Hewlett Packard
Enterprise

HPE Network Automation Software

Software Version: 10.00
for the Windows® and Linux® operating systems

Security Configuration Guide

Document Release Date: March 2017
Software Release Date: December 2015

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. HPE 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 HPE 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

© Copyright 2015 - 2017 Hewlett Packard Enterprise Development LP

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

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

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

Documentation Updates

The title page of this document contains the following identifying information:

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

Contents

Using this Guide

This document provides information for increasing the security of your NA installation. Before using the information in this document, make sure to install NA 10.00.02 or a higher patch. For security configuration for another version of the product, see the appropriate documentation for that version.

Unless otherwise specified within a procedure, the expected use model for the content in this document is as follows:

1. Stop all NA services (see "Start, Stop, or Restart All NA Services" on page 28).
2. Apply the desired configurations as described in this document.

   > **Note:** Remember to back up each configuration file to a location outside the NA directory structure before making any changes.

3. Start all NA services (see "Start, Stop, or Restart All NA Services" on page 28).
4. In an NA satellite environment, restart all NA remote agents:

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

User Authentication

Users can authenticate into the NA console by using a local user account or by using one of several external authentication components. Each approach requires administrative setup.

Local user accounts

Local user accounts are specific to the NA installation only. An NA administrator can set the following general behaviors that apply to all local user accounts:

- Minimum password length
- Password complexity
- Password expiration
- Password reuse
- System lock out after a configured number of consecutive failed log-in attempts

Note: If this level of user authentication configuration is not sufficient for the security standards of your environment, it is recommended to use an external mechanism for user authentication. See "External authentication" below.

Additionally, during user account creation, an NA administrator can set password options for that user account.

For information about configuring the security behaviors of local NA user accounts, see "User Authentication Page Fields," "Password Expiration," and "Password Reuse" in the *NA User Guide*.

For information about creating local NA user accounts, see "Managing Users" in the *NA User Guide*.

Note: It is recommended to require long passwords (at least 8 characters) with the following characteristics:

- At least one upper case letter and one lower case letter
- At least one digit
- At least one special character

Additionally, it is recommended to enable system lock out after a configured number of consecutive failed log-in attempts.

External authentication

The administrator of the external authentication component determines the security behaviors for all users and all applications that use that component.

- For information about the authentication components and versions that NA supports, see "Additional Compatibility Information" in the *NA Support Matrix*.
- For information about external authentication components and how to enable their use in NA, see "User Authentication" in the *NA User Guide*.

For most external authentication methods (but not Public Key Infrastructure (PKI)), you can enable authentication failover to use the local NA user account when the external authentication server is unavailable. This approach requires that you create a local NA user account for each user who normally authenticates through an external authentication server. Authentication failover is disabled by default.

NA console session timeout

By default, the NA console session timeout is 30 minutes (1800 seconds). An NA administrator can change this value for all NA console users in the **Session Timeout** field on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**).

> **Note:** It is recommended to configure the session timeout in accordance with the policy for your environment.

Clickjacking Protection

The default NA configuration supports running NA in a portal. For this reason, the default NA is unable to protect against clickjacking. If you do not integrate NA with a portal, enable clickjacking protection by adding the following lines to the `adjustable_options.rcx` file:

```
<option name="security/check_clickjacking/enable">true</option>
<option name="security/check_clickjacking/x_frame_options">DENY</option>
```

