
 Server Technology, Inc.

Sentry Smart Cabinet Distribution Unit

Firmware Revision Notes

Sentry Smart CDU Version 6.1c

July 14, 2011

=====
 Applicable Products
 =====

Sentry Smart CDU firmware only applies to products with a product code of 50 hexadecimal. The product code is the fourth octet in the Ethernet MAC address, e.g., the "50" in "00-0A-9C-50-00-00". The Ethernet MAC address is displayed on the web "Configuration - System" page and by the SHOW SYSTEM command.

Firmware Revision History
 =====

yy-mm-ddVer.	FilenameDescription
-----	-----

 Version 6.1

11-07-146.1c	smcdu-v61c.bin	Third production release
--------------	----------------	--------------------------

Added support to the NETWORK.INI file (available through the FTP server) for the new DHCP Static Fallback and Boot Delay options.

Added display of a textual identifier, either "(ME)" or "(NIM)", after the hardware revision code in the display output of the SHOW SYSTEM command and on the "Configuration - System" web page.

Fixed the "Configuration - SNMP/Thresholds - Sensor Traps and Thresholds" web page and SNMP agent to accept temperature recovery delta values up to 18 degrees when using the Fahrenheit temperature scale. Previously, the 10 degrees limit for the Celsius temperature scale was also being applied for the Fahrenheit temperature scale.

Fixed a PUT of config.bin to preserve the new DHCP Static Fallback and Boot Delay options on the target system.

11-06-296.1b	smcdu-v61b.bin	Second production release
--------------	----------------	---------------------------

An updated operation manual accompanies this release. For complete configuration and operation instructions about new features below, please refer to the new manual. Manuals are available at:

http://www.servertech.com/support/Technical_Library/Product_Manuals

Added support for two new DHCP options: Static Fallback and Boot Delay. Both options can be enabled (the default) or disabled. Disabling Static Fallback configures the DHCP client to attempt indefinitely to acquire an address from a DHCP server, never timing out to fall back to a static address. By default, the DHCP client attempts to acquire

an address for 90 seconds before falling back to a static address. With Static Fallback disabled and Boot Delay enabled, this same 90 seconds is the amount of time for DHCP acquisition attempts before allowing the boot of the CDU to complete, while DHCP acquisition continues. Disabling Boot Delay reduced the 90 seconds of attempts to just 5 seconds before allowing the boot to complete while DHCP acquisition continues.

Use of these options allows for forcing the IP address to only be acquired by DHCP, with no timeout for static fallback, and/or the completion of the boot before acquisition has succeeded.

Using the web interface, these new DHCP options are configured on the "Configuration - Network" page.

Using the command-line interface (CLI), these new DHCP options are configured with new parameters to the existing SET DHCP command:

```
SET DHCP STATICFALLBACK { ENABLED | DISABLED }
SET DHCP BOOTDELAY { ENABLED | DISABLED }
```

The SHOW NETWORK command has been updated to display the current value of these new DHCP options.

Added a new object to the SNMP MIB and agent for the temperature recovery delta. A new Sentry3.Mib file accompanies this release. SNMP MIB files are available at:

<ftp://ftp.servertech.com/pub/SNMP/sentry3/>

Fixed changing of the display orientation causing a tower offline/online communication glitch.

Other very minor miscellaneous fixes.

11-05-106.1a smcdv-v61a.bin First production release

Version 6.1 is a major new-feature release. An updated operation manual accompanies this release. For complete configuration and operation instructions about new features below, please refer to the new manual.

Added support for new Network Interface Module (NIM) hardware. This hardware is identified by a hardware revision code of 64. Note: NIM hardware requires version 6.1a or later firmware -- it cannot be downgraded to prior versions.

Updated the look-and-feel of the web interface to match the colors and styles of the Server Technology "Sentry Power Manager" (SPM) v5 software.

Added a "System - Summary" page to the web interface. This page dynamically displays a sensor graph and alarm status for each line current, temperature, and humidity measurement, as well as displaying identifying system information, the number of active users, and the total power consumption. This page automatically updates every five seconds. The summary page is available to administrators and users with environmental monitor access rights.

Improved web interface performance by reducing page sizes and optimizing web server code.

Added support for Sentry Power Manager (SPM) Secure Access. This feature will allow future versions of SPM software to securely configure and

manage CDU firmware features that are not available by SNMP.

Changed the default value for the SNMP Agent to enabled, and changed the default value for the SNMP Set Community string to blank. This allows for out-of-the-box discovery by an SNMP manager, but without the security risk of allowing write access to the MIB objects.

Changed the default values for temperature and humidity sensors to: Low Temp = 5 degrees C (41 F), High Temp = 45 degrees C (113 F), Low Humidity = 10%, and High Humidity = 90%. Prior to this, defaults were the minimum and maximum of the sensor range.

Removed the restriction that POPS SNMP objects only be available as a key-activated feature. For consistency with previously key-activated products, this feature is now always reported as enabled.

Removed the HTTP MD5 authentication/security option.

Removed "Control State" from "OSTAT <id> DETAILS" command display output.

Added a remaining-character counter to the web interface "Configuration - System - Login Banner" page.

Version 6.0

11-05-106.0r smcdu-v60r.bin Thirteenth production release

Fixed RF Code support for accumulation/reporting of outlet average RMS current not occurring in master-only POPS systems.

Fixed internal string length initialization of the DHCP FQDN hostname in the DHCP request packet, which may be responsible for failures of the DHCP server to support the hostname.

Fixed a PUT of config.bin to the FTP server to only restore the email "from" address and the SNMP sysName value on the unit from which config.bin was originally retrieved, in order to not overwrite unique-per-unit values on other units.

Fixed rare cases of LDAP authentications failing due to timeouts, by increasing the timeout from 5 to 10 seconds.

Fixed rare cases of LDAP authentications failing due to out-of-memory problems, by increasing the heap size.

11-02-236.0q smcdu-v60q.bin Twelfth production release

Added support to preserve the value of the FQDN string upon a "reset to factory defaults, except network".

Fixed cases of communication failing to a UPS when DHCP is in use and the host was configured using a hostname.

Updated the starting and ending dates that will be used in a regenerated X.509 certificate. A new certificate will now be valid from February 1, 2011 to February 1, 2021.

Changed the delay between detection attempts for an RF Code tag from one to ten seconds.

Changed "Include Authorization Messages:" to "Include Authentication

Messages:" on the "Configuration - Email" web page.

Fixed the log message for changing the authentication order to say "Authentication" instead of "Authorization".

Fixed the log message for changing the FQDN string to include the new value.

Fixed the header of SYSLOG messages to use the DHCP-acquired IP address (when DHCP is enabled and successful) instead of the static address.

Added "[Sentry3_xxxxxx]" (where "xxxxxx" is the last three octets of the MAC address) to the start of SYSLOG messages, before "AUTH:", "EVENT:", etc., as a unique-per-unit source identifier.

Updated the copyright year in the footer of the web interface to 2011.

Removed the patent list from the footer of the web interface.

11-01-186.0p smcdu-v60p.bin Eleventh production release

Changed the default FQDN hostname from "Sentry3_xxxxxx" to "sentry3-xxxxxx". The underscore was changed to a hyphen because underscores are not valid in a hostname, per RFC 952, and thus may not be supported by some DHCP/DNS servers. The "S" was changed to lowercase because hostnames are more commonly lowercase.

Fixed RADIUS support not closing sockets, leading to auto-restarts due to running out of sockets.

10-12-026.0n smcdu-v60n.bin Tenth production release

Added support for DHCP Option 81, Fully-Qualified Domain Name (FQDN). With this option, the DHCP client requests that the DHCP server perform DNS updates for FQDN-to-IP-address mapping.

The default FQDN hostname is "Sentry3_xxxxxx", where "xxxxxx" is the last three octets of the MAC address. This FQDN value can be edited, allowing a different name to be chosen, and/or to expand the value to include a domain name.

Using the web interface, the DHCP FQDN option is configured on the "Configuration - Network" page.

Using the command-line interface (CLI), the DHCP FQDN options is configured with new parameters to the existing SET DHCP command:

```
SET DHCP FQDN <string>
```

The maximum length of the FQDN string is 63 characters.

Setting the FQDN value to an empty string disables use of the FQDN option.

