spectracom

Technical Note: NetClock™ 9483

Compliance to NENA Standard #75-001: Security for Next-Gen 911

Introduction

This technical note documents the compatibility of NetClock® model 9483 master clock with the relevant sections of the National Emergency Number Association's (NENA) Security for Next-Generation 9-1-1 Standard (NG-SEC). This report also applies to the SecureSync® time and frequency reference system as it shares the same software.

This paper also describes the NetClock configuration settings required to meet the relevant NG-SEC requirements.

Requirements

5.7 Safeguarding Electronic Information

5.7	Where Sensitive (Most Sensitive Information) data is allowed to be stored or transmitted on a network between devices, whether inside or outside the NG9-1-1 Entity it must be encrypted.	The only Most Sensitive Information is passwords sent over a network as part of the normal login process. See "Configuring Network Security" section of the SecureSync Manual to configure SecureSync to encrypt such network transactions.
	In NG9-1-1 systems, the encryption algorithm shall be AES.	SecureSync supports SSL and AES encryption algorithms.

5.10 Sensitive Information Destruction & Sanitization

5.10.2	All media types shall have Sensitive information sanitized (rendered irretrievable), in a manner that will prevent misuse or unauthorized disclosure prior to repair, reuse or disposal.	The SecureSync supports clearing configuration to as an aid to removing sensitive data. The only NG-SEC Sensitive information stored by a SecureSync is contained in the CF memory. Contact customer support for instructions on how to open the SecureSync unit and remove the CF as part of repair, reuse or disposal. Note that the media is FLASH based, not magnetic, so magnetic erasing procedures are not effective.

6.4.4 Controlling Points of Access

	All administrative access to any network shall be precisely controlled with appropriate identification, authentication and logging capabilities.	Access to a SecureSync requires authentication and is logged in the Authentication log.

7 Safeguarding Information Assets

7.1.1	All computer resources, systems, applications, and networks, which process Public Safety data, or data of others that Public Safety is obligated to protect, shall positively and uniquely identify and authenticate individual users prior to granting access.	Access to a SecureSync requires authentication.
7.1.2	Personnel performing entity or security administration functions shall be responsible for ensuring that only approved entities are granted use and access to Public Safety's information resources. This requires that the identity of the requestor and of the approver, if required, be validated. This includes requests for password/PIN resets.	The default "admin" account password can be reset from the front panel. To ensure that password is not reset without approval, enable the "Keypad Lock" feature on the Setup / Front Panel web page.

7.1.2.1	Changing Access When a user changes job assignment, including promotion, demotion or termination: 1. The user's manager shall review the users access needs and notify all responsible administrators/help desks of job assignment changes within 24 hours. 2. Administrators or help desks shall delete or disable the IDs, or modify command and data access permissions of users within 24 hours of notification. Where access is no longer required the User ID shall be disabled and ultimately deleted when all use of the account is complete.	Accounts are deleted with the Manage Users tab of the Tools / Users web page.
7.1.4	A failed login attempt shall not identify the reason for the failure to the user, only that the login was incorrect, so as not to aid in subsequent unauthorized attempts to guess the right combination.	The only feedback provided by SecureSync after an incorrect login is "Permission denied".
	System login procedures shall be designed and implemented with a mechanism that will prevent the use of repeated login attempts to guess or otherwise determine a valid login identification and authentication combination. Systems shall lock the user out after no more than 5 failed login attempts.	After 5 unsuccessful login attempts, the SecureSync will lockout the user for a 60 seconds.
7.1.5	Null and factory default credentials shall be changed whenever installing new equipment or software.	There are two default accounts that provide access to a SecureSync. The password for the default "admin" account can be changed. The default "factory" account can be removed from the Security tab of the Tools / Users web page.
	Authentication credentials shall not be visibly displayed when entered on computer screens, and when stored on computers, they shall be encrypted.	Password characters are not displayed when being entered. Passwords are encrypted on the system using the Linux Shadow system.
7.1.5.1	All User Accounts shall require a password.	SecureSync does not allow accounts without passwords.
	Passwords are not based on the user's account name.	If the "Complex Password" feature on the Security tab of the Tools / Users web page is enabled, passwords based on the account name are not allowed.
	Contains characters from three of the following four categories: • Uppercase alphabet characters (A–Z) • Lowercase alphabet characters (a–z) • Arabic numerals (0–9) • Non-alphanumeric characters (for example, !$#,%)	If the "Complex Password" feature on the Security tab of the Tools / Users web page is enabled, passwords must consist of at least one character from each of the three groups.
	Minimum password length The setting determines the minimum number of characters that a user's password must contain. It is recommended that you change this setting from the default value of 0.	SecureSync passwords have a minimum length of 8 characters.
	Minimum password age This setting determines the number of days that must pass before a user can change his or her password.	Minimum password age configured on the on the Security tab of the Tools / Users web page.
	Maximum password age This setting determines the period of time (in days)	The maximum password age can be configured on the Security tab of the Tools / Users web page.

	that a password can be used before the system requires the user to change it.	
	Enforce password history This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be re-used.	SecureSync remembers the previous 10 passwords for a user and does not allow them be reused.

