Hewlett Packard
Enterprise

HPE Network Automation Software

Software Version: 10.20
for the Windows® and Linux® operating systems

Hardening Guide

Document Release Date: November 2016
Software Release Date: July 2016

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

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

Contents 4
Using this Guide 5
Communication Configuration 6
Configure TLS Protocols 6
Remote Agents on NA Satellites 7
NA Core and Remote Gateways 7
NA Integrated with HPE Server Automation 7
Enable SSL Communications over RMI 8
Enable Secure Communication with Satellites 12
User Authentication 14
Compliance Features 16
Clickjacking Protection 17
Prevent Web Browser Caching 18
Restrict Email Forwarding 19
Enable the Check for Email Injection 20
Strengthen Security 21
Configure the Ciphers Used by the NA Web Server 21
Configure the NA SSH Server 23
Configure the NA SSH Server to Require a Stronger HMAC Algorithm 23
Configure the NA SSH Server to Require a Stronger Cipher List 23
Configure the NA SSH Server to Require a Stronger Key Exchange Method 25
Disable FTP Access to Managed Devices 25
Limit User Access to the NA Web Server 26
Common Procedures 27
Start, Stop, or Restart All NA Services 27
Disable All NA Services 28
Working with .rcx Files 28
We appreciate your feedback! 30

Using this Guide

This document provides information for increasing the security of your NA installation. The information in this document applies to NA 10.20. 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 27).
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 27).
4. In an NA satellite environment, restart all NA remote agents:

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

Communication Configuration

This topic describes the default security configurations for encryption, hashing, and secure communication within NA.

- During installation, NA generates a self-signed certificate using a 2048-bit encryption key, SHA 256, and RSA.

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

  For a new installation or an upgraded installation that was previously using the NA-provided self-signed certificate, you can install a CA-signed certificate as described in the "Adding a CA-Signed Certificate to NA" section of the "Using Certificates with NA" chapter of the *NA Administration Guide*.

  For an upgraded installation that was previously using a CA-signed certificate, the upgrade process backed up that certificate before installing the self-signed certificate. You must re-enable the CA-signed certificate as described in "Configuring the User-added CA-signed Certificate in NA after Upgrade" of the *NA Installation and Upgrade Guide*.
- The default SSL protocols for HTTPS communication with the NA web server are TLSv1.0, TSLv1.1 and TLSv1.2.

  Note: It is recommended to disable TLSv1.0 and TLSv1.1 unless they are needed for communicating with applications that do not support TLSv1.2. For instructions, see "Configure TLS Protocols" below.
- For local authentication into NA, NA uses the SHA 512 algorithm for hashing and storing NA user passwords.
- For encryption of database and device passwords, NA uses the AES 256 algorithm.
- For SSH communication to the NA proxy:
  - Default ciphers: 3des-cbc, aes128-cbc, aes128-ctr, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr
  - Default hmac: hmac-sha2-256, hmac-sha256, hmac-sha256@ssh.com
  - Default key exchange cipher: diffie-hellman-group-exchange-sha256

For communications from the NA core server to devices, NA supports the following methods:

- Default compression algorithms: none, zlib, zlib@openssh.com|
- Default public keys: ssh-dss, ssh-rsa|
- Default hmac: hmac-sha1, hmac-md5, hmac-md5-96, hmac-sha1-96|
- Default ciphers: aes128-cbc, 3des-cbc, blowfish-cbc, aes128-ctr, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr, twofish128-cbc, twofish192-cbc, twofish256-cbc, cast128-cbc|
- Default key exchange ciphers: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1

Configure TLS Protocols

It is recommended to disable TLSv1.0 and TLSv1.1 unless they are needed for communicating with applications that do not support TLSv1.2.

To do so, follow the steps outlined here. Complete the steps in the presented order:

1. Configure all NA remote agents.
2. Configure all NA gateways (core and remote).
3. On all NA core servers, configure the protocol for NA interactions with HPE Server Automation (SA).

