spectracom

Technical Note: SecureSync™

NERC CIP-007 Security Report

Introduction

This technical note documents the compatibility of SecureSync with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) "CIP-007 Standard Cyber Security – Systems Security Management".

This paper also describes the SecureSync configuration settings required to meet the CIP-007 requirement.

Requirements

R1 - Test Procedures

R1	The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	The SecureSync software is regularly updated with security patches and upgrades.
R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R1.3	The Responsible Entity shall document test results.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.

R2 - Ports and Services

R2	The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	SecureSync can be configured to disable features not required by the customer. See specific features below.
R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	See "Configuring Network Security" section of the SecureSync Manual.
R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	See "Configuring Network Security" section of the SecureSync Manual.
R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.

R3 - Security Patch Management

R3	The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for	Spectracom periodically runs scanning software on a SecureSync unit to identify packages with security issues. Required fixes are incorporated into regular SecureSync software updates.

	tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	
R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	A security scan is run at least once a month.
R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Customers are not provided with individual patches, rather security patches are incorporated into SecureSync releases and documented in the release notes.

R4 - Malicious Software Prevention

R4	The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	A SecureSync can only run SecureSync software, so there is no opportunity for the customer to introduce malicious software.
R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Linux uses a system of access restrictions, rather than anti-virus scanning software. The current standard approach for Linux servers is to not incorporate anti-virus software, particularly because no large scale Linux viruses are known to exist.
R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	SecureSync does not use a signature based security system. (See above)

R5 - Account Management

R5	The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	All access to SecureSync requires authentication.
R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	SecureSync supports two levels of accounts, users and administrator. See the "User Accounts" section of the SecureSync manual.
R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	The SecureSync Authentication log shows which users accessed the unit. Changes to the configuration are documented in the Journal log.
R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	The current set of user accounts on the SecureSync is shown in the "Manage User Accounts" tab of the **Tools / Users** web page.
R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator,	The "user" and admin group features of SecureSync allow the roles of user accounts to be

	shared, and other generic account privileges including factory default accounts.	limited.
R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	There are two default accounts that provide access to a SecureSync. The password for the default "spadmin" account can be changed. The default "spfactory" account can be removed from the security tab of the **Tools / Users** web page.
R5.2.2	The Responsible Entity shall identify those individuals with access to shared accounts.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	The SecureSync Authentication log shows access activity from all accounts, including shared accounts. Accounts can be secured by changing passwords or removing the account from the "Manage Users" tab of the **Tools / Users** web page.
R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	All SecureSync accounts must have passwords.
R5.3.1	Each password shall be a minimum of six characters.	The SecureSync software rejects passwords less than 8 characters.
R5.3.2	Each password shall consist of a combination of alpha, numeric, and "special" characters.	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 all three groups.
R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	The "Password Aging" feature on the Security tab of the **Tools / Users** web page supports forcing the user to change their password after a set time period.

R6 - Security Status Monitoring

R6	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	The SecureSync Authentication log shows which users accessed the unit as well as unsuccessful attempts to access the system.
R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	Manual alerts are possible by monitoring the Authentication log. The Authentication log events can also be echoed to a remote machine using syslog. A system where unexpected activity in the logs would generate an alert could be implemented by the customer.
R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	The SecureSync will store up to 375 Kilobytes of log events for each log. Logs can be manually moved off the unit for long term storage, or can be automatically collected on a remote computer using syslog.
R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	Since the SecureSync stores logs by size, rather than time period, the customer will need to

		transfer the logs off the unit using the methods described above to guarantee ninety days of logs are preserved.
R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	Logs can be viewed using the web interface, or using any the tools of their choice, if the logs are archived off the SecureSync unit.

R7 - Disposal or Redeployment

R7	The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Although this is primarily a customer requirement, the SecureSync has features to aid in preserving security after disposal.
R7.1	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	The SecureSync supports clearing configuration as an aid to removing sensitive data.
R7.2	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	Unlike magnetic hard drives, SecureSyncs use solid state memory drives that do not preserve erased data. If clearing configuration is not considered sufficient, contact Spectracom customer support for instruction on how to remove the CF storage and the GPS receiver.
R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.

R8 - Cyber Vulnerability Assessment

R8	The Responsible Entity shall perform a cyber-vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	These requirements apply to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.
R8.1	A document identifying the vulnerability assessment process	
R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled	
R8.3	A review of controls for default accounts	
R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	

R9- Documentation Review and Maintenance

R9	The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	The requirement applies to procedures or documentation of the Responsible Entity and not directly to the SecureSync device.

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