7.1.5.3 Digital Certificates

	Where digital certificates are used for authentication, a revocation process shall exist in case of their compromise.	When a SSL certificate is installed in a SecureSync, the previous certificate is removed.

7.2.1 Least Privilege

	All access to computer resources shall be restricted to only the commands, data and systems necessary to perform authorized functions.	The "user" and "admin" group features of SecureSync allow the roles of users to be limited.
3	All unnecessary services and network services shall be disabled.	See the "Configuring Network Security" section of the SecureSync Manual for instructions on how to disable unnecessary services.
	Any application service which allows the user escape to a shell, provide access to critical system files, or maps/promotes IDs to privileged user levels, shall be disabled.	SecureSync supports a shell-like Command Line Interface (CLI). Linux file permissions are used to limit users to approved actions.
4	Administrators shall ensure that system access controls, e.g., filters that restrict access from only authorized source systems, are used where they exist and shall only contain necessary system authorizations.	Spectracom periodically runs scanning software on a SecureSync unit to identify packages with security issues.
	Using a shared generic Administrator accounts (i.e. the Default Administrator account) shall not be used except during initial installation or under disaster recovery scenarios. Individuals who require Administrative access shall be assigned unique Administrative accounts where operating systems permit.	SecureSync supports a shared default "admin" account, but this account does not have administrative access to the operating system. Individual accounts can be given "admin" (vs. "user") group access, which allows the same level of access as the default "admin" account.

7.2.2 Warning Messages

	A formal statement of resource intent, i.e., a warning notice, shall be made visible to all those who access Public Safety computer resources and private internal networks. … The login Warning notice shall be issued during the logon sequence (either directly before or after the authentication, preferably before, but it shall be displayed before any substantive data). … The Warning message shall remain displayed until positive action by the user is taken to acknowledge the message.	A warning message can be configured using the Banner tab of the Network / General Setup web page. The banner is displayed before the user logs in. The action of logging in removes the warning banner.

7.2.3 Access Control Measures

Access control measures shall be utilized by all computer resources, systems, applications and networks at all times to restrict access to sensitive information or system/network processors to authorized personnel only. Such measures could include the use of system configuration, file system permissions, system rights or access control software, etc. Where possible access control shall be accomplished with "role-based" privileges that assign users to roles and grant access to members of a role rather than to individuals.	The "user" and "admin" group features of SecureSync create two groups of users. Admin group users have full access to all the configurable features of the SecureSync. User group users have read-only access to network and security features, but write access to time and frequency features.

7.2.4 Sensitive File/Resource Access Permissions

Non-privileged users shall not have read/write access to system files or resources such as protected memory, critical devices, executable programs, network configuration data, application file systems, etc. Only users who have administrative responsibilities, e.g., administrators and their designated backups, may be assigned passwords to access and modify these sensitive files/resources.	Admin group users may change the network configuration; however they don't have direct access to the network configuration data. No users have access to protected memory, critical devices, executable programs etc.

7.2.7 Screensavers and Inactive Sessions

Devices not capable of enforcing a password protected screensaver or a keyboard lock, such as dumb terminals, shall have at least one of the following: … 6. Have session inactivity timeouts set for 15 minutes.	SecureSync supports a configurable session timeout administered on the Security tab of the Tools / Users web page.

7.3.3.2 Key Lifecycle Management

Asymmetric keys shall be at least 1024 bits in length. However, this shall be increased to 2048 bits where feasible.	SecureSync supports both 1024 and 2048 key lengths.

7.4.1 Obtaining Files or Software

All files and software shall be obtained from trusted sources, and shall be scanned for viruses and malicious code. Any binary or executable files obtained from un-trusted sources, shall be verified to be free of logic bombs or other malicious code before being used. Freeware, Shareware & Open Source software shall be obtained from a reputable source, e.g. Public Software Library (PSL).	All third party packages used in SecureSync are obtained from reputable sources. All packages are obtained as source code, none are obtained as binaries or executable files.

USA | 1565 Jefferson Road, Suite 460 | Rochester, NY 14623 | +1.585.321.5800 | sales@spectracomcorp.com
FRANCE | 3 Avenue du Canada | 91974 Les Ulis, Cedex | +33 (0)1 64 53 39 80 | sales@spectracom.fr
UK | 6A Beechwood | Chineham Park | Basingstoke, Hants, RG24 8WA | +44 (0)1256 303630 | info@spectracom.co.uk
BRAZIL | Rua Jose Alves dos Santos | Sao Jose dos Campos | SP – Brazil 12230-081 | +55 12 3933 2330 | sales@spectracomcorp.com