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

Remote Agents on NA Satellites

In an NA satellite environment, to configure the protocol for the NA remote agent onan NA remote gateway server, do the following:

1. In the `/opt/opsware/nassat/server/ext/tomcat/conf/server.xml` file, locate the HTTP connector element.

   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=...
   />
   ```

   Revise the `sslEnabledProtocols` list as appropriate.
2. Restart the NA remote agent (**`/etc/init.d/nassat restart`**).

NA Core and Remote Gateways

In an NA satellite environment, to configure the 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 Integrated with HPE Server Automation

When NA is integrated with HPE Server Automation (SA), on all NA core servers, configure the NA Twist client to use TLS as follows:

1. 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>
```

2. Restart all NA services (see "Start, Stop, or Restart All NA Services" on page 27).

Enable SSL Communications over RMI

By default, the RMI communications between NA core servers in a Horizontal Scalability or Multimaster Distributed System environment are not secure.

To secure the RMI communications by passing them through secure socket layer (SSL) sockets, update the RMI configuration and then exchange certificates among the NA core servers. Follow these steps:

1. On *each* NA core server in the distributed environment, make all of the following changes in the `<NA_HOME>/server/ext/jboss/server/default/deploy/remoting-jboss-beans.xml` file:
   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>
</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.keystore
</property>
    <property name="keyStorePass">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,registerDirectly=tru
e)
    </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 the NA core 1 server, export the NA certificate to a file.
   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. 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
      ```

3. On the remaining NA core servers in the distributed environment, import the NA core 1 server certificate into the `truecontrol.truststore` file as follows:
   a. 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`
   b. Change to that directory.
   c. 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 2.
>
> 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
```

d. Repeat step a through step c as needed until the `truecontrol.truststore` files on all NA core servers contain the NA core 1 server certificate.

4. Repeat step 2 and step 3 as needed until the `truecontrol.truststore` files on all NA core servers contain the NA certificates from all other NA core servers in the distributed environment.

Enable Secure Communication with Satellites

Note: Use this procedure only after installing the NA 10.20.001 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.

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.

Tip: For local accounts, NA requires each new user to reset their password on first login.

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.

Compliance Features

FIPS

As of NA 10.10:

- FIPS mode is enabled by default for the following types of connections to the NA core:
  - SSL (HTTPS)
  - SSH
  - SCP
  - SFTP
- FIPS mode is disabled by default for SSH connections from the NA core to devices.

  For information about enabling FIPS mode to devices, see "Enabling FIPS Mode" in the *NA Administration Guide*.

Note: If FIPS mode was explicitly disabled in the `adjustable_options.rcx` file prior to upgrading to NA 10.20, the upgrade honors that setting and FIPS remains disabled.

NA console logon banner

You can enable a banner page that appears and must be acknowledged before a user can access the NA console login page. For information about enabling this functionality, see "Enabling the Logon Banner" in the *NA User Guide*.

User authentication events

As of NA 10.10, NA generates an event for every user login, logout, or failed log-in attempt. For the event names, see "Event Descriptions" in the *NA User Guide*.

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.

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>
```

Strengthen Security

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

- "Configure the Ciphers Used by the NA Web Server" below
- "Configure the NA SSH Server to Require a Stronger HMAC Algorithm" on page 23
- "Disable FTP Access to Managed Devices" on page 25
- "Limit User Access to the NA Web Server" on page 26

Configure the Ciphers Used by the NA Web Server

NA supports the following ciphers for secure communications with the NA web server. The ciphers in this list are known to be compatible with RSA BSAFE and FIPS mode:

- 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_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Note: At the time of this release, NA does not support elliptical curve cryptography (ECC) as it conflicts with FIPS mode.

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.

HPE 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_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

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_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_
AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256"
/>
```

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_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_
AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256"
/>
```

Configure the NA SSH Server

Configure the NA SSH Server to Require a Stronger HMAC Algorithm

When FIPS mode is enabled for SSH connections to the NA core, NA uses the following keyed-hash message authentication code (HMAC) encryption algorithms:

- hmac-sha2-256
- hmac-sha256
- hmac-sha256@ssh.com

This configuration is the default behavior for new installations of NA 10.10 or later.