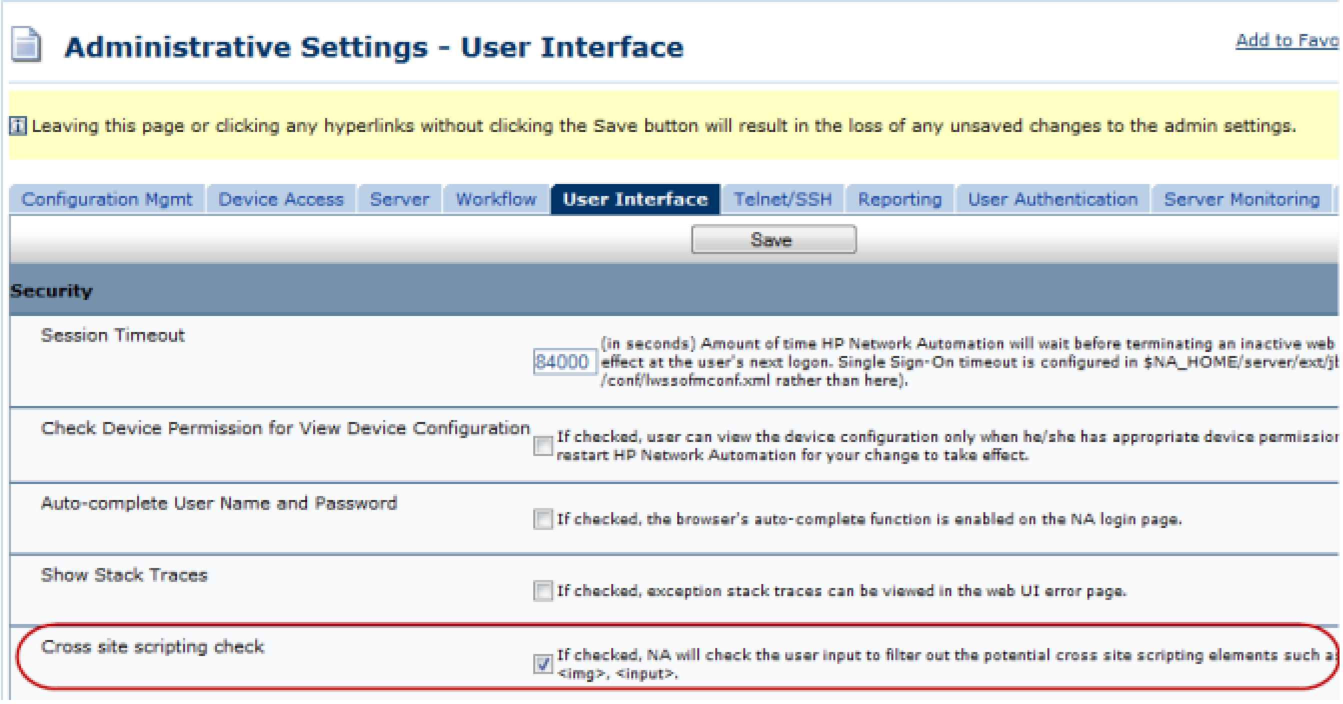
Tip: The value `DENY` is case-insensitive.

Note: It is recommended to enable clickjacking protection as described here.

Enable the Cross-Site Scripting (XSS) Filter

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

Verify the NA 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.



Leaving this page or clicking any hyperlinks without clicking the Save button will result in the loss of any unsaved changes to the admin settings.

Security

Session Timeout	84000	(in seconds) Amount of time HP Network Automation will wait before terminating an inactive web effect at the user's next logon. Single Sign-On timeout is configured in $NA_HOME/server/ext/j /conf/lwssofmconf.xml rather than here).
Check Device Permission for View Device Configuration	□	If checked, user can view the device configuration only when he/she has appropriate device permissio restart HP Network Automation for your change to take effect.
Auto-complete User Name and Password	□	If checked, the browser's auto-complete function is enabled on the NA login page.
Show Stack Traces	□	If checked, exception stack traces can be viewed in the web UI error page.
Cross site scripting check	☑	If checked, NA will check the user input to filter out the potential cross site scripting elements such a <img>, <input>.

Prevent Web Browser Caching

Some companies have requirements that web browser caching not be used with NA.

By default, the web browser caches NA content for faster loading of pages in the NA console. To disable all caching of NA content, add the following line to the `adjustable_options.rcx` file:

```
<option name="security/cache_control/enabled">true</option>
```

Note: Enabling this options sets all NA cache-control responses to no-cache, no-store, which means that NA must completely build each NA console page each time a user requests the page. This behavior change could impact NA performance at higher scale.

Restrict Email Forwarding

> **Note:** It is recommended to configure the SMTP server used by NA to limit the domains that the email server sends messages to. This configuration occurs outside NA and applies to all applications that use the SMTP server.

By default, NA does not verify email addresses before sending email messages from the NA core server. It is recommended to configure NA to send email messages only within your company's domain. Alternatively, you can configure NA to accept only specific email addresses.

Restrict the email addresses to which NA sends email messages by adding a customized version of one of the following line groups to the `adjustable_options.rcx` file:

- The following lines restrict NA to sending email messages to only the specified domains:

  ```
  <!-- e-mail restrictions -->
  <option name="email/allowed/prefs">domain</option>
  <option name="email/domain/allowed">*</option>
  ```

  Set `email/domain/allowed` to a comma-separated list of the permitted domains.

