Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document

November 9, 2023

1.3

Prepared By:

Acumen Security
2400 Research Blvd Suite 395
Rockville, MD, 20850
www.acumensecurity.net

Prepared for:
Ciena Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America www.ciena.com

Table of Contents

1 Overview

This document is intended to be a supplement to the Waveserver 5 Rel 2.3.12 User Guide (323-3001-100) documentation. This Common Criteria guidance document contains configuration information needed to configure and administer the Waveserver 5. The Waveserver 5 conforms to the Common Criteria Network Device Protection Profile v2.2e (NDcPP v2.2e). The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the Waveserver 5.

1.1 TOE Overview

The Ciena Waveserver 5 Rel 2.3.12 (herein referred to as the TOE) is a network device which offers ultrahigh capacity connections between data centre locations thus reducing the network costs for both enterprises and content providers. The Wavesever 5 utilizes Ciena's WaveLogic 5 Extreme technology. The Ciena Waveserver 5 is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all of the criteria to meet the collaborative Protection Profile for Network Devices, Version 2.2e.

1.2 TOE Description

The Ciena Waveserver 5 is a purpose-built, data center interconnect (DCI) platform designed to facilitate high-speed, high-capacity connections between data centers. This platform has been designed to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP 2.2e]. The Waveserver 5 incorporates a range of advanced security features to ensure the integrity and confidentiality of network communications.

While not an exhaustive list, some the main security mechanisms being leveraged include the following. For information on all the supported security mechanisms, please refer to Section 1.2.2:

1. Encrypted SSH Administration: The device supports encrypted SSH connections for secure remote administration, protecting the communication channel between administrators and the device from unauthorized access and eavesdropping.

2. RADIUS via TLS: The Waveserver 5 is capable of using RADIUS authentication with TLS encryption, ensuring the secure transmission of login credentials and providing an added layer of protection for user authentication.

3. Encrypted Syslog Traffic: The platform can encrypt syslog traffic via TLS to a syslog server, safeguarding the privacy and confidentiality of logs and preventing unauthorized access to sensitive log data.

4. NTP with SHA Authentication: The Waveserver 5 supports the use of NTP with SHA authentication, providing a secure method for time synchronization across network devices and reducing the risk of time-based attacks.

These highlighted security mechanisms, along with other measures, contribute to the Ciena Waveserver 5's ability to not only meet the collaborative Protection Profile for Network Devices, Version 2.2e, but also deliver a comprehensive and secure networking solution for end users.

The TOE is comprised of the following model:

Waveserver 5 front panel:

Waveserver 5 rear panel: AC power and fan modules

Waveserver 5 rear panel: DC power and fan modules

Waveserver 5 rear panel: DC power and fan modules

Waveserver 5 Appliance	Hardware Specifics
Processor	Marvell CN9130
Enclosure	Dual rack unit
Power Supply	AC or DC power AC input voltage range: 100 Vac to 277 Vac DC input voltage range: 180 Vdc to 300 Vdc Power consumption: 0.4 W/Gb
Environment Characteristics	Normal operating temperature: -5 °C to +45 °C (23 °F to 113 °F)

Table 1 Supported Platform

1.3 Assumptions

The following Assumptions are for the Operational Environment:

Assumptions	Operational Environment
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

Assumptions	Operational Environment
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 2 Supported Platform

1.4 TOE Delivery

The TOE is delivered via commercial carrier (i.e. FedEx, UPS, Expeditors etc). The TOE will contain a packing slip with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed in the packing slip. The TOE is shipped with the software preinstalled on it. Software updates are available for download from the Ciena website. When software updates are available via the http://www.ciena.com website, they can obtain, verify the integrity and install the updates.

2 Logging into Waveserver 5

2.1 Using Terminal emulator and SSH :

Before beginning this procedure, ensure that:

- You have installed the Waveserver 5 node and provisioned it with an IP address and gateway for the management network interface, and the Waveserver 5 node is connected to the management network.
- You have installed a terminal emulator application (for example, PuTTY) on your PC, and the terminal emulator is running.

Steps:

1. Open the terminal emulator on your PC. Specify the IP address of the Waveserver 5 node that you want to connect to. If this is the first time anyone has connected to this Waveserver 5 from a terminal using SSH, you are prompted to add this Waveserver 5 to your known hosts list.
2. Enter the username of the default user account: su
3. Enter a short sequence of random characters for the password. The default super user account has no default password.

Note: Waveserver 5 units have one factory-set user account: su (super user). Use this account to log in to Waveserver 5 after it initializes.

2.2 Using Local Access :

Prior to beginning this procedure please ensure that:

- You have installed the Waveserver 5 node and provisioned it with an IP address and gateway for the management network interface, and the Waveserver 5 node is connected to the management network.

Steps to access :

1. Initially make sure the TOE is in an active state up and running.
2. For direct access of the TOE, connect a USB type-C port one to the TOE and other to the management/user's laptop.

3. Power up the laptop and navigate to the section “This PC” by following the steps Windows -> Documents -> This PC.
4. Under the Devices and drives section you can find the TOE connected to the laptop as a device.
5. The above can also be done with the help of connecting a console cable between the TOE and User’s system.

3 Enabling CC-NDcPP Compliance

Administration of the TOE takes place over the local CLI console and SSH for remote authentication.

```
Starting autobaud on ttyS0

Waveserver-5 login: su
Password:

!!! This is a private network. Any unauthorized access or use will lead to prosecution!!



Welcome to Waveserver CLI!
Waveserver-5# exit
Starting autobaud on ttyS0

Waveserver-5 login: su
Password:
```

```
root@ciena-linux-vm:~#
root@ciena-linux-vm:~# ssh su@10.1.5.111
(su@10.1.5.111) Password:

!!! This is a private network. Any unauthorized access or use will lead to prosecution!!



Welcome to Waveserver CLI!
Waveserver-5*#
```

NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested. For the purpose of this CC Guidance document the focus would be limited to local CLI and remote SSH interfaces.