The SHOW NETWORK command has been updated to display the current value of FQDN string.

Added RF Code support for wire-free monitoring of power and alarm information from PIPS and PIPS+POPS CDUs. An RF Code active-RFID tag plugs into the CDU serial port and is automatically recognized and used.

Added support with PIPS hardware to continue to report/display the line

current when in an overload condition.

Added support for a second pair of temperature/humidity sensors internal to the master unit.

Fixed the possible lack of update of the total system watts upon disconnect of a link unit from a master.

Fixed the improper reporting of PIPS voltages as 65535 when the measurement value was not available. The value in this case is now properly reported as -1.

Fixed a possible error in the calculation of the power factor with initial PIPS hardware that may not detect the reactance properly. Suppressed reporting of the reactance in this case.

Fixed cases of LDAP serial-debugging output overflowing the serial buffer and resulting in garbage or truncated output.

Fixed a system crash and automatic restart cause by overly long outlet names in non-3-phase branch-current-monitoring products. This problem was introduced after version 6.0g.

Fixed a problem with absolute outlet names not being properly adjusted to exclude the infeed identifier in single-phase products. This problem was introduced after version 6.0g.

Fixed a problem of failing to bring on-line some early hardware revisions of TrueRMS current-measurement boards. This problem was introduced after version 6.0g.

Fixed a buffer overrun, and a resulting crash of the web server, that occurs when visiting the "Configuration - System - Login Banner" web page with a current banner that includes enough non-web-safe characters to exceed 5120 characters after expansion to safe numeric character reference form.

Fixed presentation in the web interface of remotely-authenticated usernames that include spaces.

Fixed the "Configuration - SNMP/Thresholds" web page to not log a change to the "Error Trap Repeat Time:" when there was no change.

10-09-036.0m smcdu-v60m.bin Ninth production release

Added support for a ten-outlet board with integrated branch status sensing.

Added support for PIPS single-phase 24-outlet two-branch products.

Added support for 100A TrueRMS current-measuring hardware.

Improved the integrity checks on the decompression of the flash image into ram by the addition of a 32-bit CRC.

10-07-076.0k smcdu-v60k.bin Eighth production release

Added support to extend serial number ranges.

Changed the SNMP agent to automatically skip MIB objects that are not supported by the detected hardware, for example, PIPS and POPS objects.

10-06-116.0j smcdu-v60j.bin Seventh production release

Added Per-Inlet Power Sensing (PIPS) support.

Updated the SNMP MIB and agent to support PIPS objects. See the descriptions in the new Sentry3.Mib file that accompanies this release.

Added support in the SNMP agent to use cached IP addresses of trap destinations when the trap destinations are defined as host names. The IP addresses of the host names are looked up by DNS and cached for five seconds. This avoids excessive DNS lookups when many SNMP traps are sent in a short period of time.

Changed the maximum 3-phase load out-of-balance threshold to 200% from 100%, as 200% is the maximum in a wye-load system.

Changed "value suspect" to "power calculations may be inaccurate" in the message for 3-phase unbalanced loads that occurs when beyond the out-of-balance threshold.

Updated the OSTAT command for POPS data to no longer default to a target of "ALL" outlets if a target is not specified, and to instead display help text. This gives the user the chance to see that the DETAILS option is available.

Removed support in the TLS/SSL server for the weak 56-bit TLS_RSA_WITH_DES_CBC_SHA symmetric cryptography cipher.

Fixed several cases of CLI keywords not being accepted in uppercase.

Fixed duplicate default input-feed names occurring on 3-phase branch-current-monitoring products.

Fixed load value strings remaining at "N/A" when an overload condition is present at boot, until the overload condition clears.

Fixed cases of the email client failing to send emails (until a restart) after a loss of the socket connection to the SMTP email server.

Fixed a rounding error that could allow for a slight disparity between Amps displayed in the various user interfaces and the values reported by SNMP.

Fixed spurious fan errors.

Fixed spurious cases of an infeed overloading and recovering, and a humidity sensor reading 127% and recovering.

Fixed total system power calculations to exclude the fourth neutral current measurement in 3-phase wye-load products.

Updated the starting and ending dates that will be used in a regenerated X.509 certificate. A new certificate will now be valid from November 1, 2009 to November 1, 2019.

Updated the Serial Command Protocol (SCP) and specification document to version 2.0h. This version now supports PIPS.

Fixed cases of a possibly incorrect status being shown in log messages for water sensor errors and outlet load errors.

Changed SYSLOG messages that were improperly using a facility code of

LOG_SYSLOG to properly use LOG_DAEMON.

Updated the copyright year in the footer of the web interface to 2010.

09-03-106.0h smcdu-v60h.bin Sixth production release

Added Per-Outlet Power Sensing (POPS) support.

Added an OSTAT CLI command for POPS information.

Updated the SNMP MIB and agent to support POPS objects. These objects are feature-key activated. See the descriptions in the new Sentry3.Mib file that accompanies this release.

Added support to inform the backup master in new TrueRMS power supply hardware of display orientation changes, such that the backup master will write to the display in the same orientation as the network-card master.

Fixed cases of the reported system uptime diverging slightly from the actual system uptime.

Updated the Serial Command Protocol (SCP) and specification document to version 2.0g. This version now supports POPS.

08-11-256.0g smcdu-v60g.bin Fifth production release

Added RADIUS support. RADIUS (Remote Authentication Dial-In User Service) is a centralized authentication, authorization, and accounting service. Smart CDU firmware supports the authentication and authorization features of RADIUS.

With RADIUS enabled and configured, user login attempts to the Smart CDU result in authentication requests to the RADIUS server to determine access. Replies from the RADIUS server approve or deny access, and, if approved, also determined the authorized access level and access control lists for the user.

RADIUS network communication is secured by a shared secret. The shared secret is used to sign RADIUS data packets to ensure they are coming from a trusted source, and to encrypt user passwords. The shared secret is configured on both the Smart CDU and the RADIUS server.

A user's authorized access level and access control lists are configured only on the RADIUS server using Server Technology Vendor Specific Attribute (VSA) dictionary entries. These are defined in the file "dictionary.sti". See "dictionary.sti" for attribute usage notes and examples.

Smart CDU RADIUS client supported features:

Authentication and authorization per RFC 2865

Two RADIUS servers, each configurable with:

Host name/IP (63 characters maximum)
 Shared secret (48 characters maximum)
 Port (1 to 65535, default = 1812)
 Timeout (1 to 30 seconds, default = 5)
 Retries (0 to 10, default = 2)

Authentication order configurable to "Remote->Local"

or "Remote Only".

Password Authentication Protocol (PAP) authentication method.

Maximum 32-character usernames and passwords.

Server Technology Vendor Specific Attributes (see dictionary.sti).

Unique "NAS-Identifier" (per Smart CDU) in requests to the RADIUS servers, for filtering. The "NAS-Identifier" value is "Sentry3_XXXXXX", where "XXXXXX" is the last three octets of the MAC address.

Using the web interface, the RADIUS options are configured on the "Configuration - RADIUS" page.

Using the command-line interface (CLI), the RADIUS options are configured with the new command:

```
SET RADIUS { ENABLED | DISABLED }
SET RADIUS { PRIMARY | SECONDARY } { SERVER | SECRET |
PORT | TIMEOUT | RETRIES }
```

A SHOW RADIUS command has been added to display the RADIUS settings.

Added configuration of user session timeout periods for the web and command-line interfaces. Previously, these session timeout periods were fixed at 5 minutes. The web and command-line interface session timeouts can now be separately configured for a timeout period between 1 minute and 1440 minutes (24-hours).

Using the web interface, the user session timeouts are configured on the "Configuration - System" page.

Using the command-line interface (CLI), the user session timeouts are configured with new parameters to the existing SET OPTION command:

```
SET OPTION { CLITIMEOUT | WEBTIMEOUT }
```

The SHOW OPTIONS command has been updated to display the user session timeouts.

Added support to display up to a 32-character username for the active user in the web interface, above the navigation menu, with the name wrapping after 16 characters.

Added support for log messages to include up to 32-character usernames when remote authentication is used (LDAP, TACACS+, and RADIUS). Previously, even though usernames could be longer than sixteen characters for remote authentications, only the first sixteen characters were logged.