- The following lines restrict NA to sending email messages to only the specified email addresses:

  ```
  <!-- e-mail restrictions -->
  <option name="email/allowed/prefs">address</option>
  <option name="email/addresses/allowed">*</option>
  ```

  Set `email/addresses/allowed` to a comma-separated list of the permitted email addresses.

- The following lines restrict NA to sending email messages to only the specified domains and email addresses:

  ```
  <!-- e-mail restrictions -->
  <option name="email/allowed/prefs">both</option>
  <option name="email/domain/allowed">*</option>
  <option name="email/addresses/allowed">*</option>
  ```

  Set `email/domain/allowed` to a comma-separated list of the permitted domains.

  Set `email/addresses/allowed` to a comma-separated list of the permitted email addresses. The domains of the specified email addresses do not need to be included in the list of permitted domains.

Enable the Check for Email Injection

By default, NA does not examine outgoing email messages to verify that no non-NA content has been added to the messages. It is recommended to enable such checking.

To configure NA to check all outgoing email messages for email injection (and prevent sending any messages that have been subjected to email injection), add the following line the `adjustable_options.rcx` file:

```
<option name="security/emailInjection/check">true</option>
```

Enable SSL Communications over RMI

To secure the RMI communications by passing them through secure socket layer (SSL) sockets, follow these steps:

1. On *each*NA core server, make all of the following changes in the `<NA_HOME>/server/ext/jboss/server/default/deploy/remoting-jboss-beans.xml` file:

   Note: Perform this step in a single-core as well as multi-core NA environments.

   a. Within the `deployment` block, add the following lines:

      On Windows:

```
<bean name="sslServerSocketFactoryEJB2"
class="org.jboss.security.ssl.DomainServerSocketFactory">
    <constructor>
        <parameter><inject bean="EJB2SSLDomain"/></parameter>
    </constructor>
    <property name="protocols">TLSv1.2</property>
    <property name="cipherSuites">TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_
RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA</property>
</bean>
<bean name="EJB2SSLDomain"
class="org.jboss.security.plugins.JaasSecurityDomain">
    <constructor>
         <parameter>EJB2SSLDomain</parameter>
    </constructor>
    <property name="keyStoreURL"><NA_
Home>\server\ext\jboss\server\default\conf\truecontrol.keystore</property>
    <property name="keyStorePass">sentinel</property>

<property name="trustStoreURL"><NA_
Home>\server\ext\jboss\server\default\conf\truecontrol.truststore</property>

<property name="trustStorePass">sentinel</property>


</bean>
```

On Linux:

```
<bean name="sslServerSocketFactoryEJB2"
class="org.jboss.security.ssl.DomainServerSocketFactory">
    <constructor>
        <parameter><inject bean="EJB2SSLDomain"/></parameter>
    </constructor>
    <property name="protocols">TLSv1.2</property>
    <property name="cipherSuites">TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_
RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA</property>
</bean>
<bean name="EJB2SSLDomain"
class="org.jboss.security.plugins.JaasSecurityDomain">
    <constructor>
         <parameter>EJB2SSLDomain</parameter>
    </constructor>
    <property
name="keyStoreURL">/opt/NA/server/ext/jboss/server/default/conf/truecontrol.k
eystore</property>
    <property name="keyStorePass">sentinel</property>

<property name="trustStoreURL"><NA_
Home>/server/ext/jboss/server/default/conf/truecontrol.truststore</property>

<property name="trustStorePass">sentinel</property>


</bean>
```

b. In the `<bean name="UnifiedInvokerConfiguration" class="org.jboss.remoting.transport.Connector">` block, add the following lines:

```
<!-- added to configure the SSL socket for the UnifiedInvoker -->
<property name="serverSocketFactory"><inject
bean="sslServerSocketFactoryEJB2"/></property>
```