3.1 Enabling CC-NDPP Compliance Using the CLI interface

Disable diag shell admin-state (will cause system cold restart). This would block any access to Linux environment.

- **system environment diag disable diag-shell**

If using manually configured IP address:

- **dhcp client disable**
- **interface set interface local ip X.X.X.X/<mask> gateway Y.Y.Y.Y**

Create users in CC-NDPP for testing

- **user create user limited password <password> access-level limited**
- **user create user super password <password> access-level super**

Setup Remote File Transfer method

- **system xftp set mode scp**
- **system xftp set scp-server X.X.X.X login-id <user> password <password>**
- **system xftp set sftp-server Y.Y.Y.Y login-id <user> password <password>**

Enable DNS Resolving

- **dns client enable**
- **dns client add server <DNS server IPv4>**
- **dns client set domain-name <domain name>**

Enable SNMP

- **snmp enable**

NOTE: SNMP is enabled as part of the evaluated configuration, but SNMP interface was not evaluated

Install CA chain and Entity certificates.

- **certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>**
- **certificates entity install cert-name <Entity Name> default-scp-server filename <Path/File.p12> certpassphrase ************

Generate CSR

certificates entity csr generate cert-name csr_pass key-type rsa2048 default-scp-server filename /<path>/csr_pass.cnf

NOTE: Only RSA key sizes of 2048 and 3072 are supported for generation of the CSR.

Cert Name “csr_pass” has to be specified in csr_pass.cnf file.

Install certificate back

certificates entity install cert-name <Entity Name> default-scp-server filename <Path/File.crt> certificate-only

Set password for root account

- **system environment root set <password>**

Set password for su account

- **user set user password <password>**

Create collector for syslog-tls server

- **syslog tls set cert-name <Entity Name>**
- **syslog tls create collector <IPv4/IPv6/Hostname> port <#> severity all**

Setup syslog and RADSEC

- **radsec set cert-name <Entity Name>**
- **radsec add server <IPv4/IPv6/Hostname> port <#> priority <#>**

Setup HTTPs

- **system server https set cert-name <Entity Name>**

Setup NTP with SHA1 Key

- **ntp sha1-key enable**
- **ntp sha1-key add key-id <1….65534> sha1 <SHA1 string[2..40]>**
- **ntp client add server <ip address> key-id <sha1-key-id>**

Default cryptographic functionality:

```
WS5_0195*# ssl algorithm show
+-------------------- TLS Cipher Suites ------------------------+
| Cipher suite Name                              | Admin State  |
+------------------------------------------------+--------------+
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384        | Enabled      |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384        | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384          | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384          | Enabled      |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256            | Disabled     |
| TLS_RSA_WITH_AES_256_GCM_SHA384                | Disabled     |
| TLS_RSA_WITH_AES_256_CBC_SHA256                | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256        | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256        | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256          | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256          | Disabled     |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384            | Disabled     |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256            | Disabled     |
| TLS_RSA_WITH_AES_128_CBC_SHA256                | Disabled     |
+------------------------------------------------+--------------+
```

```
WS5_0195*# ssh algorithm show

+----------SSH Key Exchange Algorithms-----------------------+
| Algorithm Name                              | Admin State  |
+---------------------------------------------+--------------+
| ecdh-sha2-nistp521                          | Enabled      |
| ecdh-sha2-nistp384                          | Enabled      |
| ecdh-sha2-nistp256                          | Enabled      |
| diffie-hellman-group14-sha1                 | Enabled      |
+---------------------------------------------+--------------+
+----------SSH Encryption Algorithms-------------------------+
| Algorithm Name                              | Admin State  |
+---------------------------------------------+--------------+
| aes256-gcm                                  | Enabled      |
| aes256-ctr                                  | Enabled      |
| aes128-gcm                                  | Enabled      |
| aes128-ctr                                  | Enabled      |
+---------------------------------------------+--------------+


+----------SSH Message Authentication Code Algorithms--------+
| Algorithm Name                              | Admin State  |
+---------------------------------------------+--------------+
| hmac-sha2-512                               | Enabled      |
| hmac-sha2-256                               | Enabled      |
+---------------------------------------------+--------------+
+----------SSH Public Key Authentication Algorithms----------+
| Algorithm Name                              | Admin State  |
+---------------------------------------------+--------------+
| ssh-rsa                                     | Enabled      |
| ecdsa-sha2-nistp256                         | Enabled      |
| ecdsa-sha2-nistp384                         | Enabled      |
| ecdsa-sha2-nistp521                         | Enabled      |
+---------------------------------------------+--------------+
```

Save the provisioned setting to the configuration file:

- **configuration save**

The following ECC curves are supported by default on the device and no other curves are allowed or enabled:

- **secp256r1**
- **secp384r1**
- **secp521r1**
- **DH Group 14**

NOTE: For all the servers that use TLS, the Admin provisions the server information and the TOE automatically creates the TLS connection to the server. When a connection is severed then the TOE will detect that state and will automatically re-connect and perform retry attempts as needed. The administrator does not need to perform any actions. This applies to RADsec and TLS-Syslog. If the IT entity server is non-functional then that equipment and application will need to be recovered.

3.2 Configuring SSH Thresholds

The TOE is capable of rekeying. The TOE verifies the following thresholds:

- No longer than one hour
- No more than 1GB of transmitted data

The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.

NOTE: There is no additional configuration necessary to enable SSH thresholds as it is supported by default.

4 Using an Audit Server

Use the following procedure to configure an audit server.

4.1 Prerequisites

- You must be logged in to Waveserver 5 using an account with at least admin access privileges.
- You have the server IP or host name and filename for the X.509 certificate files.
- Device certificate with private key and CA certificate has been installed on the TLS syslog server.
- You know the IP address or host name for the TLS syslog server.

4.2 Audit Server Requirements

The audit server must be a Syslog server that supports TCP and TLS v1.2 or TLS v1.1.