Changed all user-authentication input methods to limit accepted usernames and passwords to 32 characters, and to allow remote authentication attempts with blank passwords.

Fixed the failure to receive network settings by DHCP due to initial

connectivity delays introduced by various features of advanced switches (see <http://www.cisco.com/warp/public/473/12.html>). These switches block network traffic for up to a minute after a link is established, preventing DHCP requests from reaching the DHCP server during that time. The DHCP client was only retrying for up to 30 seconds, giving up, and falling back to static network settings. An additional minute of DHCP request attempts has been added to overcome this problem. Note: units with static network settings can still have other early network traffic, such as an SNMP startup trap, blocked.

Fixed the problem of no response to SNMP GET and SET requests when the defined community strings were the maximum length.

Fixed the local display logic to not write to the first display until after a successful initialization of the power supply board that performs the current measurements. Previously, the first display would blank if the power supply board failed to initialize successfully, which was inconsistent with the behavior for additional displays, which would remain blinking dash-dash ("--").

Fixed the "rem_addr" (remote address) field in TACACS+ authentication and authorization request packets to not change when the SNMP "sysName" value is changed. The value now remains fixed at "Sentry3_XXXXXX", where "XXXXXX" is the last three octets of the MAC address. This keeps the remote address unique to each CDU.

Fixed a log entry missing for an automatic web user logout that occurs when the maximum number of simultaneous web user sessions has been reached and the oldest inactive web user's session is ended and re-allocated for use by a new session.

Fixed a very obscure case in which a user's password could show up in log messages as part of the user's name.

Fixed SET SYSTEM AREA, SET SYSTEM PF, and SET SYSTEM BALANCE to only accept valid value strings with the appropriate number of decimal places.

Fixed inconsistent SNMP log messages that reported "by user SNMP" to report just "by SNMP".

Fixed login failures to the FTP server, and a stack overflow of the FTP server, when logging into the FTP server using LDAP or TACACS+ remote authentication.

Fixed buffer overruns in the FTP server that prevented proper restoration/setting of several values in FTP.INI when the values were longer than sixteen characters.

Fixed several FTP server log messages to be consistent with other user interfaces.

Fixed the FTP server to always require both a username and password be entered before authentication of the credentials is started.

Fixed possibly-incorrect source IP addresses being logged in the logout messages of web users.

Fixed an improper error message with the SET SYSTEM AREA command.

Fixed minor inconsistencies in the titles and text of various web pages.

Fixed the javascript input validation for the Area, Power Factor, and 3-Phase Load Out-of-Balance Threshold on the "Configuration - System" web page.

Fixed the web pages to show the correct/current IP address of the CDU when the IP address configuration has changed, but a restart has not yet been performed.

Fixed web pages to show graphic image tooltips in FireFox.

08-07-246.0f smcdu-v60f.bin Fourth production release

Fixed watt calculations for 3-phase products that measure phase current instead of line current. In this case only, the previous watt calculation would under-report power consumption by the $\sqrt{3}$. Note: this fix only affects Smart CDU model number "CS-6DVDW413".

Fixed the 3-phase out-of-balance check to not apply to products that measure multiple branch currents per phase, in which case it is not applicable. Note: this fix only affects Smart CDU model number "CS-6DVDW413".

Fixed the SHOW TOWERS command to display the product serial number, model number, power type, and 3-phase indicator.

08-07-106.0e smcdu-v60e.bin Third production release

Added support to select a square meter or a square foot as the unit of area. The unit of area applies to the user-configured system area (footprint) and the system-calculated watts per area unit. The unit of area was previously a square foot, and not configurable.

Using the web interface, the unit of area is configured on the "Configuration - System" page using a new drop-down selection box to the right of the input box for the area value.

Using the command-line interface, the unit of area is configured with the new command:

```
SET SYSTEM AREAUNIT { SQUAREMETER | SQUAREFOOT }
```

The SHOW SYSTEM command has been updated to display the selected unit of area after the area value.

Upon a reset to factory defaults, the unit of area is now a square meter.

Updated the SNMP MIB and agent to support reading and writing the new area of unit and the existing system power factor, as well as making the system area value writable. See the descriptions in the new Sentry3.Mib file.

Updated patent numbers in the web page footer.

Updated the Serial Command Protocol (SCP) and specification document to version 2.0f. This version now supports all the features new to v6.

Fixed spurious false fan failure and internal over-temperature errors.

Fixed an improper case of flashing "oL" (for overload) on the input feed load displays of a linked unit when it was connected to a master unit running v6.0d firmware and a CRC error occurred reading the NVM in the linked unit.

Fixed possible cases of an invalid CRC having been written to the NVM of a linked unit during the factory configuration process. Valid data with a specific CRC error is automatically detected and corrected in deployed units.

Fixed an input validation error on the "Input Feed Traps and Thresholds" web page when a linked product has been disconnected.

Fixed a problem introduced in v6.0d that caused the load to temporarily display as 0.65535 in the user interfaces immediately after a linked product was disconnected.

Fixed inconsistent table row highlighting on the "Sensors" web page.

Built with updated SSL, Web, and Email libraries.

08-02-286.0d smcdu-v60d.bin Second production release

Added support for new v6 input-feed current-measurement hardware that supplies hundredth-Amp resolution with better than two percent accuracy.

Changed the code that reports the current measured by v5 and earlier input-feed current-measurement hardware to report the value in increments equal to the internally-measured resolution. Previously, the value was reported in increments that were twice the internally-measured resolution. Products that previously reported in 1/4 Amp increments now report in 1/8 Amp increments and products that previously reported in 1/2 Amp increments now report in 1/4 Amp increments. Products with new v6 input-feed current-measurement hardware report in 1/100 Amp increments. Regardless of the resolution, the minimum reported input-feed current above zero is 1/4 Amp.

Changed the LED display code to show current readings in 0.1 Amp increments up to ten Amps when new v6 input-feed current-measurement hardware is detected.

Fixed the LDAP code to replace up to three occurrences of "%s" in the "User Search Filter" with the username supplied during login. Previously only the first occurrence of "%s" was replaced. This change allows complex search filters with logical operations between multiple filters, per RFC 2254.

Fixed cases of factory-configurations not being entirely locked on specific models.

08-01-226.0c smcdu-v60c.bin First production release

Version 6.0 is a major new-feature release. Updated manuals accompany this release for complete configuration and operation instructions. Manuals are available on the Server Technology web site (<http://www.servertech.com>).

Updated the look-and-feel of the HTML interface to match the Server Technology corporate web site colors and styles.

Added the ability to configure various product characteristics. These include the product serial number, model number, input feed voltage, input feed maximum load capacity, power type (AC/DC), and 3-phase indicator (for AC products only).

New products will have the characteristics set at the factory. The product serial number, model number, power type, and 3-phase indicator are locked (not changeable by the end-user) when set at the factory.

Already-delivered products that are firmware-upgraded will allow the customer to configure the product characteristics, and the values will not be locked.

When configured, the product characteristics will allow for additional features, such as asset tracking and power consumption calculation and reporting.

Added power consumption (watts) calculation and reporting. Power consumption is calculated individually for each input feed and is summed for a total system power consumption. The power factor used in the calculations is configurable. 3-phase power calculations for balanced loads are automatically applied if the 3-phase product characteristic is set.

Added a 3-Phase out-of-balance threshold. Loads on all three phase pairs of a 3-phase product are constantly checked for being within a configurable percent level of the other two phase pairs. If a phase imbalance occurs outside of the configured threshold, the condition is noted in the user interfaces.

The mean of the three loads is calculated first. If the mean is less than 1/2 Amp, the loads are considered balanced. Otherwise, the maximum deviation of the three loads from the mean is calculated. If the maximum deviation is less than 1/2 Amp, the loads are considered balanced. Otherwise, the maximum deviation is calculated as a percentage of the mean. If this percentage is greater than the configured "3-Phase Load Out-Of-Balance Threshold", then the loads are considered to be out-of-balance.

Added system watts per square feet calculation and reporting. The square feet of the footprint of the system (usually the cabinet footprint size) is configurable. When configured, the total system watts is divided by the footprint square feet to determine and report the system watts per square feet.

Added a configurable temperature recovery delta. After exceeding the high temperature threshold (thus entering an alarm condition) the temperature value must fall below the high temperature threshold by the recovery delta number of degrees before recovering. The default is 1 degree Celsius, 2 degrees Fahrenheit.

