

## Sentry Security Features

This Technical Note provides an overview of the security features of Server Technology’s Sentry products using firmware versions 5.3x and later.

### Product Overview

The Sentry products provide the capability to control and/or monitor cabinet power remotely for a data center or remote branch office. Sentry products combine remote configuration and management with power distribution and power/environmental monitoring. Available features include the rebooting of a single or dual power server with one command, the receiving of SNMP alerts when power or environmental conditions exceed thresholds, and the assignment of specific access rights to designated user groups or individuals.

The Sentry product line provides the flexibility needed for data centers and remote sites, as well as power requirements for high-amperage, high voltage, UL 60950-1 Branch Circuit Protection, and SNMP traps with current monitoring.

Additional Features:

- Easy to use secure, integral, web-based GUI configuration and control tool.
- Temperature support (Celsius or Fahrenheit).
- Logging of all authentications, configuration changes, and system events.
- Syslog logging protocol support.
- Email notifications for multiple users of log, event, authorization, power, and configuration messages.
- Automatic firmware updates by FTP server.
- Strong password support and pre-login banner.
- Ability to ping an IP address to determine if the device is working properly.
- Grouping of outlets across multiple Sentry products.
- SNMP traps based on status, changes, load, temperature, and humidity.
- Supports 128 user accounts, 22 simultaneous logins, and a dedicated SNMP connection.

The following server protocols and features may be enabled or disabled:

Protocol	Default State
FTP	Enabled
HTTP (Basic and MD5 message-digest)	Enabled
HTTPS (SSLv3/TLSv1)	Enabled but not required
Serial Port – Command Line Interface	Enabled
SNMPv2	Disabled
SSHv2	Enabled
Telnet	Enabled

The following client protocols and features may be enabled or disabled:

Protocol	Default State
Automatic Updates by FTP Client	Disabled
DHCP	Enabled
Email	Disabled
LDAPS	Disabled
LDAPv3	Disabled
SNTP	Disabled
Syslog	Disabled
TACACS+	Disabled

The following non-protocol features may be enabled or disabled:

Protocol	Default State
Strong Password Enforcement	Disabled

## ***Protocol/Feature Definitions and Specifications***

### **Console/RS-232, RJ45**

Sentry products are equipped with an RJ45 Serial RS-232 port for attachment to a PC, networked terminal server, or console using the supplied RJ45 to RJ45 crossover cable and RJ45 to DB9F serial port adapter as required. Refer to the appropriate product instruction manual for more information. The console interface supports only one session at a time.

### **DHCP**

DHCP is enabled by default and is used for the automatic retrieval of the IP address setting from a networked DHCP server.

### **Email**

The Email client in the Sentry product supports transmission of SMTP log entries and alerts.

### **Event Logs**

The Sentry family of products supports logging of system events both internally and externally. An internal log of more than 4,000 events is automatically maintained for the review by administrative users. For permanent/long-term log storage, Sentry supports the Syslog protocol; for immediate notification, Sentry supports Email notifications.

The log entries include a sequential entry number, date/time stamp, and event message. The event message is preceded with a message 'type' heading, and if the event is tied to a user, the username is included.

### **FTP**

The FTP server is used for configuration backup and restore.

### **HTTP**

The HTTP server supports two authentication methods for security and validation of the username-password: (1) Basic and (2) MD5 digest. The Basic method uses Base64 encoding to encode and deliver the username-password over the network to the HTTP server for decoding and authentication. The Basic method is supported by all web browsers and offers a minimum level of security. The MD5 digest method provides stronger protection using one-way encoded hash numbers, and MD5 digest does not place the username-password on the network. Instead, the sending browser creates a challenge code based on the hash algorithm, provided username-password, and unique items such as the device IP address and timestamp, which is compared against the HTTP server internal user database of valid challenge codes. The MD5 digest method offers a higher level of security than the Basic method but at present MD5 digest is not supported by all browsers. The HTTP server supports up to 8 simultaneous sessions.

### **HTTPS**

Secure HTTP-over-SSL web interface protocol;  
 Secure Sockets Layer (SSL) version 3;  
 Transport Layer Security (TLS) version 1 (RFC 2246);  
 SSL/TLS-enabled HTTPS server (RFC 2818);  
 Self-Signed X.509 Certificate version 3 (RFC 2459);  
 Asymmetric Cryptography: 1024-bit RSA Key Exchange.

#### Symmetric Cryptography Ciphers:

TLS\_RSA\_WITH\_DES\_CBC\_SHA (56-bit)

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (128-bit)

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (168-bit)

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (256-bit)

With HTTPS (SSL/TLS), the maximum number of simultaneous user sessions is four. SSL is enabled by default, but may be disabled if desired. By default, SSL connections are optional, meaning both insecure HTTP (http://) and secure HTTPS (https://) connections may be established. SSL connections may be configured to be required, meaning only the HTTPS connections will be established (and not the HTTP connections).

## LDAP

The LDAP v3 support allows for centralized username/password management on a networked directory server instead of locally on each Sentry product.