For example:

```
<bean name="UnifiedInvokerConfiguration"
class="org.jboss.remoting.transport.Connector">
    <annotation>@org.jboss.aop.microcontainer.aspects.jmx.JMX
(name="jboss.remoting:service=Connector,transport=socket",
exposedInterface=org.jboss.remoting.transport.ConnectorMBean.class,registerDirect
ly=true)
    </annotation>
    <property name="serverConfiguration"><inject
bean="UnifiedInvokerConfiguration"/></property>
    <!-- added to configure the SSL socket for the UnifiedInvoker -->
    <property name="serverSocketFactory"><inject
bean="sslServerSocketFactoryEJB2"/></property>
</bean>
```

c. In the `<bean name="UnifiedInvokerConfiguration" class="org.jboss.remoting.ServerConfiguration">` block, make both of the following edits:
   - Change the transport parameter to `sslsocket`.
   - After the `<entry><key>dataType</key>     <value>invocation</value></entry>` line, add the following line:

     ```
     <entry><key>enabledProtocols</key>     <value>TLSv1.2</value></entry>
     ```

   For example:

   ```
   <bean name="UnifiedInvokerConfiguration"
   class="org.jboss.remoting.ServerConfiguration">
       <constructor>
           <!-- transport: Others include sslsocket, bisocket, sslbisocket, http,
   https, rmi, sslrmi, servlet, sslservlet. -->
           <parameter>sslsocket</parameter><!-- changed from socket to sslsocket -->
       </constructor>
       ...
       <entry><key>dataType</key>     <value>invocation</value></entry>
       <entry><key>enabledProtocols</key>     <value>TLSv1.2</value></entry>
       ...
   </bean>
   ```

2. On *each*NA core server, add the following lines under the `# Java Additional Parameters` section in the `<NA_HOME>/server/ext/jboss/server/default/conf/syslog_wrapper.conf` file:

   Note: Perform this step in a single-core as well as multi-core NA environments.

   - On Windows, add the following lines:

     ```
     wrapper.java.additional.3 = -Djavax.net.ssl.keyStore=<NA_
     Home>\server\ext\jboss\server\default\conf\truecontrol.keystore

     wrapper.java.additional.4 = -Djavax.net.ssl.keyStorePassword=sentinel

     wrapper.java.additional.5=-Djavax.net.ssl.trustStore=<NA_
     Home>\server\ext\jboss\server\default\conf\truecontrol.truststore

     wrapper.java.additional.6=-Djavax.net.ssl.trustStorePassword=sentinel
     ```

   - On Linux, add the following lines:

     ```
     wrapper.java.additional.3 = -Djavax.net.ssl.keyStore=<NA_
     Home>/server/ext/jboss/server/default/conf/truecontrol.keystore

     wrapper.java.additional.4 = -Djavax.net.ssl.keyStorePassword=sentinel

     wrapper.java.additional.5=-Djavax.net.ssl.trustStore=<NA_
     Home>/server/ext/jboss/server/default/conf/truecontrol.truststore

     wrapper.java.additional.6=-Djavax.net.ssl.trustStorePassword=sentinel
     ```

3. In distributed NA environments with multiple NA cores, follow these steps:

a. On the NA core 1 server, export the NA certificate to a file.

   i. 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`

   ii. Run the `keytool` command. For example:

   - *Windows*:
     ```
     <NA_HOME>\jre\bin\keytool.exe -export -alias sentinel \
     -file na1cert.cer -keystore truecontrol.keystore
     ```
   - *Linux*:
     ```
     <NA_HOME>/jre/bin/keytool -export -alias sentinel -file na1cert.cer \
     -keystore truecontrol.keystore
     ```

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

   > **Tip:** The output file (for example, `na1cert.cer`) is created in the location from which the command is run.

   The command output is of the following form:

   ```
   Certificate stored in file na1cert.cer
   ```

b. On the remaining NA core servers in the distributed environment, import the NA core 1 server certificate into the `truecontrol.truststore` file as follows:

   i. Copy the exported file (for example, `na1cert.cer`) from its current location on the NA core 1 server to another NA core server in the distributed environment. Place the file in 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`

   ii. Change to that directory.

   iii. Run the `keytool` command. For example:

   - *Windows*:
     ```
     <NA_HOME>\jre\bin\keytool.exe -import -alias na1cert \
     -file na1cert.cer -keystore truecontrol.truststore
     ```
   - *Linux*:
     ```
     <NA_HOME>/jre/bin/keytool -import -alias na1cert -file na1cert.cer \
     -keystore truecontrol.truststore
     ```

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

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

   > **Tip:** Specify the file (for example, `na1cert.cer`) created in step a.
   >
   > The alias is the identifier of the new certificate in the `truecontrol.truststore` file on the additional NA core server. It does not need to match the alias in the `truecontrol.keystore` file on NA core 1 server.