4.3 System Behavior

The TOE can be configured to export audit events securely to a syslog server using TLS v1.2 or TLSv1.1 protocol using X.509 certificates. No configuration is necessary to enforce TLSv1.2 or TLSv1.1 connection due to the device denying connections from clients requesting any lower SSL versions.

The TOE stores audit data locally. When a file is full, a new file is created. When the local data is full, the oldest file is overwritten to allow new audit events to be created.

The TOE transmits audit data to an external syslog server in real time. If there is a TLS connection failure, the TOE will continue to store local audit events on the TOE , and will transmit any locally stored contents when connectivity to the syslog server is restored.

4.4 Audit Server Configuration

1. To use an audit server:
   create a private key and install a device trusted CA certificate as follows:
   - **certificates authorities install {default-ftp-server | default-sftp-server | default-tftserver | defaultserver | default-scpserver | sftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scp-server <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]>**

   - For example**: certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>**

2. Set the TLS syslog certificate name to the certificate you installed in step 1:
   - **syslog tls set cert-name <String: cert_name> For example: syslog tls set cert-name tlssyslogcert**

3. Set the global administrative state of TLS syslog message logging:
   - **syslog tls <disable | enable>**

4. Create a collector for TLS syslog with the desired attributes to enable the TOE to communicate with syslog server:
   - **syslog tls create collector <IP address or host name> [custom-prefix <String: 1...15>] [fingerprint <fingerprint>] [facility <Number: 0..24>] [port <Number: 1..65535>]**

[severity <emergency | alert | error | warning | notice | info | debug | all>] [trusted-dns <trusteddns>]

Note: It is recommended that OCSP be used to perform real time certificate status checks when validating a Syslog server's X.509 certificate.

5. Enable Syslog with OCSP:
    - **syslog tls ocsp enable**

6. Set the default OCSP responder:
    - **syslog tls ocsp set default-responder <String: [1..255]>**

7. To set the OCSP responder preference
    - **syslog tls ocsp set responder-preference <aia | default responder>**

8. To set whether you would like the OCSP responders to contain nonce:
    - **syslog tls ocsp set nonce <on | off>**

9. Optionally, retrieve TLS syslog OCSP settings:
    - **syslog tls ocsp show**

Note: OCSP revocation status checks take place wherever a TLS certificate connection is implemented (RADsec and Audit server). If a connection can't be validated, the TOE does not accept the certificate and the connection is not established.

10. Save the provisioned settings to the configuration file:
    - **configuration save**

Note: The default value for the [default-responder] attribute is blank

4.5 Auditable Events

4.5.1 Format

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 3. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event.

All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection.

4.5.2 NDcPP Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Records
FAU_GEN.1	Start-up of the audit function	None	17548: 2023-06-30T19:13:08+00:00 [UTC] Sev: 5 chassis : Chassis reboot has been requested, reason User Cold
	Shutdown of the audit function	None	17548: 2023-06-30T19:13:08+00:00 [UTC] Sev: 5 chassis : Chassis reboot has been requested, reason User Cold
	Administrative Login	Name of user account shall be logged if individual user accounts are required for Administrators	2023-04-25T09:55:20+00:00 [UTC] Sev: 6 auth : cli user successfully logged in from IP Console-1 username su in session 76
	Administrative Logout		2023-04-26T16:48:35+00:00 [UTC] Sev: 6 auth : cli user logged out from IP Console-1 username su out of session 84
	Changes to TSF data related to configuration changes	In addition to the information that a change occurred, it shall be logged what has been changed	2022-10-26T14:26:01+00:00 [UTC] Sev: 6 syslogTLS : SyslogTLS connection established. Collector: 10.1.5.110 2022-10-27T14:38:52+00:00 [UTC] Sev: 6 RadsecEvent_X509VerifySuccess : /C=CC/ST=STATE/L=Local/O=Org/OU=Uorg/ CN=ciena.acumen.com/emailAddress= general@acumen.com : Server: ciena.acumen.com 2022-10-25T14:20:39+00:00 [UTC] Sev: 4 ntpc : NTP Disabled
	Generating/import of cryptographic keys	In addition to the action itself, a unique key name or	2022-10-31T18:20:30+00:00 [UTC] Sev: 5 logging : 2022-10-31T18:20:28+00:00 - ssh server key install *ser ecdsa256 sftp-server 127.0.0.1 login-id su password **********

	Changing of cryptographic keys	key reference shall be logged	2022-10-31T18:10:13+00:00 [UTC] Sev: 6 ssh : Ssh server key install, user: ecdsa256
	Deleting of cryptographic keys		2022-10-31T18:20:59+00:00 [UTC] Sev: 5 logging : 2022-10-31T18:20:59+00:00 - ssh server key delete *ser ecdsa256
	Resetting passwords	Name of related user account shall be logged.	17826: 2023-08-24T17:35:57+00:00 [UTC] Sev: 6 auth : Password Set for User test 17827: 2023-08-24T17:35:57+00:00 [UTC] Sev: 5 logging : 2023-08-24T17:35:57+00:00 - user set user test password **********
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	HTTPS certificate error: 2022-10-28T14:14:51+00:00 [UTC] Sev: 6 HTTPSTLSError : Client did not return a certificate. Client: 10.1.5.110
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if New or removed time server	Configure NTP time 2022-10-25T10:33:10+00:00 [UTC] Sev: 4 chassis: System Time Set 10:33:00 2022-11-03T16:06:24+00:00 [UTC] Sev: 5 logging : 2022-11-03T16:06:24+00:00 - ntp client disable 2022-11-03T18:09:59+00:00 [UTC] Sev: 5 logging : 2022-11-03T18:09:59+00:00 - system show time
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	2022-10-18T17:31:29+00:00 [UTC] Sev: 6 auth : User authentication failed from IP 10.1.5.110:43532 username ***** 2022-10-31T18:50:46+00:00 [UTC] Sev: 6 ssh : SSH connection with 10.1.5.110 failed: no matching host_key_type found

FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	Failure to establish TLSC connection: 2022-10-18T18:12:13+00:00 [UTC] Sev: 6 RadsecEvent_TLSError : X509 verification error : unsupported certificate purpose : Server: ciena.acumen.com 2022-10-24T17:37:17+00:00 [UTC] Sev: 4 syslogTLS : Syslog TLS Failed due to Certificate not found EKU TLS Server Authentication, to address ciena.acumen.com
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	Failure to establish TLSS connection: 2022-10-28T14:14:51+00:00 [UTC] Sev: 6 HTTPSTLSError : Client did not return a certificate. Client: 10.1.5.110 2022-10-07T18:21:47+00:00 [UTC] Sev: 6 HTTPSTLSError : Handshake Failed. Client : 10.1.5.110
FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure	Failure to establish TLSS connection: 2022-10-17T20:15:36+00:00 [UTC] Sev: 6 HTTPSTLSError : Client certificate has a bad signature. Client: 10.1.5.110
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g. IP address).	Unsuccessful login limit met: 2022-11-01T14:45:00+00:00 [UTC] Sev: 6 Auth : User authentication lockout from IP 10.1.5.110 username lockout
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	Local console login: 2022-11-01T17:12:17+00:00 10.1..111 CienaWavserver -5-R2.3.11(7930) cli user successfully logged in from IP console-1 username su in session 615 SSH login: 2022-10-18T17:20:08+00:00 [UTC] Sev: 6 auth : cli user successfully logged in from IP 10.1.5.110:55064 username su in session 61

FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	SSH password based remote login 2022-10-18T17:19:48+00:00 [UTC] Sev: 6 auth : cli user successfully logged in from IP 10.1.5.110:56708 username su in session 60 SSH key-based authentication: 2022-10-31T18:20:35+00:00 [UTC] Sev: 6 auth : cli user successfully logged in from IP 10.1.5.110:35056 username ecdsa256 in session 542
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Certificate validation failure: 2022-10-26T14:46:33+00:00 [UTC] Sev: 6 RadsecEvent_X509VerifyFailed : /C=CC/ST=STATE/L=Local/O=Org/OU=Uorg/CN=ciena.acumen.com/emailAddress=expired@acumen.com : Server: ciena.acumen.com 2022-10-27T16:06:12+00:00 [UTC] Sev: 6 DeviceCertificateAdd : X.509 Device Certificate Name csr_202210271210 Installed 2022-10-26T14:25:56+00:00 [UTC] Sev: 4 syslogTLS : Syslog Add TLS Collector ciena.acumen.com 2022-10-26T14:41:40+00:00 [UTC] Sev: 6 CaCertificateRemove : X.509 CA Certificate int1CA with hash d120634b Uninstalled
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	Software update failure: 2022-11-20T15:05:44+00:00 [UTC] Sev : 4 SoftwareUpgrade : Software install request. URL: 2022-11-03T17:59:01+00:00 [UTC] Sev: 4 a : 9 Sev:major (Chassis): :Upgrade Download Failed raised

FMT_MTD.1/CoreData	All management activities of TSF data.	None.	SSH key Generated: 2022-11-01T17:53:18+00:00 [UTC] Sev : 5 logging : 2022-11-01T17:53:16+00:00 ssh server key generate key-type rsa2048 force 2022-11-01T15:53:52+00:00 [UTC] Sev : 5 logging : 2022-11-01T15:53:52+00:00 – syslog tls show
FMT_SMF.1	All Management of TSF data	None.	Ability to start and stop services: 2022-11-04T18:00:52+00:00 [UTC] Sev: 6 syslogTLS : SyslogTLS connection established. Collector: ciena.acumen.com 2022-11-04T18:00:53+00:00 [UTC] Sev: 4 syslogTLS : Syslog Remove TLS Collector ciena.acumen.com Ability to configure audit behaviour: **Refer to above logs* Ability to modify the behaviour of the transmission of audit data to an external IT entity: **Refer to above logs** Ability to re-enable an Administrator account: 2022-11-01T14:47:15+00:00 [UTC] Sev: 6 auth : cli user successfully logged in from IP 10.1.5.110:60860 username lockout in session 607 Ability to set the time which is used for time-stamps: 2022-10-25T10:21:00+00:00 [UTC] Sev: 4 chassis : System Time Set to 10:21:00

			Ability to configure NTP: 2022-10-25T10:33:34+00:00 [UTC] Sev: 4 NtpConfAdd : NTP Config Server Add IP 10.1.5.110 Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors: 2022-10-26T14:15:24+00:00 [UTC] Sev: 6 CaCertificateAdd : X.509 CA Certificate rootCA with hash 556fc382 Installed Ability to manage the cryptographic keys: 2022-10-31T18:20:29+00:00 [UTC] Sev: 6 ssh : Ssh server key install, user: ecdsa256 Ability to import X.509v3 certificates to the TOE's trust store: 2022-10-26T14:15:26+00:00 [UTC] Sev: 6 CaCertificateAdd : X.509 CA Certificate int1CARevoke with hash c1b9713a Installed Ability to administer the TOE locally and remotely: 2023-03-29T15:14:35+00:00 [UTC] Sev: 6 auth : cli user logged out from IP 10.1.5.110:48592 username su out of session 10 2023-03-29T15:23:12+00:00 [UTC] Sev: 6 auth : cli user logged out from IP Console-1 username su out of session 12 Ability to configure the access banner: 2022-11-01T18:12:04+00:00 [UTC] Sev: 6 WelcomeBannerSet : System Welcome Banner File Set to /home/su/welcome_banner.txt