## LDAPS

LDAP over TLS/SSL support. TLS/SSL provides an encrypted connection between the client and server for all LDAP communication.

The LDAPS TLS/SSL client supports:

- Secure Sockets Layer (SSL) version 3;
- Transport Layer Security (TLS) version 1 (RFC 2246);
- X.509 version 3 (RFC 2459) server certificates with RSA key sizes up to 4,096 bits.

Symmetric Cryptography Ciphers:

- |   |  |
|---|--|
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (168-bit) | TLS_RSA_WITH_AES_128_CBC_SHA (128-bit) |
| TLS_RSA_WITH_DES_CBC_SHA (56-bit)       | TLS_RSA_WITH_AES_256_CBC_SHA (256-bit) |

Server certificates are accepted and used dynamically.

A NULL client certificate is sent to the server if a client certificate is requested

## SNMP

Allows network management systems to use SNMP requests to retrieve information and control power for individual outlets. The Sentry includes an SNMP v2c agent supporting standard MIB I and MIB II objects. A private enterprise MIB extension (Sentry3 MIB) is also supported to provide remote power control.

Supports SNMP source IP restriction for SNMP manager GET and SET requests to only be allowed from the IP addresses of the defined traps destinations.

When SNMP is restricted to the traps destinations, and the traps destinations are defined as host names, the IP addresses of the host names are looked up by DNS and cached for five seconds to avoid excessive DNS lookups with SNMP requests.

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 destinations.

## SNTP

Sentry supports the use of a network time service to provide a synchronized time reference to date/time stamp log entries.

## SSH

Secure network shell with terminal emulation.

The SSH server supports:

- SSHv2 standard

Asymmetric Cryptography:

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

Symmetric Cryptography Ciphers:

- |                 |                 |                  |
|-----------------|-----------------|------------------|
| AES256-CBC      | RIJNDAEL192-CBC | BLOWFISH-128-CBC |
| RIJNDAEL256-CBC | AES128-CBC      | 3DES-192-CBC     |
| AES192-CBC      | RIJNDAEL128-CBC | ARCFOUR-128      |

Message Integrity:

- |               |              |
|---------------|--------------|
| HMAC-SHA1-160 | HMAC-MD5-128 |
| HMAC-SHA1-96  | HMAC-MD5-96  |

## SSH (continued)

### Authentication:

Username/Password  
Session Channel Break Extension (for RS232 Break)

SSH shares the four simultaneous user sessions that were previously reserved for Telnet, allowing for up to four simultaneous SSH user sessions.

SSH sessions take six seconds to connect.

The IETF-Draft "Session Channel Break Extension" is supported for the generation of a ½ second RS232 break when an SSH session has been connected to a serial port by the CONNECT command.

SSH is enabled by default, but may be disabled if desired.

The SSH port number defaults to 22 (the IANA assigned number) but may be changed if desired. Using the web interface, the SSH options are configured and displayed on the "Configuration – Telnet/SSH" page.

### Strong Password Enforcement

Sentry supports the enforcement of strong passwords for enhanced security. When enabled, new strong passwords must be from 8-16 characters in length with at least one uppercase letter, one lowercase letter, one number, and one special character.

Examples of acceptable strong passwords:

n0tOnmyw@tch  
john2STI?  
H3reUgo!

---

**NOTE: Strong passwords require a minimum change of four characters when defining a new strong password.**

---

### Syslog

Sentry Syslog support is RFC3164-compliant and enables off-Sentry viewing and storage of log messages. Sentry products support external logging to (up to two) Syslog servers.

### TACACS+

The Sentry product family supports the Terminal Access Controller Access Control System (TACACS+) protocol, which enables authentication and authorization with a central TACACS+ server. User accounts do not need to be individually created locally on each Sentry unit. Administrators may pre-define and configure (in each Sentry product and in the TACACS+ server) a set of necessary TACACS+ privilege levels and user access rights for each level. User access rights may then be assigned or revoked by making the user a member of one or more pre-defined Sentry TACACS+ privilege levels. User account rights may be added, deleted, or changed within TACACS+ without any changes needed on individual Sentry products.

### Telnet

Insecure network terminal emulation.

### Usernames and Passwords

Sentry has one pre-defined administrative user account (username/password is admn/admn), and supports a maximum of 128 defined user accounts. Only an administrative-level user may perform operations such as creating/removing user accounts and command privileges, changing passwords, and displaying user information. An administrator may also view the status of all sensors and power inputs. Usernames must be 1-16 characters in length, spaces are not allowed, and usernames are not case-sensitive. Passwords must be 1-16 characters in length, spaces are not allowed, and passwords are case-sensitive.

## Username and Passwords (continued)

Administrative account usernames and passwords may be changed. Multiple administrators are supported. Additional user accounts may be assigned one of five access levels:

- power-user
- reboot-only
- ON-only
- view-only

All levels under power-user have admin-defined outlet and group access lists.

---

**NOTE: For security, Server Technology recommends removal of the pre-defined administrative user account after a new account with administrative rights has been created.**

---

Sentry is a trademark of Server Technology, Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products.

Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.