   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 truststore
```

iv. Repeat step i through step iii as needed until the `truecontrol.truststore` files on all NA core servers contain the NA core 1 server certificate.

Enable Secure Communication with Satellites

> **Note:** Use this procedure only after installing the NA `10.00.021` patch. The steps provided in this section fail to work when the patch is not installed.

This section provides a procedure to enable a more secure mode of communication between NA cores and satellites.

In an environment with a single NA core:

1. Open the `adjustable_options.rcx` file from the following location:
   - *Windows: <NA_HOME>*`\jre`
   - *Linux: <NA_HOME>*`/jre`
2. Add the following line:

   ```
   <option name="rpc/isnextgenprotocol">true</option>
   ```
3. Save the file.
4. Restart the 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
     ```
5. Redeploy the NA remote agent on all the satellites.

In a Horizontal Scalability environment:

1. Follow these steps on each NA core:
   a. Open the `adjustable_options.rcx` file from the following location:
      - *Windows:<NA_HOME>*`\jre`
      - *Linux:<NA_HOME>*`/jre`

   b. Add the following line:

      ```
      <option name="rpc/isnextgenprotocol">true</option>
      ```

   c. Save the file.

   d. Restart the 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
  ```

2. Redeploy the NA remote agent on all the satellites of any one NA core.

   This procedure creates additional keystore and truststore files (`corerpc.keystore`, `corerpc.truststore`, `satelliterpc.keystore`, and `satelliterpc.truststore`) on the NA core. These files are placed in the following directory:

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

3. Copy these newly generated files and place them in the same directory on all other NA cores.
4. Redeploy the NA remote agent on all the satellites of all other NA cores.

Strengthen Security

You can strengthen the security of NA by applying any or all of the following changes:

- "Disable SSLv3" below
- "Configure the Ciphers Used by the NA Web Server" on page 23
- "Configure the NA SSH Server to Use Stronger HMAC and Key Exchange Algorithms" on page 25
- "Install the Stronger Self-Signed Certificate Provided by NA" on page 26
- "Disable FTP Access to Managed Devices" on page 26
- "Limit User Access to the NA Web Server" on page 27

Disable SSLv3

HP recommends disabling the SSLv3 protocol because it is affected by the POODLE vulnerability. For more information about the POODLE vulnerability, see CVE-2014-3566.

The procedure in this topic configures NA to only support the TLS secure protocol. After following the instructions given here to disable the SSLv3 protocol, NA will no longer accept or initiate connections using the SSLv3 protocol.

> **Note:** Certain versions of Mozilla Firefox do not support TLSv1.1 or TLSv1.2. For information about whether your Firefox version supports these protocol versions and any needed configuration, see the applicable Firefox documentation.

If NA is integrated with any of the following products, see the related documents about configuration of those products for any changes required to address the POODLE issue.

- HP Network Node Manager i

  For HP NNMi, see document KM01235890, "How to configure NNMi to disable the SSLv3 protocol."
- HP Server Automation

  For HP SA, see document KM01225418, "Server Automation Alert: POODLE: SSLv3 Vulnerability."
- HP Operations Orchestration

  For HP OO, see document KM01214975, "Operations Orchestration (OO) : SSLv3 security vulnerability (Poodle)."

> **Note:** Some integrations may not support TLS v1.1 or TLS v1.2 or will support these protocols in the future. For information, see the support documentation for the integrated products.

To disable the SSLv3 protocol in the NA environment, follow the steps outlined here. Complete the steps in the presented order. That is:

1. Configure all NA remote agents.
2. Configure the jboss server on all NA core servers.

3. Configure all NA gateways (core and remote).
4. On all NA core servers, configure the protocols for NA interactions with other processes.

> **Note:** Stop, start, and restart the various processes as described throughout these procedures.

