSED			jcs.region.DEVICE_LASTUSEDVO_REGION.cacheattributes.MaxObjects
Device	RN_DEVICE			jcs.region.DEVICE_VO_REGION.cacheattributes.MaxObjects
Name of the driver and family for a device	RN_DRIVER_LOOKUP			jcs.region.DRIVERLOOKUP_VO_REGION.cacheattributes.MaxObjects
Device IP address	RN_IP			jcs.region.IPVO_REGION.cacheattributes.MaxObjects

3. For each of these values, determine a new configuration value by adding a buffer to account for network growth.

4. Set the cache size for the identified object types.
   a. Change to the following directory:
      - *Windows*: `<NA_HOME>\jre`
      - *Linux*: `<NA_HOME>/jre`
   b. Back up the `cache.ccf` file to a location outside the `<NA_HOME>` directory.
   c. In a text editor such as WordPad or vi, open the `cache.ccf` file.
   d. For each row of the table in step 2, set the configuration parameter to the new value.
   e. Save the `cache.ccf` file.
5. In an NA Horizontal Scalability or Multimaster Distributed System environment, repeat the previous steps on each NA core server.
6. On each NA core server, restart all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

Configuring the Java Virtual Machine

The recommended configuration of the Java virtual machine (JVM) heap and young generation sizes depend on the size of the NA core server.

The following table lists the recommended initial Java heap size depending on the NA core server size:

NA Core Server Size	**Initial Java Heap Size**
Small NA Core Server	at least 8 GB (8192)
Standard NA Core Server	at least 16 GB (16384)
High Powered NA Core Server	at least 50 GB (51200)

The recommended Java virtual machine (JVM) configuration is:

- Initial Java heap size: from the table
- Maximum Java heap size: the same value as the initial Java heap size
- Young generation size: one-third of the initial Java heap size

> **Note:** The JVM configuration is specified in megabytes.

To set the JVM heap and young generation size, follow these steps:

1. Change to the directory that contains the JVM configuration files:
   - *Windows*: `<HA_HOME>\server\ext\wrapper\conf`
   - *Linux*: `<HA_HOME>/server/ext/wrapper/conf`
2. Back up the `jboss_wrapper.conf` file to a location outside the `<NA_HOME>` directory.
3. In a text editor such as WordPad or vi, open the `jboss_wrapper.conf` file.
4. Search for the string `initmemory` to locate the lines similar to the following lines:

   ```
   # Initial Java Heap Size (in MB)
   wrapper.java.initmemory=8192
   # Maximum Java Heap Size (in MB)
   wrapper.java.maxmemory=8192
   ```

5. Compare the values of the `wrapper.java.initmemory` and `wrapper.java.maxmemory` parameters to the minimums given for the initial and maximum Java heap size.
   - If the values meet or exceed the recommendations, no action is required and you can stop here.
   - If the values are lower than the recommendations, continue with step 6.
6. If necessary, set the `wrapper.java.initmemory` and `wrapper.java.maxmemory` parameters to the minimums given for the initial and maximum Java heap size.
7. Set the young generation size as follows:
   a. Determine whether the young generation size has been set previously by searching for the string `-Xmn`.
      - If this string is in the file, edit this line to set the recommended value for the young generation size as described earlier.

        For example:

        ```
        wrapper.java.additional.3=-Xmn2730m
        ```

      - If this string is not in the file, continue with step b.

   b. Search for the string `Additional` to locate the `Java Additional Parameters` section.

   c. After the last uncommented line in this section, add the following line:

      ```
      wrapper.java.additional.N=-XmnYGm
      ```

   d. In the newly added line, make the following substitutions:

- Replace *N* with the next number in the sequence of uncommented `wrapper.java.additional` parameters.

  For example, if the `wrapper.java.additional.11` parameter is uncommented and the `wrapper.java.additional.12` parameter is commented out with a number sign (#), set *N* to 12.

- Replace *YG* with the recommended value for the young generation size.

  For example:

  ```
  wrapper.java.additional.12=-Xmn2730m
  ```

8. Set the metaspace sizing as follows:

   a. Add the following lines:

      - `wrapper.java.additional.N=-XX:-UseCompressedClassPointers`
      - `wrapper.java.additional.N+1=-XX:-UseCompressedOops`
      - `wrapper.java.additional.N+2=-XX:MaxMetaspaceSize=3072m`
      - `wrapper.java.additional.N+3=-XX:MinMetaspaceFreeRatio=40`

   b. Replace *N* with the next number in the sequence of uncommented `wrapper.java.additional` parameters.

9. Restart all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

For NA installed on a Linux operating system, you must edit the `truecontrol` file (`/etc/init.d/truecontrol`) to avoid any performance issues with JVM. To edit the file, follow these steps:

1. In the truecontrol file, add the following lines after `umask 077`:

   ```
   MALLOC_CHECK_=0
   export MALLOC_CHECK_
   ```

2. Save the file.

3. Restart NA.

Optimizing Dynamic Group Calculation

The dynamic group calculation is initiated by device events, startup thread, and so on.

The dynamic group calculation has the following categories:

- Full cycle update
- Event driven update - The event driven updat"Configuring NA to Support SAML User Authentication" on page 70e can be one of the following:
  - Live update
  - Queued update

It is recommended that you set the full cycle update interval for the non-peak hours. For example, if the full cycle update takes eight hours to complete, set the interval to 1440 minutes (24 hours), and restart the NA services during the non business hours.

Dynamic Group Calculation in a Single Core Environment

In a single core environment, the device group calculation is enabled by default. However, the live event driven update is disabled by adding the following parameter in the `adjustable_options.rcx` file:

```
<option name="dynamic_group/disable_event_listener">true</option>
```

Dynamic Group Calculation in a Horizontal Scalability Environment

In an HS environment, the dynamic group calculation is enabled by default on all the cores. This can result in degraded performance of the NA cores. For better performance, do the following:

- Enable full cycle update on one core
- Enable event driven update on the second core
- Disable dynamic group calculation on the remaining cores.

To enable the full cycle update on one core, follow these steps:

1. Identify the core on which the full cycle update is to be enabled.
2. On the core, add the following parameters in the `adjustable_options.rcx` file:

   ```
   <option name="dynamic_group/disable">false</option>
   <option name="dynamic_group/disable_event_listener">true</option>
   <option name="dynamic_group/disable_queued">true</option>
   <option name="monitor/DynamicDeviceGroupMonitor/enabled">true</option>
   ```

```
<option name="dynamic_group/queued_update_interval">30</option>

<option name="performance/device_group_commit_interval">10</option>
```

To enable the event driven update on the second core, follow these steps:

1. Identify the core on which the event driven update is to be enabled.
2. On the core, add the following parameters in the `adjustable_options.rcx` file:

   ```
   <option name="dynamic_group/disable">false</option>

   <option name="dynamic_group/disable_event_listener">true</option>

   <option name="dynamic_group/disable_queued">false</option>

   <option name="monitor/DynamicDeviceGroupMonitor/enabled">true</option>

   <option name="dynamic_group/queued_update_interval">1</option>

   <option name="performance/device_group_commit_interval">10</option>
   ```

To disable the dynamic group calculation, on the rest of the cores, add the following parameters in the `adjustable_options.rcx` file:

```
<option name="dynamic_group/disable">true</option>

<option name="dynamic_group/disable_event_listener">true</option>

<option name="dynamic_group/disable_queued">true</option>

<option name="monitor/DynamicDeviceGroupMonitor/enabled">false</option>

<option name="dynamic_group/queued_update_interval">30</option>

<option name="performance/device_group_commit_interval">10</option>
```

On all the cores (irrespective of whether the dynamic group calculation is enabled or disabled), add the following parameters under `<array name="distributed/core-specific-options">` in the `adjustable_options.rcx` file:

```
<value>dynamic_group/disable</value>

<value>dynamic_group/disable_queued</value>

<value>monitor/DynamicDeviceGroupMonitor/enabled</value>

<value>dynamic_group/queued_update_interval</value>

<value>performance/device_group_commit_interval</value>
```

```
<value>dynamic_group/update_interval</value>
```

```
<value>dynamic_group/event_driven_recalc</value>
```

Configuring PostgreSQL for NA

This section describes the known tuning of PostgreSQL for NA. You must configure the tuning parameters in the `postgresql.conf` file located in the following directory:

<NA_HOME>`/postgres/data`

The number of database connections is the total number of connections that NA can make to the database at any moment. For PostgreSQL database, the recommended `max_connections` is 200.

For resource usage (except the Write Ahead Log), the tuning recommentations are as follows:

- `shared_buffers = 1GB`
- `max_prepared_transactions = 100`
- `work_mem = 10MB`
- `maintenance_work_mem = 64MB`
- `dynamic_shared_memory_type = posix`
- `vacuum_cost_delay = 10`

For Write Ahead Log, the tuning parameter is as follows:

- `wal_buffers = 1MB`

For better performance of a query, the tuning parameters are as follows:

- `seq_page_cost = 0.1`
- `random_page_cost = 0.1`
- `effective_cache_size = 2GB`

For reporting and logging errors, the required configuration is as follows:

- `logging_collector = on`
- `log_directory = pg_log`
- `log_filename = 'postgresql-%d-%H.log'`

- `log_truncate_on_rotation = on`
- `log_rotation_age = 1d`
- `log_rotation_size = 10MB`
- `log_line_prefix = '%m: %d:%p:%x'`

Autovacuum Tuning Parameters

Automatic vacuuming reclaims the storage by removing obsolete data or tuples from the database. For automatic vacuuming, the tuning parameters are as follows:

- `autovacuum = on`
- `log_autovacuum_min_duration = 0`
- `autovacuum_naptime = 300`
- `autovacuum_vacuum_scale_factor = 0.1`
- `autovacuum_analyze_scale_factor = 0.05`
- `autovacuum_vacuum_cost_delay = 50`

With these settings, `autovacuum` wakes up every five minutes (`autovacuum_naptime`), and checks the threshold and the scale factor. The `autovacuum_vacuum_threshold` is the minimum number of row updates before a vaccum run, and the default value is 50. The `autovacuum_vacuum_scale_factor` is the fraction of table size before a vacuum run, and the default value is 0.1 (which means 10% of the table size.

For new installations of NA 10.20 or later, PostgreSQL is configured with these settings.

Configuring Oracle for NA

This section describes the known tuning of Oracle for NA.

Number of Database Connections from NA

The number of database connections is the total number of connections that NA can make to the database at any moment. This number depends primarily on the NA configuration for the maximum number of concurrent tasks.

If you change the maximum data source pool size, update the Oracle database configuration for the number of database connections.

Additionally, the following errors indicate the need to update the configuration for the number of database connections:

- This task did not complete. Connections could not be acquired from the underlying database!
- This task did not complete. An SQLException was provoked by the following failure: com.mchange.v2.resourcepool.ResourcePoolException: A ResourcePool cannot acquire a new resource -- the factory or source appears to be down.
- This task did not complete. Can't find CustomScript
  Find failed: java.sql.SQLException: Connections could not be acquired from the underlying database!

For an Oracle database, the value of the `processes` parameter sets the number of database connections. The value of the `processes` parameter should be greater than or equal to the sum of the following factors:

- For *each* active NA core, the value of the maximum pool size attribute for the NA data source configuration
- For *each* active NA core, the value of the maximum pool size attribute for the NA report data source configuration
- For *each* active NA core, a buffer of 50

> **Tip:** If the active NA cores in an NA Horizontal Scalability environment are configured identically, the calculation in this step is the same as multiplying the result of the calculation for one NA core by the number of active NA cores in the NA Horizontal Scalability environment.

According to the Oracle documentation, the values of the `sessions` and `transactions` parameters are relative to the value of the `processes` parameter. If the value of the `processes` parameter needs to be changed, the values of the `sessions` and `transactions` parameters should also be updated.

Size of the NA Tablespace

The following error suggests that the NA tablespace does not have sufficient space for its contents:

```
The system could not save the data for device id 50851 - An SQLException was
provoked by the following failure:
```

```
com.mchange.v2.resourcepool.ResourcePoolException: A ResourcePool cannot acquire a
new resource -- the factory or source appears to be down.
```

```
Contact Technical Support. (Reference stack trace ID 1690)
```

Report this message to the database administrator (DBA), and suggest that the DBA evaluate the free space of the NA tablespace.

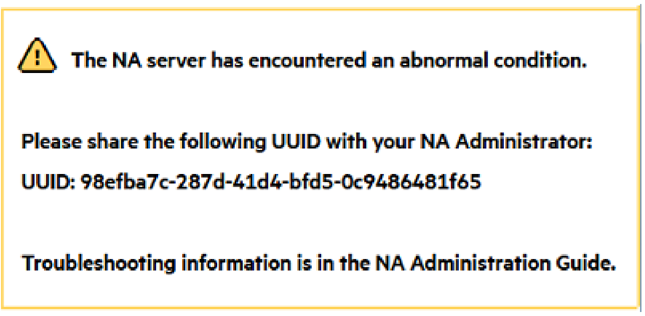
Also see "Reclaiming Unused Space (Oracle)" on page 179.

Configuring SQL Server for NA

At this time, there is no recommended tuning for Microsoft SQL Server with NA.

Troubleshooting an Abnormal Condition on the NA Server

Occasionally, NA users might see a message similar to that shown here:



⚠ The NA server has encountered an abnormal condition.

Please share the following UUID with your NA Administrator:
UUID: 98efba7c-287d-41d4-bfd5-0c9486481f65

Troubleshooting information is in the NA Administration Guide.

When such a condition occurs, NA logs a detailed message to the following file:

- *Windows*: `%NA_HOME%\server\log\jboss_wrapper.log`
- *Linux*: `$NA_HOME/server/log/jboss_wrapper.log`

In the log file, a UUID identifies the message that describes this occurance of the abnormal condition. This UUID is included in the message presented to the NA console user. The user can copy the UUID from the message for pasting into communication with the NA administrator. In the example message shown here, the UUID is `be727c42-0bbd-41cb-8699-d78f7859df83`.

For information about a specific condition, search the `jboss_wrapper.log` file for the UUID listed in the message. The relevant troubleshooting information is included in a block that begins with the following string:

```
========MSG BEGIN=============
```

The block ends with the following string:

```
=========MSG END============
```

Configuring the NA Determination of Which User Changed a Device

The Network Automation (NA) administrator can adjust the priorities that NA uses for associating a user to a specific device change. By default, NA uses the first match from the following list:

- User who scheduled a password change that was run on the device.
- User who scheduled a software update that was run on the device.
- User who deployed a configuration to the device.
- User who ran a script on the device.
- User who connected to the device through the system's proxy.
- User information gathered from AAA logs.
- User information parsed from a syslog message.
- User who scheduled a diagnostic that was run on the device.

NA associates a weighted value to each priority. These weights can be adjusted using settings in the `adjustable_options.rcx` file.

To change the default order of these priorities, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following lines:

```
<option name="changepriority/ACL_DELETE_PRIORITY">21</option>
<option name="changepriority/PASSWORD_CHANGE_PRIORITY">20</option>
<option name="changepriority/SOFTWARE_UPDATE_PRIORITY">18</option>
<option name="changepriority/CONFIGURE_SYSLOG_PRIORITY">17</option>
<option name="changepriority/CONFIG_DEPLOY_PRIORITY">16</option>
<option name="changepriority/SCRIPT_RUN_PRIORITY">15</option>
<option name="changepriority/PROXY_PRIORITY">12</option>
```

```
<option name="changepriority/SYSLOG_PRIORITY">10</option>
<option name="changepriority/AAA_PRIORITY">8</option>
<option name="changepriority/DIAGNOSTIC_RUN_PRIORITY">2</option>
<option name="changepriority/NONE_PRIORITY">0</option>
```

4. As needed, change the value for each priority to reflect the desired priority order. The higher the value, the higher the priority.

   > **Note:** Each value must be an integer and unique within this list of priorities.

5. Save the `adjustable_options.rcx` file.
6. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA management engine.

To verify that the new values are being used, set Feature/ChangeDetection to trace.

Using Certificates with NA

A certificate provides proof of identification in any of the following exchanges:

- The web server identifies itself to the browser.
- One server identifies itself to another server.
- A user identifies themself to a web server.

This certificate can be self-signed or signed by a certificate authority (CA). Network Automation (NA) uses the following certificate files:

- The Truecontrol keystore 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`
  - *Linux*:
    `<NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.keystore`
- The Truecontrol truststore 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`
  - *Linux*:
    `<NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.truststore`
- The CAcerts keystore file also stores private keys and certificates with their corresponding public keys. The NA Java processes use the cacerts file when connecting to an SSL-based service (for example LDAP over SSL). It is part of the Java Development Kit (JDK) installed with NA and is located as follows:
  - *Windows*: `<NA_HOME>\jre\lib\security\cacerts`
  - *Linux*: `<NA_HOME>/jre/lib/security/cacerts`

This chapter contains the following topics:

- "Default NA Certificates" below
- "Adding a Self-Signed Certificate to NA" on page 41
- "Adding a CA-Signed Certificate to NA" on page 47
- "Adding a CA Root Certificate to NA for Enabling PKI" on page 59
- "Troubleshooting" on page 61

Default NA Certificates

At installation, NA includes self-signed certificates in the Truecontrol keystore, Truecontrol truststore, and the CAcerts keystore. 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 41 or "Adding a CA-Signed Certificate to NA" on page 47.

Truecontrol keystore

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

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

Properties of the Default Certificate for Accessing the NA Console, continued

Property	Default Value
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 "Truecontrol keystore" on the previous page, 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 keystore

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`
   - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`
2. Examine the contents of the Truecontrol keystore file by entering the following command:
   - *Windows*:

     ```
     <NA_HOME>\jre\bin\keytool.exe -list -keystore truecontrol.keystore
     ```

- *Linux*:

  ```
  <NA_HOME>/jre/bin/keytool -list -keystore truecontrol.keystore
  ```

When prompted for the keystore password, enter: **sentinel**

The keystore 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 truststore

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 Network Node Manager i Software certificate into the `truecontrol.truststore` file, see the *HPE Network Node Manager i Software–HPE 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`
      - *Linux*: `<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 keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacert -keystore truecontrol.keystore
        ```

      - *Linux*:

        ```
        <NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacert -keystore truecontrol.keystore
        ```

      When prompted for the keystore password, enter: **sentinel**

      > **Tip:** 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.

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

        > **Tip:** 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 keystore 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
     ```

   - *Linux*:

     ```
     <NA_HOME>/jre/bin/keytool -export -alias nacert -file nacert.cer \
     -keystore truecontrol.keystore
     ```

   When prompted for the keystore password, enter: **sentinel**

   > **Tip:** Specify the alias used when generating the certificate in step 1 on page 94.
   >
   > 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 Truecontrol truststore as follows:

   a. Move the exported file from its current location to the directory that contains the `truecontrol.truststore` file:

      - *Windows*: `move nacert.cer <NA_HOME>\server\ext\jboss\server\default\conf`
      - *Linux*: `mv nacert.cer <NA_HOME>/server/ext/jboss/server/default/conf`

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

   c. Use the `keytool` command to import the new certificate into the Truecontrol keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -import -alias nacert \
        -file nacert.cer -keystore truecontrol.truststore
        ```

      - *Linux*:

```
<NA_HOME>/jre/bin/keytool -import -alias nacert -file nacert.cer \
-keystore truecontrol.truststore
```

When prompted for the keystore password, enter: **sentinel**

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

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. Also, import the exported certificate into the cacerts keystore as follows:

   a. Move the exported file from its current location to the directory that contains the `cacerts` file:

      - *Windows*: `move nacert.cer <NA_HOME>\jre\lib\security`
      - *Linux*: `mv nacert.cer <NA_HOME>/jre/lib/security`

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

      - *Windows*: `<NA_HOME>\jre\lib\security`
      - *Linux*: `<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 keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -import -alias nacert \
        -file nacert.cer -keystore cacerts
        ```

      - *Linux*:

        ```
        <NA_HOME>/jre/bin/keytool -import -alias nacert -file nacert.cer \
        -keystore cacerts
        ```

      When prompted for the keystore password, enter: **changeit**

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

> **Tip:** Specify the file (for example, `nacert.cer`) created in step 2.
>
> 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
```

5. To force NA to use the new certificate, remove the NA-provided certificate from the Truecontrol keystore 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`
      - *Linux*: `<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
        ```

      - *Linux*:

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

      When prompted for the keystore 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 keystore. For example:

- *Windows*:

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

- *Linux*:

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

When prompted for the keystore password, enter: **sentinel**

The command output is of the following form:

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

6. *Optional*. In step 1, 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`
   - *Linux*: `<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.

   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. See "Start, Stop, or Restart All NA Services" on page 195.

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

Adding a Self-Signed Certificate to NA for Authenticity, Integrity, and Confidentiality of SAML Messages

Certificates are used for signing and encryption of Security Assertion Markup Language (SAML) messages. 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. However, the NA web user interface users might require to configure their web browser to trust the new self-signed certificate.

To create a self-signed certificate and add it to NA for authenticity, integrity, and confidentiality of SAML messages, 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`
      - *Linux*: `<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 keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nasamlcert -keystore truecontrol.keystore
        ```

      - *Linux*:

        ```
        <NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nasamlcert -keystore truecontrol.keystore
        ```

      When prompted for the keystore password, enter: **sentinel**

      > **Tip:** 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.

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

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

- When prompted to confirm the organization information (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 keystore 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 nasamlcert \
   -file nasamlcert.cer -keystore truecontrol.keystore
   ```

   ○ *Linux*:

   ```
   <NA_HOME>/jre/bin/keytool -export -alias nasamlcert -file nasamlcert.cer \
   -keystore truecontrol.keystore
   ```

   When prompted for the keystore password, enter: **sentinel**

   > **Tip:** Specify the alias used when generating the certificate in "Generate a new self-signed certificate as follows:" on the previous page.
   >
   > The output file (for example, `nasamlcert.cer`) is created in the location from which the command is run.

