Server Technology, Inc.   Technical Note

PDU Security

Purpose

This Technical Note provides a quick reference for access paths to Server Technology's Power Distribution Unit (PDU) products, shows if the access path is secure, and if so, provides an overview of how the security works.

The document covers security for access paths to PDUs but security of the data center and physical access to the PDUs are not covered in this document.

Note: This document includes PDU security for both PRO1/PRO2 products (using firmware version 8.0 and later), and CDU1 products (using firmware version 7.0 and later).

Security of PDU Access Paths

Access paths to the PDU and the related security methods for those paths are provided for reference in the two tables in this document: **Table A: Server Protocol Security** and **Table B: Client Feature Security**.

Additional reference information specific to the server protocols and client features are also provided in this document, such as specifications, session-connection information, and cryptography ciphers.

Secure Hardware Communication Paths

Two physical connections allow access to the PDU via hardware communication paths:

- RS-232 serial port console or modem – secured login procedure with credentials (name and password).

- Ethernet via various network protocols, for example, HTTP/S, SSH, FTP, SFTP, SNMP, Telnet, etc. (as listed in Table A: Server Protocol Security below) – a secured login procedure with credentials (name and password), including strong password enabling. Some network protocols are secure, while others are not.

Table A: Server Protocol Security

For the protocol access paths listed in the following table, the firmware actively listens on server ports to provide security for the PDU.

Access Path to CDU	Secure?	How does it work?
HTTPS (SSL/TLS 1.2)	Yes	Provides a secure connection on default port 443 or user-configured port (secure Web).
SNMPv3	Yes	Version 3 adds security to previous SNMP versions, such as security with a special key for both read-only and read-write username, authentication type/password, and privacy type/password; only the intended IP address can receive traps; supported and implemented per IETF RFC standards.
SSHv2	Yes	Requires login credentials with password and keyboard interaction – two ways to collect credentials.
SSL/TLS 1.2	Yes	Built with Open SSL v1.0.2e, SSL/TLS 1.2 enables secure Web sessions between a PDU and a remote user; SSL provides security with authentication (connecting client is assured of the server's identity) and encryption (transmitted data between client and server is encrypted).
Serial Command Protocol (SCP)	Yes	Server Technology's proprietary protocol; a login procedure with username/password is supported, but the authentication must be enabled and used to ensure security.
SNAP	Yes	Uses Sentry Power Manager (SPM) Secure Access with encryption over SSL/TLS 1.2.
FTP	No	Login credentials are required but cross-transmission over the

Access Path to CDU	Secure?	How does it work?
		network is not secure; the protocol can be disabled to remove security risks.
SFTP	Yes	Secure File Transport Protocol. Login credentials are required and cross-transmission over the network is secure over an encrypted SSH transport.
Telnet	No	Login credentials are required but cross-transmission over the network is not secure; the protocol can be disabled to remove security risks.
HTTP	No	Password is encoded but username is not.
SNMPv1/v2c	No	SNMPv1 has well-known limited security; SNMPv1/v2c community strings are sent in clear text over the network; SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
Serial Port – Command Line Interface (CLI)	No	Requires physical access to the PDU.

Table B: Client Feature Security

For the client access paths listed in the following table, the Sentry firmware gathers user credentials and transmits them to the server to provide validation and security for the PDU over the network.