Added UPS support. This allows the voltage for an input feed to be retrieved from a UPS for more-accurate watt calculations.

Using the web interface, the UPS settings are configured on a new "Configuration - UPS" page and the status is displayed on a new "Power Monitoring - UPS" page.

Using the command-line interface, the UPS settings are configured with the SET UPS command and the status is displayed with the SHOW UPS command.

Changed the web navigation menu SNMP item to be SNMP/Thresholds, to guide users to the pages for setting thresholds, which apply for various purposes, with or without using SNMP.

Changed the default input feed high load threshold to be 80% of the factory-configured input feed maximum load capacity, instead of defaulting to 255 Amps.

Changed the CLI and web configuration of the input feed high load threshold to be limited to a maximum of the factory-configured maximum load capacity.

Changed the input feed overload determination code to indicate an overload condition when the measured input feed current is greater than 0.5 Amps above the factory-configured maximum load capacity, instead of always at 30.5 or 60.5 Amps (dependent upon the product), which should never be reached in lower capacity products.

Updated the Sentry3 SNMP MIB to include support for the product characteristics, power consumption values, and system watts per square feet.

Version 5.3

08-03-315.3q smcdu-v53q.bin Fifteenth production release

Fixed the LDAP code to replace up to three occurrences of "%s" in the "User Search Filter" with the username supplied during login. Previously only the first occurrence of "%s" was replaced. This change allows complex search filters with logical operations between multiple filters, per RFC 2254.

Fixed spurious false fan failure and internal over-temperature errors.

08-01-145.3p smcdu-v53p.bin Fourteenth production release

Fixed a security issue that could expose partial account passwords for some users under specific conditions.

Fixed the ADD and DELETE commands to accept 16 character usernames at username prompts.

Fixed several log message inconsistencies between the web and CLI interfaces.

07-12-145.3n smcdu-v53n.bin Thirteenth production release

Added support to individually enable and disable the supported SSH authentication methods (password and keyboard-interactive). This allows an SSH client to be forced to use a specific method. For example, by enabling the "keyboard-interactive" method but disabling the "password" method, the client will be forced to use "keyboard-interactive", which is required to display the login banner.

Using the web interface, the SSH authentication methods are configured on the "Configuration - Telnet/SSH" page using new checkboxes.

Using the command-line interface, the SSH authentication methods are configured with the new command:

```
SET SSH AUTHMETHOD { PASSWORD | KBINT } { ENABLED | DISABLED }
```

The SHOW NETWORK command has been updated to display the enabled SSH authentication methods.

At least one SSH authentication method must remain enabled. This is enforced by the web and command-line interfaces.

Upon factory reset, all SSH authentication methods are enabled.

Added support for an external environmental monitoring unit (an EMCU) even if the master product includes built-in support for temperature/humidity sensors. Note: a hardware update may be required to support powering an EMCU through the Link port.

Changed the time between retries of FTP firmware downloads from one second to one minute to address initial connectivity delays introduced by various features of some advanced switches (see <http://www.cisco.com/warp/public/473/12.html>).

Changed the SSH server to display the product name and version string upon a successful authentication, just prior to the location being displayed.

Changed the term "probe" to "sensor" throughout the CLI whenever referring to a temperature/humidity sensor, for consistency.

Fixed the SSH server "keyboard-interactive" authentication method to accept and use the username supplied in the initial client authentication request packet.

Fixed the SSH server "keyboard-interactive" authentication method to properly attempt displaying the logon banner. Previously, some SSH clients, such as PuTTY, would not display the login banner.

Fixed the failure of an FTP PUT of config.bin to restore the entire configuration if the FTP client was quit/exited immediately or soon after the PUT operation completed.

Fixed the SHOW TRAPS command on 60 Amp products that support only a single temperature/humidity sensor. Previously, the session would end when attempting to display the environmental monitor trap settings.

Fixed log message inconsistencies between the web and CLI interfaces.

07-09-175.3m smcdu-v53m.bin Twelfth production release

Fixed the LED display code to show "0.5" Amps on products with 60 Amp input feeds. Previously, the display would jump from "0.0" to "1.0" Amps.

07-08-275.3k smcdu-v53k.bin Eleventh production release

Added support for hardware with internal temperature sensing and fan

rotation sensing. If the necessary hardware is present, it is automatically detected and supported. When the hardware has been detected, if the internal temperature exceeds a factory-configured maximum-operating limit, or a fan significantly slows or fails, the fault will be reported.

The command-line interface will report temperature or fan faults as critical errors before each command prompt ("Smart CDU:") is displayed.

The web interface will report temperature or fan faults as critical errors in red text below the main-frame header each time a page is shown or refreshed.

Temperature and fan faults will also be logged as a system event. If setup to do so, these log entries will be sent to a syslog server and/or to an email recipient.

The SNMP agent has also been updated to report temperature or fan faults. The towerStatus object supports new 'FanFail' and 'overTemp' states, and the towerStatusEvent trap/notification will be sent during these states.

For all error-reporting methods, an over-temperature fault has a higher priority than a fan failure -- if both faults occur simultaneously, only an over-temperature fault will be reported. However, one fault for each tower/enclosure can be reported simultaneously.

The SHOW TOWERS command has been updated to automatically display the status of the internal temperature sensors and fans, if the hardware support is detected. Upon a fault, the SHOW TOWERS command will provide additional information about the fault, for example, which of several fans has failed.

The SNMP MIB has also been updated. See the descriptions in the new Sentry3.Mib file for details.

Changed the LDAP Search Bind Password and FTP client password to be hidden in the web and command-line interfaces. Asterisks or dots are shown for each character when entered and displayed. The passwords are never sent to the web browser, so they are not viewable in the web source.

Removed a connection test to the LDAP servers prior to the initial LDAP bind. This connection test was responsible for a Novell eDirectory LDAP trace showing errors prior to the login. The LDAP network connection timeout was adjusted to achieve the same purpose as the connection test, which is to avoid lengthy delays when an LDAP server is unavailable.

Fixed the TACACS+ client to accept "priv-lvl*nn" in a successful authorization response from the server in order to set the privilege level of the authorized session. The TACACS+ client now supports "priv_lvl=nn", "priv_lvl*nn", "priv-lvl=nn", and "priv-lvl*nn".

07-06-215.3j smcdcu-v53j.bin Tenth production release

Added enforcement of the mutual exclusivity between the LDAP 'Use TLS' option and an LDAP bind type of MD5, which do not operate together.

Removed the IP Address from the email subject line, per customer requests, due to security concerns. Emails from multiple products are still uniquely identifiable by the 'From' address.

Removed the OEMINFO command keyword from the SET and SHOW commands.

Fixed the email code to attempt sending to the secondary email 'To' address if the primary email address failed. Previously, a send to the secondary email address was not being attempted if the primary email address failed.

Fixed the email code to limit the email body text to a length of 8K bytes, to avoid a possible memory overwrite, crash, and auto-restart. Email bodies will now be limited to 50 log entries or 8K bytes, whichever is smaller.

Fixed a possible crash and automatic restart of the system if the 'To' or 'From' email addresses were set to the maximum length in the "Configuration - Email" web page.

Fixed the SNMP SysUpTime value to increment time at the correct rate. Previously, the return value was only incrementing one second for every ten actual seconds.

Fixed the factory default for the SNMP SysName value and the email 'From' address value to properly reflect the last three octets of the product's MAC address. Previously, after being reset to factory defaults, another restart would revert the final two octets to zero if an SNMP setting was not changed.

Updated the starting and ending dates that will be used in a regenerated X.509 certificate. A new certificate will now be valid from June 21, 2007 to June 21, 2017.

Updated the integrated board-level test code to v2.0c. Note: this functionality is only accessible and used during the factory production process.

Built with updated TCP/IP, SSL, SNMP, Web Server, and Telnet Server libraries.

07-02-075.3i smcdu-v53i.bin Ninth production release

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

Using the web interface, the LDAP TLS/SSL option is configured and displayed on the "Configuration - LDAP" page using the new "Use TLS/SSL:" drop-down selection box. The choices are "Yes" and "No".

