EndRun TECHNOLOGIES
"Smarter Timing Solutions"

PRODUCT NOTE

Secure *Your Time Server*

Network Time Servers are not typical multi-user appliances or servers. They have a very specialized function - to serve reliable and accurate time. As such, the Linux operating system has been streamlined and all unnecessary protocols removed. This greatly decreases any potential attack surface. Any software that might be connected to a CVE will probably not be present in an EndRun appliance. In addition, all convenience protocols like httpd, snmpd, telnetd and even sshd can be disabled. The serial port can also be disabled. System settings are only modifiable with administrative access (root user).

Following are the steps we recommend to further secure a Sonoma Time Server on a private network, behind a firewall. For installations on a public network there should be additional safeguards such as changing User Accounts. These additional safeguards are not described in this paper. *NOTE: Although this paper is written for Sonoma, basic steps are the same for EndRun's other products such as Meridian II, Tycho II and Ninja.*

CHANGE DEFAULT PASSWORDS

Sonoma ships from the factory with two default passwords. The passwords should be changed as soon as possible using the `passwd` command. There is usually no need for anyone other than the network administrator to log in to the time server. Therefore, only one or two persons should know the new passwords.

`passwd`
changes root user password (privileged user)

`passwd ntpuser`
changes ntpuser password (unprivileged user)

DISABLE UNNEEDED PROTOCOLS

EndRun Time Servers are shipped from the factory with the following services running. Disable all the protocols that you do not need, except do NOT disable the Network Time Protocol (NTP).

NTP (UDP 123)	Do not disable.
TELNET (TCP 23)	OK to disable.
Daytime (TCP/UDP 13)	OK to disable.
Time (TCP/UDP 37)	OK to disable.
SSH (TCP 22)	OK to disable.
SNMP (UDP 161 and 162)	OK to disable.
HTTPS (TCP 443)	OK to disable.
Optional Precision Time Protocol (UDP 319 and UDP 320)	OK to disable.

To disable unneeded protocols, see your *User Manual, Chapter 5 - Security, Disable Protocols.* Here are links to the User Manuals:

Sonoma D12 (GPS): endruntechnologies.com/pdf/USM3027-0000-000.pdf
Sonoma N12 (GPS): endruntechnologies.com/pdf/USM3029-0000-000.pdf

RESTRICT ACCESS

Sonoma Time Server should be one of the most secure boxes in your system. Many users may have clilent access via one of the timing protocols (such as NTP). But the network administrator is the only one who should have direct access. Therefore, direct access should be limited to specific hosts and one or two users. To restrict access see your *User Manual, Chapter 5 - Security, Restrict Access.*

For the most sensitive situations, you can eliminate all protocols (with the exception of NTP and any other timing protocol you need) and use the local RS-232 console port to configure and monitor the Time Server. Or, if you are more concerned about internal threats then the network administrator can disable the serial port.

ENCRYPT SESSIONS

Logging in to the system should always be done using SSH (secure shell). Therefore, Telnet should be disabled (see above). (The default SSH keys are uniquely configured for each Sonoma shipped from the factory.)

ENCRYPT COMMUNICATIONS (RSA and TLS)

EndRun uses the standard OpenSSH suite and ssh-keygen utility. We recommend you use RSA keys for encryption. These keys are stored in flash and only readable by the network administrator (root user). For instructions see your *User Manual, Chapter 5 - Security, Configure Keys.*

EndRun products also support Transport Layer Security (TLS v1.2 and v1.3).

USE NTP AUTHENTICATION

You should require that your NTP clients use MD5 authentication and disable NTP access to any host not using authentication. As shipped from the factory, the Time Server is configured to respond to NTP requests from clients that may or may not be using MD5 authentication. We recommend you modify the factory-default MD5 keys and then configure your clients to use the same MD5 authentication keys. NTP authentication must be enabled to ensure the host and client association is trusted and confirm that the timestamps are unaltered.

For instructions see your *User Manual, Chapter 3 - NTP, Configuring the NTP Server* and *Unix-like Platforms: MD5 Authenticated NTP Client Setup* or *Windows: MD5 Authenticated NTP Client Setup.*

LOCKOUT KEYPAD ACCESS

For the Sonoma with a front-panel keypad/display, the **`lockoutkp`** and **`kplockstat`** utilities can prevent unauthorized tampering with the unit. Refer to the *User Manual, Chapter 9 - Console Port Control & Status, Detailed Command Descriptions.*

KEEP LOG FILES

System logs are critical in performing troubleshooting. They also play a key role in performing forensics on a compromised machine. Sonoma is capable of sending logs to a remote collector using *syslog.* We recommend you consider doing this. One benefit is that any time someone tries to break into the unit, this occurrence will be logged including their IP address.

Consult the relevant *syslog* documentation for instructions on how to set up the associated *.conf* file. Remember to copy it to the */boot/etc* directory which will retain the settings during a reboot.

MITIGATE VULNERABILITIES

Sonoma uses a monolithic Linux kernel. There are no insertable modules which eliminates many vulnerabilities.

Some of the potential vulnerabilities found during a security scan are only a threat under conditions that do not exist in a Time Server. Most security scans just look at open ports and protocol versions. For example, your scan may list a vulnerability that exists in the SSH version resident on Sonoma. However, it is likely that Sonoma's SSH is not configured in such a way as to expose this vulnerability. Since a Time Server is not a multi-user work station, many vulnerabilities listed on your scan are not a problem in Sonoma.

Other potential vulnerabilities can be mitigated by applying the workarounds mentioned in the Network Security Bulletins here:

endruntechnologies.com/support/product-bulletins

FIRMWARE UPGRADES

Time Servers are not multi-user computer systems. They are embedded appliances with a very specialized function. In the embedded environment, the benefit of applying patches or frequently rebuilding new versions of the Linux open source binaries is questionable, just to have the illusion that the new build won't have vulnerabilities. It won't have the listed vulnerabilities but it will probably have new ones. And it may also have new bugs that were not present in the previous version.

Any serious vulnerabilities that cannot be mitigated with a reasonable workaround will be addressed as soon as possible with a firmware change. For remaining vulnerabilities, we recommend you apply the safeguards listed above and mitigate per the workarounds mentioned in the Network Security Bulletins.

FIRMWARE UPGRADES

EndRun releases new versions of firmware from time-to-time to address serious vulnerabilities, to enhance the product, and to correct known bugs. These can be found at:

endruntechnologies.com/support/software-upgrades/sonoma-gps

NTP CLIENTS

Keep your NTP clients updated with the latest software. Configure all your clients to use MD5 authentication as described in the paragraph above - *Use NTP Authentication.*

HELP

If you need help or have questions then contact EndRun technical support. Its free.

1-877-749-3878 (U.S. & Canada)
707-573-8633 (International)
support@endruntechnologies.com