   The command output is of the following form:

   ```
   Certificate stored in file nasamlcert.cer
   ```

Adding a CA-Signed Certificate to NA

> **Note:** If certificates are provided in the PKCS#12 format, see "Adding a CA-Signed PKCS#12 Certificate to NA" on page 53.

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`
      - *Linux*: `<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 keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacacert -keystore truecontrol.keystore
        ```

      - *Linux*:

        ```
        <NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacacert -keystore truecontrol.keystore
        ```

      When prompted for the keystore password, enter `sentinel`.

      > **Note:** Note the alias used for generating the new certificate. You must use this same alias for generating the certificate signing request in step 2 and for importing the generated certificates into the `truecontrol.keystore` and `truecontrol.truststore` files in step 4, step d.

      > **Tip:** 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 information (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 keystore 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
     ```

   - *Linux*:

     ```
     <NA_HOME>/jre/bin/keytool -certreq -alias nacacert -file narequest.csr \
     -keystore truecontrol.keystore
     ```

   > **Tip:** Specify the alias used when generating the local certificate in step 1.
   >
   > 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` file into the Truecontrol keystore and the `CA.crt` file into the Truecontrol truststore 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`
      - *Linux*: `<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`
- *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`

c. Create backup copies of the `truecontrol.keystore` and `truecontrol.truststore` files.

d. Use the `keytool` command to import the new certificates into the correct files. (One command for each certificate.) 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.truststore
```

- *Linux*:

```
<NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacacert \
-file server.crt -keystore truecontrol.keystore

<NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacacert \
-file CA.crt -keystore truecontrol.truststore
```

When prompted for the keystore or truststore password, enter `sentinel`

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

> **Tip:** The alias is the identifier of the new certificate in each file. It must match the alias used to generate the certificate signing request in step 2.

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 keystore 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`
      - *Linux*: `<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
        ```

      - *Linux*:

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

      When prompted for the keystore 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 keystore. For example:

      - *Windows*:

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

      - *Linux*:

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

      When prompted for the keystore 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
      - *Linux*: <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.

   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. See "Start, Stop, or Restart All NA Services" on page 195.

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.

Adding a CA-Signed PKCS#12 Certificate to NA

PKCS#12 is an archive file format that stores many cryptography objects as a single file. It belongs to the family of PKCS (Public Key Cryptography Standards). A PKCS#12 format certificate is provided with a private key pair bundled in a single .pfx file.

If certificates are provided in this format, you must create a PKCS#12 keystore, convert it into a CA-signed certificate, and then add the certificate to NA. The PKCS#12 keystore can be created using the OpenSSL utility.

To add a CA-Signed PKCS#12 Certificate to NA, follow these steps:

1. Extract the private key from the .pfx (for example, ca_cert.pfx) file:

   ```
   openssl pkcs12 -in ca_certs.pfx -nocerts -out private_key.pem -nodes
   ```

2. Extract the certificates from the .pfx file:

   ```
   openssl pkcs12 -in ca_certs.pfx -nokeys -out all_certificates.cer
   ```

3. Create a PKCS12 keystore using the extracted certificates and private key:

   > **Note:** When prompted for the keystore password, enter `sentinel`

   ```
   openssl pkcs12 -export -inkey private_key.pem -in all_certificates.cer –out
   pkcs12_keystore.p12
   ```

4. Convert the PKCS12 keystore into a Java KeyStore (JKS) and name it as `truecontrol.keystore`:

   ```
   <NA_HOME>/jre/bin/keytool -v -importkeystore –srckeystore pkcs12_keystore.p12 -
   srcstoretype PKCS12 –destkeystore truecontrol.keystore -deststoretype JKS
   ```

   > **Note:** By default, the alias given for this entry is `alias 1`. You can change the alias by using the following command:
   >
   > ```
   > <NA_HOME>/jre/bin/keytool -changealias -alias 1 -destalias sentinelpkcs -
   > keystore truecontrol.keystore
   > ```

5. Go to `<NA_HOME>/server/ext/jboss/server/default/conf/`, and rename the `truecontrol.keystore` to `truecontrol.keystore.bak`.

6. Copy the converted PKCS12 keystore (named as `truecontrol.keystore` in Step 4) to `<NA_HOME>/server/ext/jboss/server/default/conf/`.

7. Use the `keytool` command to export the certificates from keystore:

   ```
   <NA_HOME>/jre/bin/keytool -export -alias sentinelpkcs -file trust.cer -keystore

   <NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.keystore
   ```

8. Use the `keytool` command to import the certificates to truststore:

   ```
   <NA_HOME>/jre/bin/keytool -import -trustcacerts -alias sentinelpkcs -file
   trust.cer -keystore

   <NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.truststore
   ```

9. Restart the NA truecontrol services.

Adding a CA-Signed Certificate to NA for Authenticity, Integrity, and Confidentiality of SAML Messages

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 for authenticity, integrity, and confidentiality of SAML messages, 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`
      - *Linux*: `<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 keystore file. For example:

      - *Windows*:

        ```
        <NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacasamlcert -keystore truecontrol.keystore
        ```

      - *Linux*:

        ```
        <NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
        -validity 3650 -alias nacasamlcert -keystore truecontrol.keystore
        ```

      When prompted for the keystore password, enter `sentinel`.

      > **Note:** Note the alias used for generating the new certificate. You must use this same alias for generating the certificate signing request in step 2 and for importing the generated certificates into the `truecontrol.keystore` and `truecontrol.truststore` files in step 4, step d.

      > **Tip:** 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 information (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 keystore 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 nacasamlcert \
   -file narequest.csr -keystore truecontrol.keystore
   ```

   ○ *Linux*:

   ```
   <NA_HOME>/jre/bin/keytool -certreq -alias nacasamlcert -file narequest.csr \
   -keystore truecontrol.keystore
   ```

   > **Tip:** Specify the alias used when generating the local certificate in "Generate a new local certificate as follows:" on the previous page.
   >
   > 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` file into the Truecontrol keystore and the `CA.crt` file into the Truecontrol truststore 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`
   - *Linux*: `<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`
   - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`

c. Create backup copies of the `truecontrol.keystore` and `truecontrol.truststore` files.

d. Use the `keytool` command to import the new certificates into the correct files. (One command for each certificate.) For example:

   - *Windows*:

     ```
     <NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
     -alias nacasamlcert -file server.crt -keystore truecontrol.keystore

     <NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
     -alias nacasamlcert -file CA.crt -keystore truecontrol.truststore
     ```

   - *Linux*:

     ```
     <NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacasamlcert \
     -file server.crt -keystore truecontrol.keystore

     <NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacasamlcert \
     -file CA.crt -keystore truecontrol.truststore
     ```

   When prompted for the keystore or truststore password, enter `sentinel`

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

   > **Tip:** The alias is the identifier of the new certificate in each file. It must match the alias used to generate the certificate signing request in "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:" on page 56.

   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.

Adding a CA Root Certificate to NA for Enabling PKI

One step in enabling Public Key Infrastructure (PKI) user authentication is to import a copy of the certificate authority (CA) root certificate into the Truecontrol truststore. Completion of this step ensures that NA trusts the issuer of the certificates that users present while logging on to NA.

Import one copy of the root certficate for each CA that generates user certificates.

To import the CA root certificate into NA, follow these steps:

1. Obtain the root certificate from the CA.

   This procedure identifes the root certificate as `root.crt`.

2. Import the `root.crt` file into the Truecontrol truststore as follows:

   a. Copy the `root.crt` file to the directory that contains the `truecontrol.truststore` file:

      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
      - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   b. Change to the directory that contains the `truecontrol.truststore` file:

      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
      - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`

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

   d. Use the `keytool` command to import the root certificate into the Truecontrol truststore file.

For example:

- *Windows*:

  ```
  <NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
  -alias rootcert -file root.crt -keystore truecontrol.truststore
  ```

- *Linux*:

  ```
  <NA_HOME>/jre/bin/keytool -import -trustcacerts -alias rootcert \
  -file root.crt -keystore truecontrol.truststore
  ```

When prompted for the truststore password, enter: **sentinel**

> **Tip:** For more information, run the `keytool` command with no options.

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

> **Tip:** The alias is the identifier of the certificate in each file. The CA must provide the alias used in its root certificate.

The command output is of the following form:

```
Owner: CN=Issuer.FTC.PKI Root CA, DC=ftcpki, DC=com
Issuer: CN=Issuer.FTC.PKI Root CA, DC=ftcpki, DC=com
Serial number: 6a265b0a1f77939d49c0055415511857
Valid from: Sat Feb 23 09:20:01 MST 2013 until: Mon Feb 23 09:30:00 MST 2043
Certificate fingerprints:
         MD5:  6A:35:83:40:67:76:9C:D7:21:4E:C4:D4:CC:4B:6E:15
         SHA1: 93:08:EB:27:77:79:23:F9:6D:9A:B9:5E:8F:DB:EF:91:6C:6E:9C:D8
         Signature algorithm name: SHA1withRSA
         Version: 3
Extensions:

#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
```

```
0000: 41 A9 C7 28 B3 36 11 18   F8 91 4D 58 51 8F 97 16  A..(.6....MXQ...
0010: E8 5C 03 E1                                        .\..
]
]

#4: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

#5: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false

#6: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.2.3.4.1455.67.89.5]
[PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.2
  qualifier: 0000: 30 2E 1E 2C 00 4C 00 65   00 67 00 61 00 6C 00 20
0..,.L.e.g.a.l.
0010: 00 50 00 6F 00 6C 00 69   00 63 00 79 00 20 00 53  .P.o.l.i.c.y. .S
0020: 00 74 00 61 00 74 00 65   00 6D 00 65 00 6E 00 74  .t.a.t.e.m.e.n.t
], PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.1
  qualifier: 0000: 16 1F 68 74 74 70 3A 2F   2F 70 6B 69 2E 66 61 62
..http://pki.fab
0010: 72 69 6B 61 6D 2E 63 6F   6D 2F 63 70 73 2E 74 78  rikam.com/cps.tx
0020: 74                                                 t

]]  ]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

3. Restart the NA services. See "Start, Stop, or Restart All NA Services" on page 195.

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`
- *Linux*: `<NA_HOME>/jre/bin/keytool`

httpmonitor Errors

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

Correct this problem by importing the new certificate into the NA keystore as described in "Adding a Self-Signed Certificate to NA" on page 41.

Configuring Encryption Algorithms

Cipher Algorithms

The following table provides the details of the cipher algorithm options that can be configured in NA:

Algorithm	Key Size
DES	56
3DES	112, 168
Blowfish	32 - 448 (must be a multiple of 8)
AES	128, 192, 256

You can configure the cipher algorithm from the `adjustable_options.rcx` file as follows:

- `<crypto/Algorithm>`
- `<crypto/Algotrithm/KeySize>`

For example, to configure AES, add the following to the `adjustable_options.rcx` file:

- `<option name="Crypto/Algorithm">AES</option>`
- `<option name="Crypto/Algorithm/KeySize">256</option>`

> **Note:** The default cipher algorithm is AES 256.

Hashing Algorithm

The hashing algorithm options that can be configured in NA are as follows:

- SHA
- SHA_256
- SHA_512

The default algorithm is SHA_ 512. You can configure the hash algorithm from the `appserver.rcx` file as follows:

- `<option name="crypto/hash/algorithm">SHA_512</option>`

> **Note:** In a Horizontal Scalability or Multimaster Distributed System environment, you must configure the cipher algorithm and the hashing algorithm on all NA cores.

Enabling FIPS Mode

The Federal Information Processing Standardization (FIPS) specifies cryptography requirements for both software and hardware. With the FIPS mode, all the stored, sensitive data (at rest)—such as user and device passwords, device SNMP string and TACACS/Radius password— and the sensitive data in transit are encrypted using the FIPS certified module. In NA, the FIPS mode is enabled by default. However, the FIPS mode is disabled by default for communication between NA and the devices.

FIPS applies to the SSL/SSH/SCP/SFTP connections to and from NA. When enabled, the default FIPS configuration applies to the following:

- SSL (HTTPS) connections to the NA core
- SSH/SCP/SFTP connections to the NA core
- SSH/SCP/SFTP connections from the NA core to devices

  For NA managed devices, FIPS functionality is only pertinent for SSH/SCP/SFTP device access or SNMPv3 use. Devices that do not support SSH/SCP/SFTP or SNMPv3 are not affected.

> **Note:** By default, NA does not close the SSH connection when a SSH read timeout occurs. To force NA to close the SSH connection upon a SSH read timeout, follow these steps:
>
> a. Add the following line to the `adjustable_options.rcx` file:
>
> ```
> <option name="Access/SSH/SshCloseOnReadTimeout">true</option>
> ```
>
> b. Reload the `.rcx` settings by doing one of the following:
>
> - On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
> - From the NA proxy, run the `reload server options` command.
> - Restart the NA management engine.

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.

  > **Note:** Because of this restriction, NA might not be able to communicate with non-FIPS compliant devices. In this case, do one of the following:

> - Configure NA to use a protocol other than SSH/SCP/SFTP for connecting to non-FIPS compliant devices.
> - Disable FIPS for connections to all devices as described in the procedure for enabling FIPS.

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

> **Note:** The SAML assertion processing is not FIPS compliant.

To disable FIPS mode

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

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

2. Restart the NA management engine.

To enable the FIPS mode again, follow these steps:

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

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

   For data at rest, FIPS allows only AES and 3DES. For information about configuring these algorithms, see "Configuring Encryption Algorithms" on page 63.

2. *Optional*. Configure the permitted encryption algorithms for SSH/SCP/SFTP.

   a. Copy the following lines from the `appserver.rcx` file to the `adjustable_options.rcx` file:

   ```
   <array name="crypto/fips/cipher_list">
      <value>3des-cbc</value>
      <value>aes128-cbc</value>
      <value>aes128-ctr</value>
      <value>aes192-cbc</value>
      <value>aes192-ctr</value>
      <value>aes256-cbc</value>
      <value>aes256-ctr</value>
   </array>
   <array name="crypto/fips/mac_list">
      <value>hmac-sha2-256</value>
      <value>hmac-sha256</value>
   ```

```
</array>

<array name="crypto/fips/kex_list">
   <value>diffie-hellman-group-exchange-sha256</value>

</array>
```

> **Note:** The `crypto/fips/cipher_list`, `crypto/fips/mac_list` , and the `crypto/fips/kex_list` parameters are applicable only to the SSH/SCP/SFTP connections.

b. For each encryption algorithm to block, delete the associated line in the `adjustable_options.rcx` file.

3. Enable FIPS for connections to all devices by adding the following line to the `adjustable_options.rcx` file:

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

   > **Note:** You must set this option to `false` only if all the devices from the NA inventory support FIPS.

4. Restart the NA management engine.

5. Log on to the NA console as an NA administrator.

6. Open the View Details page (**Admin > System Status > BaseServerMonitor > View Details**).

   In the text, the following line indicates that FIPS mode is enabled.

   ```
   crypto/fips/enabled = true
   ```

> **Note:** In a Horizontal Scalability or Multimaster Distributed System environment, you must enable/disable FIPS on all NA cores.

Key Zeroization

Enabling FIPS mode ensures the zeroization of the keys used for encrypting the database password and the sensitive data at rest. For data in transit, the content is lost immediately when power is removed or NA is restarted; therefore, SSH/SCP/SFTP/HTTPS session keys are considered zeroized when NA is restarted or shutdown. Persistent keys are zeroized automatically in NA when FIPS is enabled.

Configuring Java in NA

You can configure NA Core and NA Satellite to use a Java Runtime Environment (JRE) that is different from Zulu JRE, the default JRE installed with NA. The supported environments are as follows:

- Oracle JRE
- OpenJDK JRE

You can configure NA to use OpenJDK or Oracle JRE, by using the `nas_configJava` tool.

On NA Core, the tool is located in the following directory:

On Windows:

<NA_HOME>\`nas_configJava.bat`

On Linux:

/opt/NA/`nas_configJava.sh`

On NA Satellite, the tool is located in the following directory:

/opt/opsware/nassat/`nassat_configJava.sh`

When you configure NA Core and NA Satellite to use the non-default JRE (OpenJDK or Oracle), make sure that only version x64 of the JRE is used. Similarly, NA Core and NA Satellite must have the same JRE configured, and should be of the same version. For example, if you configure NA Core to use OpenJDK JRE version 1.8.0_92 x64, ensure that NA Satellite must also be configured to use OpenJDK JRE version 1.8.0_92 x64.

To configure NA Core to use a JRE, follow these steps:

1. Run the following command:

   `nas_configJava` <*Path to the Java binary file*>

   For example, `nas_configJava /opt/NA/jre/bin/java`

2. Restart the NA services. For more information, see "Start, Stop, or Restart All NA Services" on page 195.

To configure NA Satellite to use a JRE, follow these steps:

1. Run the following command:

   `nassat_configJava.sh` <*NA Satellite_HOME*> <*Path to the Java binary file*>

   For example, `nassat_configJava.sh /opt/opsware/nassat /opt/opsware/nassat/jre/bin/java`

2. Restart the gateway by running the following command:

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

> **Note:** After configuring NA Satellite to use a JRE, if the NA remote agent is redeployed, you must configure NA Satellite again to use the JRE.

> **Note:** You must install the **Java Cryptography Extension (JCE) Unlimited Strength Policy Files for the Java Platform Runtime Environment 8** in the JRE that NA is configured to use.
>
> For example, you must copy the following jars from the <*NA_HOME*>`/jre/lib/security` directory to the respective location of the JRE directory that NA is configured to use:
>
> - `local_policy.jar`
> - `US_export_policy.jar`

Configuring NA to Support SAML User Authentication

NA can authenticate a user based on SAML when using the web user interface. Enabling SAML user authentication impacts all users on all NA cores.

NA supports the SAML 2.0 Web Browser Single Sign On (SSO) and Single Log Out (SLO) Profiles. The supported SSO profile and bindings are as follows:

- `urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser` with the following bindings:
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`

The supported SLO profile and bindings are as follows:

- `urn:oasis:names:tc:SAML:2.0:profiles:SSO:logout` with the following bindings:
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`

  > **Note:** NA supports only the Front Channel logout.

> **Note:** When SAML is enabled and a new user is created, the user ***must*** change the password at least once, after the first log in. To change the password, on the NA Home page, under **My Settings**, click **Change Password**, and then enter the required details. For more information about changing a password, see the *Change Password Page Fields* topic in the *User guide*.

> **Note:** When SAML is enabled, NA does not support the HPE SSO (also known as LWSSO (Light-weight Single Sign-on)) feature that is used while integrating NA with other HPE applications such as NNMi. The HPE SSO feature should not be configured if SAML is enabled on the system.

> **Note:** When SAML is enabled, NA does not support the logon banner page that is displayed when the user attempts a log on to the NA console. The NA logon banner should not be enabled when SAML is configured as the external user authentication.

For the authenticity and integrity of messages, NA supports the signing of SAML messages. NA signs authentication requests using the `RSA_SHA512` algorithm. Signing of SAML messages is mandatory and cannot be turned off.

The SAML Subject NameID should match the NA user name. When external authentication such as LDAP is configured for a CLI/API user, the CLI/API user name from the external authentication source should also match the SAML Subject NameID and the NA user name. However, the default System Administrator can always access the NA CLI/API using local credentials. That is, the default System Administrator can access NA CLI/API even if the user is not present in the external authentication source, or if the authentication source is unavailable.

NA rejects any unsigned response by the IdP—the IdP should always send a signed assertion response. Similarly, the Destination attribute must be present in the SAML authetication response. An example snippet of a SAML 2.0 Authentication Response that contains the Destination attribute is as follows:

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Destination="https://mynaserver.net/"
ID="ID_7cbdec34-b9f2-4008-a33c-a6afcd2a1809"
InResponseTo="ID_16eb3572-4913-40df-ab30-4614588d5c21"
IssueInstant="2015-09-30T06:40:49.027Z"
Version="2.0">
```

If you are encrypting the authentication response, NA requires that the entire SAML Response Assertion must be encrypted by the IdP.

As SAML messages are time-stamped, NA and the IdP must have their clocks synchronized with a trusted time source.

Note that you cannot configure SAML when NA is integrated with the HPE Server Automation software.

To configure NA to use SAML authentication to access the NA web user interface, follow these steps:

1. Make sure that all the users who have to access the NA web user interface—including the administrator—are present in the SAML Identity Provider (IdP) and are created in NA as well.

> **Note:** Make sure that the user name for the administrator is unique to NA. For example, `naadmin`.

2. *Optional*. Do the following:

   a. Update some of the SAML-related RCX options in the `adjustable_options.rcx` to make sure that future upgrades do not overwrite them.

   > **Note:** It is recommended to use the defaults unless there is a specific reason that they are not acceptable.

   > **Note:** If NA is in a multi-core setup, make sure that the same values are used on all cores.

   The following table lists the RCX options that should be updated:

RCX option	Use
`saml/keycloak/saml/binding`	To decide the type of SAML binding to be used. Valid values are: • `POST` (Default value) • `Redirect`
`saml/spmetadata/filename`	To specify the default filename for the exported SP metadata. The default value is `na_spmetadata`. However, you can use any reasonable file names without special characters.
`saml/keycloak/SSL`	• `EXTERNAL` - Only non-private IP addresses must come through HTTPS (Default value) • `ALL` - All the requests must come through HTTPS
`saml/ThrowGenericErrorOnly`	To display a generic 404 error irrespective of whether the SAML authentication fails at the protocol level (such as due to invalid signing) or at the NA level (such as due to missing user name in the database).