Access Path to CDU	Secure?	How does it work?
Cisco EnergyWise Network™	Yes	Uses a shared secret with encryption over SSL.
Email	Yes	SMTP authentication is supported; if enabled, authenticates with the server but does not encrypt the content.
LDAPS	Yes	Built-in security procedures to use LDAP over SSL/TLS 1.2.to encrypt the connection between the client and the LDAP server for all LDAP communication, as supported by IETF RFC standards. **Note:** The LDAP server must support TLS 1.2, as earlier versions of TLS will not be supported.
LDAPv3	Yes	Allows for centralized username/password management on a networked directory server instead of locally on each PDU. Provides three security methods: • Digest-MD5: The SASL authentication mechanism is required for LDAPv3 and is based on a secret known both by the client and the server, allowing for challenge-response. • SSL/TLS 1.2: The encryption and authentication method uses TLS 1.2, requiring proof of server identity and protection of data in transit. Same as LDAP over SSL (LDAPS). • Simple Bind Request: Allows the client to authenticate to the server. **Note:** The LDAP server must support TLS 1.2, as earlier versions of TLS will not be supported.
RADIUS	Yes	Uses a shared secret to authenticate communication between the RADIUS server and the client; encryption is supported and implemented per IETF RFC standards; extended security with proprietary vendor-specific attributes (VSA) provided by Server Technology.
Syslog	Yes	Provides an audit trail; PDUs also support logging of actions and audit trails (buffer stores about 4K of most recent log entries in round-robin fashion); Local log can be sent to Syslog servers; Although audit trails are local, they are permanently stored by Syslog servers.
TACACS+	Yes	Enables authentication with a central TACACS+ server, per IETF RFC standards; encryption key encodes all data packets between the PDU and the TACACS+ server.

Reset and Remote Shutdown Security

The firmware offers two additional security points:

- A configuration reset feature allows pressing a button on the PDU to reset administrator-edited configuration settings back to factory defaults, including user accounts. This pushbutton reset feature can be disabled, which may be desired in environments where the PDU is not physically secure.

- For the Remote Shutdown feature on Switched PDU products, security is provided by an encrypted key that cannot be edited.

Secure Server Protocols

HTTPS

Specifications:

- Secure HTTP over-SSL Web Interface Protocol

- Secure Sockets Layer (SSL)

- Transport Layer Security (TLS), version 1.2 (RFC 5246)

- SSL/TLS 1.2-enabled HTTPS Server (RFC 2818)

- Self-Signed X.509 Certificate, version 3 (RFC 2459)
  Note: Self-signed certificate has a 2048-bit key size and uses a SHA256 signature algorithm.
- Asymmetric Cryptography: 1024-bit RSA Key Exchange

Web Browsers Supported:

A modern web browser with TLS 1.2 support is required. Current versions of IE, Firefox, Chrome, Opera, and Safari have been tested and are supported.

Sessions and Connections:

With HTTPS (SSL/TLS 1.2), the maximum number of simultaneous user sessions is four. SSL is enabled by default, but can be disabled if desired.

By default SSL connections are optional, meaning both insecure HTTP (http://) and secure HTTPS (https://) connections can be established.

SSL connections can be configured to be required, such that only secure HTTPS connections can be established (not the HTTP connections).

Symmetric Cryptography Ciphers:

For firmware version 8.0g, or later:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA – Default
- TLS_RSA_WITH_AES_128_CBC_SHA

For firmware version 7.1a:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

SNMPv1/v2c

Specifications:

SNMP allows network management systems to use SNMP requests to retrieve information and control power for individual outlets. The PDU products include an SNMP v2c agent supporting standard MIB 1 and MIB 2 objects. A private enterprise MIB extension (Sentry3 MIB) is also supported to provide remote power control, monitoring, and limited configuration.

The PDU products support SNMP source IP Restriction for SNMP manager Get and Set requests to only be allowed from the IP addresses of the defined trap destinations.

A blank read/write community string is allowed to make all SNMP actions read-only.

SNMP supports one session; however, SNMP can accept an indefinite number of SNMP requests in the queue FIFO-style, and traps can be sent to two trap destinations.

Notes for SNMPv1/v2c/v3:

- SNMPv1/v2c: no security; community strings are sent in clear text over the network. SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
- SNMPv1/v2c and SNMPv3 can be enabled or disabled independently; this means having SNMPv1/v2c and/or SNMPv3, or none.

SNMPv3

Per-User Authentication and Encryption:

SNMP version 3 supports authentication and encryption on a per-user basis. Authentication types are None and MD5. Encryption types are None and DES.

If authentication is used, encryption must be used. Encryption with SNMPv3 is supported and implemented per IETF RFC standards.

Two SNMPv3 users are supported: one user with read-write (RW) access, and one user with read-only (RO) access. Both users have the same configuration parameters, and each user can be configured independently.