			Ability to configure the session inactivity time before session termination or locking: 2023-09-13T18:51:25+00:00 [UTC] Sev: 5 logging : 2023-09-13T18:51:25+00:00 - system server set global-inactivity-timeout 20 Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates: 2022-11-02T15:05:44+00:00 [UTC] Sev: 4 SoftwareUpgrade : Software install request, URL: Ability to configure the authentication failure parameters for FIA_AFL.1: 2023-09-13T18:47:07+00:00 [UTC] Sev: 5 logging : 2023-09-13T18:47:07+00:00 - user set max-login-attempt 5
FPT_STM.1	Discontinuous changes to time - either Admin actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See application note on FPT_STM_EXT .1)	For discontinuous changes to time. The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	System Set time: 2022-10-25T10:21:00+00:00 [UTC] Sev : 5 logging : 2022-10-25:T10:21:49+00:00 System Set Time 10:21:00 NTP update show time: 2022-10-25T14:26:33+00:00 [UTC] Sev : 5 logging : 2022-10-25:T14:26:33+00:00 System Show Time

FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	Software updates install failure: 2022-11-02T18:36:47+00:00 10.1.5.111 Ciena-Waveserver-5-R2.3.11[6551] 6 Sev:major (Chassis): :Upgrade Installation Failed raised Successful software update: 2022-11-02T15:21:08+00:00 [UTC] Sev : 0 UpgradeCommitComplete
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.	2023-03-29T14:52:04+00:00 [UTC] Sev: 6 auth : cli user logged out from IP Cosole-1 username su out of session 4
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	2023-03-29T15:05:24+00:00 [UTC] Sev: 4 auth : cli user logged out from IP 10.1.5.110 username su out of session 7
FTA_SSL.4	The termination of an interactive session.	None.	2023-03-29T15:34:55+00:00 [UTC] Sev: 6 auth : cli user logged out from IP 10.1.5.110:33498 username su out of session 14
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identificati on of the initiator and target of failed trusted channels establishm ent attempt.	Failed to establish connection to SYSLOG server: 2022-11-04T18:00:52+00:00 [UTC] Sev: 6 syslogTLS : SyslogTLS connection established. Collector: ciena.acumen.com 2022-11-04T18:00:53+00:00 [UTC] Sev: 4 syslogTLS : Syslog Remove TLS Collector ciena.acumen.com 2022-10-24T17:37:17+00:00 [UTC] Sev: 4 syslogTLS : Syslog TLS Failed due to Certificate not found EKU TLS Server Authentication, to address ciena.acumen.com

			Failed to establish connection to RADSEC server: 20336: 2022-11-04T17:40:17+00:00 [UTC] Sev: 6 TlsConnecting : RadSec beginning connection. Server: ciena.acumen.com 20337: 2022-11-04T17:40:27+00:00 [UTC] Sev: 6 RadsecEvent_TLSError : Error connecting : Timeout : Server: ciena.acumen.com 2022-10-18T18:12:13+00:00 [UTC] Sev: 6 RadsecEvent_TLSError : X509 verification error : unsupported certificate purpose : Server: ciena.acumen.com
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identificati on of the initiator and target of failed trusted channels establishm ent attempt.	Failed to establish connection to SYSLOG server: 2022-11-04T18:00:52+00:00 [UTC] Sev: 6 syslogTLS : SyslogTLS connection established. Collector: ciena.acumen.com 2022-11-04T18:00:53+00:00 [UTC] Sev: 4 syslogTLS : Syslog Remove TLS Collector ciena.acumen.com 2022-10-24T17:37:17+00:00 [UTC] Sev: 4 syslogTLS : Syslog TLS Failed due to Certificate not found EKU TLS Server Authentication, to address ciena.acumen.com Failed to establish connection to RADSEC server: 20336: 2022-11-04T17:40:17+00:00 [UTC] Sev: 6 TlsConnecting : RadSec beginning connection. Server: ciena.acumen.com 20337: 2022-11-04T17:40:27+00:00 [UTC] Sev: 6 RadsecEvent_TLSError : Error connecting : Timeout : Server: ciena.acumen.com 2022-10-18T18:12:13+00:00 [UTC] Sev: 6 RadsecEvent_TLSError : X509 verification error : unsupported certificate purpose : Server: ciena.acumen.com

Table 3 NDcPP Audit Events

5 Configuring RADSec authentication

5.1 Prerequisites:

- You must be logged in to Waveserver 5 using an account with super user access privileges.
- You have the server IP address or host name and the filename for the X.509 certificate files.
- You know the IP address or host name and port number for each RADSec server to be added.
- A valid X.509 certificate has been installed on the RADSec server.
- The RADSec server must be a server that supports TCP and TLS v1.2 or TLS v1.1.

1. Install the X.509 certificate for RADSec:
    - certificates entity install cert-name <String: cert_name> {default-ftp-server | default-sftp-server | default-tftpserver | default-server | default-scp-server | sftpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftpserver <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]> certpassphrase [certificate-only]

- For example:
    - certificates entity **install cert-name <Entity Name> default-scp-server filename <Path/File.p12> certpassphrase **********
    - **certificates entity install cert-name <Entity Name> scp-server <IP address> login-id <user-name> password <password> filename <Path/File.p12> cert-passphrase **********

2. Optionally, display the installed certificate:
    - **certificates authorities show**
    - **certificates entity show**

3. Specify the global RADSec settings:
    - **radsec set [cert-name <String: cert_name>] [timeout <Seconds: 1..30>]**

4. Add a RADSec server to the Waveserver 5 system, specifying a priority for the server:
    - **radsec add server <IP address or host name> [priority <Number:1...8>] [port <Number:1...65535>]**

Note 1: Repeat step 5 for each RADSec server you want to add. You can add up to eight RADSec servers. Note 2: For the [priority] attribute, 1 is the highest priority. Note 3: The default value for the [port] attribute is 2083.

5. It is recommended that OCSP be used to perform real time certificate status checks when validating a RADSec server's X.509 certificate. Enable RADSec with OCSP:
    - **radsec ocsp enable**

6. Set the default OCSP responder:
    - **radsec ocsp set default-response <String: [1..255]>**

Note: The default value for the [default-responder] attribute is blank.