Remote Agents on NA Satellites

In an NA satellite environment, to disable the SSLv3 protocol for the NA remote agent on an NA remote gateway server, do the following:

1. Ensure that the NA remote agent was redeployed to the NA remote gateway server as part of the patch installation process.
2. Edit the HTTP connector element in the `/opt/opsware/nassat/server/ext/tomcat/conf/server.xml` file to add the following text:

   ```
   sslEnabledProtocols = "TLSv1,TLSv1.1,TLSv1.2"
   ```

   For example, the HTTP connector element for an NA satellite might look like:

   ```
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
             sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
        keystoreFile="conf/nassat.keystore"
             keystorePass="sentinel"
        ciphers=...
   />
   ```

3. Add the following line to the `/opt/opsware/nassat/jre/nassat.rcx` file:

   ```
   <option name="rpc/client/sslprotocol"><TLS_ALGORITHM></option>
   ```

   Set `<`*`TLS_ALGORITHM`*`>` to either TLSv1.1 or TLSv1.2.
4. Restart the NA remote agent (**`/etc/init.d/nassat restart`**).

NA Cores

To disable the SSLv3 protocol far an NA core, do the following:

> **Note:** If this step is performed before disabling SSLv3 on all NA satellites, the NA remote agent deployment will fail as the installer tries to communicate with NA using SSL. To work around this issue, temporarily enable SSLv3 on the NA core server. Then disable SSLv3 on all NA remote agents before disabling SSLv3 on the NA core servers.

1. Edit the XML block for `Connector port="443"` in the `<NA_HOME>/server/ext/jboss/server/default/deploy/jbossweb.sar/server.xml` file to add the following text:
   - For NA with integrations that do not support TLS v1.1 or v1.2:

     ```
     sslProtocols = "SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
     ```

- Otherwise:

  ```
  sslProtocols = "TLSv1.1,TLSv1.2"
  ```

For example, the HTTP connector element for the NA core might look like:

```
<Connector port="443" address="${jboss.bind.address}" protocol="HTTP/1.1"
     minSpareThreads="5" maxSpareThreads="75"
     enableLookups="true" disableUploadTimeout="true"
     acceptCount="100" maxThreads="200"
     scheme="https" secure="true" SSLEnabled="true"
     keystoreFile="${jboss.server.home.dir}/conf/
          truecontrol.keystore" keystorePass="sentinel"
     truststoreFile="${jboss.server.home.dir}/conf/
          truecontrol.truststore" truststorePass="sentinel"
     clientAuth="want" sslProtocol="TLS" sslProtocols = "TLSv1.1,TLSv1.2"
     useBodyEncodingForURI="true"
     compression="on" compressionMinSize="2048"
          compressableMimeType="text/html,text/xml,text/css,
          text/javascript"
     ciphers=...
/>
```

2. Restart the NA services (see "Start, Stop, or Restart All NA Services" on page 28).

NA Core and Remote Gateways

In an NA satellite environment, to disable the SSLv3 protocol for an NA core gateway or an NA remote gateway, do the following:

1. In the `/var/opt/opsware/crypto/opswgw-<gateway_name>/opswgw-admin.pem` file, locate the following line:

   ```
   opswgw.crypto.SSLVersion=TLSv1,SSLv3,SSLv2-hello
   ```

   Edit this line to read:

   ```
   opswgw.crypto.SSLVersion=TLSv1
   ```

2. Restart the NA gateway (**`/etc/init.d/opswgw-<gateway_name> restart`**).

NA As a Client to Other Processes

To disable the SSLv3 protocol for NA interactions with other processes, do the following:

1. For all deployments, on all NA core servers, configure the NA RPC client to use TLS.

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

   ```
   <option name="rpc/client/sslprotocol">TLSv1.2</option>
   ```

2. For all deployments, on all NA core servers, configure the NA SSLUTIL class to use TLS.

   Add the following lines to the `adjustable_options.rcx` file:

   ```
   <option name="sslutil/client/sslprotocol">TLSv1.2</option>
   ```

> **Note:** The XML block for `Connector port="443"` in the `<NA_HOME>/server/ext/jboss/server/default/deploy/jbossweb.sar/server.xml` file on the NA core servers must include TLSv1.2 in the `sslEnabledProtocols` list.

3. In an NA satellite environment, on all NA core servers, configure the NA gateway client to use TLS.

   Add the following lines to the `adjustable_options.rcx` file:

   ```
   <option name="gateway/client/sslprotocol"><TLS_ALGORITHM></option>
   ```

   Set `<TLS_ALGORITHM>` to either TLS or TLSv1.

   Use the same value as specified in the `/var/opt/opsware/crypto/opswgw-<gateway_name>/opswgw-admin.pem` file on the NA gateways.