RCX option	Use
	Valid values are: • `false` - Displays the 404 error when the SAML Authentication fails at the protocol level (Default value) • `true` - Displays the 404 error whenever the SAML authentication fails This option does not require a SAML reconfiguration.
`saml/attribute/username/enable`	Enables the usage of SAML Attribute Value as a user name instead of the subject name ID value. This option should be used in combination with the `saml/attribute/username/attributename` RCX option. Valid values are: • `false` (Default value) • `true`
`saml/attribute/username/attributename`	Gives the attribute name value to be used as the user name. You can use a valid SAML attribute name.
`saml/keycloak/SIGNALG`	The algorithm used for signing requests. Valid values are: • `RSA_SHA1` • `RSA_SHA256` • `RSA_SHA512` (Default value) • `DSA_SHA1`

b. Run the `reload server options` command from the NA proxy to ensure that NA reads the new RCX values after they are changed in the file.

3. Select the key pair that you want to use for signing or encryption. You can do one of the following:

   - Use the existing SSL certificate by using the alias name as `sentinel`.
   - Choose the key pair for signing or encryption. For more information, see the following topics:

- "Adding a Self-Signed Certificate to NA for Authenticity, Integrity, and Confidentiality of SAML Messages" on page 46
- "Adding a CA-Signed Certificate to NA for Authenticity, Integrity, and Confidentiality of SAML Messages" on page 55

> **Note:** If the certificates used for SAML are replaced in the keystore, the SAML configuration file must be regenerated and NA must be restarted.

4. Get the IdP metadata from you identity provider.
5. On the NA console, do the following:

   a. On the menu bar under **Admin**, select **External Authentication Setup**, and then click **SAML Setup**. The **Build SAML Configuration File** page opens.

   b. On the page, enter the required details.

   The following table describes the fields that appear on the page:

Field	**Description**
SP Entity ID	The unique identifier for the SAML SP entity.
Alias for signing certificate	The certificate alias used for signing the SAML authentication request.
Use same certificate	Select the checkbox if you want to use the same certificate for both signing and encryption.
Alias for encryption certificate	The certificate alias used for encrypting the SAML authentication response.
NameId Format	Select the name identifier format. The default value is `transient`.
IDP metadata file	Browse for the IdP metadata file that you want to import.

   c. Do one of the following:

   - Click **Save & Export** if you want to configure NA as the SAML SP, and generate the SP metadata file. You must click this button when you set up NA as the SAML SP for the first time.
   - Click **Export** if you want to only generate the SP metadata file.

   On successful generation of the SP metadata file (which is `na_spmetadata.xml` by default), the **Download NA SAML SP Metadata** page appears.

   d. On the page, click **Download**. The downloaded SP metadata file is used for identity assertion from the IdP.

6. In an NA Horizontal Scalability or Multimaster environment, repeat step 3 to step 5 on each NA core.
7. On the NA console, go to the User Authentication page, and then select **SAML 2.0** as the external authetication type for each NA core.
8. Restart the NA services on each core.
9. *Optional*. Enable LDAP authentication for CLI/API. To achieve this, on the NA console, follow these steps:
   a. On the menu bar under Admin, select Administrative Settings and click User Authentication. The Administrative Settings - User Authentication page opens.
   b. On the User Authentication page, in the SAML Authentication section, select LDAP as the authentication source for CLI/API when SAML is enabled as the external authentication method for web user interface (**Authentication source for CLI/API when using SAML** field).
   c. Click **Save**.
   d. In the SAML Authentication section, click the LDAP Setup link to configure the NA connection to the LDAP directory service. For more infomation, see the *LDAP External Authentication Setup* section in the *User guide*.

   > Note: When SAML is enabled, on the LDAP Setup Wizard, **Simple Auth** is enabled by default. This indicates that LDAP is used only for authentication—NA does not automatically add LDAP users or groups and does not synchronize user information.

Disable SAML User Authentication

If you have access to the NA web user interface disable SAML user authentication by following these steps:

1. Log on to the NA web user interface as a user with administrator privileges.
2. On the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), set External Authentication Type to anything other than **SAML**.

3. Click **Save**.
4. Restart the NA services.

If you do not have access to the NA web user interface, disable SAML user authentication by following these steps:

> **Caution:** This procedure requires editing configuration files that are crucial to NA functionality. Only follow these steps if you do not have access to the NA web user interface. Verify all changes before saving the configuration files.

1. Stop the NA services. See "Start, Stop, or Restart All NA Services" on page 195.
2. Disable SAML user authentication at the NA web user interface level.
   a. Change to the directory that contains the `.rcx` files:
      - *Windows*: `<NA_HOME>\jre`
      - *Linux*: `<NA_HOME>/jre`

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

   c. In the `site_options.rcx` file, locate the following lines:

   ```
   <option name="authentication/external/type">
     <title>External Authentication Type</title>
     …
     <comment>Choose the type of external authentication you would like   to
   use. &lt;br&gt;
      If you choose TACACS+, RADIUS, Server Automation, or
     PKI, configure that type in the related section on this page.
     &lt;br&gt;SecurID has no additional external authentication
     options. &lt;br&gt;
     </comment>samlauth</option>
   ```

   d. Change the option type from `samlauth` to `local`:

   ```
   </comment>local</option>
   ```

   > **Tip:** Be sure that you are working in the `<option name="authentication/external/type">` block.

3. Start the NA services. See "Start, Stop, or Restart All NA Services" on page 195.

Users should now be able to log on to the NA web user interface with the user name and password configured on the All Users (**Admin** > **Users**) page in the NA console.

Troubleshooting SAML in NA

This section discusses the potential problems related to enabling SAML authetication in NA, and the possible workarounds to the problems.

1. **Enabling SAML Logging**

   In addition to the normal NA loggers such as `system`, and `authenticate`, SAML has a new logger at a protocol-handling library level.

   To enable this logging for advanced troubleshooting, follow these steps:

   > **Caution:** Enabling this logging greater than the `INFO` level can print out the entire SAML Authentication packet traces into the log file. You must use it as required and should remember to turn it back to `INFO` level.

   a. Open the following file:

      Windows

      ```
      <NA_HOME>\server\ext\jboss\server\default\deploy\jboss-logging.xml
      ```

      Linux

      ```
      <NA_HOME>/server/ext/jboss/server/default/deploy/jboss-logging.xml
      ```

   b. In the file, change `<logger category="org.keycloak" use-parent-handlers="false"> <level name="INFO"/>` to `<logger category="org.keycloak" use-parent-handlers="false"> <level name="TRACE"/>`.

   c. Save the file.

      > **Caution:** Note the following:
      >
      > i. Do not make any syntax error in the file.
      >
      > ii. Do not try to save a backup copy of the file in the same (or nearby) directories.
      >
      > iii. If you want to save a backup copy of the file, save it outside the NA installation directory.

The logging turns on in a few seconds. The log file is available as part of the standard `Troubleshooting.zip` deliverable from the NA web user interface.

The log file is generated in the following location:

Windows

```
<NA_HOME>\server\ext\jboss\server\default\log\keycloak.log
```

Linux

```
<NA_HOME>/server/ext/jboss/server/default/log/keycloak.log
```

2. **RedirectToLastRequestedPage RCX Option**

   The following RCX option is ignored when SAML is enabled:

   - `"<option name="WebUI/RedirectToLastRequestedPage">true</option>”`

   This option defaults to `true`.

3. **SAML logging configuration changes do not take effect**

   If the SAML logging configuration changes do not take effect, do the following:

   Restart the NA services. For more information, see "Start, Stop, or Restart All NA Services" on page 195.

Configuring NA to Support PKI User Authentication

NA can authenticate a user based on the information in an X.509 format certificate. The certificate can be installed into the browser that runs the NA console. Alternatively, the certificate can be on a separate device, such as a smart card, that the user connects to the computer before opening the NA console. Public Key Infrastructure (PKI) user authentication enables both Common Access Card (CAC) and Personal Identity Verification (PIV) for user authentication into NA.

Enabling PKI user authentication impacts all users on all NA cores. Ensure that all NA users have X.509-format certificates or use an alternate user authentication method.

Enabling PKI user authentication does not impact device authentication.

While PKI user authentication is enabled, NA proxy sessions initiated from the NA console also use PKI user authentication. The NA API and NA proxy sessions initiated outside the NA console (for example, through telnet or SSH) do not support PKI user authentication.

This chapter contains the following topics:

- "Configure NA for PKI User Authentication" below
- "Configure NA for Smart Card Authentication" on page 81
- "Distinguished Names Example" on page 81
- Clear Authentication Data in the Browser
- "Disable PKI User Authentication" on page 83

For information about how NA determines whether to grant access to a PKI certificate user, see “User Authentication” in the *User guide*.

Configure NA for PKI User Authentication

To configure NA to use X.509 format certificate authentication for accessing the NA console and the NA proxy from the NA console, follow these steps:

1. Import the certificate authority root certificate into the NA truststore as described in "Adding a CA Root Certificate to NA for Enabling PKI" on page 59.

   In a Horizontal Scalability or Multimaster Distributed System environment, import the certificate authority root certificate into the NA truststore on each NA core.

2. After restarting the NA services, log on to the NA console as a user with administrator privileges.

3. Configure NA user names and privileges.

   NA consults a user directory to determine each user's access privileges. Each NA user name must match the certificate subject according to the mapping rules set on the Administrative Settings – User Authentication page of the NA console. For information about available mapping options, see "User Authentication" in the *User guide*.

   > **Note:** When the certificate subject includes the at sign (@), you can replace this character with the underscore character (_) in the NA user name. However, you can set the `replaceAtSign` parameter to `false`, and retain the at sign (@) in the NA user name in the certificate subject. To achieve this, follow these steps:
   >
   > a. In the `appserver.rcx` file, set the following parameter to `false`:
   >
   > ```
   > <option name="authentication/pki/replaceAtSign">false</option>
   > ```
   >
   > b. Save the `appserver.rcx` file.
   >
   > c. Reload the `.rcx` settings.

   - To use the NA database as the user directory, create and configure each NA user from the All Users page (**Admin** > **Users**) in the NA console.

     > **Note:** With PKI user authentication, the process of connecting to the NA console validates that the password for the NA user in the NA database meets the security policies and has not expired. Additionally NA user passwords might be used for device authentication.

   - To use a directory service as the user directory, use the LDAP Set-up Wizard as described in "LDAP External Authentication Setup" in the *User guide*.

4. Verify that at least one of the NA users configured in step 3 belongs to the Administrator group.

   > **Note:** While PKI user authentication is enabled, if the user name of the administrator user account created during NA installation does not correspond to a certificate, that account is not available for connecting to the NA console

5. In the PKI Authentication section of the Administrative Settings – User Authentication page

(**Admin** > **Administrative Settings** > **User Authentication**), specify the following:

- The location of the NA user directory
- The certificate fields that contain the NA user name (see "Distinguished Names Example" below)
- The distinguished names of the trusted certificate issuers
- The certificate revocation checking configuration

For more information about these fields, see “User Authentication” in the *User guide*.

6. In the External Authentication Type section of the Administrative Settings – User Authentication page, select **PKI**.
7. Click **Save**.

Configure NA for Smart Card Authentication

To configure NA to use smart card authentication for accessing the NA console and the NA proxy from the NA console, follow the steps in "Configure NA for PKI User Authentication" on page 79. In the PKI Authentication section of the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), for the Extended Key Usage field, enter `1.3.6.1.4.1.311.20.2.2` (for smart card certificates).

Distinguished Names Example

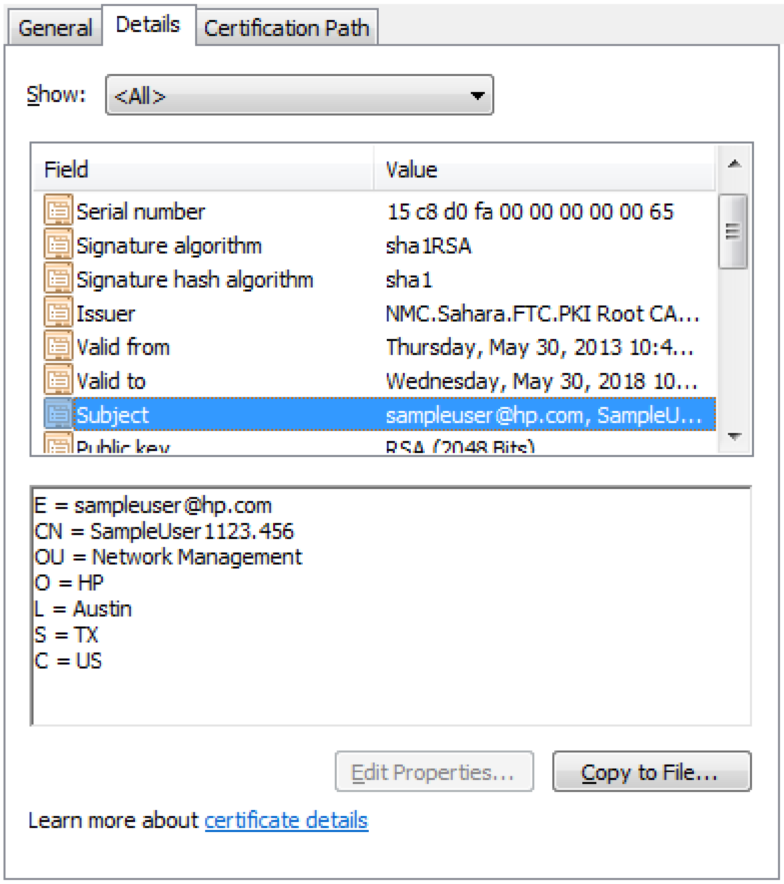
This section contains the following examples:

- "Certificate Subject" below
- Certificate Subject Alternative Name

Certificate Subject

The following image shows the Subject field of an X.509 format certificate. This Subject field contains the distinguished name of the certificate owner.

Subject Example



Field	Value
Serial number	15 c8 d0 fa 00 00 00 00 00 65
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	NMC.Sahara.FTC.PKI Root CA...
Valid from	Thursday, May 30, 2013 10:4...
Valid to	Wednesday, May 30, 2018 10...
Subject	sampleuser@hp.com, SampleU...
Public key	RSA (2048 Bits)

E = sampleuser@hp.com
CN = SampleUser1123.456
OU = Network Management
O = HP
L = Austin
S = TX
C = US

In this example, the elements of the distinguished name are as follows:

- Email address (`sampleuser@hpe.com`)
- Common name (`SampleUser1123.456`)
- Organizational unit (`Network Management`)
- Organization (HPE)
- Location (`Austin`)
- State (TX)
- Country (US)

To use the entire email address as the NA user name, enter `EMAILADDRESS` in the **Ordered Subject Attribute** field on the Administrative Settings – User Authentication page.

To use a portion of the email address as the NA user name, enter `EMAILADDRESS=`*`<regular_expression>`* in the **Ordered Subject Attribute** field on the Administrative Settings – User Authentication page. Craft the regular expression to extract the NA user name from the email address.

To use the common name as the NA user name, enter `COMMONNAME` in the Ordered Subject Attribute field on the Administrative Settings – User Authentication page.

Disable PKI User Authentication

If you have access to the NA console, disable PKI user authentication by following these steps:

1. Log on to the NA console as a user with administrator privileges.
2. On the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), set External Authentication Type to anything other than **PKI**.
3. Click **Save**.

If you do not have access to the NA console, disable PKI user authentication by following these steps:

> **Caution:** This procedure requires editing configuration files that are crucial to NA functionality. Only follow these steps if you do not have access to the NA console. Verify all changes before saving the configuration files.

1. Stop the NA services. See "Start, Stop, or Restart All NA Services" on page 195.
2. Disable PKI user authentication in the PKI configuration file.
   a. Change to the directory that contains the configuration file:
      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
      - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   b. Back up the `nms-auth-config.xml` file to a location outside the `<NA_HOME>` directory.

   c. In the `nms-auth-config.xml` file, locate the following lines:

```
<realms>
  <!-- valid modes are X509, BASIC or FORM. Not all realms support
  all modes. -->
  <realm name="console">
    <mode>X509</mode>
  </realm>
</realms>
```

d. Change the mode line to read:

```
<mode>FORM</mode>
```

3. Disable PKI user authentication at the NA console level.

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

      - *Windows*: `<NA_HOME>\jre`
      - *Linux*: `<NA_HOME>/jre`

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

   c. In the `site_options.rcx` file, locate the following lines:

```
<option name="authentication/external/type">
  <title>External Authentication Type</title>
  …
  <comment>Choose the type of external authentication you would like   to
use. &lt;br&gt;
   If you choose TACACS+, RADIUS, HPE Server Automation Software, or
  PKI, configure that type in the related section on this page.
  &lt;br&gt;SecurID has no additional external authentication
  options. &lt;br&gt;
  </comment>certificate</option>
```

   d. Change the option type from certificate to local:

```
</comment>local</option>
```

> **Tip:** Be sure that you are working in the `<option name="authentication/external/type">` block.

4. Start the NA services. See "Start, Stop, or Restart All NA Services" on page 195.

Users should now be able to log on to the NA console with the user name and password configured on the All Users (**Admin** > **Users**) page in the NA console.

Customizing LDAP User Authentication in NA

When NA is integrated with a directory service using LDAP, NA creates a corresponding user in the NA database the first time that user logs in to the NA console. NA then updates that user information in the NA database with subsequent changes.

By default, NA sets the user’s email address to the value of the `userprincipalname` field in the directory service. To configure NA to use the value of the `mail` field in the directory service as the user’s email address, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `appserver.rcx` file, locate the following line:

   ```
   <option name="ldap_server/attr_
   mapping/ActiveDirectory/email">userprincipalname,mail</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="ldap_server/attr_
   mapping/ActiveDirectory/email">mail,userprincipalname</option>
   ```

5. Save the `adjustable_options.rcx` file.
6. Reload the `.rcx` settings by doing one of the following:
   - From the NA proxy, run the `reload server options` command.
   - Restart the NA management engine.
7. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:
   - *On 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 Syslog Server`

    - `TrueControl TFTP Server`
    - `TrueControl SA Client`
  - *On Linux:* Run the following command:

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

To customize group search for Generic and Active Directory LDAP user authentication, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `appserver.rcx` file, locate the following lines based on the Generic and Active Directory LDAP setups:

   ```
   <option name="ldap_server/attr_mapping/Generic/group_
   search">group,organizationalunit,container,groupOfUniqueNames</option>
   ```

   ```
   <option name="ldap_server/attr_mapping/ActiveDirectory/group_
   search">group,organizationalunit,container</option>
   ```

3. Copy the lines from the `appserver.rcx` file to the `adjustable_options.rcx` file.
4. Update the customized group in the respective lines of `adjustable_options.rcx`.
5. Save the `adjustable_options.rcx` file.
6. Reload the `.rcx` settings by doing one of the following:
   - From the NA proxy, run the `reload server options` command.
   - Restart the NA management engine.

Enabling the Cross-Site Scripting (XSS) Filter

By default, the cross-site scripting (XSS) filter is enabled. This is the recommended configuration.

Verify the XSS filter configuration on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**). The **Cross site scripting check** check box should be selected.

Configuring the Cross-Site Scripting Check Box

As of NA 10.30, for a new installation, the **Cross site scripting check** check box is read-only. For an installation prior to NA10.30, it is recommended to configure the **Cross site scripting check** check box to be read-only.

Configure the **Cross site scripting check** check box behavior by adding one of the following line groups to the `site_options.rcx` file:

- The following lines enable the XSS filter and set the **Cross site scripting check** check box to be read-only:

  ```
  <!-- Security Setting -->

  <option name="security/check_xsite_script">true

  <title>Cross site scripting check</title>

  <section>Security</section>

  <type>CheckboxReadOnly</type>

  </option>
  ```

- The following lines disable the XSS filter and set the **Cross site scripting check** check box to be read-only:

  ```
  <!-- Security Setting -->

  <option name="security/check_xsite_script">false

  <title>Cross site scripting check</title>

  <section>Security</section>
  ```

```
<type>CheckboxReadOnly</type>

</option>
```

- The following lines enable the XSS filter and set the **Cross site scripting check** check box to be read-write (any user with access to the Administrative Settings - User Interface page can change the setting):

  ```
  <!-- Security Setting -->

  <option name="security/check_xsite_script">true

  <title>Cross site scripting check</title>

  <section>Security</section>

  <type>Checkbox</type>

  </option>
  ```

XSS Filter Exceptions

NA ships with a pre-defined set of XSS filter bypass rules.

If the `jboss_wrapper.log` file includes a `UI Request rejected for security reasons` message, you can create a new XSS filter bypass rule for the specific servlet mentioned in the message.

Add the rule to the `securityfilter_additional_init.rcx` file. Follow the formatting instructions in that file.

Enabling the *Filter HTML Output* Option

By default, the **Filter HTML Output** option is enabled. This is the recommended configuration.

Verify the **Filter HTML Output** option filter configuration on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**). The **Filter HTML Output** check box should be selected.

Configuring the Filter HTML Output Option Check Box

As of NA 10.30, for a new installation, the **Filter HTML Output option** check box is read-only.

Configure the **Filter HTML Output option** check box behavior by adding one of the following line groups to the `site_options.rcx` file:

- The following lines enable the **Filter HTML Output** option and set the **Filter HTML Output option** check box to be read-only:

  ```
  <!-- Security Setting -->

  <option name="security/sanitize_html">true

  <title>Filter HTML Output</title>

  <section>Security</section>

  <type>CheckboxReadOnly</type>

  </option>
  ```

- The following lines disable the **Filter HTML Output** option and set the **Filter HTML Output option** check box to be read-only:

  ```
  <!-- Security Setting -->

  <option name="security/sanitize_html">false

  <title>Filter HTML Output</title>

  <section>Security</section>

  <type>CheckboxReadOnly</type>

  </option>
  ```

- The following lines enable the **Filter HTML Output** option and set the **Filter HTML Output option** check box to be read-write (any user with access to the Administrative Settings - User Interface page can change the setting):

```
<!-- Security Setting -->

<option name="security/sanitize_html">true

<title>Filter HTML Output</title>

<section>Security</section>

<type>Checkbox</type>

</option>
```

Configuring NA to Permit Editing of Tasks Waiting for Approval

This topic applies only when NA is configured with workflow approval rules.