7. Set the OCSP responder preference.
    - **radsec ocsp set responder-preference <aia | default-responder>**

Note: The default value for the [responder-preference] attribute is aia.

8. Set whether you want the OCSP responders to contain nonce:
    - **radsec ocsp set nonce <on | off>**

Note: The default value for the [nonce] attribute is on.

9. Set the order of available authentication providers:

- **user auth set order radsec [,radius][,local]**

Note: Set RADIUS and/or local authentication as a backup provider to ensure access to the Waveserver 5 in the event that RADSec services are unavailable.

10. Set RADSec as the authentication method for all remote connections over SSH:
    - **user auth set method radsec scope remote**

11. Configuring RADSec for both remote and local connections:
    - **user auth set method radsec scope all**

12. Optionally, view RADSec summary or statistics information for all configured RADSec servers:
    - **radsec show [statistics]**

Note: RADSec servers are listed by priority, with the highest priority server displayed first.

13. Save the provisioned settings to the configuration file:
    - **configuration save**

Note: If a connection can't be established to the OCSP responder, the TOE will not accept the certificate and the administrator must reattempt the connection when the responder is back online.

6 Authentication

6.1 Password Management

Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“ ?”, “ ‘ “, “ + “, “ / “, “ : ”, “ ; “, “ < “, “ > “, “ = “, “ [“, “] “, “, “ ~ “, “ { “, “ } “, “ |”.

The TOE is capable of configuring strong passwords, such as those with at least 15 characters long and the following complexity rules:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

Minimum password lengths shall be configurable to 8 characters to maximum of 128 characters. The default minimum password length is 8 characters. The TOE only supports the creation of strong passwords.

1. To create a user account and setting of the password use the following command:
    - **user create user <String: 1...32> access-level <limited | admin | super> [password <String: [8...128>]**

2. To set the minimum password length, use the following command:

- **user set min-password-length [8..128]**

6.2 Configuring SSH Public Keys

Use the commands in this section to create a new public key for SSH user authentication. You can use this key instead of the password to authenticate the remote user.

1. Create a user:
    - **user create user rsa4096 access-level super password ************
2. Create the public key using Linux ssh-keygen (The key file name should be the same as user name) on the remote server.
    - ssh-keygen -t rsa -b 4096 -f Documents/rsa4096ssh-keygen -t rsa-sha2-256 -f Documents/rsa4096_sha2
    - ssh-keygen -t rsa-sha2-512 -f Documents/rsa4096_sha2512
    - ssh-keygen -t ecdsa-sha2-nistp256 -f Documents/rsa4096_ecd
    - ssh-keygen -t ecdsa-sha2-nistp384 -f Documents/rsa4096_ecd384
    - ssh-keygen -t ecdsa-sha2-nistp521 -f Documents/rsa4096_ecd521
3. Install the public key associating with the pre-created user
    - **ssh server key install user rsa4096 sftp-server <IP address> login-id <user> password ***********

6.3 Configuring X.509 Certificate Authentication for TLS Mutual Authentication

The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication is performed when the TOE acts as TLS Server or Client. By default, mutual authentication is disabled on the device.

Enabling mutual authentication:

- **system server https mutual-authentication enable**

The Supported Elliptic Curves extension are enabled by default. Refer to Section 3.1 for details.

When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules:

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.

The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE

- The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960.

- NOTE: If a connection can't be established to the OCSP responder, the TOE will not accept the certificate and the administrator must reattempt the connection when the responder is back online.

The TSF shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field

Note: The Waveserver device does not support any fallback authentication for new TLS connections.

6.4 Configuring Reference Identifiers

The TOE supports DNS name and IP addresses as its reference identifiers.

When the syslog client or RADsec client receives an X.509 certificate from their respective servers, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type in the certificate, then the TSF will compare the reference identifier to the Common Name (CN) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes and additional verification actions can proceed.

The TLS server setup must match the Certificate identifier scheme configuration with DNS vs IP Address format that is intended to be used otherwise the certificate will be rejected.

i.e. When users expect the TLS server certificate with an IP address format reference identifier, users shall configure the TOE to add the TLS server using IP address format. When users expect the TLS server certificate with an DNS format reference identifier, users shall configure the TOE to add the TLS server using DNS format.

6.5 Generation of a Certificate Signing Request

1. On the external xFTP (FTP, SFTP, SCP or TFTP) server, create a device certificate configuration file (.cnf file), the configuration file must contain the configuration for the certificate. The device certificate configuration file fields are shown below:

   {{[req]prompt = no}} {{distinguished_name = req_distinguished_name}} {{[req_distinguished_name]}} {{C = GB}} {{ST = Test State}} {{L = Test Locality}} {{O = Organization Name}} {{OU = Organization Unit Name}} {{CN = Common Name}} {{emailAddress = test@email.com}}

   For Example:
   [req]
   prompt = no
   distinguished_name = req_distinguished_name

   [req_distinguished_name]
   C = Country
   ST = Test State
   L = Test Locality
   O = Organization Name
   OU = Organization Unit Name
   CN = Common Name
   emailAddress = test@email.com

2. To issue a certificate signing request (CSR), the following command must be executed:
   - **certificates entity csr generate cert-name csr_pass key-type rsa2048 default-scp-server filename /<path>/csr_pass.cnf**

   Cert Name “csr_pass” has to be specified in csr_pass.cnf file.

3. Sign the certificate using a Certificate Authority or an OpenSSL tool.

4. On the Waveserver 5, install the signed device certificate with “certificate-only” option
   - certificates entity install cert-name <String: cert_name> {default-ftp-server | default-sftp-server | default-tftpserver | default-server | default-scp-server | sftpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftpserver <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]> certificateonly
   - For example: **certificates entity install cert-name test1 tftp-server X.X.X.X filename test.pem certificate-only**
5. Optionally display the summary information for the private key and device certificate.