Note: If the `crypto/fips/mac_list` parameter was explicitly configured in the `adjustable_options.rcx` file prior to upgrading to NA 10.20, the upgrade honors that setting and the default behavior described here does not apply.

The full list of supported HMAC algorithms is as follows:

- hmac-sha256
- hmac-md5
- hmac-sha1
- hmac-md5-96
- hmac-sha1-96
- hmac-sha2-256
- hmac-sha256@ssh.com

Example

To limit HMAC to hmac-sha2-256, add one of the following lines to the `adjustable_options.rcx` file:

- When the FIPS mode is enabled:

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

- When the FIPS mode is not enabled:

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

Configure the NA SSH Server to Require a Stronger Cipher List

When FIPS mode is enabled for SSH connections to the NA core, NA uses the following cipher lists:

- 3des-cbc
- aes128-cbc
- aes128-ctr
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr

This configuration is the default behavior for new installations of NA 10.10 or later.

Note: If the `crypto/fips/cipher_list` parameter was explicitly configured in the `adjustable_options.rcx` file prior to upgrading to NA 10.20, the upgrade honors that setting and the default behavior described here does not apply.

The complete list of supported ciphers is as follows:

- 3des-cbc
- aes128-cbc
- aes128-ctr
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- 3des-ctr
- blowfish-cbc
- arcfour
- arcfour128
- arcfour256

Example

To limit the cipher list to `aes256-ctr`, add one of the following lines to the `adjustable_options.rcx` file:

- When the FIPS mode is enabled:

```
<array name="crypto/fips/cipher_list">
     <value>aes256-ctr</value>
</array>
```

- When the FIPS mode is not enabled:

```
<array name="crypto/general/cipher_list">
     <value>aes256-ctr</value>
</array>
```

Configure the NA SSH Server to Require a Stronger Key Exchange Method

When FIPS mode is enabled for SSH connections to the NA core, NA uses the `diffie-hellman-group-exchange-sha256` key exchange method.

This configuration is the default behavior for new installations of NA 10.10 or later.

Note: If the `crypto/fips/kex_list` parameter was explicitly configured in the `adjustable_options.rcx` file prior to upgrading to NA 10.20, the upgrade honors that setting and the default behavior described here does not apply.

The complete list of supported key exchange methods is as follows:

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256

Example

To limit the key exchange method list to `diffie-hellman-group-exchange-sha256`, add one of the following lines to the `adjustable_options.rcx` file:

- When the FIPS mode is enabled:

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

- When the FIPS mode is not enabled:

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

Disable FTP Access to Managed Devices

Because FTP transfers information in clear text, it is considered to be a non-secure protocol. It is recommended to disable the FTP protocol if it is not required in your NA environment and to use SSH instead.

Note: Some managed devices may be accessible only using FTP. Disabling the NA FTP server effectively disables NA access to these devices.

Disable the NA FTP server by editing the `/etc/init.d/truecontrol` file to comment out the `StartFTP` statement in the `start()` function and the `StopWrapper FTP "TrueControl FTP Server"` statement in the `stop()` function.

For example:

```
start() {
```

```
cd /opt/NA/server/ext/wrapper/bin

StartTFTP

StartSyslog

StartJBoss

#StartFTP

Startsaclient

#StartPerl

}

stop ()
     cd /opt/NA/server/ext/wrapper/bin
     StopWrapper JBoss "TrueControl Management Engine"
     StopWrapper Syslog "TrueControl Syslog Server"
     StopWrapper TFTP "TrueControl TFTP Server"
     # StopWrapper FTP "TrueControl FTP Server"
```

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**.

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.

  For information about the ports that NA uses, see "HPE Network Automation Software Ports" in the *NA Administration Guide*.
- Isolate user access to the NA core server on specific network interfaces only.

Common Procedures

This section describes procedures that are common to many HPE 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 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 HPE 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 Hardening Guide, November 2016 (Network Automation Software 10.20)

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.