As of NA 10.30, tasks in the Requested state can be viewed but cannot be edited.

To permit editing of tasks waiting for approval

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="workflow/disable_task_edit">false</option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA management engine.

Configuring Dynamic Group Calculation

NA provides the following types of dynamic group recalculation:

- Periodic dynamic group recalculation for all devices

  By default, NA determines the membership of all dynamic groups for all devices in the NA inventory every 60 minutes. This frequency is configurable.

- Event-driven dynamic group recalculation for one device

  After a device change event, NA compares the impacted device to the dynamic group definitions and updates dynamic group membership as needed for that device only.

  NA supports the following time frames for event-driven focused dynamic group recalculation:

  - Immediate — Recalculation occurs immediately after the device change event.
  - Queued — NA collects the list of devices impacted by device change events in a queue. After a device has been in the queue for a designated waiting period, NA runs recalculation for that device. If other events for that device have arrived during the waiting period, NA processes all events for that device at the same time. By default, the frequency of checking the queue for updates is one minute and the length of the waiting period is ten minutes. Both values are configurable.

  It is recommended to enable immediate or queued event-driven dynamic group recalculation, but not both.

All types of dynamic group recalculation can be disabled.

> **Tip:** Enable and disable the dynamic group monitor (DynamicDeviceGroupMonitor) on the Administrative Settings - Server Monitoring page.

Configuration Options for Periodic Dynamic Group Calculation for All Devices

NA provides the following options for configuring periodic dynamic group recalculation for all devices:

- Frequency

  To set the frequency, on the Administrative Settings - Server page (**Admin > Administrative Settings > Server**), change the value of the **Dynamic Group Auto-Recalculation** field (under Dynamic Groups).

- Enabled or disabled

  To disable this calculation, in the `adjustable_options.rcx` file, add the following line:

  ```
  <option name="dynamic_group/disable">true</option>
  ```

For information about editing RCX files and forcing NA to re-read RCX files, see "Working with .rcx Files" on page 197.

Configuration Options for Event-Driven Dynamic Group Calculation for One Device

Triggering Events

To select the device change events that cause dynamic group calculation, on the Administrative Settings - Server page (**Admin > Administrative Settings > Server**), select the relevant events in the **Device Change Events** list (under Dynamic Groups).

> **Tip:** This list of events applies to both immediate and queued event-driven dynamic group calculation.

Immediate Calculation

In addition to the list of device events, NA provide the following option for configuring dynamic group recalculation for one device immediately after a device change event:

- Enabled or disabled

  To disable this calculation, in the `adjustable_options.rcx` file, add the following line:

  ```
  <option name="dynamic_group/disable_event_listener">true</option>
  ```

Queued Calculation

In addition to the list of device events, NA provide the following options for configuring dynamic group recalculation for one device queued to take place some time after a device change event:

- Frequency of checking the queue

  To set the frequency, in the `adjustable_options.rcx` file, add the following line:

  ```
  <option name="dynamic_group/queued_update_interval">M</option>
  ```

  Replace *M* with the frequency in minutes.

- The length of the waiting period

  To set the waiting period, in the `adjustable_options.rcx` file, add the following line:

  ```
  <option name="performance/device_group_commit_interval">M</option>
  ```

  Replace *M* with the length in minutes.

- Enabled or disabled

  To disable this calculation, in the `adjustable_options.rcx` file, add the following line:

  ```
  <option name="dynamic_group/disable_queued">true</option>
  ```

For information about editing RCX files and forcing NA to re-read RCX files, see "Working with .rcx Files" on page 197.

Configuring the Task Completion Email Content

For each task, you can set NA to send an email message upon task completion. A group task is one that works on multiple devices. The devices on which a group task runs can be identified individually, through device groups, or by a combination of both approaches. For a group task NA sends only one email message upon completion of the group task.

> **Note:** Enabled event rules might send email messages regarding child task completion. To prevent these additional email messages, disable these event rules.

The format of the email content (subject and body) is the same for all tasks types but depends on whether the task is for one device or is a group task.

Single Task Completion Email Message Format

For a non-device task or a task that works on only one device, the default email message recipient is the task originator. This default is configurable.

For a non-device task or a task that works on only one device, the default format of the email message subject is as follows:

```
Task $TaskName$ completed. Task status: $TaskStatus$
```

For a non-device task or a task that works on only one device, the default format of the email message body is as follows:

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

The default format produces an email message similar to the example shown in the following table.

Example of the Default Task Completion Email Message for a Single Task

Content Type	**Example**
Subject	Task Run Diagnostics completed. Task status: Succeeded
Body	Task : Run Diagnostics originated by : admin scheduled on : 2013-05-18 03:53:04.0 completed with the following status: Succeeded. The following devices have been processed: cisco_c3560 (10.78.60.36) Task comments : View the task information here: https://server.example.com:8443//task.view.htm?taskID=2801

Alternatively, the email message body can contain details of the task results. Enabling the task results option overrides the message body. The following table shows an example email message with task results.

Example Email Message with Task Results

Content Type	**Example**
Subject	Task Run Diagnostics completed. Task status: Succeeded
Body	Task Name: Run Diagnostics Task ID: 192511 Status: Succeeded Comments: Added by: admin (chris admin) Task Priority: 3 Create Date: 2013-05-18 04:29:19.0 Device: cisco_c3560 (10.78.60.36)

Example Email Message with Task Results, continued

Content Type	Example
	Schedule Date: As Soon As Possible Start Date: As Soon As Possible Complete Date: Sat May 18 04:29:19 MDT 2013 Duration: 1 Repeat type: Non-recurring View Task Details (may not be available if the records were pruned) Result Details: Diagnostic 'Hardware Information for Cisco IOS enable' completed. Policy check has failed. View Policy Events **Connect** - Succeeded Connected via telnet to 10.78.60.36 [in realm Default Realm] **Login / Authentication** - Succeeded Successfully used: Last successful password (Password rule Manager) View Hardware Information

To change the any of the format, contents, language, or default recipient of the email content for a single task, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` 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>`
   - `<option name="task/email/text">...</option>`
   - `<option name="task/email/includeResultDetails">false</option>`
4. Edit the subject and text values. The Variables for the Task Completion Email Content table lists the available variables for use in these options.

5. To enable the inclusion of detailed task results in the message, set the `task/email/includeResultDetails` option to `true`:

   ```
   <option name="task/email/includeResultDetails">true</option>
   ```

6. To change the default email message recipient, do the following:

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

      ```
      <option name="task/email/recipient"></option>
      ```

   b. Insert a comma-separated list of email address recipients.

      > **Tip:** To remove the default email message recipient, do not enter any email addresses. In this case, if the NA user who schedules the task neglects to enter an email address, the resulting message cannot be delivered.

7. Save the `adjustable_options.rcx` file.
8. Restart the NA services on all cores in the NA environment.

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.
$OriginatorEmail$	The email address of the task originator.
$OriginatorFirstName$	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.

Variables for the Task Completion Email Content, continued

Variable	Description
$TaskStatus$	The task status. For example; Succeeded, Failed, or Skipped.

Group Task Completion Email Message Format

For a task that works on multiple devices, the default email message recipient is the task originator. This default is configurable.

For a task that works on multiple devices, the default format of the email message subject is as follows:

```
$TaskName$ on group <device group name> completed with status $TaskStatus$
```

For example:

```
Take Snapshot on group Group1 completed with status Succeeded
```

For a task that works on multiple devices, the email message body contains a summary of the group task and a table of details for each child task associated with the group task. For more information, click the **View details of this task on NA** link.

For a task that works on multiple devices, the format of the email message body is not configurable.

An example group task completion email message follows:

```
Task Name: Take Snapshot
Task ID: 99701
Status: Succeeded
Comments:
Added by: Chris (Chris Admin)
Task Priority: 3
Create Date: 2013-01-22 20:02:56.0
Device Group: Group1
Schedule Date: As Soon As Possible
Start Date: As Soon As Possible
Complete Date: Tue Jan 22 20:03:16 MST 2013
Duration: 21
Repeat type: Non-recurring

View details of this task on NA (may not be available if the records were pruned)
```

```
Child tasks:
Succeeded      3
Failed         0
Skipped/Others 0
Total          3
```

```
Child task details:
Task  Task     Schedule   Host/Group     Task      Prior Partition Sched Comments
ID    Name     Date                      Status                    By

99711 Take     As Soon As "TFastIronEdge Succeeded 3     Default   Chris
      Snapshot Possible   X424 Premium"                  Site     (Chris
                          (16.78.58.55)                            Admin)

99721 Take     As Soon As lab-HPProc-540 Succeeded 3     Default   Chris
      Snapshot Possible   6zl                            Site      (Chris
                          (16.78.58.116)                           Admin)

99731 Take     As Soon As ProCurveHPSwit Succeeded 3     Default   Chris
      Snapshot Possible   ch*4204*vl                     Site      (Chris
                          (16.78.58.138)                           Admin)
```

To change the default email message recipient, the format of the email message subject, or both for a group task, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. To change the default email message recipient, do the following:

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

      ```
      <option name="task/email/recipient"></option>
      ```

   b. Insert a comma-separated list of email address recipients.

      > **Tip:** To remove the default email message recipient, do not enter any email addresses. In this case, if the NA user who schedules the task neglects to enter an email address, the resulting message cannot be delivered.

3. To change the format of the email message subject, do the following:

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

      ```
      <option name="grouptask/email/subject">$TaskName$ on group <device group
      name> completed with status $TaskStatus$</option>
      ```

   b. Edit the subject and text values. The *Variables for the Task Completion Email Content* table in "Single Task Completion Email Message Format" on page 95 lists the available variables for use in these options.

4. Save the `adjustable_options.rcx` file.
5. Restart the NA services on all cores in the NA environment.

Configuring the Default Setting of the Force Save Option 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 Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Backup Device Software
- Reboot Device
- Run Device Script
- Delete ACLs
- VLAN Task
- Port Scan
- Add Device Context

- Remove Device Context
- Provision Device
- Batch Insert ACL Line
- Batch Remove ACL Line

Possible values for *setting* are:

- true—The Force Save option 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 **If applicable, save the running configuration to the startup configuration upon task completion** check box.
- false—The Force Save option 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 **If applicable, save the running configuration to the startup configuration upon task completion** check box.
- disabled—The Force Save option 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 **If applicable, save the running configuration to the startup configuration upon task completion** 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>` 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 all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

> **Note:** The change takes effect for new tasks only.

Configuring the Update Device Software Task Status to Be Cumulative

By default, the status of the Update Device Software task reflects the status of that one task and does not consider the status of any child tasks that the Update Device Software task spawns. In this way, the Update Device Software task can have status Succeeded when one if its child tasks failed.

This topic describes how to change this behavior so that the Update Device Software task has status Warning if one of its child tasks fails.

To configure the Update Device Software task status to consider the status of its child tasks

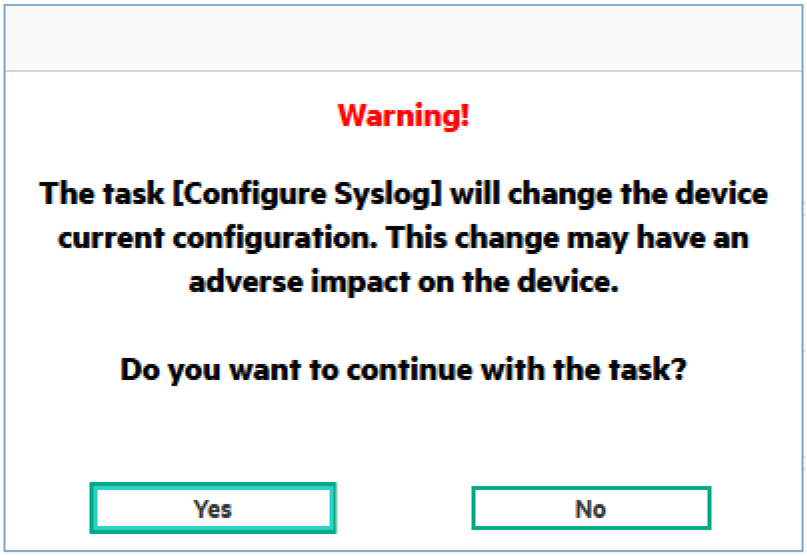
1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="deploy/child/warning">true</option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA management engine.

Configuring NA to Warn Before a Task Modifies a Device

Many of the tasks available in NA change the configuration of the target devices. Some tasks also reboot devices, temporarily making them unavailable and changing the device configuration when the startup and running configurations differ. For a list of the tasks that change devices, see the *User guide*.

By default NA completes these tasks as scheduled, without reminding the user that the tasks impact device configurations. As of 10.30, NA can warn that a task will change the target devices and give users a chance to cancel the task before it is scheduled. For example:



Warning!

The task [Configure Syslog] will change the device current configuration. This change may have an adverse impact on the device.

Do you want to continue with the task?

The warning appears for all the users, for all the tasks that change the target devices.

> **Note:** The following exceptions apply:
>
> - NA always warns before running the Reboot Device task regardless of the configuration described in this section.
> - NA always warns before running the Update Device Software task. The warning message is more detailed when the configuration described in this section is enabled.

Alternatively, use the Workflow feature to mandate that a second person reviews and approves the configured tasks before NA runs them. Workflow can be configured for some or all users, some or all task types, and some or all devices in the NA inventory.

To configure NA to display the warning message for tasks that change devices, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. Add the following line to the `adjustable_options.rcx` file:

   ```
   <option name="task/UI/WarnOnDeviceAlteringTask">true</option>
   ```

3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing one of the following:
   - In the NA console, on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**), click **Save**.
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA services.

Specifying the Base Directory for Import Tasks

You can specify the base directory to which the import file for the import tasks (import device and device group, import user and user group, and add resource identity and password) belongs, in the `adjustable_options.rcx` file. By default, the base directory for all the tasks are set as `<NA_HOME>/imports` in `appserver.rcx`.

The parameters that you can use to modify the base directory in the `adjustable_options.rcx` file are as follows:

- For the import device task:
  - `<option name="import/basedir/device"><NA_HOME>/imports</option>`
  - `<option name="import/basedir/devicegroup"><NA_HOME>/imports</option>`
- For the import user task:
  - `<option name="import/basedir/user"><NA_HOME>/imports</option>`
  - `<option name="import/basedir/usergroup"><NA_HOME>/imports</option>`
- For the add resource identities task:
  - `<option name="import/basedir/resourceidentity"><NA_HOME>/imports</option>`
  - `<option name="import/basedir/password"><NA_HOME>/imports</option>`

> **Note:** The `<option name="import/overwrite/logfile">false</option>` parameter in `adjustable_options.rcx` ensures that the log file, on which NA writes the information about the import task, cannot be overwritten by default. This means that if you want to append the information to an existing log file, you must set the parameter to `true`.

After modifying the `adjustable_options.rcx` file, restart the NA services.

Configuring the Diagnostic Policy Compliance Check Setting Default

To change default setting of the **Run compliance check when change detected** check box to unselected, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="Device/Diagnostics/RunComplianceCheckDefault">false</option>
   ```

3. Save the `adjustable_options.rcx` file.
4. Restart all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

> **Note:** The change takes effect for new tasks only.

Configuring the Size of the Output from the Command-Line Interface

By default, the commands in the NA command-line interface return no more than 10,000 items.

To configure the maximum command output

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="cli/max_rows_returned">10000</option>
   ```

   Replace `1000` with the maximum number of items to return.
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA management engine.

Configuring the NA Syslog Server

The following configuration settings are available for the Network Automation (NA) syslog server:

- The interface to listen for syslog messages. The default is to listen on all interfaces.
- The UDP port to listen for syslog messages. The default is 514.
- A hostname to forward syslog messages. Syslog forwarding is off by default.
- The UDP port to forward syslog messages to. The default is 514.

To change the default configuration for incoming syslog messages, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file as follows:
   a. Add the following lines:

      ```
      <option name="syslog/listener_address">192.168.1.12</option>
      <option name="syslog/listener_port">514</option>
      ```

   b. Change `192.168.1.12` to the IP address of the NA syslog server.

   c. Change `514` to the UDP port on the NA syslog server that should receive syslog messages.
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA services.

To enable syslog forwarding, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file as follows:
   a. Add the following lines:

   ```
   <array name="syslog/handlers">
     <value>com.hp.nas.syslog.NASSyslogHandler</value>
     <value>com.hp.nas.syslog.NASSyslogForwarder</value>
   </array>
   <option name="syslog/forward_host">10.1.2.3</option>
   <option name="syslog/forward_port">514</option>
   ```

   b. Change `10.1.2.3` to the IP address of the system to receive the forwarded syslog messages.

   c. Change `514` to the UDP port on the system to receive the forwarded syslog messages.

   > **Note:** If the `NASSyslogHandler` is removed from the array of syslog handlers, NA forwards syslog messages but does not initiate any device snapshots after receiving a syslog message.

4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA services.

To set up logging for syslog forwarding, follow these steps:

1. Open the Troubleshooting page (**Admin > Troubleshooting**) of the NA console.
2. In the **Enable logging for** field, select **external/syslog/forward**.
3. In the **at level** field, select **Trace (most messages)**.
4. Click **Submit**.

With this configuration, NA logs syslog status to the `syslog_wrapper.log` file.

Setting the Preferred Credentials for Accessing a Device

NA administrators can configure the types of device credentials that NA uses for each task type. By default, this configuration is the same for all the devices. Set this configuration in the **Task Credentials** section of the Administrative Settings - Device Access page (**Admin > Administrative Settings > Device Access**).

When a task type is configured for multiple device credential types, the user creating a task can select the device credential type to use for the task. The list of possible device credential types appears in the **Device Credentials Options** section of the task page.

NA administrators can determine which device credential type takes precedence for a task on a per-device basis. This approach uses a custom field named **Device Credentials** (by default) that can be set for each device. The possible values are as follows:

- **(unset)** - No preference. For each task, honor the user selection in the **Device Credentials Options** section of the task page. If this section is not available, use the device credential type enabled on the Administrative Settings - Device Access page.
- **User AAA** - Always use the task owner’s AAA credentials to access this device from any task type that enables user AAA credentials on the Administrative Settings - Device Access page.
- **Standard** - Always use the standard device-specific credentials or the first matching network-wide password rule to access this device from any task type that enables standard credentials on the Administrative Settings - Device Access page.

The precedence setting applies only when the task type permits the device credential type on the Administrative Settings - Device Access page. For example, consider the following:

- Device XYZ with User AAA as the preferred device credential type
- The Snapshot task type configured for both standard device credentials and user AAA credentials on the Administrative Settings - Device Access page
- The Change Plan type configured for standard device credentials on the Administrative Settings - Device Access page

In this case, NA behaves as follows:

- A Snapshot task against the device (XYZ) uses the task owner's AAA credentials to access the device. NA ignores the selection in the **Device Credentials Options** section of the task page.
- A Deploy Change Plan task against the device (XYZ) uses the standard device-specific credentials or the first matching network-wide password rule to access the device. This task does not use AAA credentials, because that option is not enabled on the Administrative Settings - Device Access page.

To enable the specification of preferred credentials for a device, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - **Windows:**`<NA_HOME>\jre`
   - **Linux:** `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="per_device/task_credentials/enabled">true</option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing one of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA management engine.
6. In the NA console , open the **Custom Data Setup** page (**Admin > Custom Data Setup**), and do the following:

   a. From the **Custom Data Setup** list, select **Devices**.

   b. Select the check box for an unused custom field, and then do the following:

      i. Set **API Name** to `devicecreds`.

      ii. Set **Display Name** to `Device Credentials`.

      iii. For the **Values** field do the following:

      - Clear the **Can Contain HTML** check box.
      - Select the **Limit to** check box, and then enter `User AAA,Standard`.

   c. Click **Save**.

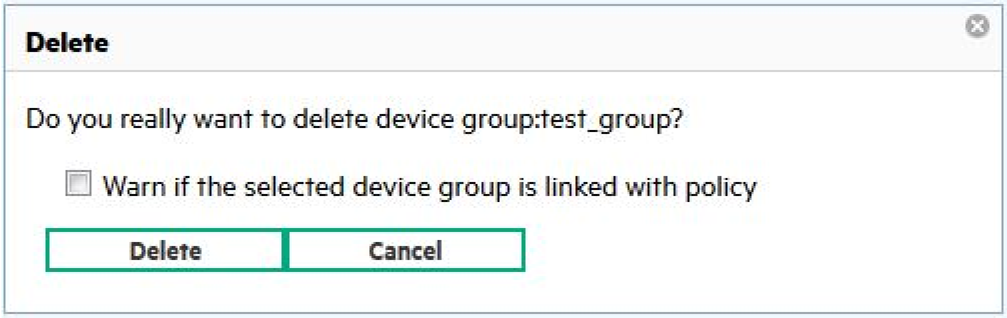
> **Tip:** The display name appears in the NA console. You can customize it for your environment.
>
> The API name and limiting values are embedded in the NA code. Use the exact strings listed here.

To set the preferred credentials for a device, follow these steps:

1. Navigate to the **Device Details** page.
2. From the **Edit** drop-down menu, select **Edit Device**. The **Edit Device** page appears.
3. In the **Additional Information** section, select a value for the **Device Credentials** field (or the customized display name that corresponds to the `devicecreds` API name).

Configuring NA to Warn Before Deleting a Device Group Linked With Policies

On the NA console, when the user tries to delete a device group, an option to warn the user appears so that if the device group is linked with a policy, it does not get deleted. Instead, a warning message is displayed.



Do you really want to delete device group:test_group?