Using the command-line interface, the LDAP TLS/SSL option is configured with the new command:

```
SET LDAP USETLS { YES | NO }
```

The SHOW LDAP command has been updated to display the current setting.

Upon factory reset, the default value is NO.

When LDAP is configured to use TLS/SSL, the LDAP port number

must be changed to match the encrypted port number of the LDAP directory server. The IANA well-known port number for LDAPS is 636.

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 4096 bits
Symmetric Cryptography Ciphers:
  TLS_RSA_WITH_3DES_EDE_CBC_SHA (168-bit)
  TLS_RSA_WITH_DES_CBC_SHA (56-bit)
  TLS_RSA_WITH_AES_128_CBC_SHA (128-bit)
  TLS_RSA_WITH_AES_256_CBC_SHA (256-bit)
Server certificates are accepted and used on-the-fly
A NULL client certificate is sent to the server if a
  client certificate is requested
```

Added SNMP source IP restriction support. This allows SNMP manager GET and SET requests to only be allowed from the IP addresses of the defined traps destinations.

Using the web interface, the SNMP IP Restriction option is configured and displayed on the "Configuration - SNMP" page using the new "IP Restriction:" drop-down selection box. The choices are "No Restrictions" and "Trap Destinations Only".

Using the command-line interface, the SNMP IP Restriction option is configured with the new command:

```
SET SNMP IPRESTRICT { NONE | TRAPDESTS }
```

The SHOW SNMP command has been updated to display the current setting.

Upon factory reset, the default value is NONE/No Restrictions.

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.

Added support to log the source IP address of HTTPS sessions. The remote source IP addresses of HTTPS sessions are now retrieved from the SSL/TLS proxy and used in HTTPS login, logout, and authentication failure log messages.

Fixed the possible loss of a configured host IP address (for the FTP, SNMP, Sntp, Syslog, LDAP, and TACACS protocols) if firmware was updated from v5.3e or earlier to v5.3f or later, followed by a command-line interface change to a non-hostname configuration item for that protocol.

Built with updated TCP/IP and SSL libraries.

06-11-305.3h smcdv-v53h.bin Eighth production release

Added code to the web interface to highlight the background of every other row in all tables.

Added "More (Y/N)" prompting between each page of the SHOW LOG display.

- Added and changed the navigation links on the "Tools - View Log" web page to include "<< First Page", "< Previous Page", "Next Page >", and "Last Page >>".
- Added "(SCP)" after "Coldboot Alert" in the SHOW OPTIONS display to indicate a relationship between the Serial Command Protocol (SCP) and the Coldboot Alert features. Upon a coldboot of the system, if the coldboot alert feature is enabled, the system will send a 1/2 second RS-232 break out any serial ports that also have the SCP enabled.
- Improved the robustness of the NVM/I2C communication code and changed NVM/I2C status messages to only be displayed during the boot if significant errors are detected.
- Improved the speed of configuration restores. A PUT of config.bin now immediately restores the configuration to RAM and begins writing the configuration to NVM in the background. Upon the FTP session ending, the restart process starts immediately, but delays until all NVM writes have completed. Unnecessary writes of unchanged default configurations no longer occur, making the time to complete all writes much shorter.
- Changed the SSH code to guarantee that any startup errors (such as invalid keys) are sent out the Console port prior to the system boot completing.
- Changed the syslog message for host name fields to show "(undefined)" if the name is set to blank.
- Removed unnecessary memory usage by the Telnet server.
- Fixed a stack overflow and memory overwrite in the email thread that could cause various system crashes and automatic restarts.
- Fixed a temporary run down of the network heap each time an IP address DNS lookup was performed on a host name, which could lead to a low-heap automatic restart if many DNS lookups occurred within a short period of time.
- Fixed sluggish performance problems with multiple concurrent HTTPS sessions.
- Fixed the Login link on the web "Restarting" page, which was using the static IP address even when DHCP was enabled.
- Fixed a bug in the "Configuration - TACACS" web page. When applying the key form, the key data was being written to the incorrect location in NVM. This was causing the key to not be restored after a reset, and was causing the login banner to be trashed.
- Fixed a bug in the "Tools - View Log" web page. When selecting the "Previous 100 entries" link to go back to the first 100 log entries, the data was not being displayed properly.
- Fixed the SNMP trap code to not send traps twice to the first trap destination when the second trap destination is blank.
- Fixed the local load display to blink "FE" (for Fuse Error) on displays for third and fourth input feeds that have a removed/blown branch fuse. The code was previously only working on displays for first and second input feeds.

Fixed the FTP server to accurately show the size of files in a directory list, to list the files in alphabetical order, and to only show a date/time when available.

Fixed the FTP put of config.bin to restore the email configuration, which was previously not occurring.

Fixed the FTP get and put of config.bin to backup and restore the entire configuration for products with third and fourth enclosures in the system. Previously for these products, only the configuration for the first and second enclosures were being backed-up and restored.

Fixed various minor command parsing problems with the SET INFEED, SET SYSLOG, SET SCPAUTH, SET TRAP, and SET EMAIL commands.

Fixed the "SHOW commands are:" list to show PORTS instead of PORT, to match the actual valid command parameter. This typo was introduced in v5.3g.

Updated the integrated board-level test code to v2.0b. Note: this functionality is only accessible and used during the factory production process.

06-09-215.3g smcdu-v53g.bin Seventh production release

Added code to detect a hung communication bus (for example, to a slave enclosure) and to prevent a hung bus from causing a system slowdown.

Re-ordered the command keywords in the top-level command list, as well as the SET and SHOW command lists, for a more logical grouping of commands by functionality and purpose.

Changed/moved the CLI command for setting the display orientation to SET OPTION DISPLAY from just SET DISPLAY. Removed the SHOW DISPLAY command and added the display orientation to the SHOW OPTIONS command.

Changed the name of the FTP "filepath" configuration item to FTP "directory" in both the command-line interface (CLI) and the FTP.INI file. This was done to be consistent with the web interface and because "directory" is the more-common term. For backwards compatibility, "filepath" is still accepted.

Changed the OEMINFO string to not be cleared upon a reset to factory defaults.

Updated the Serial Command Protocol to version 2.0e.

Increased by one year the start and end dates of a newly re/generated X.509 certificate. A new certificate will now be valid from September 1, 2006 to September 1, 2016.

Fixed LDAP login attempts to the secondary LDAP host possibly always failing. This problem was introduced in v5.3f when hostname support was added -- the previous IP address of the secondary LDAP host was still being used, instead of the new configured hostname.

Fixed FTP downloads to not fail when the user-configurable FTP strings (username, password, directory, and filename) are at their maximum sizes.

Fixed DNS-server connection test code to work properly when DHCP is enabled or one or both DNS server IP addresses are 0.0.0.0. This fix avoids several cases of unnecessary timeout delays when the DNS servers are unreachable.

Fixed host connection test code to immediately fail when link integrity is down. This avoids unnecessary timeout delays in several cases when the network is disconnected or down.

Fixed the FTP download code to perform a link-integrity and host connection test prior to attempting a download. This avoids unnecessary timeout delays if the host is unreachable.

Fixed the FTP download code to detect and report when the FTP host name cannot be resolved, and to then skip the FTP download attempt. This avoids unnecessary timeout delays.

Fixed the LDAP and TACACS+ login code, the SNMP traps sending code, and the FTP download code to skip attempts when the host name is blank. This avoids unnecessary timeout delays.

Fixed some SNMP set operations not being logged. This included set operations applied to sysContact, sysName, and sysLocation objects.

Fixed the display code to illuminate the extra/outer decimal point on the first load display when the configuration reset button is pressed and the display orientation is set to inverted. Previously, the inner decimal point (between the two numbers, which is unused when inverted) was being illuminated.

Integrated board-level test code v2.0a into the application build. Note: this functionality is only accessible and used during the factory production process.

Added support for automatic retrieval of pre-generated certificates and keys after the serial number assignment. Note: this functionality is only accessible and used during the factory production process.

06-06-225.3f smcdu-v53f.bin Sixth production release

Added Dynamic Host Configuration Protocol (DHCP) support to allow for the automatic acquisition of an IP address, subnet mask, gateway, and DNS server addresses from a network DHCP server.

Note: when loading version 5.3f over a previous version that only supported static addressing, DHCP will initially be disabled. Upon a reset to factory defaults, however, DHCP will default to enabled.

Using the web interface, DHCP is configured and displayed on the "Configuration - Network" page.

Using the command-line interface, DHCP is configured with the new command:

```
SET DHCP { ENABLED | DISABLED }
```

The SHOW NETWORK command has been updated to display the current DHCP setting.

When DHCP is enabled, the product will attempt to acquire an address from a DHCP server upon boot, prior to the boot completing. If successful, the acquired addresses will be displayed in the web and command-line interfaces. If unsuccessful, the acquisition attempt will timeout at 30 seconds, and the product will complete the boot using the previously assigned (or default) static addresses.

When DHCP is disabled, the product boots with the static addresses, as in previous versions.

To view or change the static addresses, DHCP must first be disabled.

Upon a lease expiration of addresses assigned by DHCP, a lease renewal is requested. If the DHCP server assigns a lease with a different address, or a timeout occurs during the request, the product will automatically restart. This will allow the product to boot with the new addresses, or fallback to the static addresses.

Added hostname support for all host IP address fields: FTP server, SNMP traps destinations, LDAP servers, TACACS servers, SMTP servers, Syslog servers, and SMTP (email) server.

A fully-qualified domain name may now be entered instead of an IP address. For example, the LDAP host fields will now accept "serverpdc.reno.servertech.com" instead of just an IP address. Host names will be translated to IP addresses using DNS. Host names can be up to 63 characters.

Added support for temperature values to be entered and reported in either the Celsius or Fahrenheit temperature scale. Previous versions always used Celsius.

Using the web interface, the temperature scale is configured and displayed on the "Configuration - System" page.

Using the command-line interface, the temperature scale is selected with the new command:

```
SET OPTION TEMPSCALE { CELSIUS | FAHRENHEIT }
```

The SHOW OPTIONS command has been updated to display the current setting.

When the temperature scale is changed, all thresholds are automatically converted to the newly-selected scale.

The supported range and resolution of the temperature scales are:

```
Celsius: 0 to 123.5 degrees, with 0.5 degree
resolution, reported in 1/2 degree increments.
```

```
Fahrenheit: 32 to 254.5 degrees, with 0.9 degree
resolution, rounded to and reported in the nearest
1/2 degree increment.
```

Entry of temperature thresholds is automatically limited to the whole values in the ranges shown above for the selected scale.

The SNMP MIB has also been updated to support selecting and using the temperature scale. See the descriptions in the new

Sentry3.Mib file.

Added email support for notification of log messages, including which categories of log messages are to be emailed, and support for two recipients.

Using the web interface, Email is configured and displayed on the new "Configuration - Email" page.

Using the command-line interface, Email is configured with a new set of SET EMAIL commands. A new SHOW EMAIL command has been added to display the current Email settings.

The items that can be configured are:

Email enabled/disabled.

```
SET EMAIL { ENABLED | DISABLED }
```

Default: DISABLED

SMTP host and port -- the host name/IP and port number of the SMTP server that will deliver the email.

```
SET EMAIL SMTP { HOST hostname | PORT port }
```

Default HOST: blank/undefined

Default PORT: 25

'From' address -- the address from which the email reports that it came.

```
SET EMAIL FROM address
```

Default: Sentry3_XXXXXX@, where XXXXXX is the last three octets of the product's MAC address.

Primary and Secondary 'Send To' addresses -- the recipient email addresses.

```
SET EMAIL { PRIMARYTO | SECONDARYTO } address
```

Defaults: blank/undefined

Categories of log messages to be included in the email.

```
SET EMAIL { EVENT | AUTH | CONFIG }
           { ENABLED | DISABLED }
```

Defaults: EVENT ENABLED, others DISABLED.

Every minute, up to fifty new log messages in the enabled categories are placed in the body of an email and sent to both recipients. Multiple emails will be sent if there are more than fifty new log entries in the enabled categories.

Added automatic firmware updates. When enabled, the product will periodically, or on a schedule, check the configured FTP server for a newer version of firmware. If found, an automatic restart and load of the new firmware will occur.

Using the web interface, automatic update settings are configured and displayed on the "Configuration - FTP" page.

Using the command-line interface, automatic update settings are configured with a new subset of SET FTP commands. The SHOW FTP command has been updated to display the current automatic update settings.

The items that can be configured are:

Automatic updates enabled/disabled.

```
SET FTP AUTOUPDATE { ENABLED | DISABLED }
```

Default: DISABLED

Schedule Day upon which to perform a new firmware check.

```
SET FTP AUTOUPDATE DAY { SUNDAY | MONDAY |
                        TUESDAY | WEDNESDAY |
                        THURSDAY | FRIDAY |
                        SATURDAY | EVERYDAY }
```

Default: EVERYDAY

Schedule Hour upon which to perform a new firmware check.

```
SET FTP AUTOUPDATE HOUR { 12AM | 1AM | 2AM |
                          3AM | 4AM | 5AM |
                          6AM | 7AM | 8AM |
                          9AM | 10AM | 11AM |
                          12PM | 1PM | 2PM |
                          3PM | 4PM | 5PM |
                          6PM | 7PM | 8PM |
                          9PM | 10PM | 11PM }
```

Default: 12AM

To perform the check for new firmware at the scheduled day and hour, the product must be configured to get real time from an SNTP server, and must have successfully done so. Otherwise, the product will perform the check every 24 hours since the product last booted.

To avoid too many simultaneous FTP sessions from multiple products with the same schedule, each product will randomly add a delay (up to one minute) upon the scheduled day/hour, or the period expiring, before connecting to the FTP server. Additionally, up to three attempts to connect will be made, with 15 seconds between each.

Added support to the FTP server for two new text files: FTP.INI and SNTP.INI. These allow for common FTP configuration settings, automatic update settings and schedule, and SNTP options to be duplicated across a number of products by a FTP put to each.

Added support to restart to factory defaults, while preserving the network configuration. This allows for a remote configuration reset, without losing network connectivity.

Using the web interface, this new restart option has been added to the choices on the "Tools - Restart" page. The new choice is "Restart and reset to factory defaults, except network".

Using the command-line interface, this new restart option is invoked by a new optional sub-parameter to the RESTART FACTORY command:

```
RESTART FACTORY { KEEPNET }
```

All configuration items will be reset to factory defaults except for the DHCP setting, IP address, subnet mask, gateway, and DNS server addresses.

Added support for Server Technology's proprietary Serial Command Protocol (SCP). The SCP allows for control and monitoring of the product through a serial connection to the console and/or modem port using a command-response protocol that allows for simplified communication compared to scripting sessions to the command-line interface. This feature was previously available only in custom OEM builds.

Added the source IP address of network authentication attempts (both successes and failures) to the log entries. Log entries for logouts also include the source IP address. These apply to all network sessions except those by HTTPS, because the SSL/TLS proxy hides the source IP address from the web server.

Added the CLI command "SET OPTION MORE { ENABLED | DISABLED }" to enable or disable the "More (Y/N)" prompting between each page of information for long information displays. The "SHOW OPTIONS" display has also been updated to display the current setting. The default is ENABLED.

Added write-behind caching support for NVM write operations. This feature is used by SNMP to greatly improved the speed of SNMP write operations for objects that are written to NVM.

Added robustness improvements to the non-volatile memory (NVM) access routines.

Added support to display a blinking "FE" (for Fuse Error) on the local load display of an input feed that has a removed/blown branch fuse. The blinking "FE" display alternates with the load display, so that the load on other branches can still be seen.

Added support for a serial port data rate of 115200 bps.

Added an option on the web "Configuration - System" page to disable the configuration reset button. The feature was added in v5.3e, but the web configuration was accidentally left out.

Added support for new hardware models with additional link capabilities.

Fixed the problem of not being able to turn off (uncheck) the Location blink option on the web "Configuration - System" page, which was a problem that was introduced in v5.3e.

Fixed two LDAP problems. One fix avoids a possible "Out of memory" error during searches, and the other avoids a possible improper parsing of the Group Membership Value Type when type "DN" is selected.

Fixed the SSH server to log authentication attempts when using the

password authentication method. Previously, only the keyboard-interactive authentication method logged authentication attempts.

Fixed the SSH server to not prematurely fail a third authentication attempt. Previously, depending on the SSH client, a third attempt to authenticate would either fail immediately after entering the username, or would accept both the username and password and fail even if they were valid. Three full login attempts can now be made. The server will disconnect the session after the third attempt, if it fails.

Fixed the "Configuration - Serial" web page to no longer cause an "error on page" when submitting the form immediately after having followed an "Edit" link on the page and then returning to that page.

06-02-285.3e smcdu-v53e.bin Fifth production release

Added logging of all authentications (including failed attempts), configuration changes, and system events.

The log is stored in RAM and can hold up to 4097 entries. Additional log entries will automatically wrap around over the oldest log entries. The log is cleared upon a restart or power loss. For permanent off-product log storage, the Syslog protocol is supported (see below).

Each log entry includes a sequential log-entry number, a date/time-stamp (if a date/time has been retrieved by SNMP), and a message. Each log message begins with a category heading of either "AUTH:", "CONFIG:", or "EVENT:", and is followed by the message information.

The log can only be viewed by administrators.

Using the web interface, the log is viewed by selecting the new "View Log" item under the "Tools" menu.

Using the command-line interface, the log is viewed with the new command:

```
SHOW LOG
```

Note: Web authentications (and failed attempts) are only logged when the web server is set for Basic authentication.

Added support for the Syslog protocol. The Syslog support is RFC3164-compliant and provides for off-system viewing and permanent storage of log messages.

Two Syslog servers are supported. The Syslog support is enabled by configuring the IP address of one or both Syslog servers. The port number used with the Syslog protocol is also configurable. The default port is 514, which is the well-known port for Syslog.

Using the web interface, Syslog options are configured and displayed on the new "Configuration - SNMP/Syslog" page.

Using the command-line interface, the Syslog server IP addresses and port number are configured with the new commands:

```

SET SYSLOG [ HOSTIP1 | HOSTIP2 ] { ipaddress }
SET SYSLOG PORT { number }

```

A new SHOW SYSLOG command has been added to display the current values.

Added support to configure a local GMT Offset to the date/time returned by SNTP. This was added because the Syslog RFC requires that the date/time be provided in local time.

The offset can be configured in whole hours between plus and minus twelve hours.

Using the web interface, the SNTP GMT offset is configured and displayed on the new "Configuration - SNTP/Syslog" page. This page uses the configured GMT offset to show the current date/time in local time.

Using the command-line interface, the SNTP GMT offset is configured with the new command:

```

SET SNTP GMTOFFSET { -12 .. +12 }

```

The SHOW SYSLOG command has been updated to display the current GMT offset value. The SHOW SYSLOG command has also been updated to use the configured GMT offset to show the current date/time in local time.

Note: There is currently no automatic adjustment for daylight savings.

Added the ability for a user to change their password. Previously, only an administrator could change account passwords.

Using the web interface, a user can change their password using the new "Change Password" item under the "Tools" menu.

Using the command-line interface, a user can change their password with the new command:

```

PASSWORD

```

By the web or command-line interface, the user must enter their current password, their new password, and a verification of their new password.

By allowing a user to change their own password, they can change it from the initial password that was assigned when the account was created, without divulging the new password to an administrator. Once a user changes their own password, an administrator cannot lookup the new password, though an administrator can always assign a new password.

This behavior is important for accountability assessment of log entries, which include, when relevant, the name of the user that performed the authentication or configuration change that was logged.

Added the ability to enforce the usage of strong passwords. Strong password support, when enabled, requires passwords be a minimum of 8 characters with at least one uppercase letter, one lowercase letter, one digit, and one special character.

When a password is changed, strong password support requires that the new password differ in at least four character positions from the old password.

Using the web interface, the strong password option is configured and displayed on the "Configuration - System" page.

Using the command-line interface, strong password support is enabled or disabled using the new command:

```
SET OPTION STRONGPASSWORDS { ENABLED | DISABLED }
```

A new SHOW OPTIONS command has been added to display the current value.

Added an option to disable the external configuration reset button. In an insecure location, this button may pose a security threat since it could be used to return the unit to factory defaults, which would then allow a login using the default administrator account. Disabling the button removes this security concern.

Using the command-line interface, the configuration reset button is enabled or disabled using the new command:

```
SET OPTION BUTTON { ENABLED | DISABLED }
```

A new SHOW OPTIONS command has been added to display the current value.

Added support to configure a pre-login banner. This feature allows an administrator to configure up to 2070 characters of text that will be displayed prior to a login. This can be used for displaying any message, such as legal text or disclaimers.

Using the web interface, the login banner is configured and displayed on the new "Configuration - System - Login Banner" page. A link to this new page has been added to the "Configuration - System" page.

Using the command-line interface, the login banner is configured using the new command:

```
SET BANNER
```

For serial and Telnet sessions, the banner is automatically displayed before the login prompts. For SSH sessions, the "keyboard-interactive" authentication method must be used to be presented with the login banner. For web browser sessions, if the banner is not blank, the default page will display the banner in a fixed-width font, followed by a link to login. If the banner is blank, the default page is automatically adjusted so that the banner page is skipped, making the web login process identical to previous versions.

Added support for the upload and download of configurations. This feature allows for configuration backup and restore, as well as a common/template configuration to be uploaded to multiple products.

The upload/download of configurations is supported via a built-in FTP server. A single administrator login (at a time) is supported by the FTP server. The FTP server has a fixed

one-minute timeout.

Two files can be uploaded/downloaded from the root of the FTP server:

CONFIG.BIN contains the entire configuration, excluding TCP/IP settings, serialized and factory-only configurations, the X.509 certificate, and SSH keys. This file is encoded as to not be user readable or editable. Although encoded, this file should be kept in a secure location. This file should not be edited. If edited, the file will be invalid when uploaded.

NETWORK.INI contains just the TCP/IP settings (IP address, subnet mask, gateway, DNS1, and DNS2). This file is user readable and editable.

When uploaded, the NETWORK.INI settings only take a few seconds to be stored. When CONFIG.BIN is uploaded, several minutes are needed to store the entire configuration. During this time, an additional upload will not succeed. Thus, if both files are to be uploaded, NETWORK.INI should be uploaded first.

If either NETWORK.INI or CONFIG.BIN are uploaded, then upon a timeout or logout from the FTP server, an automatic restart is set to occur, pending the successful completion of the uploaded settings being stored. The restart will cause the product to boot with the new settings applied.

The FTP server, and thus the configuration upload/download feature, can be disabled, if considered a security risk.

Using the web interface, the FTP Server setting is configured and displayed on the "Configuration - FTP" page.

Using the command-line interface, the FTP Server is enabled or disabled using the new command:

```
SET FTP SERVER { ENABLED | DISABLED }
```

The SHOW NETWORK command has been updated to display the current FTP Server setting.

Note: The FTP Server does not support web browser FTP file transfers. A non-web-browser FTP client must be used.

Added web security checks to prevent out-of-order submittals of form items from being applied.

Changed all web security realms to have the same realm name. This should cause web browsers to clear all cached passwords for the product when an error 401 (not authorized) page is sent.

Fixed the web login code to ignore case when comparing the entered username with names already in the active-session table. This prevents identical account logins from using multiple sessions if the username is entered in a different case.

Added support to the SSH server for the "keyboard-interactive" authentication method. This method must be used to be presented with the pre-login banner text.

Fixed the SSH server so that it no longer reports to an SSH client that "public-key" is a supported authentication method. The methods currently supported are "keyboard-interactive" and "password".

Added code to prevent port names from being set to "ALL", which is a reserved keyword.

Fixed the ADD and DELETE commands to always accept the absolute port IDs for the Console and Modem ports.

Fixed the command-line interface to not allow the port name MODEM to be used with the ADD and DELETE commands on products that do not have a MODEM port.

Removed debugging options that could expose account passwords to administrators.

Changed "baud rate" to "data rate" in the command-line interface.

Fixed another serial driver problem that could allow the command-line interface to get behind by one character for a session started on the Console or Modem port.

Built with updated TCP/IP, SSL, and FTP Server libraries.

05-12-015.3d smcdu-v53d.bin Fourth production release

Fixed the system failing to boot when configured with an invalid IP Address and Subnet Mask combination in which the bits in the host portion of the IP Address are all ones (the subnet broadcast address). The TCP/IP stack no longer attempts to load when the bits in the host portion of the IP Address are either all ones or all zeros, as both cases are invalid for a host IP address. The web user interface no longer allows these invalid combinations.

Fixed several cases of TCP/IP sockets not being closed upon TACACS+ authentication failures. This fix avoids an automatic restart that would otherwise occur if all socket resources became unavailable.

Added support to the LDAP and TACACS+ clients to cause a fallback to local authentication when the destination network or host is unreachable and the Authentication Order is set to Remote-Only. Previously, this fallback would only occur when the host refused the connection or when the connection to the host timed-out. These additions cover additional cases in which the host may be unavailable, but fallback should occur.

05-11-165.3c smcdu-v53c.bin Third production release

Fixed a critical security flaw affecting HTTP/S authentications when the web server is set for Basic authentication.

Fixed the SNMP agent to allow the temperature and humidity threshold objects to be set through SNMP. Previously, noSuchName or notWritable was being returned for these objects.

Fixed cases of spurious SNMP traps being generated for temperature and humidity sensors that are connected to an environmental monitor that goes off-line and then back on-line.

- Fixed a serial driver problem that could allow the command-line interface to get behind by one character.
- Fixed a problem in the LDAP client that allowed a directory server group name to match local user account names, instead of just local LDAP group account names.
- Fixed the problem of a branch fuse error being reported for the branches of an input feed that is off. The input feed is now properly reported as being off, instead of reporting a fuse error. This only applies to products with branch-circuit fuse sensing.
- Fixed the command-line interface to not allow the port name MODEM to be used with the SET PORT command on products that do not have a MODEM port.
- Fixed the command-line interface to not allow the ID or name of a slave tower to be used with the SET TOWER command when a slave tower is not connected.
- Fixed a spelling error in an error message that can occur on the "Configuration - Users" web page.
- Added robustness improvements to the non-volatile memory (NVM) access routines.
- Added robustness improvements to the internal communications bus access routines. Eliminated unnecessary bus communications for features that are not supported by the hardware.
- Added support for the serial port data rate to be changed without requiring a restart. The change now occurs upon logout of the current session. A message that the data rate is changing is sent at the current data rate just before the data rate is changed. This same message is also sent upon a boot completing if the administrator-configured data rate is different than the fixed console-port boot data rate of 9600 bps.
- Added support to configure the TACACS+ port number.
- Using the web interface, the TACACS+ port number is configured and displayed on the "Configuration - TACACS+" page.
- Using the command-line interface, the TACACS+ port number is configured with the new command:
- ```
SET TACACS PORT { number }
```
- The SHOW TACACS command displays the current value.
- Added support for the keyword ALL to be specified as the group name in the ADD/DELETE GROUPxxxxxxxxxx commands.
- Added a check to the LDAP client that DNS can resolve the LDAP host address when the bind type is set to MD5, which is required with MD5 LDAP binds.
- Added the brief display of dash-dash on load displays during off-line to on-line transitions while the initial load reading is occurring.

Added support for new load measurement hardware that supports 60 Amp input feeds.

05-07-175.3b smcdu-v53b.bin Second production release

Completely redesigned and re-implemented the LDAP authentication feature to support a wide variety of directory services and non-standard schemas. LDAP bind, search, and filter strings are now configurable by an administrator to match their particular directory service and schema. See ldap\_update.txt for more information.

Fixed the LDAP implementation to support simple binds with Active Directory servers.

Fixed the LDAP implementation to not require uppercase usernames for HTTP logins when authenticating with an Active Directory server using MD5 binds.

Added an option to invert the load displays. When inverted, the load values for all input feeds in the system will be written upside-down, and in whole amps, to the respective displays.

This feature is to allow for upside-down mounting of vertical products when the power is fed from the ceiling.

Using the web interface, the display orientation is displayed and configured on the "Configuration - System" page.

Using the command-line interface, the display orientation is configured with the new command:

```
SET DISPLAY { NORMAL | INVERTED }
```

A new SHOW DISPLAY command displays the current setting.

Upon factory reset, the default is determined by an internal factory-installed jumper/switch position. Unless the product was specifically ordered with inverted displays, this jumper/switch position will be open, resulting in normal display orientation.

Added medium-speed (1/2 second on/off) blinking of load displays when the input feed load value is above the preset SNMP trap threshold.

Added support to the CLI and Web interfaces to allow an administrator to configure the SNMP MIB-II sysName, sysLocation, and sysContact objects.

Using the web interface, the SNMP MIB-II sysXXXXXX objects are display and configured on the "Configuration - SNMP" page.

Using the command-line interface, the SNMP MIB-II sysXXXXXX objects are configured with the new commands:

```
SET SNMP SYSNAME { string }
SET SNMP SYSLOCATION { string }
SET SNMP SYSCONTACT { string }
```

The SHOW SNMP command has been updated to display the current values.

- Removed code from the Telnet and serial port login routines that caused the entered username to be uppercased. This could prevent TACACS+ logins from succeeding.
- Fixed the SET USER ACCESS command to properly set the web access rights level to allow web users to view the environmental monitoring data.
- Fixed the problem of default non-administrative TACACS+ privilege-level accounts not having appropriate access rights to login through the web interface.
- Added HTTP session cookies to force re-authentication after a timeout or logout of a web browser session when the web server is set for Basic authentication.
- Fixed the web server to no longer be vulnerable to the Cross Site Scripting (XSS) vulnerability (CAN-2003-0218).
- Fixed memory leaks and handling of low memory conditions in the HTTPS (SSL/TLS) code that could cause the web server to hang.
- Fixed problems where corrosive page refreshes could cause the web server to hang.
- Fixed absolute URLs not being handled correctly when accessed from HTTP V1.0 browsers.
- Changed hyperlinks on the HTML logout and error pages to be absolute, not relative, to avoid possible broken links.
- Added a hint in the web error message box for an invalid IP address to indicate that 0.0.0.0 should be used for none.
- Fixed the problem of closing the web browser before the Restarting page is displayed, but after confirming a restart, from preventing the restart and no longer allowing another restart to be issued, by web or CLI. The restart will still not occur, but another restart can now be performed.
- Changed the TACACS+ web configuration page to not send the current encryption key to the browser because, even though it was shown as dots, viewing the source would show it in clear text. The status of the key is now shown as just "(blank)" or "(set)" and a separate form allows for a new key to be entered and verified.
- Changed the User Edit web page to not send the current password to the browser because, even though it was shown as dots, viewing the source would show it in clear text. A new password can now be entered and verified on the page, or left blank for no change.
- Fixed improper handling of low memory conditions in the Telnet server that could cause the server thread to end.
- Fixed improper handling of low memory conditions in the SSH server that could cause the server thread to end.
- Fixed problems in the SSH socket handling code that could cause the product to crash and automatically restart.
- Fixed the TCP/IP stack to no longer be vulnerable to Blind TCP Reset

attacks (CAN-2004-0790).

Added code to monitor the TCP/IP socket usage and to perform an automatic restart if all socket resources unexpectedly become unavailable.

Fixed the PING command to always close sockets in case of errors.

Increased the stack size of the SNMP trap thread to avoid potential system crashes.

Fixed a problem that caused SNMP SET (write) operations to fail for the Sentry3-MIB systemLocation object.

Fixed the SNMP agent to not match object IDs (OIDs) that are too long.

Fixed the SNMP agent to not allow objects to be lexicographically out of order.

Fixed the SNMP agent to return SNMP v2c error values when SNMP v2c protocol data units are used.

Fixed the SNMP agent to check for and properly handle negative table index values.

Fixed the CLI SET SNMP xxxCOMM commands to allow spaces in the community strings. Previously the string would be truncated at the first space.

Fixed an incorrect internal SNMP message length that could cause memory to be overwritten.

Fixed corruption of an internal debugging log by messages that were too long.

Added debug logging of thread peak stack usage.

Changed the behavior of beta code versions to not disable auto-crash recovery (auto-restart) code.

Added debugging code to record in flash the running thread during a crash, before an auto-restart.

Added reset of a communication bus multiplexor when the selected channel is hung. This fix works in conjunction with updated hardware to avoid a non-powered, but connected, slave product from hanging the internal communication on the master.

Built with all available updated system libraries.

05-04-225.3a smcdu-v53a.bin First production release

=====

Copyright (C) 2011 Server Technology, Inc.