orolia

The Global Leader in Resilient PNT

Tech Tip: SecureSync 1200 Security Hardening Recommendations

Feature	Default Setting	Recommended Setting	Where to Configure	Online Manual Links
HTTP	Enabled	Disabled	Web UI or CLI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_NetwServic.htm
HTTPS	Enabled (It is recommended that you consult your Certificate Authority for the required fields in an X 509-Certificate request. Orolia recommends all fields be filled out and match the information given to your Certificate Authority.)		Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_Config.htm?Highlight=https
SNMP	Enabled	Engine Id must be a hexadecimal number at least 10 digits long (such as 0x123456789A). The Id originates from the MIB Browser/SNMP Manager.	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Intro.htm http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_V3.htm
NTP	Enabled (with no MD5 values entered)	Enabled (use MD5 authentication with user-defined keys)	Web UI	http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/ConfNTPsymmKeys.htm
Command Line Interface				
Serial Port	Available	Available	N/A	
Telnet	Enabled	Disabled (use SSH instead)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_NetwServic.htm
SSH	Enabled (default private keys provided)	Enabled	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm
File Transfer				
FTP	Enabled	Disable (use SFTP or SCP)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_NetwServic.htm
SCP	Available	Disable (use SFTP or SCP)	Web UI	
SFTP	Available	Disable (use SFTP or SCP)	Web UI	
Managing User and Security				
Password Security	Default (minimum length 8)	Change to meet organizational requirements.	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Passwords.htm
LDAP	Available	LDAP utilizing a certificate between the server and client is more secure.	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/LDAP_Authentication.htm
RADIUS	Available	Configure for off box authentication (encrypts password only)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/RADIUS_Auth.htm
TACACS+	Available	Configure for off box authentication (encrypts full content of each packet)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm
Password Policy	Available	- Configure to Security Policy - Change spadmin password (up to 32 character)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Passwords.htm
Network Access Control				
Access Control	Available	Use as needed to limit network/node access	Web UI	http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_AccsRestrict.htm
Login Banner	Available	Recommended	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Banner.htm
Symmetric Keys	Available	Recommended between stratums1 and stratum2 servers	Web UI	http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/ConfNTPautokey.htm
NTP Access Restrictions	Available (unrestricted)	Configured for end to end encryption (no authentication) between stratum1 and stratum2 servers	Web UI	http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_AccsRestrict.htm

Autokey	Available in some early S/W versions	Not recommended, NTP is deprecating this feature in the future	Web UI	http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/ConfNTPautokey.htm
Web Interface Settings	- Default (Timeout 60 minutes) - Set to medium (TLSv1, TLSv1.1, TLS1.2 are enabled)	Enable high security as needed	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/HTTPSsecurityLevel.htm
Physical Security				
Sanitizing	Available	Available (as needed)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Sanitizing.htm
Keypad Lock Out	Unlocked	Lock as required	Front Panel	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INSTALL/Keypad_Usage.htm

AAA Feature on SecureSync

Note: Recommend customer to utilize Authentication Authorization and Accounting (AAA) security framework to enhance security around SecureSync in production.

Note: Utilize TACACS/LDAP/RADIUS for centralized authentication.

Note: Customer can setup users/group with different privilege level and grant access to system based on user or admin role. Customer can integrate such authorization feature with centralize server like AD and LDAP.

Note: Customer can configure SecureSync to send all the logs in real-time to remote log server.

Note: Customer can also configure SNMP setting to send alerts to a SNMP Servers.

IPtables

Note: IPtables is supported in SecureSync, customer should utilize iptables in SecureSync as last resort of firewall - to protect unwanted and unauthorized access to devices from unknown system and network.