Notes for SNMPv1/v2c:

- SNMPv1/v2c: no security; community strings are sent in clear text over the network. SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
- SNMPv1/v2c can be enabled or disabled independently; this means having SNMPv1 and or SNMPv2, or none.

SSHv2

Supported with terminal emulation and SSHv2 server standard.

Authentication:

Username/Password: Entry is by the 'Password' or 'Keyboard-interactive' SSH methods.

Asymmetric Cryptography Ciphers:

Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification.

Message Integrity:

- HMAC-SHA1-160
- HMAC-MD5-128

Symmetric Cryptography Ciphers:

- AES256-CBC
- RIJNDAEL192-CBC
- 3DES-192-CBC
- RIJNDAEL256-CBC
- AES128-CBC
- AES192-CBC
- RIJNDAEL128-CBC

Sessions:

Up to four simultaneous SSH user sessions are supported. These four sessions are also used by Telnet connections.

Port Numbers:

The SSH port number defaults to 22 (the IANA assigned number) but may be changed if desired.

SSL/TLS 1.2

Specifications:

- Transport Layer Security (TLS) version 1.2 (RFC 5246).
- SSL/TLS 1.2 build with OpenSSL v1.0.2.
- SSL/TLS 1.2-enabled HTTPS server (RFC 2818)
- Self-Signed X.509 Certificate version 3 (RFC 2459)
  Note: Self-signed certificate has a 2048-bit key size and uses a SHA256 signature algorithm.

Web Browsers Supported:

A modern web browser with TLS 1.2 support is required. Current versions of IE, Firefox, Chrome, Opera, and Safari have been tested and are supported.

Asymmetric Cryptography Ciphers:

- Up to 4096-bit RSA Key Exchange

Symmetric Cryptography Ciphers:

Both use HMAC-SHA-1 as the Message Authentication Code algorithm:

- TLS_RSA_WITH_AES_128_CBC_SHA (128-bit)
- TLS_RSA_WITH_AES_256_CBC_SHA (256-bit) – Default

For firmware version 8.0g, or later:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA – Default
- TLS_RSA_WITH_AES_128_CBC_SHA

For firmware version 7.1a:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

Secure Client Features

Cisco EnergyWise Network^{TM}

This network feature uses a shared secret with encryption over SSL.

Email

The Email client in the PDU supports transmission of log entries and alerts. SMTP authentication is supported, if enabled.

LDAPS

Specifications:

- Secure Sockets Layer (SSL)

- Transport Layer Security (TLS), version 1.2 (RFC 5246)

- X.509 version 3 (RFC 2459) server certificates with RSA key sizes up to 4,096 bits

Note: The LDAP server must support TLS 1.2, as earlier versions of TLS will not be supported.

Server-Client Certificates:

Server certificates are accepted and used dynamically. A NULL client certificate is sent to the server if a client certificate is requested. Both 2048-bit and 4096-bit RSA keys are supported.

LDAPv3

Allows for centralized username/password management on a networked directory server instead of locally on each PDU. Provides three security methods:

- Digest-MD5: The SASL authentication mechanism is required for LDAPv3 and is based on a secret known both by the client and the server, allowing for challenge-response.

- SSL/TLS 1.2: The encryption and authentication method uses TLS 1.2, requiring proof of server identity and protecting of data in transit. Same as LDAP over SSL (LDAPS).

- Simple Bind Request: is sent in clear text over the network.

Note: The LDAP server must support TLS 1.2, as earlier versions of TLS will not be supported.

RADIUS

Centralized Network Protocol:

The RADIUS protocol is supported to provide a high-performance, centralized network protocol that enables remote authentication and authorization, such as usernames and passwords.

Extended Authentication Process:

In addition to the protocol-required attributes, the RADIUS authentication process can be extended by using private vendor-specific attributes (VSA). This extension allows Server Technology to create its own proprietary attributes to support features and services using the PDU in the RADIUS authentication process.

Vendor-Specific Attributes (VSA):

Server Technology has defined and formatted the Vendor-Specific Attributes (VSA) for RADIUS in the **dictionary.sti** file, which is available from Server Technology.