□ Warn if the selected device group is linked with policy

To configure NA to display the warning message, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. Set the following line in the `adjustable_options.rcx` file to `false`:

   ```
   <option name="allow/delete_device_group/with_policy">false</option>
   ```

3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing one of the following:
   - In the NA console, on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**), click **Save**.
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA services.

Configuring NA to Not Override Host Names

In the Network Automation (NA) context, each network device has the following host names:

- Operating system host name—the name of a network device in the operating system running on the device
- DNS host name—the name associated with the IP address of a network device
- NA host name—the name of a network device in the NA database

It is recommended that the same value be used for all of these host names.

By default, NA stores the operating system host name as the NA host name for each managed device. When NA detects a configuration change on a device (for example, after driver discovery), NA sets the NA host name to be the same as the operating system host name.

If you want NA to store a host name that is different from the operating system host name of each device, configure NA to not update any NA host names when device operating system host names change. Follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file to add the following line:

   ```
   <option name="FastLookup/Hostname"></option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA

console, click **Save**.

- Restart the NA services.

To restore the default behavior of the NA host name always matching the operating system host name of each devices, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file to locate the following line:

   ```
   <option name="FastLookup/Hostname"></option>
   ```
4. Edit the located line to read as follows:

   ```
    <option name="FastLookup/Hostname">Device.HostName</option>
   ```
5. Save the `adjustable_options.rcx` file.
6. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
   - Restart the NA services.

Parsing Cisco ACS 5.x Logs for Change Detection

Network Automation (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.

> **Note:** 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>` 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. See "Start, Stop, or Restart All NA Services" on page 195.
4. In the NA console, go to Admin > Administrative Settings > Configuration Mgmt, and then add the pattern "CSCOacs" to the Syslog Detection Patterns list.

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>` 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>
     ```

   > **Tip:** 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.

Defining Dynamic Device Groups Using XML

The `add device group` and `mod device group` commands take an XML-formatted filter as an argument to define the search criteria for a dynamic device group. This chapter describes the format of the filter. The format must contain the following tags:

- Filter
- Condition
- Expression
- Label
- Name
- Operator
- Value

The following table explains each tag:

Tag	**Description**
Filter	The root element of the XML format. This tag includes at least one and up to 10 `<condition>` tags and only one `<expression>` tag.
Condition	A condition of the search criteria. `<condition>` is a child element of the `<filter>` tag. This tag includes the following elements: • Label: The identity of the `<condition>` tag. You can use values from **A** through **J** for this tag. The `<condition>` tag must have only one `<label>` tag, and the identifier must be unique across all the conditions. • Name:The name of the parameter. For example, `<name>Uptime</name>`. The `<condition>` tag must have only one `<name>` tag. • Operator: The operation that is applied to the name of the parameter in the `<name>` tag. For example, `<operator>is greater than</operator>`.

Tag	Description
	The <condition> tag must have only one <operator> tag. • Value: The value with which the specified parameter name is operated. Use commas to separate multiple values (for example, <value>switch,l3switch</value>). All the values within this tag must be XML-encoded. The <condition> tag must have only one <value> tag.
Expression	The logical operations to be performed on the conditions of the search criteria. <expression> is a child element of the <filter> tag.

An example of the XML format used to define the dynamic device groups is as follows:

```
<filter>
 <condition>
 <label>A</label>
 <name>Uptime</name>
 <operator>is greater than</operator>
 <value>10</value>
 </condition>
 <condition>
 <label>B</label>
 <name>Uptime stored date</name>
 <operator>since</operator>
 <value>2014:08:01:00:00</value>
 </condition>
 <condition>
 <label>C</label>
 <name>device type</name>
 <operator>equals</operator>
 <value>switch,l3switch</value>
 </condition>
 <expression> (A and B) OR C </expression>
 </filter>
```

Defining Change Conditions Using XML

The XML format to add or modify a condition for a change plan, must contain the following tags:

- Filter
- Condition
- Label
- Name
- Operator
- Value
- Result Operator
- Result Value
- Expression

The following table explains each tag:

Tag	Description
Filter	The root element of the XML format.
Condition	A condition of the change plan. `<condition>` is a child element of the `<filter>` tag. This tag includes the following elements: • Label: The identity of the `<condition>` tag. The `<condition>` tag must have only one `<label>` tag, and the identifier must be unique across all the conditions. • Name:The name of the parameter. For a Diagnostic condition, the value of the `<name>` tag is always "Diagnostic Script ID". For a Device Group condition, the value of the `<name>` tag is always "Device Group". For Device Attribute condition, the `<name>` tag should be the respective attribute name. For example, `<name>Device Model</name>`. • Operator: The operation that is applied to the name of the parameter in the

Tag	Description
	<name> tag. For example, <operator>contains</operator>. For a Diagnostic condition, the value of the <operator> tag is always equals. For a Device Groups condition, the value of the <operator> tag is one of the following: ○ Any of selected groups ○ All of selected groups ○ None of selected groups The <condition> tag must have only one <operator> tag. • Value: The value with which the specified parameter name is operated. Use commas to separate multiple values (for example, <value>ddd,a</value>). For a Diagnostic condition, the <value> tag should be the ID of the Diagnostic script. All the values within this tag must be XML-encoded. The <condition> tag must have only one <value> tag. • Result Operator: This field is applicable only for a Diagnostic condition. The available options are: ○ contains ○ does not contain ○ equals ○ does not equal ○ matches ○ is less than ○ is greater than ○ between ○ contains (regex) ○ does not contain (regex) • Result Value: This field is applicable only for a Diagnostic condition. You can use any of the applicable operators to compare the result of the diagnostic.
Expression	The logical operations to be performed on the conditions of the change plan. <expression> is a child element of the <filter> tag. The <expression> tag is mandatory.

For example, for *add change plan -name "Set Banner If Not Set" -desc "Set Banner if No banner in device" -family "Cisco IOS" -sitename "Default Site" -changeid 68 -conditions*, the XML format for the conditions option is as follows:

```
<filter>
 <condition>
 <label>A</label>
 <name>Device Model</name>
 <operator>contains</operator>
 <value>Cisco</value>
 </condition>
 <condition>
 <label>B</label>
 <name>Device Group</name>
 <operator>any of</operator>
 <value>ddd,a</value>
 </condition>
 <condition>
 <label>C</label>
 <name>Diagnostic Script ID</name>
 <operator>equals</operator>
 <value>16</value>
 <resultOperator>contains</resultOperator>
 <resultValue>Any String</resultValue>
 </condition>
 <expression> A and B and C </expression>
 </filter>
```

Configuring NA to Run as a Non-Root User

This chapter describes the one-time configuration required to run NA as a non-root user for the NA core and NA satellite on a Linux operating system. This configuration is independent of the NA database. These instructions work for all supported database types.

NA installations on a Linux operating system include several scripts that implement the functionality to run NA as a non-root user. The `<NA_HOME>/server/lib/scripts/nonroot` directory contains the following files:

- `truecontrol`—The script that starts the NA services. Overwrite the installed `truecontrol` script with this version, which includes the following changes to support running NA as a non-root user:
  - Changes the directory that stores the process identifier (PID) files for the NA services to a location inside the `<NA_HOME>` directory structure. The script creates this directory if necessary.
  - Verifies that this script is run by the user that owns the `<NA_HOME>` directory.
- `change-file-permissions.sh`—Run this script one time to make the following updates:
  - Change the owner and group of all files and directories in the NA installation directory (`<NA_HOME>`).
  - Change the owner and group of other files and directories on which NA depends, for example the Perl libraries for the API.
- `port-translation.sh`—Run this script one time to create the `/tmp/npt.rules` file that contains port translation rules in the Linux firewall for forwarding traffic from the root-owned ports to the non-root user-owned ports for the following services:
  - HTTP
  - HTTPS
  - TFTP
  - FTP
  - Syslog
  - SCP

  > **Note:** For SCP, the choice is between the following ports:

- Port 22 to use the Linux operating system SCP service, which is root owned
- Port 8022 to use the NA proxy SCP, which is owned by the NA user

Configuring an NA Core to Run as a Non-Root User

> **Note:** Currently, this procedure works for NA cores that use IPv4 addresses for incoming and outgoing communications but not IPv6 addresses. For more information, see "IPv6 Considerations" on page 146.

In a Horizontal Scalability or Multimaster Distributed System environment, perform this procedure on each NA core in sequence. That is, complete the entire procedure on one NA core before initiating the procedure on the next NA core.

To configure an NA core to be run by a specific non-root user, follow these steps:

1. As a root user, install NA, and then verify that the product functions correctly.
2. Back up the NA installation directory (`<NA_HOME>`), which is `/opt/NA` by default.
3. Back up the `/etc/init.d/truecontrol` file.
4. Create an operating system user and a group to own the NA installation. The provided script expects that the user name and group name are both `na`, but you can use any acceptable names such as `groupadd na` or `useradd na -g na`.
5. Determine the non-root ports for the services in the following table, and complete the “Custom port” column:

   > **Note:** The port numbers must be greater than 1024 to be owned by a non-root user.

   > **Tip:** It is recommended that the custom ports all start with the same leading digits. For example, select all ports in the 6000 or 12000 range.

Service	Standard port	Example port in this document	Custom port
NA HTTP	80	9080	
NA HTTPS	443	9443	

Service	Standard port	Example port in this document	Custom port
NA TFTP	69	9069	
NA FTP	21	9021	
NA syslog	514	9514	

6. Log on to the NA console as an NA administrator.
7. On the Administrative Settings – Server page (**Admin > Administrative Settings > Server**), set the TFTP Server Port, Syslog Server Port, and FTP Server Port fields to the custom ports in the previous table.
8. Stop all NA services by running the following command:

   ```
   /etc/init.d/truecontrol stop
   ```

9. In the `<NA_HOME>/server/ext/jboss/server/default/deploy/jbossweb.sar/server.xml` file, change the NA configuration for the HTTP and HTTPS ports by editing two of the `Connector` blocks.

   For example:

   For HTTP port 9080, modify the `Connector` block as follows:

   ```
   <Connector port="9080" address="${jboss.bind.address}" protocol="HTTP/1.1"
      maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"
      emptySessionPath="true"
      maxPostSize="262144000"
      enableLookups="false" redirectPort="9443" acceptCount="100"
      …
   ```

   For HTTP port 9443, modify the `Connector` block as follows:

   ```
   <Connector port="9443" address="${jboss.bind.address}" protocol="HTTP/1.1"
      minSpareThreads="5" maxSpareThreads="75"
      enableLookups="true" disableUploadTimeout="true"
      acceptCount="100"  maxThreads="200"
      scheme="https" secure="true" SSLEnabled="true"
    …
   ```

10. Make the scripts readable and executable by running the following command:

    ```
    chmod +rx <NA_HOME>/server/lib/scripts/nonroot/*
    ```

11. Copy the `<NA_HOME>/server/lib/scripts/nonroot/truecontrol` script file to overwrite the installed `/etc/init.d/truecontrol` file.
12. Verify that the `/etc/init.d/truecontrol` file is owned by root and is writeable only by root. For example, the output of the `ls -l /etc/init.d/truecontrol` command should be of the following format:

    ```
    -rwxr-xr-x 1 root root 10068 Apr 3 2014 /etc/init.d/truecontrol
    ```

13. Change to the `<NA_HOME>/server/lib/scripts/nonroot` directory.
14. If both the non-root user and group names are not `na`, edit the `change-file-permissions.sh` file to change the values of the `USER` and `GROUP` variables to the actual user name and group name for the non-root NA owner.
15. Update the ownership of the NA files and directories by running the following command:

    ```
    ./change-file-permissions.sh
    ```

    The output of this command might include the following types of messages:

    - `Ignoring` - This message indicates a file whose ownership did not change. No further action is needed.
    - `Does not exist` - This message indicates that the script could not find the named file. No further action is needed.

16. If the `iptables nat` table on the NA core server contains pre-existing port mappings, edit the `port-translation.sh` file to comment out the `flush` command.

    ```
    # echo "iptables -t nat --flush" >> "$OUT"
    ```

    Doing so preserves the pre-existing port mappings.

    > **Tip:** To check for pre-existing mappings, use the following command:
    >
    > ```
    > iptables -nt nat -vL
    > ```

17. Create port translation rules by running the following command:

    ```
    ./port-translation.sh
    ```

    Respond to the prompts with the custom port numbers for NA services. For information about possible values for the SCP port, see "SCP Considerations" on page 132.

18. Apply the port translation rules to the `iptables firewall` table by running the following command:

```
sh /tmp/npt.rules
```

19. Verify the `iptables` changes by running the following command:

    ```
    iptables -nt nat -vL
    ```

20. Start the NA services by running the following command:

    ```
    /etc/init.d/truecontrol start
    ```

21. Check the following processes to make sure that the NA core services are running:

    > **Note:** You must verify these processes as root or the NA owner.

    - Identify `ps -afe |grep DTCMgmtEngine`—the NA Management Engine
    - Verify that the TFTP server process is owned by the non-root user and is running:

      ```
      ps -afe | grep DTCTFTP
      ```

    - Verify that the syslog server process is owned by the non-root user and is running:

      ```
      ps -afe | grep TCSyslog
      ```

    - Verify that the FTP server process is owned by the non-root user and is running:

      ```
      ps -afe | grep DTCFTP
      ```

    - Verify that the SA Client process is owned by the non-root user and is running:

      ```
      ps -afe | grep Dsaclient
      ```

    - Verify that HTTP, HTTPS, TFTP, syslog, and the FTP service are listening on the new port numbers:

      ```
      netstat -an |egrep ’(udp)|(tcp.*LISTEN)’
      ```

    For examples of the expected output of these commands, see "Example Output for the NA Core Running Process Checks" on page 133.

22. Verify the HTTP and HTTPS connectivity. To achieve this follow these steps:

    a. On the NA core server, log on to the NA console as any user. Do not specify a port in the URL so the browser connects to either port 80 or 443.

    > **Note:** If the NA core server does not support a web browser, use a command such as wget to connect to the NA HTTP and HTTPS services.

b. On a different computer, log on to the NA console as any user. Do not specify a port in the URL so the browser connects to either port 80 or 443 and gets redirected to the new port number.

23. After all verification succeeds, persist the configuration of the port translation rules by running the following command:

   - *For Red Hat Enterprise Linux*:

     ```
     /sbin/service iptables save
     ```

   - *For SUSE Linux Enterprise Server*:

     ```
     /usr/sbin/iptables-save
     ```

   - *For Linux 7.x*:

     ```
     /usr/sbin/iptables-save
     ```

> **Note:** If you have configured NA Core to use a JRE different from Zulu JRE (***the default JRE installed with NA***), make sure that the configured non-root user has the permission to execute the new Java. For more information about configuring Java, see "Configuring Java in NA" on page 68.

To enable the *configured* non-root user to run the PostgreSQL services, follow these steps:

1. Stop the PostgreSQL services by running the following command:

   ```
   /etc/init.d/postgres stop
   ```

2. Change the ownership to the *configured* non-root user by running the following command:

   ```
   chown na:na /opt/postgres/ -R
   ```

3. Change `PGUSER` in the following file to the *configured* non-root user:

   ```
   /etc/init.d/postgres
   ```

4. Restart the PostgreSQL server.

SCP Considerations

The `port-translation.sh` script prompts for the non-root port numbers to use for various ports that the NA core uses. For this discussion, note the following:

- Inbound SCP traffic are the packets that devices sent to NA.
- SCP and SSH use the same port and process on the NA core server. Therefore, inbound SCP traffic is also inbound SSH traffic.

The value of the SCP port for inbound SCP file transfers depends on your environment. Take a note of the following points:

- To disable inbound SCP file transfers over the NA SCP server, do not configure SCP port translation for NA.
- To use the operating system SCP server for inbound file transfers, do not configure SCP port translation for NA.
- To use the NA SCP server for inbound file transfers on all interfaces, do the following:
    - Set the SSH proxy port to a high port number (for example, 8022).
    - Translate the high port number (for example, 8022) to port 22. This approach implies that the operating system SCP server is either down or listening on a non-standard port.
- To use the operating system SCP server on some IP interfaces (called “A”) and the NA SCP server on other IP interfaces (called “B”) with both SCP servers using port 22, do the following:
    - Configure the operating system SCP server to listen on the desired IP interfaces (“A”) only.
    - Set the SSH proxy port to a high port number (for example, 8022).
    - Translate the high port number (for example, 8022) to port 22 for the IP interfaces that should use the NA SCP server (“B”).

Example Output for the NA Core Running Process Checks

This section provides an example output of the commands used to verify that the NA core services are running.

NA Management Engine

The expected output of the `ps -afe | grep DTCMgmtEngine` command is of the following form:

```
na        1212  1206 43 15:45 ?        00:02:35 /opt/NA/jre/bin/java -
DTCMgmtEngine=1 -Duser.dir=/opt/NA/server/ext/jboss/bin -Djava.awt.headless=true
```

```
-Dfile.encoding=UTF8 -
Djavax.net.ssl.trustStore=/opt/NA/server/ext/jboss/server/default/conf/truecontr
ol.truststore -Djava.endorsed.dirs=/opt/NA/server/ext/jboss/lib/endorsed -
Dlogging.configuration=file:/opt/NA/server/ext/jboss/bin/logging.properties -
XX:HeapDumpPath=/opt/NA/server/log/nas.hprof -XX:MaxPermSize=512m -server -
Djavax.net.ssl.trustStorePassword=sentinel -d64 -Xms2048m -Xmx2048m -
Djava.library.path=/opt/NA/server/ext/wrapper/lib:/opt/NA/jre/lib -classpath
/opt/NA/server/ext/wrapper/lib/wrapper.jar:/opt/NA/server/ext/jboss/bin/run.jar:
/opt/NA/jre/lib/tools.jar:/opt/NA/server/ext/wrapper/lib/JavaPerl.jar:/opt/NA/se
rver/ext/jboss/lib/jboss-logmanager.jar -
Dwrapper.key=lVLVlV7HD3NActHTXOcDeOoHNIE7hiPR -Dwrapper.port=32000 -
Dwrapper.jvm.port.min=31000 -Dwrapper.jvm.port.max=31999 -Dwrapper.pid=1206 -
Dwrapper.version=3.3.1-st -Dwrapper.native_library=wrapper -
Dwrapper.service=TRUE -Dwrapper.disable_shutdown_hook=TRUE -
Dwrapper.cpu.timeout=0 -Dwrapper.jvmid=1
org.tanukisoftware.wrapper.WrapperSimpleApp org.jboss.Main -b 0.0.0.0
```

```
root      1885  1861  0 15:51 pts/0    00:00:00 grep DTCMgmtEngine
```

TFTP Server

The expected output of the `ps -afe | grep DTCTFTP` command is of the following form:

```
na        1190  1177  0 15:45 ?        00:00:02 /opt/NA/jre/bin/java -DTCTFTP=1
-Duser.dir=/opt/NA/server/ext/tftp -d64 -Xms16m -Xmx64m -
Djava.library.path=/opt/NA/server/ext/wrapper/lib:/opt/NA/server/lib -classpath
/opt/NA/server/ext/wrapper/lib/wrapper.jar:/opt/NA/server/ext/tftp/Tftp.jar:/opt
/NA/client/truecontrol-client.jar -Dwrapper.key=_ur4VbMojtgpOpbpSCkYuRsoVsxeiU0R
-Dwrapper.port=1795 -Dwrapper.jvm.port.min=31000 -Dwrapper.jvm.port.max=31999 -
Dwrapper.pid=1177 -Dwrapper.version=3.3.1-st -Dwrapper.native_library=wrapper -
Dwrapper.service=TRUE -Dwrapper.disable_shutdown_hook=TRUE -
Dwrapper.cpu.timeout=0 -Dwrapper.jvmid=1
org.tanukisoftware.wrapper.WrapperSimpleApp com.hpe.nas.tftp.TftpServer
/opt/NA/server/ext/tftp/tftpd.properties
```

```
root      1891  1861  0 15:51 pts/0    00:00:00 grep DTCTFTP
```

Syslog Server

The expected output of the `ps -afe | grep TCSyslog` command is of the following form:

```
na        1199  1192  0 15:45 ?        00:00:02 /opt/NA/jre/bin/java -
DTCSyslog=1 -d64 -Xms16m -Xmx64m -
Djava.library.path=/opt/NA/server/ext/wrapper/lib -classpath
/opt/NA/server/ext/wrapper/lib/wrapper-3.0.3.jar:/opt/NA/client/truecontrol-
client.jar:/opt/NA/server/ext/wrapper/lib/truecontrol-syslog.jar -Dwrapper.key=_
ur4VbMojtgpOpbpSCkYuRsoVsxeiU0R -Dwrapper.port=1777 -Dwrapper.jvm.port.min=31000
-Dwrapper.jvm.port.max=31999 -Dwrapper.pid=1192 -Dwrapper.version=3.3.1-st -
Dwrapper.native_library=wrapper -Dwrapper.service=TRUE -Dwrapper.cpu.timeout=10
-Dwrapper.jvmid=1 com.rendition.syslog.SyslogMain -config
/opt/NA/server/conf/syslog.conf
```

```
root      1895  1861  0 15:51 pts/0    00:00:00 grep TCSyslog
```

FTP Server

The expected output of the `ps -afe | grep DTCFTP` command is of the following form:

```
na        1214  1211  0 15:45 ?        00:00:02 /opt/NA/jre/bin/java -DTCFTP=1 -
d64 -Xms16m -Xmx64m -Djava.library.path=/opt/NA/server/ext/wrapper/lib -
classpath /opt/NA/server/ext/wrapper/lib/wrapper.jar:/opt/NA/client/truecontrol-
client.jar:/opt/NA/server/ext/ftp/lib/ftpserver-core-
1.0.4.jar:/opt/NA/server/ext/ftp/lib/ftplet-api-
1.0.4.jar:/opt/NA/server/ext/ftp/lib/slf4j-log4j12-
1.5.2.jar:/opt/NA/server/ext/ftp/lib/slf4j-api-
1.5.2.jar:/opt/NA/server/ext/ftp/lib/log4j-
1.2.14.jar:/opt/NA/server/ext/ftp/lib/mina-core-2.0.0-
RC1.jar:/opt/NA/server/ext/ftp/lib/truecontrol-ftp.jar -Dwrapper.key=ck2ehDv_
r8OK51aRmddfwQ6VmGHSY5Fm -Dwrapper.port=1797 -Dwrapper.jvm.port.min=31000 -
Dwrapper.jvm.port.max=31999 -Dwrapper.pid=1211 -Dwrapper.version=3.3.1-st -
Dwrapper.native_library=wrapper -Dwrapper.service=TRUE -Dwrapper.cpu.timeout=0 -
Dwrapper.jvmid=1 org.tanukisoftware.wrapper.WrapperSimpleApp
com.hpe.nas.ftp.NAFtpServer /opt/NA/server/conf/ftp.conf
```

```
root      1897  1861  0 15:52 pts/0    00:00:00 grep DTCFTP
```

Running NA Satellite as a Non-Root User

The NA satellite installation directories cannot be changed by the user. Therefore, this section gives the exact directory names for the NA satellite information.

HPE provides several scripts that implement the functionality to run NA satellites as a non-root user. The `satellite_scripts.zip` located under the *<NA_Home>*`/server/lib/scripts/nonroot` directory contains the following files:

- `Gateway-ChangeFileOwnershipForNonRoot.sh`—On each core gateway server and each remote gateway server, run this script one time to make the following updates:
  - Change the owner, group, and permissions of all files and directories in the NA gateway installation directory (`/etc/opt/opswire/opswgw-<gateway_name>`).
- `nassat`—The script that starts the NA satellite remote agent. Overwrite the installed nassat script with this version, which has some changes to support running an NA satellite remote agent as a non-root user:
  - Change the directory that stores the process identifier (PID) files for the NA remote agent services to a location inside the remote agent directory structure (`/opt/opsware/nassat`).
  - Verify that this script is run by the user that owns the `/opt/opsware/nassat` directory.
- `RemoteAgent-ChangeFileOwnershipForNonRoot.sh`—On each remote gateway server, run this script one time to make the following updates:
  - Change the owner and group of all files and directories in the NA remote agent installation directory (`/opt/opsware/nassat`).
  - Change the path to the PID files in the wrapper configuration files to the new location specified in the revised `nassat` script.
- `npt-RemoteAgent.sh`—On each remote gateway server, run this script one time to create the `/tmp/npt.rules` file that contains port translation rules in the Linux firewall for forwarding traffic from the root-owned ports to the non-root user-owned ports for the following services:
  - TFTP
  - Syslog

Configuring an NA Satellite Mesh to Run as a Non-Root User

> **Note:** Currently, this procedure works for NA satellites that use IPv4 addresses for incoming and outgoing communications that use IPv4 addresses but not IPv6 addresses. For more information, see "IPv6 Considerations" on page 146.

You must perform this procedure on each of the following elements of an NA satellite mesh:

- Core gateway on or near an NA core
- Remote gateway
- Remote agent running on a remote gateway server

These instructions are independent of the NA deployment architecture. Follow the same procedure for a standalone NA core as for NA in a Horizontal Scalability or Multimaster Distributed System environment.

When creating a new NA satellite mesh, install the NA satellite mesh as described in the *Satellite guide*. At a minimum, complete the installation process through deploying the remote agent to each remote gateway server.

- Run the NA satellite installation as the root user so the installer can access root-owned areas of the file system.
- Deploy the remote agent while the remote gateway is still running as the root user so the deployment process can access root-owned areas of the remote gateway file system.
- Configure each core gateway and each remote gateway to be run by a specific non-root user as described in "Configuring a Gateway to Run as a Non-Root User" on the next page.
- Configure each remote agent to be run by a specific non-root user as described in "Configuring a Remote Agent to Run as a Non-Root User" on page 141.

When adding a new NA satellite to an existing NA satellite mesh that has already been enabled to run as a non-root user, work only with the new NA satellite. Do not touch the non-root configuration in the existing NA satellite mesh.

- Run the NA satellite installation as the root user so the installer can access root-owned areas of the file system.
- Deploy the remote agent while the remote gateway is still running as the root user so the deployment process can access root-owned areas of the remote gateway file system.
- You can assign devices to be managed by the new NA satellite before or after enabling the new NA satellite to run as a non-root user.
- Configure each new gateway to be run by a specific non-root user as described in "Configuring a Gateway to Run as a Non-Root User" below.
- Configure each new remote agent to be run by a specific non-root user as described in "Configuring a Remote Agent to Run as a Non-Root User" on page 141.

Configuring a Gateway to Run as a Non-Root User

To configure an NA core gateway or NA remote gateway to be run by a specific non-root user, follow these steps:

1. Install the NA Gateway as a root user.
   - For a remote gateway, deploy the remote agent to the remote gateway server.
   - For information, see the *Satellite guide*.
2. Back up the NA gateway installation directory, which is `/etc/opt/opsware/opswgw-<`*`gateway_name`*`>`.
3. Create an operating system user in the root user group to own the NA gateway. The script expects that the user name is `gw`, but you can use any acceptable name. For example:

   ```
   useradd gw -g root
   ```
4. If you are configuring an NA remote gateway, stop all NA gateway services by running the following command:

   ```
   /etc/init.d/nassat stop
   ```
5. Configure the NA gateway boot file. Follow these steps:
   a. Back up all the files named `/etc/init.d/opswgw-*`.

      Each such file identifies one NA gateway. Generally, there is only one NA gateway per server.

> **Note:** In the case of multiple NA gateways on this server, repeat the edits described here for each `opswgw-<gateway_name>` file.

b. Stop each of the core gateway by running the following command:

```
/etc/init.d/opswgw-* stop
```

You can check the status by running the following command:

```
/etc/init.d/opswgw-* status
```

If the status of any process is shown as running, you must kill it.

c. In a text editor, open the `/etc/init.d/opswgw-<gateway_name>` file.

d. In the initialization section, add a line to identify the non-root owner of the NA gateway. In the following example, the text in bold font indicates the added line:

```
### BEGIN INIT INFO
# Provides:       opswgw-cgw
# Required-Start: $network $syslog
# Default-Start:  3 4 5
# Description:    The Opsware Gateway
### END INIT INFO

#
GW_USER=gw

prefix=/opt/opsware/opswgw
gateway=cgw
properties="/etc/opt/opsware/opswgw-$gateway/opswgw.properties"
```

Replace `gw` with the actual user name of the non-root owner of the NA gateway server.

e. In the appropriate section for the operating system of the NA gateway server, prepend the command for starting the NA gateway with the string `su "$GW_USER" -c` so that the NA gateway is started as the new owner of the NA gateway. In the following examples, the text in bold font indicates the change:

- Redhat:

```
if [ `uname` = "Linux" -a "$LINUX_DISTRIBUTION" = "redhat" ]; then

. /etc/init.d/functions
```

```
start () {
    echo -n $"Starting $prog: "
    su "$GW_USER" -c "$prefix/bin/opswgw --PropertiesFile
\"$properties\""
    RETVAL=$?
```

- SUSE Linux:

```
if [ `uname` = "Linux" -a "$LINUX_DISTRIBUTION" = "sles" ]; then

. /etc/rc.status
rc_reset

start () {
    echo -n $"Starting $prog: "
    su "$GW_USER" -c "$prefix/bin/opswgw --PropertiesFile
\"$properties\""
    rc_status -v
    RETVAL=$?
```

6. Extract the files from the `satellite_scripts.zip` file to the `/tmp` directory on the NA gateway server, such as the following:

   `/tmp/nonroot_scripts`

   For a remote gateway the `satellite_scripts.zip` file must be copied from the core gateway to the `/tmp` directory.

7. Make the scripts executable by running the following command:

   ```
   chmod +x /tmp/nonroot_scripts/*
   ```

8. Change to the `/tmp/nonroot_scripts` directory.

9. If the NA gateway owner is not `gw`, edit the `Gateway-ChangeFileOwnershipForNonRoot.sh` file (located under the `/tmp/nonroot_scripts/NonRoot_Support/Satellite` directory), to change the values of the `GW_USER` variable to the actual user name of the NA gateway owner.

10. As the `root` user, run the following command to update the ownership of the NA files and directories:

    ```
    ./Gateway-ChangeFileOwnershipForNonRoot.sh
    ```

11. As the root user, run the following command to start each NA gateway:

```
/etc/init.d/opswgw-<gateway_name> start
```

> **Note:** For Linux 7.x, before you execute the next command, follow these steps:
>
> a. Run the following command:
>
> ```
> systemctl daemon-reload
> ```
>
> b. Start the respective gateway by running the following command:
>
> ```
> /etc/init.d/opswgw-* start
> ```
>
> Make sure that all the processes started with the non-root user is listed.

12. As the `root` or the NA gateway owner, run the following command to verify that the NA gateway is running as the non-root owner:

    ```
    ps -afe |grep opswgw
    ```

    The expected output is of the following form:

    ```
    gw 1357 1 0 Jul23 ? 00:00:00 [opswgw-watchdog-50.0.37394.0: Default] --
    PropertiesFile /etc/opt/opsware/opswgw-Default/opswgw.properties --BinPath
    /opt/opsware/opswgw/bin/opswgw
    ```

    ```
    gw 1358  1357 0 Jul23 ? 00:03:55 [opswgw-gateway-50.0.37394.0: Default] --
    PropertiesFile /etc/opt/opsware/opswgw-Default/opswgw.properties --BinPath
    /opt/opsware/opswgw/bin/opswgw --Child true
    ```

If you are configuring an NA remote gateway, configure each remote agent to be run by a specific non-root user as described in "Configuring a Remote Agent to Run as a Non-Root User" below.

Configuring a Remote Agent to Run as a Non-Root User

To configure the remote agent for an NA satellite to be run by a specific non-root user, follow these steps:

1. Log on to the NA gateway server as a `root` user.
2. Stop the remote agent by running the following command:

   ```
   /etc/init.d/nassat stop
   ```

3. Take a backup of the remote agent installation directory, which is `/opt/opsware/nassat`.

4. Take a backup of the `/etc/init.d/nassat` file.
5. Create an operating system user and a group to own the NA remote agent. The scripts expect that the user name and group name are both na, but you can use any acceptable names. For example:

   ```
   groupadd na
   ```

   ```
   useradd na -g na
   ```

6. Determine the non-root ports for the services in the following table, and complete the "Custom port" column:

   > **Note:** The port numbers must be greater than 1024 to be owned by a non-root user.

   > **Tip:** It is recommended to use the same custom port values for the NA remote agent as for the NA core. It is also recommended that the custom ports all start with the same leading digits. For example, select all ports in the 6000 or 12000 range.

Service	Standard port	Example port in this document	Custom port
NA satellite TFTP	69	9069	
NA satellite syslog	514	9514	

7. Change the NA remote agent configuration for the TFTP and syslog ports. To achieve this, follow these steps:

   a. In a text editor, open the `/opt/opsware/nassat/jre/site_options.rcx` file.

   b. Near the end of the file, before the final `</options>` tag, add the following lines:

      > **Note:** For the TFTP and syslog ports, you can either use the example port numbers or custom port numbers. (See Step 6).

      ```
      <option name="TFTP/Port">9069
           <title>TFTP Server Port</title>
           <section>Servers</section>
           <size>5</size>
           <type>Text</type>
           <comment>TFTP server listening port, default is 69. Must restart TFTP
      server after making changes.</comment>
      </option>
      ```

```
<option name="syslog/listener_port">9514
     <title>Syslog Server Port</title>
     <section>Servers</section>
     <size>5</size>
     <type>Text</type>
     <comment>Syslog server listening port, default is 514. Must restart
Syslog server after making changes.</comment>
</option>
```

c. Save the file.

8. Copy the nassat file located under the /tmp/nonroot_scripts/NonRoot_Support/Satellite/nassat directory to overwrite the installed /etc/init.d/nassat file.

9. Verify that the /etc/init.d/nassat file is owned and is writeable only by the root user. For example, the format of the output of the ls -l /etc/init.d/nassat command should be as follows:

   ```
   -rwxr-xr-x 1 root root 10068 Apr 3 2014 /etc/init.d/nassat
   ```

10. Change to the /tmp/nonroot_scripts directory.

11. If the non-root user and group names are not both na, edit the RemoteAgent-ChangeFileOwnershipForNonRoot.sh file to change the values of the USER and GROUP variables to the actual user name and group name for the non-root NA owner.

12. Update the ownership of the NA files and directories by running the following command:

    ```
    ./RemoteAgent-ChangeFileOwnershipForNonRoot.sh
    ```

13. If the iptables nat table on the NA gateway server contains pre-existing port mappings, edit the npt-RemoteAgent.sh file to comment out the flush command.

    ```
    # echo "iptables -t nat --flush" >> "$OUT"
    ```

    Doing so preserves the pre-existing port mappings.

    > **Tip:** To check for pre-existing mappings, use the following command:
    >
    > ```
    > iptables -nt nat -vL
    > ```

14. Create port translation rules by running the following command:

    ```
    ./npt-RemoteAgent.sh
    ```

    Respond to the prompts with the custom port numbers for the NA services.

15. Apply the port translation rules to the `iptables firewall` table by running the following command:

    ```
    sh /tmp/npt.rules
    ```

16. Verify the `iptables` changes by running the following command:

    ```
    iptables -nt nat -vL
    ```

17. Start all NA services by running the following command:

    ```
    /etc/init.d/nassat start
    ```

18. Check the following processes to make sure that the NA remote agent services are running:

    > **Note:** You must verify these processes as root or the NA owner.

    - Verify that the TFTP server process is owned by the non-root user and is running:

      ```
      ps -afe | grep TCTFTP
      ```

    - Verify that the syslog server process is owned by the non-root user and is running:

      ```
      ps -afe |grep TCSyslog
      ```

    - Verify that the NA gateway remote agent is owned by the non-root user and is running:

      ```
      ps -afe |grep tomcat
      ```

    For examples of the expected output of these commands, see "Example Output for the NA Remote Agent Running Process Checks" on the next page.

19. Verify the TFTP and syslog connectivity by running the following command:

    ```
    netstat -an | grep udp
    ```

20. After all verification succeeds, persist the configuration of the port translation rules by running the following command:

    - *For Red Hat Enterprise Linux*:

      ```
      /sbin/service iptables save
      ```

    - *For SUSE Linux Enterprise Server*:

      ```
      /usr/sbin/iptables-save
      ```

    - *For Linux 7.x*:

      ```
      /usr/sbin/iptables-save
      ```

Example Output for the NA Remote Agent Running Process Checks

This section provides an example output of the commands used to verify that the NA remote agent services are running.

TFTP Server

The expected output of the `ps -afe | grep TCTFTP` command is of the following form:

```
na        1127  1113  0 13:24 ?        00:00:12 /opt/opsware/nassat/jre/bin/java
-DTCTFTP=1 -Duser.dir=/opt/opsware/nassat/server/ext/tftp -Xms16m -Xmx64m -
Djava.library.path=/opt/opsware/nassat/server/ext/wrapper/lib:/opt/opsware/nassa
t/server/lib -classpath
/opt/opsware/nassat/server/ext/wrapper/lib/wrapper.jar:/opt/opsware/nassat/serve
r/ext/tftp/Tftp.jar:/opt/opsware/nassat/client/truecontrol-client.jar -
Dwrapper.key=na_e6lEEv2l_hiwC -Dwrapper.port=1795 -Dwrapper.disable_shutdown_
hook=TRUE -Dwrapper.cpu.timeout=31557600 -Dwrapper.jvmid=1
com.silveregg.wrapper.WrapperSimpleApp gnu.inet.tftp.Tftpd
/opt/opsware/nassat/server/ext/tftp/tftpd.properties
```

```
root      1273  1253  0 15:46 pts/0    00:00:00 grep TCTFTP
```

Syslog Server

The expected output of the `ps -afe | grep TCSyslog` command is of the following form:

```
na        1172  1126  0 13:24 ?        00:00:11 /opt/opsware/nassat/jre/bin/java
-DTCSyslog=1 -Xms16m -Xmx64m -
Djava.library.path=/opt/opsware/nassat/server/ext/wrapper/lib -classpath
/opt/opsware/nassat/server/ext/wrapper/lib/wrapper.jar:/opt/opsware/nassat/clien
t/truecontrol-client.jar:/opt/opsware/nassat/server/ext/wrapper/lib/truecontrol-
syslog.jar -Dwrapper.key=3qGna8QvJwyaR4C2 -Dwrapper.port=1777 -
Dwrapper.cpu.timeout=31557600 -Dwrapper.jvmid=1 com.rendition.syslog.SyslogMain
-config /opt/opsware/nassat/server/conf/syslog.conf
```

```
root      1275  1253  0 15:46 pts/0    00:00:00 grep TCSyslog
```

NA Gateway Remote Agent

The expected output of the `ps -afe | grep tomcat` command is of the following form:

```
na        1142     1  0 13:24 ?        00:00:11 /opt/opsware/nassat/jre/bin/java
-tomcat=1 -
Djava.util.logging.config.file=/opt/opsware/nassat/server/ext/tomcat/conf/loggin
g.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Djava.endorsed.dirs=/opt/opsware/nassat/server/ext/tomcat/endorsed -classpath
/opt/opsware/nassat/server/ext/tomcat/bin/bootstrap.jar:/opt/opsware/nassat/serv
er/ext/tomcat/bin/tomcat-juli.jar -
Dcatalina.base=/opt/opsware/nassat/server/ext/tomcat -
Dcatalina.home=/opt/opsware/nassat/server/ext/tomcat -
Djava.io.tmpdir=/opt/opsware/nassat/server/ext/tomcat/temp
org.apache.catalina.startup.Bootstrap start
```

```
root      1277  1253  0 15:47 pts/0    00:00:00 grep tomcat
```

IPv6 Considerations

At this time, all the supported versions of Linux for NA include kernels in which the `ip6tables` functionality does not support the `nat` tables. Hence, it is not possible to configure port translation to map root-owned ports to non-root owned ports for servers that are reached through an IPv6 address. It is not supported to run NA as a non-root user when the NA core server is reached through an IPv6 address.

Known Issues

TFTPMonitor

When NA runs as a non-root user, the NA TFTPMonitor notices that the IP address of a TFTP reply is not the target IP address in the TFTP request. As a result, the TFTPMonitor reports failure of the TFTP service. If TFTP traffic flows correctly, you can ignore this error.

DiskMonitor

When NA runs as a non-root user, the NA DiskMonitor might return an error similar to the following:

```
Exception in DiskMonitor: java.io.IOException: Failure to parse df output.  Not
enough tokens found.
```

This text indicates that NA is unable to parse the error message returned by the DiskMonitor command (`df -k`). The actual output from the `df -k` command is similar to the following:

```
Filesystem         1K-blocks     Used Available Use% Mounted on
/dev/mapper/default-lv_root  36647628 27670252   7115744  80% /
tmpfs         4031196       80   4031116   1% /dev/shm
/dev/sda1      495844    91033    379211  20% /boot
df: `/root/.gvfs': Permission denied
```

To avoid this problem, ensure that the NA core server is not running on a desktop.

FTP Server

When NA runs as a non-root user, clicking `Stop` for the FTP Server on the `Start/Stop Services` page does not stop the NA FTP server. As a workaround, stop all the NA services from the command line by running the following command:

```
/etc/init.d/truecontrol stop
```

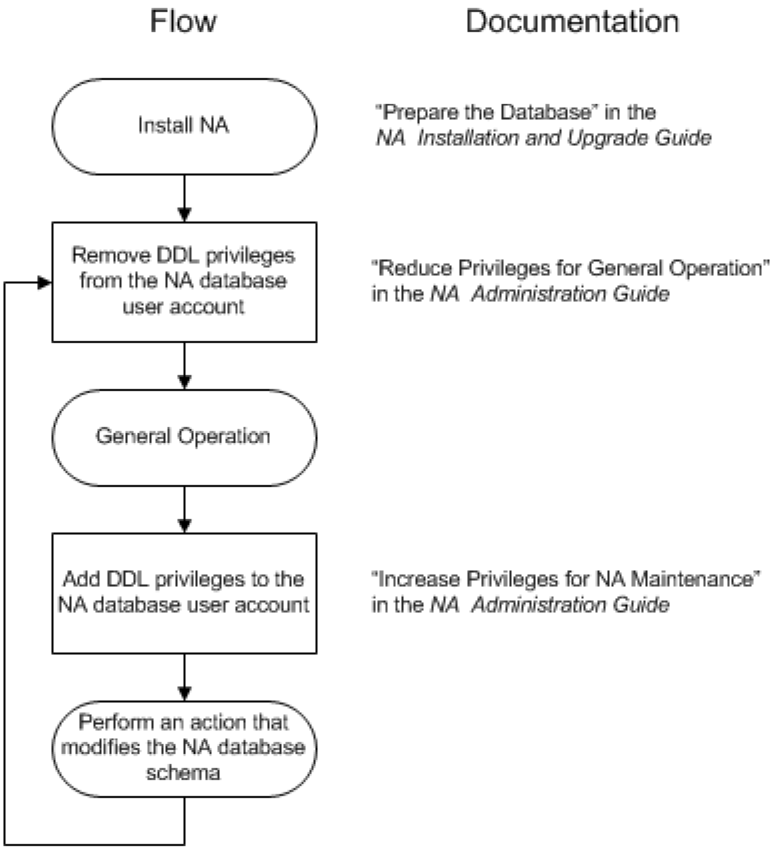
To start all the NA services, run the following command:

```
/etc/init.d/truecontrol start
```

Running NA with Minimal Database User Privileges

During installation of Network Automation (NA), the database user account that accesses the NA database must have data definition language (DDL) privileges for creating and manipulating tables in the NA schema. For general operation, this database user account requires only data manipulation language (DML) privileges. However, some database maintenance operations (including upgrading NA) require that the database user account have DDL privileges.

This chapter describes optional procedures for removing the DDL privileges from the NA database user account for general operation and for re-adding the DDL privileges when needed. The following diagram presents an overview of the privileges needed on the NA database user account at various points in time.


Flow
Documentation
Install NA
"Prepare the Database" in the *NA Installation and Upgrade Guide*
Remove DDL privileges from the NA database user account
"Reduce Privileges for General Operation" in the *NA Administration Guide*
General Operation
Add DDL privileges to the NA database user account
"Increase Privileges for NA Maintenance" in the *NA Administration Guide*
Perform an action that modifies the NA database schema

This chapter describes how to reduce database user account privileges after NA installation and how to increase those privileges for database maintenance operations. It contains the following topics:

- "Reduce Privileges for General Operation" below
- "Increase Privileges for NA Maintenance" on page 152

For information about the database user account privileges required for initial NA installation, see “Prepare the Database” in the *Install and Upgrade guide*.

Reduce Privileges for General Operation

For general NA operation, the database user account requires only DML privileges and not DDL privileges. After NA installation or maintenance, you can reduce the privileges granted to the NA database user account.

Reducing Privileges for Oracle

Complete this procedure any time you want to limit the NA database user account privileges.

1. With Oracle, revoke the following DDL privileges from the NA database user:
   - `CREATE SEQUENCE`
   - `CREATE SESSION`
   - `CREATE TABLE`
   - `CREATE PROCEDURE`
   - `SELECT ANY DICTIONARY`

   For example (for Oracle user name nauser):

   ```
   REVOKE CREATE SEQUENCE,CREATE SESSION, CREATE TABLE from nauser;
   REVOKE CREATE PROCEDURE, SELECT ANY DICTIONARY from nauser;
   ```
2. With Oracle, grant the following DML privileges to the NA database user:
   - `SELECT ANY TABLE`
   - `INSERT ANY TABLE`

- UPDATE ANY TABLE
- DELETE ANY TABLE

For example (for Oracle user name nauser):

```
GRANT SELECT ANY TABLE, INSERT ANY TABLE to nauser;
GRANT UPDATE ANY TABLE, DELETE ANY TABLE to nauser;
```

After following this procedure, the following DML privileges remain on the NA database user:

- CONNECT (a data control language privilege)
- SELECT ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE
- EXECUTE on CTXSYS.ctx_ddl

Reducing Privileges for SQL Server

The procedure for restricting database access depends on account history. For more information about specific use cases, see each procedure:

- "First Time Modification" below
- "Subsequent Modification" on page 152

First Time Modification

Complete this procedure the first time you want to limit the NA database user account privileges. This procedure removes the db_owner role from the NA database user account. This action removes all privileges from the account. The procedure then sets DML privileges on the account by initially re-adding all privileges and then removing DDL privileges.

To modify the SQL Server NA database user account to set privileges for general NA operation, follow these steps (for SQL Server user name nauser):

1. Stop all NA services. See "Start, Stop, or Restart All NA Services" on page 195.
2. Log on to SQL Server as a SQL Server administrator user with the sysadmin role (for example, SA).
3. Remove the db_owner role from the NA database user account.
   a. In Microsoft SQL Management Studio, right-click **nauser**, click Properties, and then click **User Mapping**.
   b. Under **Users mapped to this login**, select the NA schema.
   c. Under **Database role membership for <NA schema>**, clear the **db_owner** check box.
   d. Click **OK**.

   At this point, the NA database user account has no privileges and cannot access SQL Server.
4. Set permissions for the NA database user account.
   a. Give access to the NA database user account. For example:

      ```
      use NA; GRANT CONTROL to nauser; go
      ```

      This command returns all privileges associated with the db_owner role.
   b. Remove the schema modification privileges from the NA database user account. For example:

      ```
      use NA; DENY ALTER to nauser; go
      ```

      This command retains read and write privileges for the NA database user account.
   c. *Optional*. Verify the permissions required by the NA schema. For example:

      ```
      SELECT * FROM fn_my_permissions(NULL, 'DATABASE') order by permission_name;
      ```

      This command lists the 18 permissions provided to the NA schema.
   d. *Optional*. Verify the permissions granted to the NA database user account. For example:

      ```
      EXEC sp_helprotect NULL, 'nauser';
      ```
5. Start all NA services. See "Start, Stop, or Restart All NA Services" on page 195.

Subsequent Modification

Complete this procedure sometime after using the `REVOKE ALTER` command to re-add DDL privileges to the NA database user account.

To remove the DDL privileges from the NA database user account that does not have the `db_owner` role, follow these steps:

1. Log on to SQL Server as a SQL Server administrator user with the `sysadmin` role (for example, SA).
2. Remove the schema modification privileges from the NA database user account. For example:

   ```
   use NA; DENY ALTER to nauser; go
   ```

Increase Privileges for NA Maintenance

The following NA maintenance scenarios require DDL privileges:

- Upgrading NA by running a service pack installer (SPI)
- Applying an NA patch or hotfix that changes the NA database schema
- Enabling case-insensitive search or full-text search; this enablement modifies the NA database schema

The information in this section restores to the NA database user the privilege level used to create the NA database tables. After completing NA maintenance, you can follow the steps in "Reduce Privileges for General Operation" on page 149 to remove the DDL privileges.

Increasing Privileges for Oracle

Complete this procedure to re-add DDL privileges to the NA database user account after following the procedure in "Reducing Privileges for Oracle" on page 149.

With Oracle, grant the following DDL privileges to the NA database user:

- CREATE SEQUENCE
- CREATE SESSION
- CREATE TABLE
- CREATE PROCEDURE
- SELECT ANY DICTIONARY
- ALTER ANY INDEX
- CREATE ANY INDEX

For example (for Oracle user name nauser):

```
GRANT CREATE SEQUENCE, CREATE SESSION, CREATE TABLE to nauser;
GRANT CREATE PROCEDURE, SELECT ANY DICTIONARY to nauser;
```

After granting DDL privileges, the NA database user has the privileges listed in “Oracle Database Options” in the *Install and Upgrade guide* version 10.30 or later. Additionally, the NA user has the following DML privileges which are eclipsed by the DDL CREATE privileges:

- SELECT ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE

These privileges are a result of following the procedure in "Reducing Privileges for Oracle" on page 149.

Increasing Privileges for SQL Server

Complete this procedure to re-add DDL privileges to the NA database user account after following either of the procedures in "Reducing Privileges for SQL Server " on page 150.

To modify the SQL Server NA database user account to grant DDL privileges to the NA database user account, follow these steps (for SQL Server user name nauser):

1. Log on to SQL Server as a SQL Server administrator user with the sysadmin role (for example, SA).

2. Grant database modification privileges to the NA database user account. For example:

   ```
   use NA; REVOKE ALTER to nauser; go
   ```

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.

Before changing the credentials, follow the **Prepare the Database** section in the *Install 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`
   - *Linux*: `<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. From the `tc_tools` prompt, exit the utility.
5. Restart the NA management engine.

The credentials for accessing the NA database are stored in the `a.da` file. By default, NA encrypts the `a.da` file using TripleDES. To ensure stronger encrytion, you can change the algorithm for the file to AES256. To achieve this, follow these steps:

1. Stop all NA services on all NA cores. For information about stopping the NA services, see Start, Stop, or Restart All NA Services.

2. On each NA core, add the following line to the `adjustable_options.rcx` file:

   ```
   <option name="database/credentials/useAES256Encryption">true</option>
   ```

3. Back up the `<NA_HOME>/a.da` file to a location outside the NA directory structure.

4. Edit the a.da file as follows:

   a. Locate the line that starts with the `U=` string.

   b. Edit that line to delete all the characters after the equals sign (=).

   c. Locate the line that starts with the `S=` string.

   d. Edit that line to delete all the characters after the equals sign (=).

5. Verify that the resulting `a.da` file is similar to the following example:

   ```
   ##generated, do not edit this file

   #Wed Jul 25 14:15:15 MDT 2012

   U=

   S=
   ```

This process removes the NA database credentials from the `a.da` file. This results in NA unable to connect to the NA database. You must reconfigure NA to connect to the database location by using the tc_tools utility.

Full-Text Search of Configuration Text

Network Automation (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.

> **Note:** To move the contains (full text) and does not contain (full text) search operators to the top of the list, add the following line to the `adjustable_options.rcx` file:
> `<option name="fulltextsearch/operators_first">true</option>`

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 topic contains the following topics:

- "Enabling Full-Text Search of Configuration Text" below
- "Disabling Full-Text Search" on page 164

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.

> **Note:** 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:** 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" below
- "Enabling Full-Text Search on Microsoft SQL Server" on page 160
- "Enabling Full-Text Search on PostgreSQL Database" on page 161

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:
   1. Connect to the NA proxy with the credentials of the user created by the NA installer.
   2. Run the following command:

      ```
      fulltextsearch -option analyze
      ```

   3. 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*.

> **Tip:** Another information source is the Oracle MetaLink document collection (such as 579601.1: *Manual installation, deinstallation and verification of Oracle Text 11gR1*), for which you must have a MetaLink account with Oracle.

- 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 *Install 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*.
  - Consider the approximate time required for the index generation process. The analyze command calculates time based on the use of a single thread. You can reduce this time by using multiple threads while generating the index. To figure the adjusted approximate time, divide the suggested time by the number of threads that will be used in step 3.

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.

> **Tip:** 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. See "Start, Stop, or Restart All NA Services" on page 195.

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

> **Note:** 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 *Install and Upgrade guide*.

2. Generate the full-text index:

   a. Connect to the NA proxy with the credentials of the user created by the NA installer.

   b. Run the following command:

   ```
   fulltextsearch -option enable
   ```

> **Note:** 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.

3. 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.

> **Tip:** 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. See "Start, Stop, or Restart All NA Services" on page 195.

Enabling Full-Text Search on PostgreSQL Database

To enable full-text on a PostgreSQL database, follow these steps:

1. Verify that the PostgreSQL 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.

2. Generate the full-text index. To achieve this, follow these steps:

   a. Connect to the NA proxy with the credentials of the user created by the NA installer.

   b. Run the following command:

   ```
   fulltextsearch -option enable
   ```

3. Disable the full-text search. For more information, see "Disabling Full-Text Search" on page 164.

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 "Generate the full-text index. To achieve this, follow these steps:" above.
   - If the status is NOT PRESENT, do the following:
     - In the `adjustable_options.rcx` and `appserver.rcx` files, modify the `status` and `starttimeinms` parameters to the following:
       - `<option name="fulltextsearch/postgres/status">none</option>`
       - `<option name="fulltextsearch/postgres/starttimeinms">0</option>`

Adding a Reminder to Use Full-Text Search Where Applicable

NA supports adding a custom message to the Configuration Text field on the applicable search pages. The message describes when NA users should use the **contains (full text)** search operator. The message is the same for all Configuration Text fields and is visible only when full-text search is enabled.

To add a message to the Configuration Text fields, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows:* `<NA_HOME>\jre`
   - *Linux:* `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="fulltextsearch/warning_msg">HTML_formatted_text</option>
   ```

4. Replace `HTML_formatted_text` with text formatted in an HTML table cell and the span identifier `fulltextwarning`. For example:

   ```
   <option name="fulltextsearch/warning_msg">
    <![CDATA[
    <td> <span id="fulltextwarning"> It's highly recommended to use Full Text
   Search. For more information check
    <a class="help" href="#" onclick="var hw = window.open
   ('tcdocs/en/htmlHelp/naHelp/Content/NA_User_Guide/Performing_Searches/Using_
   the_Full_Text_
   Sear.htm','WWHFrame','scrollbars=yes,alwaysRaised=yes,resizable=yes,dependent=y
   es'); hw.focus(); return false;">Full Text Search</a>
    </span> </td> ]]>
    </option>
   ```

5. Save the `adjustable_options.rcx` file.
6. 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.
7. 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 Syslog Server`

    - `TrueControl TFTP Server`
    - `TrueControl SA Client`
  - *Linux:* 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. Connect to the NA proxy with the credentials of the user created by the NA installer.
   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`
      - *Linux*: `<NA_HOME>/jre`
   b. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` 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. See "Start, Stop, or Restart All NA Services" on page 195.

Enabling Regular Expression Search Functionality in Microsoft SQL

The regular expression (regex or regexp) search functionality is disabled by default for NA running with a Microsoft SQL (MS SQL) database.

To enable the functionality, you must first implement the Regular Expression clause (such as `dbo.RegExMatch`) using the SQL Server supported Common language runtime (CLR). For information about regular expression in SQL using CLR, see Microsoft Help.

The options to configure regex search in NA are as follows:

- Enable the regex search option - To enable the option, add the following in the `adjustable_options.rcx` file:

  ```
  <option name="regexp_search/mssql/enabled">true</option>
  ```

- Change the value of the regex search function - For an MS SQL database, the default value of the regex search function is set to `dbo.RegExMatch`. If the regex search function is implemented with a different function name in database, add the following option in the `adjustable_options.rcx` file, with the value set as the one available in database:

  ```
  <option name="regexp_search/mssql/function"></option>
  ```

- Change the order of argument in the regex search function - The default first argument in the regex search function is set to the `pattern` argument. To change the order of argument, add the following option in `adjustable_options.rcx`:

  ```
  <option name="regexp_search/mssql/pattern_is_first_argument">false</option>
  ```

After configuring the required options, make sure that you restart the NA services. For more information, see "Start, Stop, or Restart All NA Services" on page 195.

Enabling Case-Insensitive Search (Oracle and PostgreSQL)

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

This topic contains the following sections:

- "Affected Fields" below
- "Enabling Case-Insensitive Search of an Oracle or a PostgreSQL Database (Standalone and Horizontal Scalability)" on page 171
- "Disabling Case-Insensitive Search (Standalone and Horizontal Scalability)" on page 172
- "Enabling or Disabling Case-Insensitive Search in an Oracle Multimaster Distributed System Environment" on page 173

Affected Fields

When enabled, case-insensitive search is available for most text fields in the NA console, as described here. Additionally, the command-line interface is case-insensitive for device hostname.

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 or a PostgreSQL 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

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

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	• ACL Type • Module Slot • Module Description • Module Model • Module Serial • Module Firmware Version • Module Hardware Revision	• Comments • Configuration Text • ACL Configuration • ACL Application

Case Sensitivity of Report Search Fields , continued

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
	• Device Software Version • Device Firmware Version • Device Description • Password Rule • ACL ID • ACL Handle	• ROM Version • Service Type • Custom Service Type • VTP Domain Name • VTP Operating Mode	
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	• Scheduled By	• Comments

Case Sensitivity of Report Search Fields , continued

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
	• Host Name		• Result
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 or a PostgreSQL Database (Standalone and Horizontal Scalability)

For an Oracle or a PostgreSQL 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. Note that, in a Horizontal Scalability environment, you can enable case-insensitive search only of NA with an Oracle database.

> **Caution:** With an Oracle database, in a Multimaster Distributed System environment, follow the procedure described in "Enabling or Disabling Case-Insensitive Search in an Oracle Multimaster Distributed System Environment" on page 173.

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

1. Connect to the NA proxy with the credentials of the user created by the NA installer.
2. Run the following command:

   ```
   mod caseinsensitive -option enable
   ```

   With an Oracle database, you can alternatively run the following command:

   ```
   mod oraclecaseinsensitive -option enable
   ```

   > **Note:** An error message similar to the following example indicates that the NA database was locked when the command was run:
   >
   > ```
   > GEN_FAILURE: Failed to modify database
   > ```
   >
   > Wait several minutes for the database lock to clear, and then rerun the command.

   > **Tip:** Running this command triggers a recalculation of dynamic group membership.

3. *Oracle Only*. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database. See "Start, Stop, or Restart All NA Services" on page 195.

4. *Oracle Only*. If a previous implementation of case-insensitive search has been enabled in the NA environment, clean up the NA configuration by deleting the following deprecated configuration option:

   ```
   <option name="database/oracle_case_insensitive">true</option>
   ```

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

      - *Windows*: `<NA_HOME>\jre`
      - *Linux*: `<NA_HOME>/jre`

   b. Search for the string `oracle_case_insensitive` in all `.rcx` files.

   c. If you locate the string, back up the containing file to a location outside the `<NA_HOME>` directory, and then delete the containing line.

Disabling Case-Insensitive Search (Standalone and Horizontal Scalability)

In a Horizontal Scalability environment, disable case-insensitive searching on *one* NA server. Note that, in a Horizontal Scalability environment, you can disable case-insensitive search only of NA with an Oracle database.

> **Caution:** With an Oracle database, in a Multimaster Distributed System environment, follow the procedure described in "Enabling or Disabling Case-Insensitive Search in an Oracle Multimaster Distributed System Environment" on the next page.

To permanently disable case-insensitive search of NA with an Oracle or a PostgreSQL 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 of the user created by the NA installer.

   b. Run the following command:

      ```
      mod caseinsensitive -option disable
      ```

      With an Oracle database, you can alternatively run the following command:

      ```
      mod oraclecaseinsensitive -option disable
      ```

      > **Tip:** Running this command triggers a recalculation of dynamic group membership.

4. *Oracle Only*. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database. See "Start, Stop, or Restart All NA Services" on page 195.

Enabling or Disabling Case-Insensitive Search in an Oracle Multimaster Distributed System Environment

After enabling or disabling case-insensitive search, regenerate the database replication to ensure that the index information is synchronized.

To enable case-insensitive search in an Oracle Multimaster Distributed System environment

1. Prepare to stop NA.

   a. Notify users to log out.

   b. Log on to the NA console for one of the NA cores.

   c. Pause tasks scheduled to start during the next few hours. Include time for the currently running tasks to complete. For example:

      i. On the Search for Task page (**Reports > Search For > Tasks**), for the `Schedule Date` field, set since to `Now` and until to `2 hours later`.

      ii. On the Task Search Results page, pause each listed task.

   d. On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

      If any critical tasks are running, wait for them to complete before continuing with step 2, next.

2. On *each* NA core, generate case-insensitive indexes:

   a. Connect to the NA proxy with the credentials of the user created by the NA installer.

   b. Run the following command:

      ```
      mod oraclecaseinsensitive -option enable
      ```

      > **Note:** An error message similar to the following example indicates that the NA database was locked when the command was run:
      >
      > ```
      > GEN_FAILURE: Failed to modify database
      > ```
      >
      > Wait several minutes for the database lock to clear, and then rerun the command.

      > **Tip:** Running this command triggers a recalculation of dynamic group membership.

   c. If a previous implementation of case-insensitive search has been enabled in the NA environment, clean up the NA configuration by deleting the following deprecated configuration option:

      ```
      <option name="database/oracle_case_insensitive">true</option>
      ```

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

         - *Windows*: `<NA_HOME>\jre`
         - *Linux*: `<NA_HOME>/jre`

      ii. Search for the string `oracle_case_insensitive` in all `.rcx` files.

      iii. If you locate the string, back up the containing file to a location outside the `<NA_HOME>` directory, and then delete the containing line.

3. Stop all NA services on all NA cores. See "Start, Stop, or Restart All NA Services" on page 195.

4. Regenerate the database replication as described in "Regenerating Replication" in the *Multimaster Distributed System on Oracle*.

5. Start all NA services on all NA cores. See "Start, Stop, or Restart All NA Services" on page 195.

6. If necessary, resume the tasks that were paused in step 1.

a. Log on to the NA console for one of the NA cores.

b. On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **`Paused`**.

c. On the Task Search Results page, resume each listed task.

> **Tip:** Later instances of periodic tasks remove the paused instances of those tasks.

To disable case-insensitive search in an Oracle Multimaster Distributed System environment

1. Prepare to stop NA.

   a. Notify users to log out.

   b. Log on to the NA console for one of the NA cores.

   c. Pause tasks scheduled to start during the next few hours. Include time for the currently running tasks to complete. For example:

      i. On the Search for Task page (**Reports > Search For > Tasks**), for the `Schedule Date` field, set since to **`Now`** and until to **`2 hours later`**.

      ii. On the Task Search Results page, pause each listed task.

   d. On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

   If any critical tasks are running, wait for them to complete before continuing with step 2, next.

2. On *each* NA core, permanently disable case-insensitive search and remove the case-insensitive indexes from the database:

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

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

   c. Remove the case-insensitive indexes:

      i. Connect to the NA proxy with the credentials of the user created by the NA installer.

      ii. Run the following command:

```
mod oraclecaseinsensitive -option disable
```

> **Tip:** Running this command triggers a recalculation of dynamic group membership.

3. Stop all NA services on all NA cores. See "Start, Stop, or Restart All NA Services" on page 195.
4. Regenerate the database replication as described in "Regenerating Replication" in the *Multimaster Distributed System on Oracle*.
5. Start all NA services on all NA cores. See "Start, Stop, or Restart All NA Services" on page 195.
6. If necessary, resume the tasks that were paused in step 1.
   a. Log on to the NA console for one of the NA cores.
   b. On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **Paused**.
   c. On the Task Search Results page, resume each listed task.

> **Tip:** Later instances of periodic tasks remove the paused instances of those tasks.

Configuring SecureFiles Large Object (LOB) and Advanced LOB Compression for an Oracle Database

> **Caution:** Consult your Database Administrator to perform these Oracle database-related operations.

In an Oracle database, you can store large unstructured and semi-structured data as Large Objects (LOBs). Oracle SecureFiles is such an LOB storage mechanism. For Oracle 12c, SecureFiles is the default storage method. However, for Oracle 11g, you must enable Securefiles, and then migrate the data from BasicFiles to SecureFiles.