- **certificates authorities show**
- **certificates entity show**

6.6 Authentication Failure Handling

The Administrator can configure the maximum number of failed attempts for the CLI interface. The lockout feature can be configured from 2-10 unsuccessful attempts. The default maximum attempts is 5 attempts and the default lockout interval time is 10 minutes. When the defined number of unsuccessful attempts have been met, the TOE will not allow the user to login until the defined time period has elapsed. If the lockout attempts is set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct.

To set the maximum number of login attempts and to define a lockout interval, use the CLI command

- **user set [max-login-attempt <Number: 2..10>] [lockout-interval <Number: <1..30>]**

The authentication failures cannot lead to a situation where no administrator access is available as the local CLI access would be accessible to the user as the local CLI cannot be locked out.

6.7 Role Based Access Control (RBAC)

The TOE implements Role Based Access Control (RBAC). Administrative users are required to login before being provided with access to any administrative functions. The TOE restricts the ability to manage the TOE to Security Administrators.

The TOE maintains the following roles: Security administrator (super user), Admin user, and User (Limited user). Each role defined has a set of permissions that will grant them access to the TOE data.

For the purpose of the Common Criteria, only the Security Administrator and the User roles were tested.

Roles	**Permissions**
Security Administrator (super user)	Can configure user accounts and manage users and their associated privileges.
	Ability to administer the TOE locally and remotely
	Ability to configure the access banner

Roles	Permissions
	Ability to configure the session inactivity time before session termination or locking
	Ability to update the TOE, and to verify the updates using digital signatures capability prior to installing those updates
	Ability to configure audit behavior
	Ability to set the time which is used for time-stamps
	Ability to configure the reference identifier for the peer
	Ability to start and stop services: • Syslog TLS • RADsec via TLS • SSH Administrator Access • NTP Synchronization
User (Limited user)	Able to carry out system monitoring and gather information about the configuration and performance of the system.
	Can change their own password, but not other user's passwords

Table 4 Roles and Permissions

6.7.1 Creating a user account

1. To create a local user account, use the command:
    - **user create user <String: 1...32> access-level <limited | admin | super> [password <String: 8...128>]**

2. Save the provisioned settings to the configuration file:
    - **configuration save**

6.7.2 Deleting a user account

1. To delete a local user account, use the command:
    - **user delete user <String: 1...32>**

2. Save the provisioned settings to the configuration file:
    - **configuration** save

6.8 Logging out of the local CLI and remote SSH interfaces

To facilitate ending a session, the administrative user must log out of the TOE.

1. Local CLI and remote SSH, use the following command:
    - **exit**

7 Cryptographic Protocols

Enabling CC-NDcPP compliance will ensure that only certified algorithms and key sizes are available for use by the appliance.

7.1 SSH

No configuration is required, please refer to Section 3.1. The device defaults to only certified algorithms for SSH.

7.2 TLS

Enabling mutual authentication:

- **system server https mutual-authentication enable**

No further configuration is needed. Please refer to Section 3.1.

The TOE will automatically attempt to re-establish an unintentionally disrupted channel to the remote audit server indefinitely. During this time, audit messages continue to be stored locally on the TOE. Once the disruption has been corrected, the syslog client on the TOE will automatically attempt to renegotiate the TLS channel upon the next retry. OCSP is used to detect the validity of a client or server certificate when it is presented to the TOE.

8 Self-Tests

8.1 Cryptographic POST

All crypto algorithms used by the management interface must go through power up self-tests (KAT) before they can be used to provide service.

When Waveserver 5 detects a failure during one or more of the self-tests, it raises an alarm. The administrator can attempt to reboot the TOE to clear the error. If rebooting the Waveserver 5 does not resolve the issue, then the administrator should contact their next level of support or their Ciena support group for further assistance. All power up self-tests execution are logged for both successful and unsuccessful completion.

The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.

Note: The cryptographic POST is run automatically when the appliance is turned on or restarted, regardless of whether the appliance has been put in FIPS 140-3 or CC-NDPP compliance.

The appliance will not run if the digital signature validation fails upon restart:

1. Power up self-test

If the self-tests pass then the following message is displayed:

selfTest passed

Sep 30 10:32:05 WaveserverOS wolfcrypt-self-test[4638]: FIPS Self-Test Suite: Started

Sep 30 10:32:08 WaveserverOS wolfcrypt-self-test[4753]: SSH KDF KAT success

Sep 30 10:32:11 WaveserverOS wolfcrypt-self-test[4638]: FIPS Self-Test Suite: self-tests for all algorithms successful

If the POST fails, the Waveserver 5 would leave console log to indicate self-test failure, such as:

```
[FAILED] Failed to start FIPS Self-Tests for WolfCrypt
```

and automatically cold restart the chassis.

9 Performing Manual Software Updates on the TOE

Security Administrators have the ability to query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the "software show" command.

When software updates are available via the http://www.ciena.com website, they can obtain, verify the integrity and install the updates.

The software images are digitally signed using RSA digital signature mechanism. The TOE will use a public key in order to verify the digital signature, upon successful verification then the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.

9.1 Prerequisites

The upgrade software has been downloaded from the Ciena portal and saved to the designated remote server. You must have the IP address and host name of the server as well as the user name and password.

Note 1: To access the software server where the upgrade software is located, you must have the IP address or host name of the server, along with a user name and password if the server is an SFTP. server.

- You are logged in to Waveserver 5 using an account with at least admin privileges.
- You have saved a copy of the active configuration file to a remote server.
- Enough memory is available in the Waveserver 5 memory to support the new software load. To ensure that there is sufficient memory space, delete any unnecessary software files.