The PDU is configured to recognize and use the configuration values in the **dictionary.sti** file, as specified by the network administrator. The values indicate to the RADIUS server that the defined attributes are based on the unique enterprise vendor code of Server Technology, supporting several VSAs.

SNAP

Uses Sentry Power Manager (SPM) Secure Access with encryption over SSL/TLS 1.2.

Syslog

Provides an audit trail; PDUs also support logging of actions and audit trails (buffer stores about 4K of most recent log entries in round-robin fashion); Local log can be sent to Syslog servers; Although audit trails are local, they are permanently stored by Syslog servers.

TACACS+

The TACACS+ protocol enables authentication and authorization with a central TACACS+ server.

User Accounts:

User accounts do not need to be individually created locally on each PDU. Administrators can pre-define and configure (in each PDU and in the TACACS+ server) a set of necessary TACACS+ privilege levels and user access rights for each level. There are 16 privilege levels (0-15).

User access rights can then be granted or denied by making the user a member of one or more pre-defined TACACS+ privilege levels. User account rights can be added, deleted, or changed within TACACS+ without any changes needed on individual PDU products.

Usernames and Passwords

Default Administrative User Account: admn

Server Technology PDUs have one pre-defined administrative user account: username is **admn**; password is **admn**.

Notes:

- There is no "i" in the **admn** username or password.
- For security, Server Technology recommends creating a new user account, granting administrative rights to the new user account, and then removing the default **admn** account.

Only an administrative-level user can perform operations such as creating/removing user accounts and command rights, changing passwords, and displaying user information. An administrator can also view the status of all sensors and power inputs.

Administrative account usernames and passwords can be changed by an administrator. Multiple administrative users are supported.

Username Restrictions:

Usernames must be 1-16 characters in length, spaces are **not** allowed; usernames are **not** case-sensitive.

Password Restrictions:

Passwords must be 1-16 characters in length, spaces are allowed; passwords are case-sensitive.

PDU Access with User Accounts:

The maximum number of locally-stored and defined user accounts supported in the PDU is 112. These accounts are either local user accounts or local LDAP user groups.

User Access Levels

In addition to security over the access paths to the PDU with user authentication, Sentry firmware provides user access levels to PDU features for further restriction over outlets, outlet groups, ports, LDAP, RADIUS, and more.

The administrator can assign one of the following system access levels to a user account:

User Access Level	Description
Admin (administrator)	Full-access for all configuration, control (On, Off, Reboot), status, and serial/pass-thru ports.
Power User	Full-access for all control (On, Off, Reboot), status, and serial/pass-thru ports.
User	Partial-access for control (On, Off, Reboot); status; and pass-thru of <u>assigned</u> outlets, groups, and serial/Pass-thru ports. Has admin-defined access list for outlets and outlet groups.
Reboot-Only	Partial-access for control (Reboot); status, and pass-thru of <u>assigned</u> outlets, groups, and serial/pass-thru ports. Has admin-defined access list for outlets and outlet groups.
On-Only	Partial-access for control (On); status; and pass-thru of <u>assigned</u> outlets, groups, and serial/pass-thru ports. Has admin-defined access list for outlets and outlet groups.
View-Only	Partial-access for status and pass-thru of <u>assigned</u> outlets, groups, and serial/pass-thru ports. Has admin-defined access list for outlets and outlet groups.

Note: For security, Server Technology recommends that the administrator creates a new user account first, assigns administrative rights to the new user, and then removes the default **admn** user account.

Using Strong Passwords

The firmware supports strong passwords for enhanced security. When enabled, a new strong password must be 8-16 characters long with at least one uppercase letter, one lowercase letter, one number, and one special character.

Examples of acceptable strong passwords:

    n0tOnmyw@tch
    john2STI?
    H3reUgo!

Notes:

- The use of strong passwords applies only to local access and authentication – remote authentication. Strong passwords are stored in the user account and are not available for remote access.

- Strong passwords require a minimum change of four characters when defining a new strong password.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.

1040 Sandhill Drive	Tel: 1-800-835-1515	Web:	www.servertech.com
Reno, Nevada 89521 USA	Fax: 775-284-2065	Email:	support@servertech.com