EndRun TECHNOLOGIES
"Smarter Timing Solutions"

PRODUCT NOTE
SHA-1 AUTHENTICATION FOR ENDRUN TIME SERVER PRODUCTS

1.0 PURPOSE

This document provides instructions for setting up SHA1 NTP authentication in Endrun time servers.

2.0 OVERVIEW

In order to properly configure an EndRun product for SHA1 authentication, keys must be created manually in /etc/ntp.keys and those keys must be designated as “trusted” in /etc/ntp.conf. To enable NTP clients to authenticate your EndRun Time Server as a NTP time source, the keys must be copied to each client; and each client must also be configured (ntp.conf in UNIX/Linux OS) to recognize these keys as “trusted” keys.

Section 3.1 includes the procedure for creating the keys and configuring ntp.conf in the EndRun time server. Configuring the clients for SHA1 in both UNIX/Linux and Windows OS is described in sections 3.2 and 3.3 of this procedure.

Although using SHA256 authentication appears to function when tested in the models listed above, the 256 bit key is actually truncated to 160 bits. Therefore SHA256 authentication will not be covered in this Product Note.

3.0 PROCEDURE

3.1 Configure EndRun Device for SHA1

Login to the interface (CLI) as **root** and complete this section.

3.1.1 With your Endrun product’s command line, **configure /etc/ntp.keys**

3.1.1.1 Navigate to `/etc` directory by running command:

```
cd /etc<Enter>
```

3.1.1.2 Modify ntp.keys in “Joes’s own Editor” by running command:

```
joe ntp.keys<Enter>
```

3.1.1.3 For SHA1 authentication, type a string with following syntax for each SHA1 key that you wish to create:

```
n<sp>SHA1<sp>xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx<sp>#description
```

Where *n*=key number (1 to 65535), <sp>and
`xxxx...x` = key consisting of up to 20 ASCII characters or up to 40 hex-decimal characters
The description at the end of the string is optional.

3.1.1.4 When the ntp.keys file is completed, it should appear similar to the example below. It may be necessary to change the header text for documentation accuracy :

```
# Sonoma_D12 GPS Authentication Keys
# For MD5 or SHA1, Keys longer than 20 characters must only be hex characters
1 SHA1 EndRunNTP #SHA1 key
15 SHA1 3c1cdbafed123456f4d2cc4b1802cb60dcb24d5e #SHA1 key
```

3.1.1.5 To exit the joe editor and save the modified ntp.keys file, type <Ctrl-k> then hit x.

3.1.1.6 To make changes persistent, ntp.keys must be copied to the non-volatile memory partition. Do that by typing: `cp -p /etc/ntp.keys /boot/etc .`

3.1.2 Configure "ntp.conf"

3.1.2.1 Navigate to `/etc` and type `joe ntp.conf<Enter>`

3.1.2.2 At the end of the file, find the lines below and Modify the key numbers accordingly as shown:

```
keys<sp>/etc/ntp.keys
trustedkey<sp>1<sp>15
```

Notice that the key numbers in this file and ntp.keys match.

3.1.2.3 To make changes persistent, ntp.conf must be copied to the non-volatile memory partition. Do that by typing:

```
cp -p /etc/ntp.conf /boot/etc .
```

3.1.3 For changes to take effect:

Choose one of two methods for making changes take effect. 1.) Reboot the EndRun unit by typing: reboot<Enter> **.** 2.) Restart the NTP daemon by sending command:

```
/etc/rc.d/rc.ntpd restart
```

3.2 Configure Unix\Linux Client

3.2.1 **Configuration:** If section 3.1 is successfully completed, the /etc/ntp.keys file client must be copied from the EndRun device for to /etc directory in the client. Then the key numbers need to be added to the ntp.conf file.

3.2.1.1 From the EndRun Device's command line, run the command below:

```
scp -p /etc/ntp.keys root@<IP address of client device>:/etc
```

3.2.1.2 In the client device's /etc/ntp.conf file, add the key numbers to the server directives and `trustedkeys` list as shown in **`bold`** below.

```
server 192.168.1.123 key 1
server 192.168.1.202 key 15

# Authentication
keysdir /etc
keys /etc/ntp.keys
trustedkey 1 15
```

3.2.1.3 Perform the required steps for the client device to make changes introduced in the previous step persistent, then reboot the client device.

3.2.2 **Testing Configuration:** From the client's command line interface, run the command below.

```
ntpq -p
```

You should see a response similar to the table below. Look for the IP address of your EndRun device in the "remote" column and verify that you see the appropriate reference source in the corresponding `refid` column – in this case "`.GPS.`". This indicates that the client is able to pole the NTP server. If the `refid` indicates ".INIT." or ".STEP.", the previously modified configuration files should be checked for typos.

```
root@Sup_Lab_Mtower:/etc# ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.         10 l    4   64    1    0.000    0.000   0.001
 192.168.1.123   .GPS.           1 u    3   64    1    0.888  374.921   0.001
 192.168.1.202   .GPS.           1 u    3   64    1    1.012  571.043   0.001
```

Eventually after 20-30 minutes a fresh run of the command below:

```
ntpq -p
```

should yield results similar to those shown in the table below. A "*" character to the left of the NTP server's IP address in the "remote" column indicates the source from which the client is synchronized. A "+" character in the same position indicates a candidate synchronization source.

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        .LOCL.         10 l    4   64    1    0.000    0.000   0.001
*192.168.1.123   .GPS.           1 u  377   64    1    0.176    0.030   0.069
+192.168.1.202   .GPS.           1 u  377   64    1    0.180    0.049   0.079
```

3.3 Configure Windows Client

If section 3.1 is successfully completed, a Windows OS client can be configured for SHA1 *provided* the client NTP software supports authentication. NTP Client configurations can be very challenging on most Windows OS when using utilities that are included with the OS package. In many cases, third party software such as Greyware's Time Domain II makes the task of configuring authentication much less difficult. For more information go to: https://www.greyware.com/software/domaintime/ .

4.0 SUPPORT

If assistance is needed for completing this procedure, please call please contact EndRun Technical Support.