Verify version of the software

```
WS5-0133# software show
+----------------- SOFTWARE STATE INFORMATION -----------------+
|         Parameter           |              Value             |
+-----------------------------+--------------------------------+
| Software Operational State  | Normal                         |
| Upgrade  Operational State  | Idle                           |
+-----------------------------+--------------------------------+
```

```
+----------------- ACTIVE RELEASE INFORMATION -----------------+
|         Parameter           |              Value              |
+-----------------------------+---------------------------------+
| Version                     | 2.3.11                          |
| Build                       | 179                             |
| Build Tag                   | GA                              |
| Build Date                  | 2022-11-09T17:51:43+00:00       |
+-----------------------------+---------------------------------+

+-------- WAVESERVER CONTROL SUBSYSTEM SOFTWARE STATUS --------+
|         Parameter           |              Value              |
+-----------------------------+---------------------------------+
| Boot Zone                   | A                               |
| Last Restart Time           | 2023-03-27T08:20:07+00:00       |
+-----------------------------+---------------------------------+
| Boot Firmware Bank A        | BOOT_ws5cp_807-r0.bin           |
| Boot Firmware Bank B        | BOOT_ws5cp_807-r0.bin           |
| ONIE Bank A                 | ONIE_1083-r0.bin                |
| ONIE Bank B                 | ONIE_1083-r0.bin                |
| FPGA Version                | 85                              |
+-----------------------------+---------------------------------+
+--------------------------+--------+--------------+---------+---------+
| Licensed Feature         | In-Use | Availability | Type    | Status |
+--------------------------+--------+--------------+---------+---------+
| Software Release 2.3.0   | Yes    | Held         | PreAuth | Valid  |
+--------------------------+--------+--------------+---------+---------+
```

1. Downloading the software version to Waveserver-5:
    - **software download url <> login-id <String> password <String>**

    For example: **software download url sftp://X.X.X.X/path/waveserver-x.x.x.xxx.tar.gz login-id userid password my_password**

Note: The target software upgrade file should end with .tar.gz. Software download can take several minutes to complete.

2. To view the status of this process, use the command:
    - software show upgrade-status

3. Activate the upgrade software:
    - software activate version <version> [auto-commit] [delete-from-load]

Note: You can use the auto-commit option to automatically commit the software upgrade. You can also use the delete-from-load option to delete the previous software load after the upgrade software is committed. Waveserver 5 initiates a warm restart. This process can take several minutes to complete.

4. Manually commit the upgrade software:
    - **software commit [delete-from-load]**

Note: The delete-from-load option automatically deletes the previous software load after the upgrade software is committed. The software upgrade process can take several minutes to complete. The upgrade is complete when the Upgrade State is "Commit Complete".

5. To retrieve the software upgrade status, use the command:
    - **software show upgrade-status**

10 Setting Time Manually

For CC-NDcPP compliance, time can be manually set. Ensure that NTP client has been disabled. To set the date and time, use the following commands:

1. Disable NTP
    - **ntp client disable**

2. Set the system date:
    - **system set date <Date: yyyy-mm-dd | yy-mm-dd | mm-dd>**

3. Set the system time, a time offset, and a timestamp:
    - **system set time <Time: hh:mm:ss | hh:mm> time-offset <43200..50400> timestamp <local|UTC>**

Note: The time-offset attribute specifies the offset in seconds from the specified timestamp, that is either local time or UTC (Coordinated Universal Time)

4. Confirm the system time and date:
    - **system show time**
    - **system show date**

5. Save the provisioned setting to the configuration file:
    - **configuration save**

11 Setting Time Using NTP Synchronization

For CC-NDcPP compliance, time can also be synced to NTP servers. NTPv4 is used by default on the device. To enable NTP connections on the Waveserver, use the following commands:

1. Enable NTP
    - **ntp client enable**

2. Add/Remove the NTP Server to Sync to:
    - **ntp client add/remove server X.X.X.X**

3. To enable a secure connection to the NTP server using a SHA1 key, use the following command:
    - **ntp sha1-auth add key-id <id> sha1 <key-value>**
    - **ntp client add server X.X.X.X key-id <id>**

4. To verify the NTP servers enabled:
    - **ntp client show**

5. Confirm the system time and date:
    - **system show time**
    - **system show date**

6. Save the provisioned setting to the configuration file:
    - **configuration save**

Note: The Waveserver device does not accept broadcast and multicast NTP packets by default hence there are no provisioning steps.

12 Automatic Logout due to Session Inactivity

A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local console CLI and remote SSH CLI interfaces. The default value is 10 minutes for the local console CLI and remote SSH CLI interfaces. The configuration of inactivity periods is a global parameter for the chassis and it get applied to all connections. Each connection has its own count down but the timeout

value is global. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.

1. Setting the inactivity period for both local CLI and remote SSH, use the following commands:

- **system server set global-inactivity-timer on**
- **system server set global-inactivity-timeout <# of minutes>**

13 Setting Login Banners

Security Administrators can create a customized login banner that will be displayed at the following interfaces:

- Local console CLI
- Remote SSH CLI

This banner will be displayed prior to allowing Security Administrator access through those interfaces. There are two banners that can be configured: Login Banner and Welcome banner. The Login Banner and Welcome Banner attributes specify the paths and names of the login and welcome banner files, respectively.

13.1 Customizing Login Banners and Messages Using the local CLI and remote SSH Interfaces

Use the following command to configure the Login Banner:

- **system shell set login-banner-file <filename>**

Use the following command to configure the Welcome Banner:

- **system shell set welcome-banner-file <filename>**

Example:

```
WS5_0195# system xftp getfile default-scp-server local-filename welcome
remote-filename /<path>/welcome.txt
WORKING: SCP file transfer in progress
WS5_0195*# system xftp getfile default-scp-server local-filename login
remote-filename login.txt
WORKING: SCP file transfer in progress
WS5_0195*# system shell set login-banner-file /home/su/login WS5_0195*#
system shell set welcome-banner-file /home/su/welcome
```

14 References

- Waveserver 5 Rel 2.3 User Guide (323-3001-100)
- Ciena Waveserver 5 Rel 2.3.12 Security Target v1.5