Tech Tip: SecureSync 2400 Security Hardening Recommendations

Feature	Default Setting	Recommended Setting	Where to Configure	Online Manual Links
HTTP	Enabled	Disabled	Web UI or CLI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/SETUP/NCSS_NetwServic.htm
HTTPS	Enabled (It is recommended that you consult your Certificate Authority for the required fields in an X 509-Certificate request. Orolia recommends all fields be filled out and match the information given to your Certificate Authority.)		Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/ADMIN/HTTPSsecurityLevel.htm
SNMP	Enabled	Engine Id must be a hexadecimal number at least 10 digits long (such as 0x123456789A). The Id originates from the MIB Browser/SNMP Manager.	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Intro.htm#Conf_SNMP_StatusSettings http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Traps.htm
NTP	Enabled (with no MD5 values entered)	Enabled (use MD5 authentication with user-defined keys)	Web UI	http://manuals.spectracom.com/2400/Content/_Global/Topics/NTP/ConfNTPsymmKeys.htm
Command Line Interface				
Serial Port	Available	Available	N/A	
Telnet	Disabled	Disabled (use SSH instead)	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Specs_Protocols.htm?Highlight=telnet
SSH	Enabled (default private keys provided)	Enabled	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm?Highlight=ssh
File Transfer				
FTP	Enabled	Disable (use SFTP or SCP)	Web UI	http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_NetwServic.htm
SCP	Available	Disable (use SFTP or SCP)	Web UI	
SFTP	Available	Disable (use SFTP or SCP)	Web UI	
Managing User and Security				
Password Security	Default (minimum length 8)	- Change to meet organizational requirements. - Configure to Security Policy - Change spadmin password (up to 32 character)	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/ADMIN/Passwords.htm?Highlight=password
LDAP	Available	LDAP utilizing a certificate between the server and client is more secure.	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/CONFIG/LDAP_Authentication2.htm
RADIUS	Available	Configure for off box authentication (encrypts password only)	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/ADMIN/RADIUS_Auth.htm?Highlight=http
TACACS+	Available	Configure for off box authentication (encrypts full content of each packet)	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm?Highlight=http
Network Access Control				
Access Control	Available	Use as needed to limit network/node access	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/SETUP/AccessRules.htm?Highlight=Access%20Control
Login Banner	Available	Recommended	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/CONFIG/Banner.htm?Highlight=Telnet
Symmetric Keys	Available	Recommended between stratums1 and stratum2 servers	Web UI	http://manuals.spectracom.com/2400/Content/_Global/Topics/NTP/ConfNTPsymmKeys.htm?Highlight=Symmetric%20Keys

NTP Access Restrictions	Available (unrestricted)	Configured for end to end encryption (no authentication) between stratum1 and stratum2 servers	Web UI	http://manuals.spectracom.com/2400/Content/_Global/Topics/NTP/NTP_AccsRestrict.htm?Highlight=NTP%20Access%20Restrictions
Web Interface Settings	- Default (Timeout 60 minutes) - Set to medium (TLSv1, TLSv1.1, TLS1.2 are enabled)	Enable high security as needed	Web UI	http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/OPRTN/UItimeout.htm?Highlight=UI%20Timeout
Physical Security				
Sanitizing	Available	Available (as needed)	Web UI	http://manuals.spectracom.com/2400/Content/_Global/Topics/GNSS/GNSS_recPosDel.htm?Highlight=Sanitizing
Keypad Lock Out	Unlocked	Lock as required	Front Panel	http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Front_Panel_Config.htm?Highlight=lock

Note: Utilize TACACS/LDAP/RADIUS for centralized authentication.

Note: Customer can setup users/group with different privilege level and grant access to system based on user or admin role. Customer can integrate such authorization feature with centralize server like AD and LDAP.

Note: Customer can configure SecureSync to send all the logs in real-time to remote log server.

Note: Customer can also configure SNMP setting to send alerts to a SNMP Servers.

IPtables

Note: IPtables is supported in SecureSync, customer should utilize iptables in SecureSync as last resort of firewall - to protect unwanted and unauthorized access to devices from unknown system and network. Iptables is always ON, and its policies can only be accessed via the Command Line Interface (see CLI Commands) in combination with the Sudo command.

04 October, 2021. Tech Tip SS 1200, SS 2400
Specifications subject to change or improvement without notice