With Advanced LOB Compression, large data such as configurations, documents or XML files, stored in the columns of Large Objects type, experience a reduction of two to three times in size. Advanced LOB Compression automatically avoids compressing data that does not benefit from compression—for example, a document that is compressed through a third party tool and is inserted into the database as a SecureFiles file.

> **Note:** The Oracle database needs to be licensed with the Oracle Advanced Compression option to enable Advanced LOB Compression.

Applications can still perform random reads and writes on the compressed SecureFiles data as the compressed data is internally broken down into small chunks of data. This improves performance when compared to compressing the entire files before inserting them into the database.

There are three levels of Advanced LOB Compression. They are as follows:

- Low - Optimized for high performance
- **Medium - The default level and ideal for NA**
- High - Though achieves the highest storage savings, this level incurs the most CPU overhead

The various LOB columns in NA include `DATABLOCK` in the `RN_DEVICE_DATA` table, `EVENTDATA/EVENTTEXT` in the `RN_EVENT` table, `DATABLOCK` in the `RN_DIAGNOSTIC_DATA` table and so on.

To configure the SecureFiles LOB and Advanced LOB Compression, follow these steps:

1. Backup the entire database.
2. Enable the SecureFile LOB. (Enabled by default in Oracle 12c.)
3. Migrate data from BasicFile to SecureFile.
4. Enable the Advanced LOB Compression to **Medium** level.

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.

Network Automation (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.

> **Caution:** 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. The following table lists the NA database tables and the associated LOB columns that are most frequently affected by fragmentation.

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

NA Database Tables Frequently Affected by Fragmentation, continued

Table Name	Target LOB Columns
	• 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> ENABLE 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);
      ```

   > **Tip:** 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.

Migrate to a Different PostgreSQL Database

The NA installer provides you with an embedded PostgreSQL instance that can be used as the NA database. After installation, you can follow this procedure to migrate from this embedded database to a different, remote PostgreSQL database.

1. Log on to the NA core.
2. Stop NA services (see "Start, Stop, or Restart All NA Services" on page 195).
3. Take a backup of the embedded NA database by using the `pg_dump` tool.
4. Restore the backed-up database to the remote PostgreSQL database by using the `pg_restore` tool.
5. Run the `tc_tools` utility on the NA core server:
   a. At a command prompt, run the following command:
      - *Windows*: `<installdir>\client\tc_tools.bat`
      - *Linux*: `<installdir>/client/tc_tools.sh`

   b. Type **1** .

   c. At each prompt, do *one* of the following:
      - Type the new value for the prompt.

        > **Note:** Type new values for the following properties:
        >
        > - Database server name
        > - Database port

      - Press **Enter** to retain the value between the brackets ([ ]).

   d. From the `tc_tools` prompt, exit the utility.

   e. Restart the NA management engine.

Restoring Databases

Oracle

For information on restoring Oracle databases, contact 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** > **Add**.
7. Open the file browser under **File name** and select the filename you want to restore.
8. Click **OK** for the next three times it appears.
9. Click the **Options** tab.
10. Select **Force restore** over existing database.
11. 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.

PostgreSQL

The PostgreSQL database backup and restore can be performed with the following utilities:

- `pg_dump`
- `pg_restore`

For more information about backing up restoring PostgreSQL databases, contact your PostgreSQL database administrator.

Troubleshooting

This section discusses the potential administration problems and the possible workarounds to the problems.

1. ***Problem:*** If all the customer-created NA user groups do not have the view partition permission specified (view partition permission is set to **None**), NA adds all the users in one of those user groups to the **View All Partitions** user group. When at least one customer-created NA user group specifies a view partition permission, this behavior is no longer seen.

   Solution: Verify the permissions of a new NA user before giving log-on information to the new user. If the new user has the View All Partitions permissions in error, do the following:

   a. Edit the user group of the new user to select the correct partition in the **View Partition Permissions** section.

   b. Edit the **View All Partitions** user group to remove the user from the **Users in Group** list.

2. ***Problem:*** When installing on a Windows system, the NA installer hangs for a long time and does not respond to mouse/keyboard inputs. The window can neither be minimized nor be moved using the title bar.

   Solution: Do the following:

   a. Exit the installer. To exit, follow these steps:

      i. From the Task Manager, select the installer and then click End Task.

      ii. Do not accept the prompt to end the task. The installer prompts to check if you want to quit.

      iii. Click **Quit**. The installer exits.

   b. Uninstall NA and start the installation afresh.

   > **Note:** This issue is observed only on high latency and low bandwidth Remote Desktop sessions.

   To install or upgrade NA on Windows systems, it is recommended to use any alternative connection mechanism to the system other than Remote Desktop or the tools that use RDP (Remote Desktop Protocol). Some suggestions are as follows:

   - Connect to the console directly with the client of the virtualization software that you use.

     > **Note:** Do not use the `/console` or the `/admin` flag of `mstsc.exe`.

   - Use VNC (Virtual Network Computing) to connect to the server where NA is installed.
   - Access the console session of the server on which NA is installed. You can access the session by connecting a physical monitor to the server.

3. ***Problem:*** The SSH Applet does not load if the browser uses Java above version 1.7.51.

   Workaround: The security restrictions in Java prevents the loading of SSH applet. To load the SSH Java applet in the browser, add the URL of the NA server to the exception list in the Java Console.

4. ***Problem:*** An event notification and response rule cannot be created when the user selects the **Update Device Software** task as the action.

   Workaround: Do the following:

   a. On the **Event Notification & Response Rules** page (**Admin > Event Notification & Response Rules**), click the **New Event Notification & Response Rule** link.

   b. On the **New Event Notification & Response Rule** page, do the following:

      i. In the **to take this action** field, select **Run Task**

      ii. From the **when the following events occur** list, select an event.

      iii. In the **run this task** field, select **Deploy Change Plan** (instead of **Update Device Software**)

   c. On the **New Task/Template - Deploy Change Plan** page, enter the following:

```
#!/usr/bin/perl

use strict;

use warnings;

use Getopt::Long;

use Opsware::NAS::Connect;


my($host, $port, $user, $pass) = ('localhost','$tc_proxy_telnet_port$','$tc_user_username$','$tc_user_password$');

my @output;
my $con = Opsware::NAS::Connect->new(-user => $user, -pass => $pass, -host
=> $host, -port => $port);


$con->login();


print "deploy image -ip $tc_device_ip$ -imageset $imageSet$ -images
$imageName$ -osimage $imageName$ -filesystem flash:\n";

@output = $con->cmd("deploy image -ip $tc_device_ip$ -imageset $imageSet$ -
images $imageName$ -osimage $imageName$ -filesystem flash:");

print join("\n", @output);


@output = $con->disconnect();


$con->logout();

undef $con;

exit(0);
```

d. Click **Done**.

5. ***Problem:*** Running the Expect script displays the following error messages:

```
bad ELF interpreter: No such file or directory

cannot open shared object file: No such file or directory
```

Solution: When you use Expect script, do the following:

On Linux:

- Before executing the `<NA_HOME>/server/ext/expect/bin/expect` utility, install the `glibc.i686 library`, by running the following command:

  ```
  yum -y install glibc.i686
  ```

  This avoids the display of the following error message:

```
-bash: <NA_HOME>/server/ext/expect/bin/expect: /lib/ld-linux.so.2: bad ELF
interpreter: No such file or directory
```

- Before executing the `<NA_HOME>/server/ext/expect/bin/expect` utility, set the `export LD_LIBRARY_PATH`, by running the following command:

  ```
  export LD_LIBRARY_PATH=<NA_HOME>/server/ext/wrapper/lib
  ```

  This avoids the display of the following error message:

  ```
  <NA_HOME>/server/ext/expect/bin/expect: error while loading shared libraries:
  libexpect5.39.so.1: cannot open shared object file: No such file or directory
  ```

On Windows:

- Before executing the `<NA_HOME>\server\ext\expect\bin\expect` utility, export the following environment variable:

  ```
  set TCL_LIBRARY=<NA_HOME>\server\ext\expect\lib\tcl8.0
  ```

6. ***Problem:*** Enabling logging in a scale environment impacts the performance of the NA server.

   Workaround: In a scale environment, enable logging at the ERROR level. the performance of the NA server is imapacted when logging is enabled at the DEBUG or TRACE level.

7. ***Problem:*** When trying to connect to the NA Proxy using an older version of SSH client, the following error message is displayed:

   ```
   Could not agree a key exchange algorithm
   ```

   Solution: This error message appears when the SSH clients lack support for stronger hash message authentication code (HMAC) and Key Exchange algorithms. With FIPS enabled by default in NA 10.30, make sure that the SSH client used to connect the NA Proxy supports the following algorithms:

   - `HMAC-SHA256` for HMAC
   - `diffie-hellman-group-exchange-sha256` for Key Exchange

   Note that the NA Proxy accepts only these algorithms when FIPS is enabled.

8. ***Problem:*** In a Multimaster Distributed environment, NA does not correctly replicate the deletion of the last item in a list on the Administrative Settings pages to the other NA cores.

   Workaround: On each of the other NA cores, run the **Admin > Distributed > Renew Configuration Options** command.

9. ***Problem (Linux Only):*** In the NA console, the NA FTP service does not respond to the **Start**, **Stop**,

and **Restart** buttons on the **Start/Stop Services** page.

Solution: To enable the **Start**, **Stop**, and **Restart** buttons, update the FTP service configuration as follows:

a. Change to the following directory:

```
<NA_HOME>/server/ext/wrapper/conf
```

b. Back up the following file to a location outside `<NA_HOME>`:

```
ftp_wrapper.conf
```

c. In a text editor (such as vi), open the `ftp_wrapper.conf` file.

d. Search for the `pid` string to locate the following line:

```
wrapper.pidfile=/var/run/Ftp.pid
```

e. Change the case of the service name (`Ftp.pid`) in the located line as shown here:

```
wrapper.pidfile=/var/run/FTP.pid
```

f. Restart the NA services:

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

10. ***Problem:*** The `mod oraclecaseinsensitive -option enable` command returns the following error message and does not enable the case-insensitive search:

```
GEN_FAILURE: Failed to modify database
```

Workaround: Wait for a few minutes, and then rerun the `mod oraclecaseinsensitive -option enable` command.

11. ***Problem:*** NA does not work as expected in Internet Explorer (version 11 and above) 64-bit browser.

Reason: NA does not support Internet Explore with EPM (Enhanced Protected Mode) enabled.

12. ***Problem:*** Many tasks, including Detect Network Devices and Discover Driver, do not use the SNMPv3 correctly with the AES192 or AES256 encryption privacy protocol.

Workaround: Use a different encryption method, such as AES128.

13. ***Problem:*** While using the `mod authentication` command for a device, if there are no device-specific authentication records to modify, the system reports the following error:

```
GEN_FAILURE: The Device Password Information for Device you requested can not
be found. It may have been deleted.
```

Workaround: To create a new entry, use the `add authentication` command.

14. ***Problem:*** When NA is installed on a Linux platform, the following error is found in the log messages or in the results of failed NA tasks:

    ```
    Caused by: java.io.IOException: error=12, Cannot allocate memory
    ```

    This error occurs when the JVM (Java process) attempts to run an external shell script, such as a custom action or memory monitor. To run the external shell script, the system must fork its process--a mechanism that requires the parent process to copy itself for the child process. Making a copy of the parent process could send a request to the system kernel for more memory than the system can allocate.

    > **Note:** This can occur on either a 64-bit or 32-bit server.

    Workaround: As root, run the following command at the root shell prompt:

    ```
    echo 1> /proc/sys/vm/overcommit_memory
    ```

15. ***Problem:*** When NA is upgraded from a 32-bit NA platform to a 64-bit platform, the NA uninstaller does not work.

    Workaround: After upgrading from a 32-bit NA platform to a 64-bit NA platform, check the NA install directory. If there is a directory named `jre_old`, do the following before uninstalling NA:

    a. Stop the NA services (this includes TFTP, Syslog, and FTP).

    b. Rename `<NA_HOME>/jre`.

    c. Rename `<NA_HOME>/jre_old` to `<NA_HOME>/jre`.

    d. Run the NA uninstaller.

16. ***Problem:*** The `NAUserManager` class utilizes a configuration option to identify the username and password of the authorized FTP account. (There is only one FTP account at this time.) If the NA administrator changes the configuration value in NA, the FTP server is not aware of the change until it has been restarted as the FTP server does not reload configuration options before performing a user check.

    Workaround: The FTP server runs as a separate process outside of NA and is not notified when changes to the `.rcx` files are made. Restart the FTP server if the FTP account username or password is changed.

17. ***Problem:*** Evil string found on the input field of the NA console.

    Solution: To avoid evil strings on the input field, do one of the following:

    - Switch off the XSS (Cross-site Scripting) filter. To switch off the filter, on the NA console, clear the **Cross site scripting check** option ((Admin > Administrative Settings > User Interface > Security).
    - Create a bypass rule for the security filter. To create the rule, follow these steps:

        i. Add the servlet path and parameter to the `securityfilter_additional_init.rcx`. For more information, see the `securityfilter_additional_init.rcx` file.

        ii. Restart the NA management engine.

18. ***Problem:*** While configuring a device to use a Bastion Host server with SSH, the Discover Driver task fails with the following error message:

    ```
    This task did not complete.
    ```

    Additionally, the Session Log is not stored for the failed task.

    Workaround: Discover the driver without the Bastion Host or assign the driver manually.

19. ***Problem:*** The Oracle database users could encounter the following error in their log files, associated with a failed query:

    ```
    java.sql.SQLException: ORA-00600: internal error code, arguments: [kglhdgn_1],
    [0xA000000], [0], [2], [], [], [], []
    ```

    Workaround: Report this error to your DBA or Oracle Support Services as this is an Oracle internal error.

    This is the generic internal error number for Oracle program exceptions. It indicates that a process has encountered a low-level, unexpected condition. The error appears as follows:

    ```
    ORA-00600 internal error code, arguments: [string], [string], [string],
    [string], [string], [string], [string], [string]
    ```

    The first argument is the internal message number. Other arguments are various numbers, names, and character strings. The numbers may change meanings between different versions of Oracle.

    Causes of this message include the following:

    - Timeouts
    - File corruption

   - Failed data checks in memory
   - Hardware, memory, or I/O errors
   - Incorrectly restored files

20. ***Problem:*** When viewing device MAC Addresses details on the MAC Address Details page, the VLAN field is not populated.

    Workaround: To view the VLAN information for a port/interface, follow these steps:

    a. On the **MAC Address Details** page, click the **Port Name** link for the required port. The Interface Details page opens.

    b. Scroll down to the Member VLANs field and view the VLAN information.

21. ***Problem:*** After running the diagnostic against a device, while creating a diagnostic with single quotes in its name, such as “Ana's Diagnostic”, the diagnostic results are not getting displayed.

    Workaround: Do not use single quotes in diagnostic names.

22. ***Problem:*** When naming a diagnostic, the user is allowed to enter up to 100 characters. However, when running the diagnostics, the name is limited to 50 characters.

    Workaround: Limit diagnostic names to 50 or less characters.

23. ***Problem:*** Devices in remote Realms cannot use the Secure Copy (SCP) Transfer Protocol as the remote Gateway Satellite Agent cannot use SSH/SCP port 22. The port is already in use by the Gateway OS, thus preventing the remote Gateway Satellite Agent from using it.

    Workaround: Disable SCP for devices in remote Realms.

24. ***Problem:*** Using SNMP device discovery over networks with latency can cause SNMP timeouts.

    Solution: To set the SNMP timeout to a higher value, follow these steps:

    a. Log on to NA.

    b. On the menu bar under **Admin**, select **Administrative Settings**, and then click **Device Access**. The **Administrative Settings - Device Access** page opens.

    c. Scroll down to the Detect Network Devices and Port Scan Task Settings section and set SNMP Timeout to a higher value, such as 2500 (milliseconds).

25. ***Problem:*** While specifying an advanced ACL script, selecting the “Update Script” button can lock-in values. As a result, running (or re-running) the script can result in variables not being updated properly.

Workaround: Avoid using the “Update Script” button with advanced ACL scripts.

26. ***Problem:*** Redundant NA Core Gateways cannot be configured in the same NA Realm as a single NA Core.

    Workaround: Edit the `adjustable_options.rcx` file to add the IP address(es)of other NA Core Gateways. In the `.rcx` file add the following:

    ```
    <array name="rpc/allowed_ips">

    <value>10.255.54.10</value>

    </array>
    ```

27. ***Problem:*** When using external authentication in a Multimaster Distributed System environment, the External Authentication Type, such as TACACS+ or Active Directory, is global (shared between all NA Cores). Specific authentication server information is NA Core specific.

    Workaround: On the **Administrative Settings > User Authentication** page, set the **External Authentication Type** to "None". Configure each NA Core individually with the authentication server information or Active Directory setup. After all NA Cores have been configured, set the External Authentication Type on any NA Core. The External Authentication Type setting is replicated to all NA Cores.

28. ***Problem:*** Even after configuring NA to contact SMTP server, NA messages do not get delivered and the following error is displayed:

    ```
    Error occurred when sending email. Please check the email address and/or your
    SMTP server settings.
    ```

    Workaround: This error occurs when the SMTP server is configured to reject messages from the NA server address for security reasons. Configure the SMTP server to enable the NA server to relay email messages through it.

29. ***Problem:*** CLI discovery fails.

    Solution: This occurs when the PollRead variable is set for all NA tasks, instead of it being set for only the discovery task. By default NA does a blocking read on the SSH connections for discovery tasks. You must configure an option that sets NA to do polling-based reads on discovery task-related SSH connections. To achieve this, follow these steps:

    a. Consult with your Support representative to evaluate the impact of this change in your environment.

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

```
<option name="Driver/Discovery/UsePollRead">true</option>
```

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

   - On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
   - From the NA proxy, run the `reload server options` command.
   - Restart the NA management engine.

> **Note:** The `Access/SSH/ReadSleepTime` option is related to the `Driver/Discovery/UsePollRead` option as it determines the frequency of the polling. The value of `Access/SSH/ReadSleepTime` is specified in milliseconds and defaults to 1000 ms (1 second).

30. ***Problem:*** Device configuration comparison does not work for large configurations.

    Solution: Enable the new difference tool library, by following these steps:

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

    ```
    <option name="data/NewDiffTool">true</option>
    ```

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

       - On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
       - From the NA proxy, run the `reload server options` command.
       - Restart the NA management engine.

31. ***Problem:*** The interface search results export includes HTML in the CSV output file.

    Solution: To remove the `<span>` HTML tags from the CSV output file of the interface search results export, follow these steps:

    a. In the `adjustable_options.rcx` file, locate the following line:

    ```
    <option name="driver/perl_wait_timeout">0</option>
    ```

    b. Add the following as the next line to the located line:

    ```
    <option name="csv/remove/html">true</option>
    ```

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

- On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
- From the NA proxy, run the `reload server options` command.
- Restart the NA management engine.

32. ***Problem:*** The **Resolve FQDN** task does not update the FQDN field that is already populated.

    Solution: To enable the **Resolve FQDN** task override the FQDN field for each device, follow these steps:

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

    ```
    <option name="dnslookup/always_override_existing_fqdn">true</option>
    ```

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

    - On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
    - From the NA proxy, run the `reload server options` command.
    - Restart the NA management engine.

33. ***Problem:*** A way to assign non-administrative users the ability to manage partitions.

    Solution: To assign non-administrative users the ability to manage partitions, follow these steps:

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

    ```
    <option name="Administration/SecurityGroupsMgmt/Configurable">true</option>
    ```

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

    - On the User Interface page (**Admin** > **Administrative Settings** > **User Interface**) of the NA console, click **Save**.
    - From the NA proxy, run the `reload server options` command.
    - Restart the NA management engine.

34. ***Problem:*** For some devices, NA reports an older configuration as the current device configuration.

    Solution: To prevent this, run the following command from the NA proxy:

    ```
    run checkdb -resolver currentconfig -verbose
    ```

    This command enables NA to reevaluate the current configuration of all managed devices. The runtime of this command is proportional to the number of devices being managed.

Common Procedures

This section describes procedures that are common to many Network Automation (NA) configuration and maintenance tasks. It includes the following topics:

- "Start, Stop, or Restart All NA Services" below
- "Disable All NA Services" on the next page
- "Working with .rcx Files" on page 197

Start, Stop, or Restart All NA Services

Stopping the NA services before changing the NA configuration prevents conflicting data from being stored in the NA database. Some procedures call for restarting the NA services to read the updated configuration.

To start all NA services

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl SA Client**
  - **TrueControl FTP Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *Linux*: Run the following command:

  ```
  /etc/init.d/truecontrol start
  ```

To stop all NA services

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

- ○ **TrueControl ManagementEngine**
- ○ **TrueControl SA Client**
- ○ **TrueControl FTP Server**
- ○ **TrueControl Syslog Server**
- ○ **TrueControl TFTP Server**

- *Linux*: Run the following command:

```
/etc/init.d/truecontrol stop
```

To 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 SA Client**
  - ○ **TrueControl FTP Server**
  - ○ **TrueControl Syslog Server**
  - ○ **TrueControl TFTP Server**
- *Linux*: Run the following command:

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

Disable All NA Services

Some procedures call for disabling automatic startup of the NA services on system boot.

To disable all NA services

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, click **Properties**, and then set Startup Type to **Disabled**:
  - ○ **TrueControl ManagementEngine**
  - ○ **TrueControl SA Client**
  - ○ **TrueControl FTP Server**

- **TrueControl Syslog Server**
- **TrueControl TFTP Server**

- *Linux*:

  ```
  mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
  ```

Working with .rcx Files

The Network Automation (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.

> **Note:** 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.

> **Tip:** 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`
- *Linux*: `<NA_HOME>/jre`

> **Caution:** 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.

> **Tip:** 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>` 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.

   > **Tip:** Some changes do not take effect until the NA services have been restarted.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Administration guide (Network Automation 10.30)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback.