SyncServer® Time Server Security

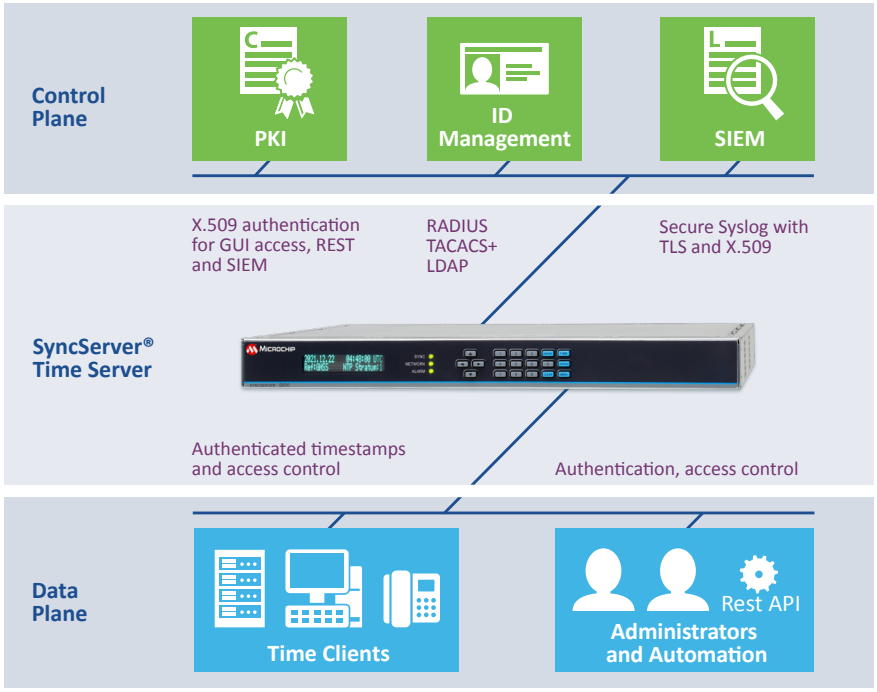
The SyncServer® S600/S650 network time server provides the comprehensive and robust security features that network security professionals expect.

Summary

Corporate and defense department network security professionals place their trust in the security-hardened SyncServer® network time server. We continually harden the SyncServer time server to stringent internal requirements, perform security scans, incorporate requested network security features and respond to any findings from robust penetration tests performed by customers. The result is a security-hardened time server that interoperates effectively with existing network security infrastructure, as well as offers a long list of security features available to the user to custom configure the SyncServer security for their network and security policies.

Key Features

- Most secure network time server
- Authenticated timestamps
- Secure syslog
- X.509 certificates/PKI
- RADIUS/TACACS+/LDAP
- Secure NTP Reflector with DoS protection
- Packet-limiting protections
- Hardened user interface
- Time source validation
- Network segmentation support
- Per-port access control
- REST API with TLS 1.3



The first line of defense in the SyncServer® S600 time server is port-by-port LAN access control lists which support the physical and logical micro-segmentation of the network. To support segmented perimeters, four to six isolated LAN ports provide NTP/PTP timing services to different network segments. There is no cross traffic between ports; each port has access control lists, and all ports can have unique network configurations. Management access is strictly limited to a single LAN port for further isolation from the network.

Protocols such as RADIUS, TACACS+, LDAP provide the robust authentication and authorization needed for access. The feature-rich web GUI is further hardened with X.509 CA-signed certificates coupled with very secure TLS 1.3 based encryption of the link. At the most basic level, NTP symmetric key authentication ensures NTP time packets are not altered in transit.

The SyncServer monitors and validates GNSS signals continuously with embedded BlueSky™ technology jamming and spoofing detection and protection capabilities.

For DoS attack protection, unique NTP Reflector technology provides line-speed, high-capacity NTP service with packet limiters to prevent host CPU overrun. At no time is there ever a risk that a DoS load will fault the CPU.

For network monitoring, logs can be sent via secure syslog that incorporates X.509 CA-signed certificates and peer verification. This syslog data is sent via TLS to prevent log file tampering or eavesdropping.

Internally, the SyncServer time server's system software is a tailored, hardened, current and embedded Linux® distribution that only includes what is needed to operate the custom hardware. This greatly decreases any potential attack surface to CVEs found in a broad Linux distribution.

SyncServer S600/S650 Time Server Trusted Time Security Check List for Zero Trust Architectures

USERS	1. RADIUS authentication (user-configurable IP port numbers from 1024 to 49151)
	2. TACACS+ authentication (user-configurable IP port numbers from 1024 to 49151, as well as standard port 49)
	3. LDAP authentication (bindings for ports, LDAP v2 or LDAPv3, up to five LDAP servers)
	4. REST API (user/password authentication on every call or token based with expiration)
	5. Administrative Security a. Web session timeouts (5/10/15/30/60 minutes) b. Lockout for failed login attempts (enable/disable), three to six failed login attempts allowed c. Login banners (standard US Government, custom banner)
	6. User Settings a. Passwords: 6 to 100 characters, mixed case, letters, numbers, special b. Password expiration: enable/disable, user set number of days c. User creation/deletion: username, password, recovery question, email
	7. SSH (allowed/denied users)
DEVICES	8. NTPd Symmetric Keys a. Generate/download/upload symmetric security keys b. SHA1/256/512 and MD5 keys
	9. NTPd Autokey Server (IFF identity scheme)
	10. NTPd Autokey Client (IFF identity scheme)
	11. HTTPS Secure Management a. Protocols: TLS 1.2 and 1.3 b. Cipher suites: SSL_High_Encryption; SSL_High_Medium_Encryption c. Session timeout: 5 to1440 minutes d. Self-signed certificate: 2048 or 4096 RSA key bits; expiration days 1–1825; customizable locality codes e. Content Security Policy (CSP) headers
	12. X.509 Cert/CSR (create and download Certificate Signing Requests (CSRs), 2048 or 4096 RSA key bits)
	13. X.509 Install (install multiple CA-signed X.509 certificates)
	14. X.509 Mapping a. Map X.509 CA-signed certificate(s) to HTTPS and/or syslogs b. Same or different X.509 CA-signed certificates for HTTPS and/or syslog
	15. X.509 Certificate Authorities (or Trusted CA Certificate Store) a. Install proprietary CA certificates b. Extensive system-default CA certificates included
	16. Software Upgrades a. System software only available from Microchip customer portal b. Requires authenticated user to access on Microchip customer portal c. Requires authorization to download the system software file and serialized authorization file d. System software images are encrypted e. All downloads include an MD5 and SHA hash to cross check for file alteration f. Software cannot be installed unless accompanied by the correct, serialized authorization file from Microchip
	17. Alarms (extensive user-configurable alarms, notification via trap, logs, email, hardware relay)
	18. Timing Security a. BlueSky™ technology GNSS jamming, spoofing detection and protection b. Alternative time sources (NTP, PTP, IRIG) c. Anti-Jam GNSS antenna d. Atomic clock upgrades for timing holdover
NETWORK	19. Access Control Lists (unique IPv4 and IPv6 access control lists per LAN port, 8–12 lists total)
	20. Service/System Control (enable/disable HTTPS, SNMP, SSH, ToD, Telnet)
	21. Packet Monitoring a. DoS/DDoS protection by hardware-based throttling of packets to the CPU b. Packet throttling on a LAN-port-by-LAN-port basis c. Customizable packet receipt alarm thresholds for each LAN port
	22. Multiple LAN Ports for Network-Segmentation a. Management/timing available on LAN1 only b. LAN2–LAN6 timing only, no management possible
ANALYTICS	23. Secure Syslog a. X.509 authentication b. TLS security c. Peer verify d. User-configurable port numbers
	24. SNMPv3 a. Authentication cryptography: MD5, SHA1/224/256/384/512 b. Privacy cryptography: AES/128/192/256

DS00005424A

MICROCHIP