   For example:

   ```
   <option name="gateway/client/sslprotocol">TLSv1</option>
   ```

4. When NA is integrated with HP Server Automation, on all NA core servers, configure the NA Twist client to use TLS.

   Add the following lines to the `adjustable_options.rcx` file:

   ```
   <option name="twist/client/sslprotocol"><TLS_ALGORITHM></option>
   ```

   Set `<TLS_ALGORITHM>` to TLSv1, TLSv1.1, or TLSv1.2.

   For example:

   ```
   <option name="twist/client/sslprotocol">TLSv1.2</option>
   ```

5. Restart all NA services (see "Start, Stop, or Restart All NA Services" on page 28).

Configure the Ciphers Used by the NA Web Server

NA supports the following ciphers for secure communications with the NA web server:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The `ciphers` parameter of the `Connector` element in the `<NA_HOME>/server/ext/jboss/server/default/deploy/jbossweb.sar/server.xml` file specifies which ciphers NA might use. This parameter contains an ordered list of one or more ciphers. If NA is unable to use the first cipher in the list to establish a connection between the NA web server and the user's web browser, NA tries to use the next cipher, and so forth. (The preceding list shows the default cipher ordering.)

You can edit the value of the `ciphers` parameter to delete ciphers that NA should not use and to change the order in which NA attempts to use the available ciphers.

Note: The value of the `ciphers` parameter must be a comma-separated list that contains no white space and is one contiguous line.

HP recommends changing the order of the ciphers list to place 256-bit encryption above 128-bit encryption and to remove the weakest encryption algorithms as follows:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Note: If NA is integrated with HP Network Node Manager i, consider the following:

A Java 7 defect causes some communication encrypted with a TLS_RSA_WITH_AES_256_CBC_SHA cipher to fail. If the integration is configured for SSL communication with NA and FIPS mode is enabled for NA, remove TLS_RSA_WITH_AES_256_CBC_SHA from the cipher list specified in the `server.xml` file on the NA core server.

On an NA satellite, this configuration is in the `/opt/opsware/nassat/server/ext/tomcat/conf/server.xml`file.

Note: The web browser must support at least one of the configured ciphers.

For example, the HTTP connector element for the NA core might look like:

```
<Connector port="443" address="${jboss.bind.address}" protocol="HTTP/1.1"
     minSpareThreads="5" maxSpareThreads="75"
     enableLookups="true" disableUploadTimeout="true"
     acceptCount="100" maxThreads="200"
     scheme="https" secure="true" SSLEnabled="true"
     keystoreFile="${jboss.server.home.dir}/conf/
          truecontrol.keystore" keystorePass="sentinel"
     truststoreFile="${jboss.server.home.dir}/conf/
          truecontrol.truststore" truststorePass="sentinel"
     clientAuth="want" sslProtocol="TLS"
     useBodyEncodingForURI="true"
     compression="on" compressionMinSize="2048"
          compressableMimeType="text/html,text/xml,text/css,
          text/javascript"
     ciphers="TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_RSA_
WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_128_CBC_SHA"
/>
```

For example, the HTTP connector element for an NA satellite might look like:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
     maxThreads="150" scheme="https" secure="true"
     clientAuth="false" sslProtocol="TLS"
     keystoreFile="conf/nassat.keystore" keystorePass="sentinel"
     ciphers="TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_RSA_
WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_128_CBC_SHA"
/>
```

Configure the NA SSH Server to Use Stronger HMAC and Key Exchange Algorithms

By default, NA uses encryption algorithms for exchanging data with older devices. These encryption algorithms might not comply with the requirements of your environment. This topic describes how to enable the hmac-sha2-256 encryption algorithm and the diffie-hellman-group-exchange-sha1 SSH key exchange (KEX) algorithm.

Note: If NA is integrated with HP Network Node Manager i, consider the following:

A Java 7 defect causes some communication encrypted with a TLS_RSA_WITH_AES_256_CBC_SHA cipher to fail. If the integration is configured for SSL communication with NA and FIPS mode is enabled for NA, remove TLS_RSA_WITH_AES_256_CBC_SHA from the cipher list specified in the `server.xml` file on the NA core server. For information about configuring the cipher list, see "Configure the Ciphers Used by the NA Web Server" on page 23.

Stronger HMAC algorithm

To use a stronger HMAC algorithm, enable FIPS mode according to the instructions in the "Enabling FIPS Mode" chapter of the *NA Administration Guide*. While configuring the list of permitted encryption algorithms for SSH/SCP/SFTP, update the `crypto/fips/mac_list` array according to the needs of your environment:

- To add hmac-sha2-256 support, use the following `crypto/fips/mac_list`:

  ```
  <array name="crypto/fips/mac_list">
       <value>hmac-sha1</value>
       <value>hmac-sha1-96</value>
       <value>hmac-sha2-256</value>
  </array>
  ```

- To limit HMAC to hmac-sha2-256, use the following `crypto/fips/mac_list`:

  ```
  <array name="crypto/fips/mac_list">
       <value>hmac-sha2-256</value>
  </array>
  ```

Note: HP recommends configuring the `crypto/fips/cipher_list` as described in the "Enabling FIPS Mode" chapter of the *NA Administration Guide* while enabling FIPS.

Stronger key exchange algorithm

To limit the key exchange (KEX) to the diffie-hellman-group-exchange-sha1 SSH KEX algorithm only, add the following lines to the `adjustable_options.rcx` file:

```
<array name="crypto/fips/kex_list">
     <value>diffie-hellman-group-exchange-sha1</value>
</array>
```

Install the Stronger Self-Signed Certificate Provided by NA

NA 10.00.02 provides a set of self-signed certificates and keystores that are generated using SHA-256 encryption with 2048 bit SSL.

The patch does not install the new certificate to avoid overwriting user customization.

> **Note:** HP recommends using a CA-signed certificate instead of the self-signed certificate provided by NA.

If you are not using a custom (CA-signed) certificate and would like to use the stronger self-signed certificate delivered in the NA patch, do the following:

1. Copy the `truecontrol.keystore` and `truecontrol.truststore` files from the `patch10.00.02/NA_Certs` directory of the patch to the `<NA_HOME>/server/ext/jboss/server/default/conf` directory on the NA core server.
2. Install the certificate provided in the `patch10.00.02/NA_Certs` directory of the patch according to the instructions in the "Adding a Self-Signed Certificate to NA" section of the "Using Certificates with NA" chapter of the *NA Administration Guide*.
3. If NA participates in any integrations, check the appropriate documentation for information about exporting the NA certificate and importing it into the integrated product.

Disable FTP Access to Managed Devices

If your NA environment does not require FTP, disable the NA FTP server by editing the `/etc/init.d/truecontrol` file to comment out the `StartFTP` statement near line 280 and the `StopWrapper FTP "TrueControl FTP Server"` statement near line 291.

For example:

```
start() {
     cd /opt/NA/server/ext/wrapper/bin
     StartTFTP
     StartSyslog
     StartJBoss
     # StartFTP
     # StartPerl
     StartSWIM
}
stop ()
     cd /opt/NA/server/ext/wrapper/bin
     StopWrapper JBoss "TrueControl Management Engine"
     StopWrapper Syslog "TrueControl Syslog Server"
     StopWrapper SWIM "TrueControl SWIM Server"
     StopWrapper TFTP "TrueControl TFTP Server"
     # StopWrapper FTP "TrueControl FTP Server"
     KillProcess wrapper swim_wrapper
}
```

After starting the NA services, disable the FTP monitor. In the NA console, on the Server Monitoring page (**Admin > Administrative Settings > Server Monitoring**), clear the **Enable the FTPMonitor** check box, and then click **Save**.

> **Note:** Some devices are only accessible using FTP. Disabling the NA FTP server effectively disables NA access to these devices.

Limit User Access to the NA Web Server

It is recommended to limit traffic to the NA web server to only those users who should have access. Possible ways to limit this traffic include:

- Configure a firewall in front of the NA core server.
- Isolate user access to the NA core server on specific network interfaces only.

Common Procedures

This section describes procedures that are common to many HP Network Automation Software (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 the next page

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 FTP Server**
  - **TrueControl SWIM 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 FTP Server**
  - **TrueControl SWIM 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 FTP Server**
  - **TrueControl SWIM 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 FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *Linux*:

  ```
  mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
  ```

Working with .rcx Files

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

> **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.

We appreciate your 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 Security Configuration Guide, March 2017 (Network Automation Software 10.00)

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.