DTS1 CSfC

1-Slot Data Transport System (CSfC)

User Guide

Part Number: DDOC0099-000-B4

This Page Intentionally Left Blank

Front Matter

Revisions

Document Number	Media	Revision	Date	Description	PCN
DDOC0099-000	PDF	A1	07/17/18	Multiple updates.	1227
DDOC0099-000	PDF	A2	08/14/18	Multiple updates.	0818-0001
DDOC0099-000	PDF	A3	10/01/18	Multiple updates.	1018-0001
DDOC0099-000	PDF	A4	11/01/18	Multiple updates.	1118-0001
DDOC0099-000	PDF	A5	01/22/19	Multiple updates.	0119-0001
DDOC0099-000	PDF	A6	04/24/19	Conversion to new format.	0419-0001
DDOC0099-000	PDF	A7	05/15/19	Corrected as noted by change bars.	0519-0005
DDOC0099-000	PDF	A8	08/15/19	Corrected as noted by change bars.	0819-0005
DDOC0099-000	PDF	A9	09/03/19	Removed references to RUGS-E system	0919-0001
DDOC0099-000	PDF	AA	09/19/19	Revised encryption password / passphrase requirements.	0919-0005
DDOC0099-000	PDF	AB	10/25/19	Revised to include video stream capture. Additional revisions / corrections as noted by change bars.	1019-0014
DDOC0099-000	PDF	AC	3/27/20	Revised format and style of illustrations and tables. Technical changes incorporated as noted by change bars.	0320-0012
DDOC0099-000	PDF	AD	4/9/20	Deleted VS-RMC-003 RMC, 1 TB and Secure Erase from Appendix C	0420-0004
DDOC0099-000	PDF	AE	5/8/20	Corrected as noted by change bars.	0520-0003
DDOC0099-000	PDF	AF	6/2/20	Corrected as noted by change bars.	0620-0003
DDOC0099-000	PDF	AG	6/8/20	Update istarget information. Corrected as noted by change bars.	0620-0005
DDOC0099-000	PDF	AH	6/29/20	Add Quick Start section. All other corrections / updates noted by change bars.	0620-0012
DDOC0099-000	PDF	AI	8/26/20	Corrected as noted by change bars.	0820-0004
DDOC0099-000	PDF	AJ	9/15/20	Add cmlog command to CLI. Corrected as noted by change bars.	0920-0005
DDOC0099-000	PDF	AK	9/30/20	Add 8 TB RMC.	0920-0007
DDOC0099-000	PDF	AL	11/5/20	Updated as noted by change bars.	1120-0004
DDOC0099-000	PDF	AM	01/28/21	Updated as noted by change bars.	0121-0008
DDOC0099-000	PDF	AN	03/24/21	Updated as noted by change bars.	0321-0007
DDOC0099-000	PDF	AO	04/05/21	Updated as noted by change bars.	0421-0001
DDOC0099-000	PDF	AP	05/11/21	Updated as noted by change bars.	0521-0003
DDOC0099-000	PDF	AQ	07/06/21	Updated as noted by change bars.	0721-0007
DDOC0099-000	PDF	AR	11/18/21	Updated as noted by change bars.	1121-0007
DDOC0099-000	PDF	AS	01/24/22	Updated as noted by change bars.	0122-0007

Document Number	Media	Revision	Date	Description	PCN
DDOC0099-000	PDF	AT	03/02/22	Remove Proprietary notification.	0322-0002
DDOC0099-000	PDF	AU	03/09/22	Updated as noted by change bars.	0322-0008
DDOC0099-000	PDF	AV	04/28/22	Update rmcfree CLI command information.	0422-0020
DDOC0099-000	PDF	AX	07/26/22	Update ground cable installation information.	0722-0003
DDOC0099-000	PDF	AY	07/29/22	Add nfsctl CLI command information and revised as noted by change bars.	0722-0005
DDOC0099-000	PDF	AZ	09/16/22	Updated as noted by change bars.	0922-0010
DDOC0099-000	PDF	B1	11/18/22	Updated as noted by change bars.	1122-0004
DDOC0099-000	PDF	B2	02/13/22	Deleted paragraph in paragraph 2.2 **Protocols**.	0223-0004
DDOC0099-000	PDF	B3	03/10/23	Updated as noted by change bars.	0323-0005
DDOC0099-000	PDF	B4	03/21/23	Updated as noted by change bars.	0323-0008

The Curtiss-Wright 1-Slot Data Transport System (CSfC) User Guide (DDOC0099-000) is made up of the following individual chapters and appendices.

Chapter / Appendix	Topic	Content Revision
1.0	**Introduction** section	3.0
2.0	**Overview** section	10.0
3.0	**Controls and Indicators** section	4.0
4.0	**Installation** section	5.0
5.0	**Encryption** section	10.0
6.0	**Quick Start** section	4.0
7.0	**Operation** section	7.0
8.0	**System Configuration** section	1.0
9.0	**Troubleshooting** section	0.0
10.0	**Remove / Replace** section	6.0
11.0	**Simple Network Management Protocol** section	1.0
12.0	**Command Line Interface** section	13.0
A	**Specifications** section	7.0
B	**Connectors / Cables** section	4.0
C	**Ordering Information** section	5.0

Changes to technical content are shown through the use of change bars placed in the left margin next to the changed material (as shown here). Corrections to typographical errors are not noted unless they significantly impact the content.

Copyright

Safety

WARNING

HAZARD. A potential hazard that could result in serious injury or death.

Information contained in WARNINGS applies to dangers and hazards that may result in injury and / or death to personnel. The actual hazard is provided in CAPITALIZED letters and the information that mitigates the danger is provided in sentence case. This information typically precedes procedural steps. It also may be present in narrative text to warn operators or maintenance personnel of dangers present in the equipment.

CAUTION

HAZARD. A potential hazard that could result in equipment damage or improper operation.

Information contained in CAUTIONS applies to dangers and hazards that may result in damage to equipment or improper operation. The actual hazard is provided in CAPITALIZED letters and the information that mitigates the danger is provided in sentence case. This information typically precedes procedural steps. It also may be present in narrative text to warn operators or maintenance personnel of dangers present in the equipment.

NOTE

Amplifying information that helps in making a task or procedure more easily understood.

NOTES are used to supply amplifying information that will result in ease of testing or be beneficial to personnel. This information typically precedes procedural steps. It also may be present in narrative text as well.

Style and Conventions

This User Guide uses the following typographical conventions.

This style	Refers to
`Ready`	Text the software displays.
go	Anything you type, exactly as it appears, whether referenced in text or at a prompt.
ENTER	Special keys on the keyboard, such as enter, alt, and spacebar.
Save	Software command buttons and sections of dialog boxes, such as group boxes, text boxes, and text fields.
File → Open	A menu and a specific menu command.
ALT+F1	Pressing more than one key at the same time.
ALT, TAB	Pressing more than one key in sequence.
xx,yy	Variable in error messages and text.
jobfile.dat	File names.
◆	Denotes the result of an action or procedure.
xyz	Hyperlink.
STOP	Controls on equipment.

Table of Contents

System Configuration

Specifications

Connectors / Cables

Ordering Information

List of Figures

List of Tables

Introduction

1.1 Purpose

The purpose of this guide is to describe the Curtiss-Wright Data Transport System 1-slot (DTS1) LRU (Line Replaceable Unit) product and to guide users through the process of unpacking, installing, configuring, and using. The unit requires the use of a Removable Memory Cartridge (RMC) module. From this point forward, the product will be referred to as the DTS1 and the associated cartridge will be referred to as the RMC module.

1.2 Scope

The information in this user guide is intended for information systems personnel, systems coordinators, or highly skilled network users. This manual contains the following information:

- An overview of the DTS1.
- Unpacking, installation, and setup information.
- User interface connections.
- User input.
- Configuration options.
- Product specifications.
- Operation requirements.
- Environmental restrictions.
- Connector pinout and specifications.
- Ordering information for related products and parts

1.3 Quality

Curtiss-Wright Controls, Inc., Electronic Systems is committed to leveraging our technology leadership to deliver products and services that meet or exceed customer requirements. In addition to the physical product, the company provides documentation, sales and marketing support, hardware and software technical support, and timely product delivery. Our quality commitment begins with product concept and continues after receipt of the purchased product.

Curtiss-Wright Controls, Inc., Electronic Systems' Quality Management System is accredited to the latest revision of the aerospace standard, AS9100 Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations.

Our Quality System addresses the following basic objectives:

- Achieve, maintain, and continually improve the quality of our products and service through established design, test, production and service procedures.
- Improve the quality of our operations to meet the needs of our customers, suppliers, and other stakeholders.
- Provide our employees with the tools and overall work environment to fulfill, maintain, and improve product and service quality.
- Ensure our customer and other stakeholders that only the highest quality product or service will be delivered.

Eagle Registrations Inc. assessed Curtiss-Wright's Quality Management System and confirmed conformance to AS9100D including ISO 9001:2015 with Certificate No. 5819. The scope of the registration is as follows: “Design manufacture, test and repair of board level products, electronic sub-systems, related software and services for commercial, aerospace and military applications.”

Customer feedback is integral to our quality and reliability program. We encourage customers to contact us with questions, suggestions, or comments regarding any of our products or services. We guarantee professional and quick responses to your questions, comments, or problems.

1.4 CE Conformity

1.4.1 DTS1

Curtiss-Wright certifies, in accordance with directives 0214/30/EU, 2011/65/EU, and 2006/1907/EC, the following units:

- VS-DTS1-F
- VS-DTS1-FD

conform to the applicable requirements of EN 55022, EN 55024, EN 50581, and EN 62368-1.

1.4.2 RMC

Curtiss-Wright certifies, in accordance with directives 0214/30/EU, 2011/65/EU, and 2006/1907/EC, the following units:

- VS-RMC256M-00
- VS-RMC1024M-00
- VS-RMC2048M-00
- VS-RMC4096M-00
- VS-RMC8192M-00

conform to the applicable requirements of EN 55022, EN 55024, EN 50581, and EN 62368-1.

1.5 Related Information

- AES (Advanced Encryption Standard). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
- EIA-232 RS-232 electrical characteristics single-ended voltage digital interface circuit. http://www.eia.org/
- VITA 46, 47, 48, and 58. https://www.vita.com/Standards
- FIPS 140-3. https://csrc.nist.gov/publications/detail/fips/140/3/final
- EMI Mil-Std-461
- NAS, http://www.pdl.cmu.edu/PDL-FTP/NASD/hotnet99.pdf
- Ruggedization, Curtiss-Wright, www.cwcdefense.com
- Curtiss-Wright Controls Defense Solutions www.cwcdefense.com
- PuTTy User Manual (client program for SSH, Telnet, and R login network protocols).
- MIL-STD-704F Department of Defense Interface Standard, Aircraft Electric Power Characteristics.
- MIL-HDBK-704-8 Guidance For Test Procedures For Demonstration Of Utilization Equipment
- Compliance To Aircraft Electrical Power Characteristics 28 VDC
- 0214/30/EU Electromagnetic Compatibility Directive
- 2011/65/EU RoHS Directive
- 2006/1907/EC REACH Directive
- EN 55022 Information Technology Equipment-Radio Disturbance Characteristics (2010)
- EN 55024 Information Technology Equipment-Immunity Characteristics Limits (2010)
- EN 50581 Technical Documentation for the Assessment of Electrical and Electronic Products with Respect to the Restriction of Hazardous Substances (2012)
- EN 62368-1 Audio/Video, Information and Communication Technology Equipment (2014)

1.6 Technical Support

Technical documentation is provided with all of our products. This documentation describes the technology, its performance characteristics, and includes some typical applications. It also includes comprehensive support information, designed to answer any technical questions that might arise concerning the use of this product. We also publish and distribute technical briefs and application notes that cover a wide assortment of topics. Although we try to tailor the applications to real scenarios, not all possible circumstances are covered.

While we have attempted to make this document comprehensive, you may have specific problems or issues this document does not satisfactorily cover. Our goal is to offer a combination of products and services that provide complete, easy-to-use solutions for your application.

If you have any technical or non-technical questions or comments, contact us. Hours of operation are from 8:00 a.m. to 5:00 p.m. Eastern Standard/Daylight Time.

- Phone: (937) 252-5601 or (800) 252-5601
- E-mail: DTN_support@curtisswright.com
- Fax: (937) 252-1465
- World Wide Web address: www.cwcdefense.com

1.7 Ordering Process

To learn more about Curtiss-Wright Defense Solutions' products or to place an order, please use the following contact information.

- E-mail: DTN_info@curtisswright.com
- World Wide Web address: http://www.cwcdefense.com/

To contact a local Curtiss-Wright sales representative go to: http://www.cwcdefense.com/sales.html and point to your location on the map presented, then click on the pop-up with the sales representative's name.

Overview

2.1 Description

The Curtiss-Wright DTS1 (Figure 2.1) is a rugged Network Attached Storage (NAS) device with solid state storage capacities from 256 GB up to 8 TB. The DTS1 provides data storage to assorted network clients via two IEEE 802.3 / 802.3u / 802.3ab Ethernet ports. The DTS1 is a ruggedized unit designed to operate on vehicles, in field stations, or in laboratories.

The DTS1 is configured/controlled through a Command Line Interface (CLI) via RS-232 or Ethernet (Telnet or SSH). The CLI utilizes Curtiss-Wright's proprietary command structure, which includes built in Help. The DTS1 uses the Commercial Solutions for Classified (CSfC) specification and associated dual layer data security system to provide a NSA-acceptable data encryption method. Data is encrypted by hardware and software to fulfill the CSfC dual layer requirements.

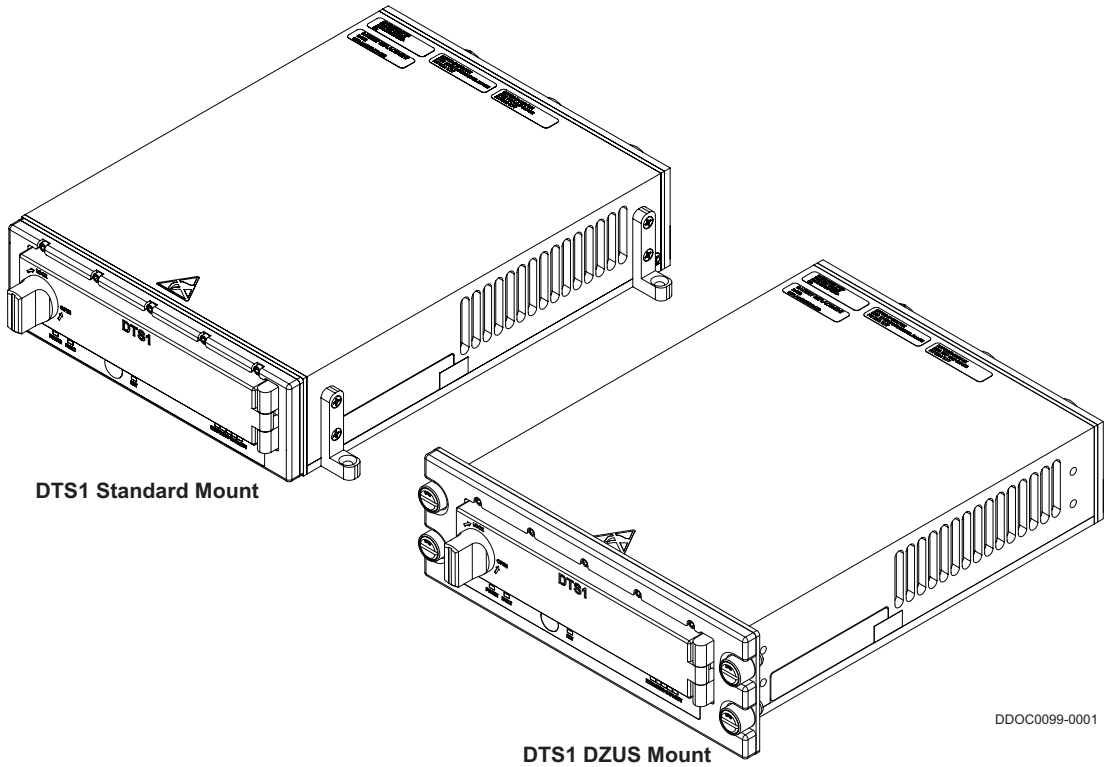

Figure 2.1 DTS1

2.1.1 Chassis

The chassis (Figure 2.2) is made up of the following major assemblies:

- RMC Module Mount
- Backplane PCB
- Power Supply PCB
- Processor Carrier PCB
- Mini Comm PCB
- USB Flash Module

It also contains a battery used to power the EPROM that stores the encryption key.

The RMC module mount positions the RMC module in the chassis. The backplane is used to interface the RMC module to the processor carrier PCB. The mini comm PCB is the primary assembly in the unit. It contains the processor / CPU, memory, and the encryption circuitry. The processor carrier PCB is used to interface the mini comm PCB to the rest of the system. It also has the utility (J2) and Ethernet (J3) connectors installed on it. The power supply assembly takes the 28 VDC input power, cleans and conditions it, and then distributes it to the entire system.

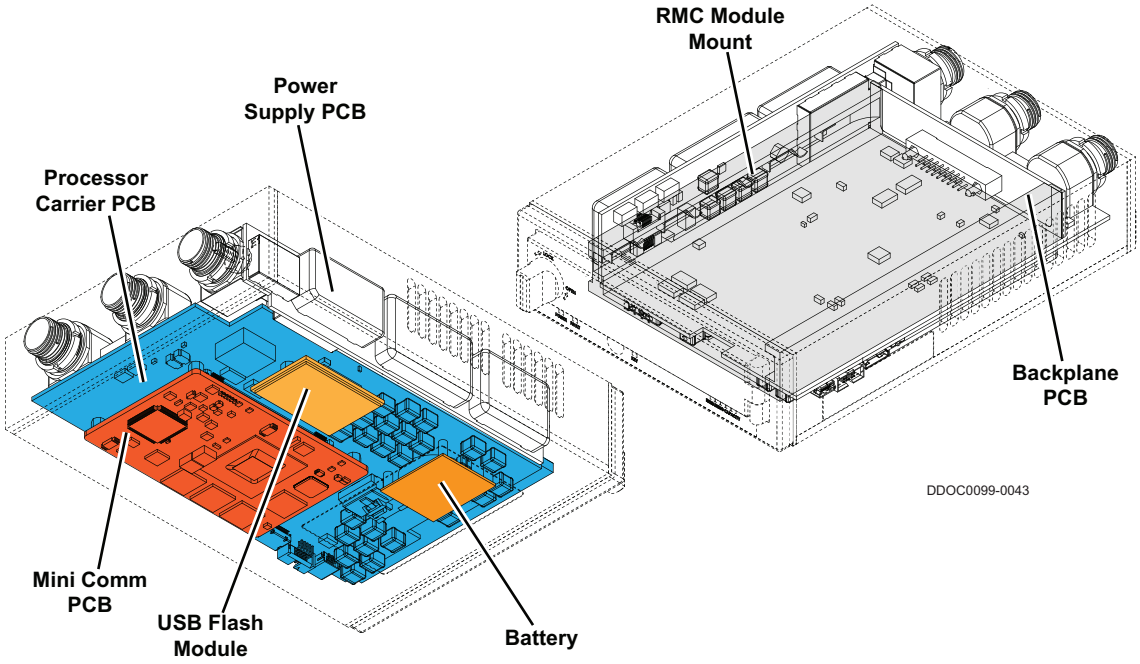

Figure 2.2 DTS1 Chassis / Components

The enclosure is compliant with Military Specification MS25212 rail mounting standard for military/ aviation utilizing Dzus quarter-turn fasteners. A standard platform mounting option is also available. Front panel LEDs give the user an at-a-glance DTS1 status report. Additional status information is available through the CLI.

Two rear panel 10/100/1000 Ethernet ports (connectors J2 and J3) (Figure 2.3) are available for network connections supporting NFS, CIFS, FTP, iSCSI, PCAP, and HTTP file transfer protocols. The DTS1 also supports the Preboot eXecution Environment (PXE) giving remote computers the capability to boot from files stored on the DTS1. Connector J2 also supports RS-232 communication protocol (primarily used for configuring the DTS1) as well as a discrete zeroize and reset function. Connector J1 is used to connect the DTS1 to 28 VDC (operating voltage). In addition, the DTS1 has a removable panel located on the underside of the unit. It is removed to allow replacement of the crypto module battery.

The E1 ground lug located on the rear of the DTS1 is electrically bonded internally to the DTS1 chassis and the EMI / safety ground on J1 pin 4. Electrically, these points are all the same. It is intended that the E1 ground lug be used as the primary equipment tie point to bond the DTS1 to the user's system/structure/facility ground. This single tie point should suffice as the chassis / EMI / safety ground for the DTS1 in most applications.

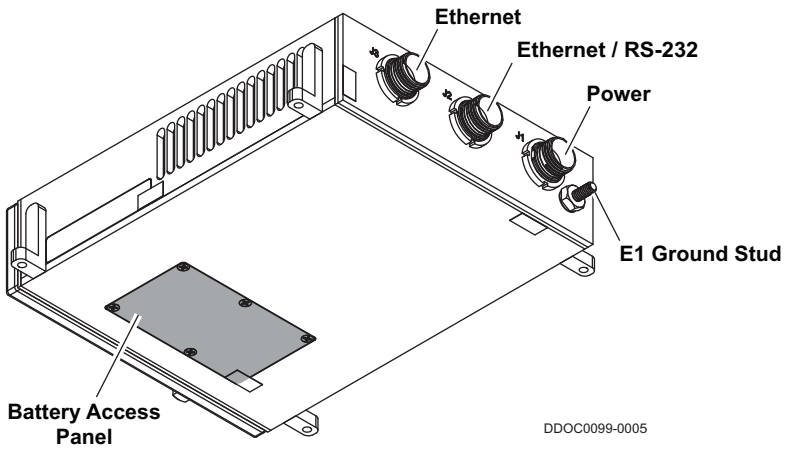

Figure 2.3 DTS1 Rear Panel / Battery Access Cover and Rear Connectors

A set of processor carrier PCB connections (Figure 2.4) is provided under a panel on the side of the DTS1. Currently they are reserved for manufacturing and service activities. Contact Curtiss-Wright for more information about end-user utilization of these connectors. A write-enable switch is provided as well. The switch must be in the READ-WRITE position to enable configuring the DTS1. Refer to paragraph 3.2.2 **Write-Enable Switch** for detailed information.

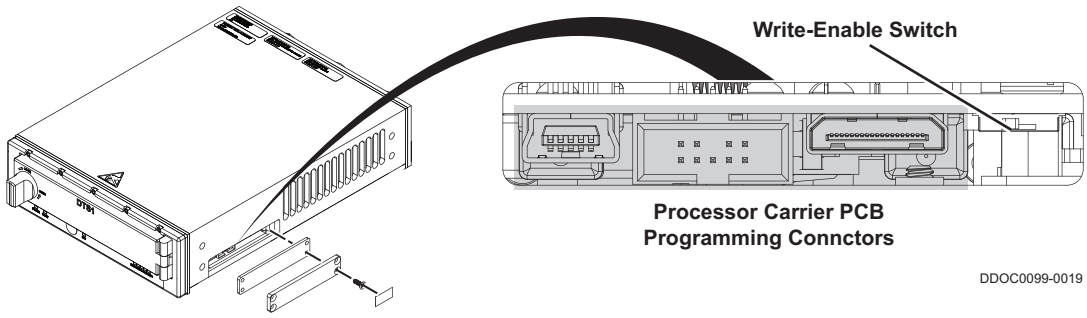

Figure 2.4 DTS1 Processor Carrier PCB Programming Connector / Write-Enable Switch

2.1.2 RMC Module

One RMC module (Figure 2.5) is housed in the DTS1. The RMC module is accessed via a sealed door with a quarter-turn latch located on the front panel of the unit. The RMC module within the DTS1 is also a rugged compact unit that can be personally transported with minimal precautions to a secure location or deployment.

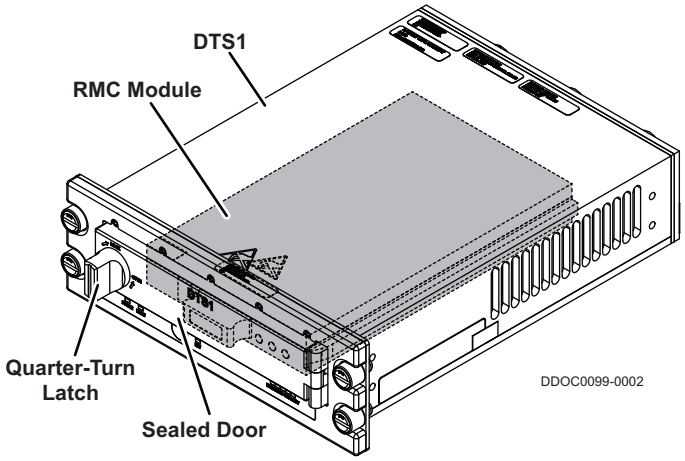

Figure 2.5 DTS1 With RMC Module

2.2 Protocols

The DTS1 supported protocols include Telnet, TFTP, CIFS, NFS, FTP, HTTP, DHCP, SNMP, and iSCSI in addition to its RS-232 console port. The CIFS and NFS protocols are enabled by default, all others are disabled. The unit also supports SSH, which is always enabled. The user can enable the desired protocols to support their application. Refer to paragraph 12.3.29 **serv** for additional information.

The FDEEEcPP20 and FDEAAcPP20 Protection Profiles did not consider, nor did they include networking protocols as part of the security functional requirements, and as a result, did not include any requirements for addressing those protocols.

Therefore, as per the FDEEEcPP20 and FDEAAcPP20, the protocols have not been examined as part of the required assurance activities and consequently the evaluation can make no claims about the DTS1's networking protocols.

2.3 CSfC Encryption

Commercial Solutions for Classified (CSfC) encryption is based on a National Security Agency (NSA) specification. The CSfC program requires multi-layered security. Hardware data encryption is used for the first security layer. The second security layer is software data encryption. Both encryption processes are performed in the DTS1, one in the HW crypto module, the other by the Processor. The hardware encryption key is retained in the DTS1 crypto module memory, the software encryption key is stored on the RMC module.

2.3.1 Hardware Encryption Layer

CAUTION
DATA LOSS. If the Specific User Token Key is lost, the user account will be rendered unusable.

NOTE
Refer to paragraph 5.3 **Hardware Layer Encryption** for information regarding the actual commands and procedures used to create and log into the hardware encryption layer.

2.3.1.1 Account Creation

Before use, an account must be created (Figure 2.6) on the DTS1 Hardware Encryption (HWE) layer. To start the account creation, the user logs into the DTS1 via the Command Line Interface (CLI). Once logged in, additional commands are entered to create an account on the DTS1 HWE layer. The HWE layer contains a Pre-Shared Key (PSK) which is generated at initial equipment power-on at the manufacturer and provided separately by Curtiss-Wright. The PSK cannot be read out of the DTS1. When the account is created, a user token key is internally generated by the HWE layer. The layer then keywraps the user token key using the PSK and supplies it to the end user through the CLI. The keywrapped user token key is validated on a third-party system by comparing the DTS1-generated HMAC and the third-party-generated HMAC. If both match, the user token is unwrapped using the PSK. The unwrapped user token key is then used in subsequent logins as the specific-user token.

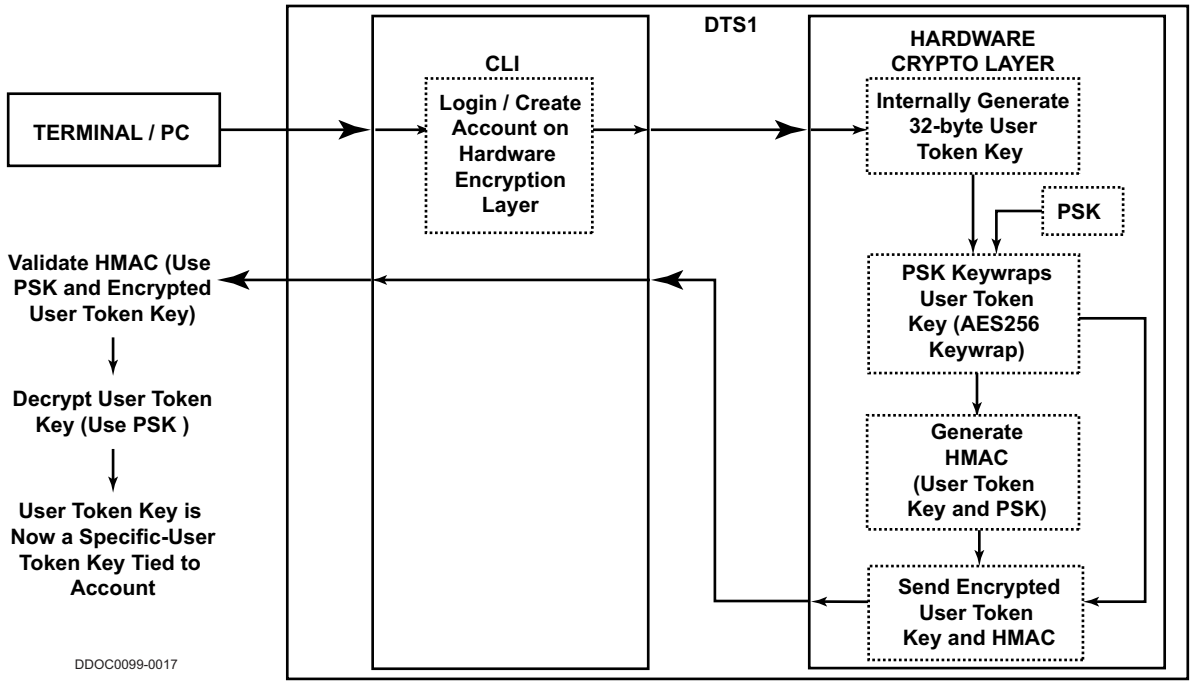

Figure 2.6 Hardware Encryption Layer Account Creation

2.3.1.2 Account Login

Any subsequent use of the equipment requires logging in (Figure 2.7) to the HWE layer before data storage and/or transfer can begin. The user enters their user name and password into the DTS1. The HWE layer checks the information against its accounts. If the user name and password are recognized, a random one-time 64-byte key (also referred to as a nonce) is generated. The nonce is sent to the end-user via the CLI. The user then enters the nonce and their specific-user token key (generated when the account was created) into a third-party HMAC-SHA384 generator using the user token as the key. The CLI then sends this data as a user-generated HMAC to the DTS1 HWE layer. The layer compares the user HMAC and the HWE layer HMAC. If they are the same, the user is logged in. If they do not compare, the user is denied access.

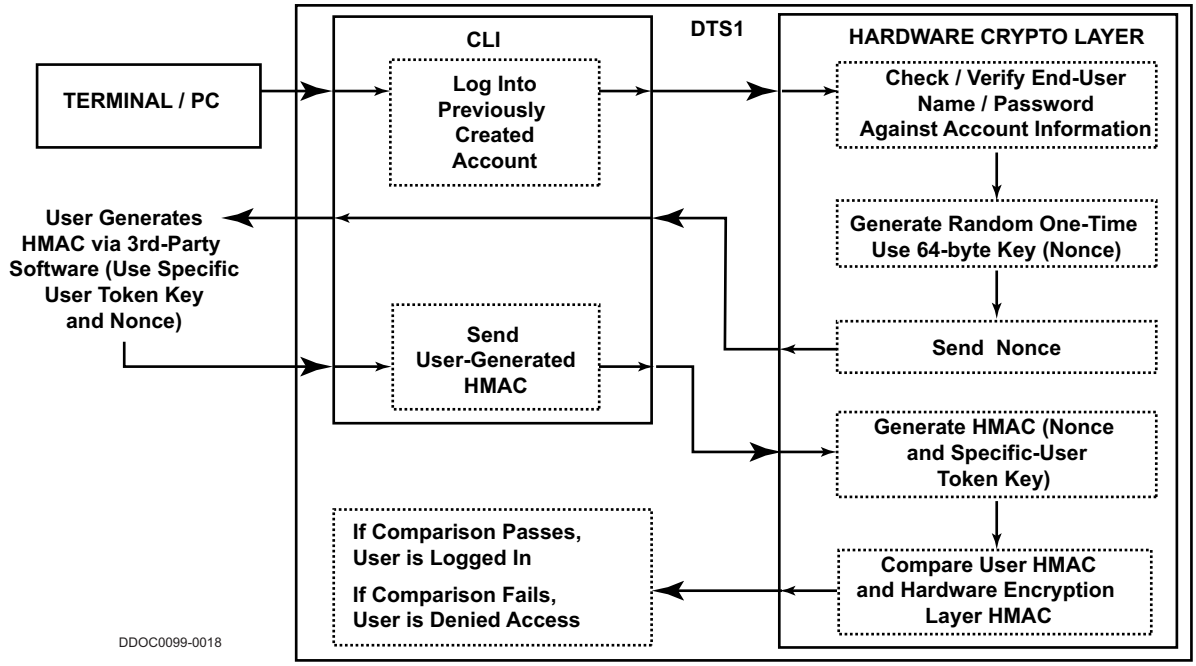

Figure 2.7 Hardware Encryption Layer Account Login

2.3.2 Software Encryption Layer

CAUTION
DATA LOSS. If the software encryption key / passphrase is lost, the RMC module will be rendered unusable.

NOTE
Refer to paragraph 5.4 **Software Layer Encryption** for information regarding the actual commands and procedures used to create and log into the software encryption layer

NOTE
If the drive is going to be partitioned, the partition(s) must be created before the software encryption is activated.

To create the software encryption layer, the user must first log into the HWE layer. After that procedure has been accomplished, creation of the Software Encryption (SWE) layer can begin.

Software encryption is performed before the RMC module is formatted or mounted. Multiple RMC modules can be encrypted using the same or different encryption key / passphrase. In addition, RMC modules can be partitioned and have each partition use the same or different encryption key / passphrase. Before attempting to encrypt the RMC module, the status should be checked. If the status is not correct, creation of the SWE layer will fail. After the software encryption has been performed, the RMC module can be formatted and mounted.

Subsequent use of the RMC module is dependent upon the proper encryption key / passphrase being entered using the CL). Failure to enter the proper information will result in the RMC module being inaccessible for data storage or use.

2.3.3 Zeroize

There are two methods to zeroize the DTS1:

- Local
- Remote

To locally initiate zeroization, the KEY CLEAR button is depressed and held for a minimum of five seconds. To remotely initiate zeroization, the Zeroize_N signal is shorted to ground for approximately five seconds.

The Zeroize_N signal (connector J2-1) is internally pulled-up to +3.3V. The external device is required to sink no more than approximately 3.3 mA when Zeroize_N is shorted to GND. This can be accomplished by a switch, relay, or an open drain/collector type semiconductor device as long as the DTS GND reference (connector J2-3) is used. Refer to paragraph B.2 **Utility Connector J2 / Utility Lab Cable** for additional information regarding external connections.

2.4 Features

- Services
  - CIFS
  - DHCP
  - FTP
  - HTTP
  - NFS
  - SNMP
  - TFTP
  - TEL
- Performance (typical)
  - NFS & CIFS, single Ethernet channel and client
    - Sustained read: 105 Megabytes per second
    - Sustained write: 108 Megabytes per second
  - NFS & CIFS, two Ethernet channels, single client per channel
    - Sustained read: 61 Megabytes per second per channel
    - Sustained write: 64 Megabytes per second per channel
- Supported block data transfer protocol
  - iSCSI
- Supported packet capture protocol
  - PCAP
- Supported video stream capture protocol
  - RTP
- Client remote boot from DTS1 via Preboot eXecution Environment (PXE)
- User control, status, & maintenance interface
  - Command Line Interface (CLI) via:
    - Secure shell (SSH)
    - Serial RS-232
    - Ethernet
  - SNMP via Ethernet
- Rear panel connections
  - J1: Power input
    - Remote Power Disable
    - MIL-STD-704E compliant +28VDC
    - 20 Watts maximum power dissipation
    - 1.3 Amps peak inrush current
  - J2: Ethernet interface, RS-232, Reset, and Zeroization
    - 10/100/1000 copper
    - IEEE 802.3, 802.u, and 802.ab
    - RS-232 serial communications
    - Zeroize discrete
    - Reset (reboot) discrete

    - J3: Ethernet interface
        - 10/100/1000 copper
        - IEEE 802.3, 802.u, and 802.ab
- Front panel controls and indicators
    - POWER LED (green)
    - FAULT LED (red)
    - KEY LOADED LED (yellow)
    - DRIVE CAPACITY LEDs
    - KEY CLEAR Button
- Built In Test (BIT) capability
    - Provides overall health and status and out-of limits detection and notification
    - Start-up BIT (SBIT) (displayed upon start up)
    - Periodic BIT (PBIT)
    - Initiated BIT (IBIT)
    - Maintenance BIT (MBIT)
    - Test control via CLI, health status query via CLI and SNMP
- Environmental, EMI Compliance, and Electrical Characteristics
    - Refer to paragraph A.5 **Environmental, EMI, Electrical Specifications** for detailed information.
- Physical
    - Dimensions and mounting compliant with Military Specification MS25212
    - Military/aviation rail mounting utilizing Dzus quarter-turn fasteners
    - Platform mounting utilizing standard L-brackets.
    - RMC module accessed via environmentally sealed front door with quarter turn locking mechanism
- Data encryption
    - Elliptical Curve Cryptography (ECC)
    - AES-256, in-line battery backed-up encryption module for encryption of data-at-rest prior to storage on RMC module
    - NIST/FIPS 140-2 certifiable
    - External encryption key loading
    - Key may be zeroized by external hardware discrete or by software command
- RMC Module
    - One module individually mounted and accessible
    - Solid-state storage
    - Optional capacities from 256 GB to 8 TB per RMC module.
    - Low insertion/removal force: 40 oz.
    - High insertion/removal cycle: > 100,000 cycles
    - Hot insertion/removal
    - User writeable cartridge/volume name/description (up to 32 characters) stored in cartridge non-volatile memory accessible via out-of-band interface.
    - RMC module removal request via front panel push button
    - LED status indicators:
        - STATUS (green): on when RMC module is installed, mounted and ready for access
        - ACTIVITY (green): on when disk is accessed (not supported on some RMC module configurations)
        - FAULT (red): DTS1 system monitor has detected a fault with the RMC module

Controls and Indicators

3.1 Chassis Indicators

The DTS1 has four LED status indicators (Figure 3.1) on the bottom of the front panel:

- POWER
- FAULT
- KEY LOADED
- DRIVE CAPACITY

The brightness of the chassis LEDs can be independently set from 0 to 100% brightness. This accomplished by changing the duty cycle of the power applied to the individual LEDs. The CLI ledctrl command is used in association with -s option to select the individual LED and -d option to select its duty cycle. See paragraph 12.3.15 **ledctrl** for detailed information.

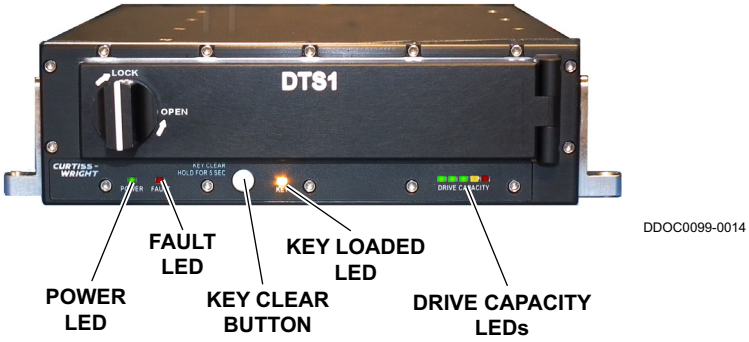

Figure 3.1 DTS1 Controls / Indicators

3.1.1 POWER LED

This LED will illuminate green shortly after the 28 volt supply is switched on. This LED remains illuminated while power is supplied.

3.1.2 FAULT LED

This LED may illuminate for a short time after power is applied (during booting) and will extinguish if the Built-In-Test (BIT) passed. The periodic BIT will illuminate this LED if it detects an anomaly such as an out of tolerance voltage level. If an error or failure has occurred in the encryption hardware or software the FAULT LED will light and no encrypted data can be transferred. If the FAULT LED remains on, try:

- Restarting the DTS1
- Reseating the RMC

Refer to the **Troubleshooting** section for possible causes and solutions. Contact Curtiss-Wright Defense Solutions if the fault indications persist.

3.1.3 KEY LOADED LED

When this yellow LED is illuminated, it indicates that the encryption key has been successfully loaded to the RMC.

3.1.4 DRIVE CAPACITY LEDs

NOTE
The capacity LEDs only correlate to the entire unpartitioned physical RMC. On partitioned RMC modules the LEDs are not valid. See paragraph 12.3.24 **rmcfree** to acquire disk and partition capacity information.

These LEDs (Figure 3.2) are an indicator of the remaining storage capacity of the installed RMC. There are 5 LEDs: 3 GREEN, 1 AMBER, and 1 RED. When all 5 LEDs are on, this indicates that there is approximately 80% to 100% of RMC storage capacity available. As storage is utilized in the RMC the LEDs will be extinguished in succession starting from left to right. LEDs may take up to a minute to change state when capacity remaining crosses the thresholds.

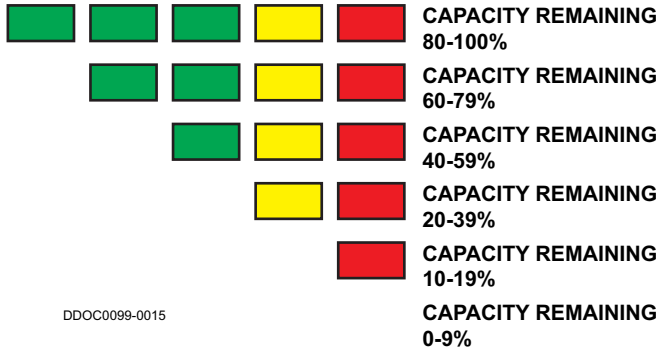

Figure 3.2 Remaining Disk Capacity Indicators

3.2 Chassis Controls

3.2.1 Key Clear Button

When this button is pushed and held for a minimum of 5 seconds, all encryption related material within the DTS1 will be erased. This includes loaded keys, stored keys, and all previously loaded login/authentication credentials (user names and passwords). After zeroization, the yellow KEY LOADED LED will turn off. In order to use the unit again the encryptor will require reinitialization and any previously loaded credentials and keys to be reloaded.

3.2.2 Write-Enable Switch

CAUTION
EQUIPMENT DAMAGE. Exercise ESD precautions when installing, removing, or handling the DTS1.

CAUTION
EQUIPMENT DAMAGE. Extreme caution must be used to ensure all ESD handling precautions are followed when setting the write-enable switch. Failure to properly handle the DTS1 will result in equipment damage.

The write-enable switch (Figure 3.3) is used to lock the USB flash memory so it cannot be inadvertently changed. The switch is placed in the READ-WRITE position to configure the flash memory. After the configuration is set, the switch is moved to the READ position.

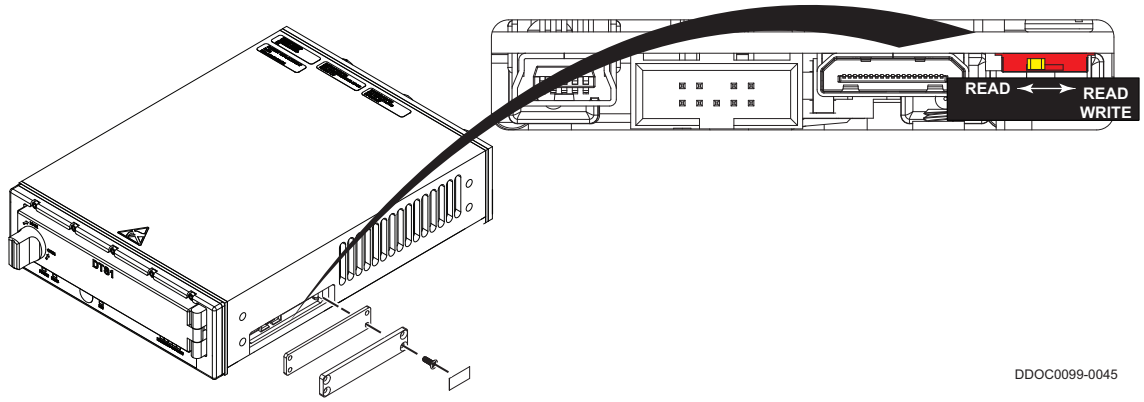

Figure 3.3 DTS1 Write-Enable Switch

3.3 RMC Module Controls / Indications

The RMC module (located behind the DTS1's storage bay door) has its own controls / indicators as shown in Figure 3.4. The function of these controls and indicators is as follows.

3.3.1 STATUS LED (Green / Left)

When this green (left) LED is illuminated it indicates that the RMC module is functioning properly. If there is a change in status or a problem, this LED will indicate the nature of the condition by the behavior outlined in Table 3.1.

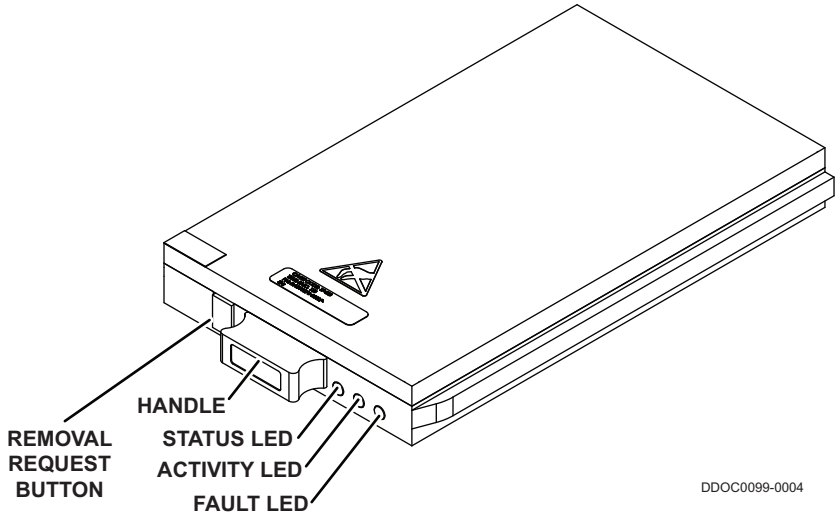

Figure 3.4 RMC Module Controls / Indicators

Table 3.1 RMC Module STATUS LED Indications

LED Behavior	Meaning
Steady On	RMC module detected, mounted, and ready
Steady Off	RMC module not detected
Slow blinking (1Hz)	RMC module detected, not mounted
Fast blinking (5Hz) for 2 seconds	Button-hold acknowledge*
1 blink, 4 seconds off	Ready for removal*
2 blink, 3 seconds off	Auto-mount failure
5 blink, 3 seconds off	RMC module monitoring error

3.3.2 ACTIVITY LED (Green / Middle)

This green (middle) LED is an indicator of SATA disk activity. This function is not supported on all configurations.

3.3.3 FAULT LED

This red LED indicates the BIT has failed or an operational anomaly was detected such as power levels, data connections, or optional security functions. This LED will be ON during initialization and then remain OFF during normal operation. See the **Troubleshooting** section for actions to take if the RMC module FAULT LED is illuminated.

3.3.4 Removal Request Button

CAUTION
EQUIPMENT DAMAGE. Exercise ESD precautions when installing, removing, or handling the RMC module.

CAUTION
EQUIPMENT DAMAGE. The RMC is hot-swappable (remove / install with power applied), however, extreme caution must be used to ensure all ESD handling precautions are followed.

Press and hold this button for three to five seconds to request removal of the RMC module. The STATUS LED will blink at 5Hz for two seconds to acknowledge the request. After acknowledgment, the system will unmount and prepare the RMC module for removal. When the RMC module is ready for removal, the STATUS LED will blink one time every five seconds. Removal may also be requested with the CLI command rmcctl.

Installation

CAUTION
EQUIPMENT DAMAGE. Exercise ESD precautions when installing, removing, or handling the DTS1.

4.1 Package

NOTE
Either L-brackets or a Dzus mount is included depending on the ordered configuration.

The DTS1 package contents are listed below:

- DTS1 Chassis
  - L-Brackets*
  - Dzus Mount*
- Product Documentation CD

Optional Items (Refer to **Ordering Information** section for part numbers).

- RMC Module(s)
- Power Lab Cable
- Utility Lab Cable
- Ethernet Lab Cable

4.2 Inspection

The DTS1 is a two-part data storage system that consists of a DTS1 chassis and a RMC module. Additional accessories may be included (if ordered). All received items should be inspected for damage. Inspect all units as follows:

- All screws should be tight.
- The door gasket should be free from any cuts, crushing, or flattening damage
- All anti-tamper labels (Figure 4.1 and Figure 4.2) should be unbroken.
- All components should be free from any dents, cracks, or damage.
- All connectors pins should be present, straight, and undamaged.

If the DTS1 chassis or any accessories were damaged in shipping or the enclosure was breached, immediately notify Curtiss-Wright Defense Solutions or your supplier.

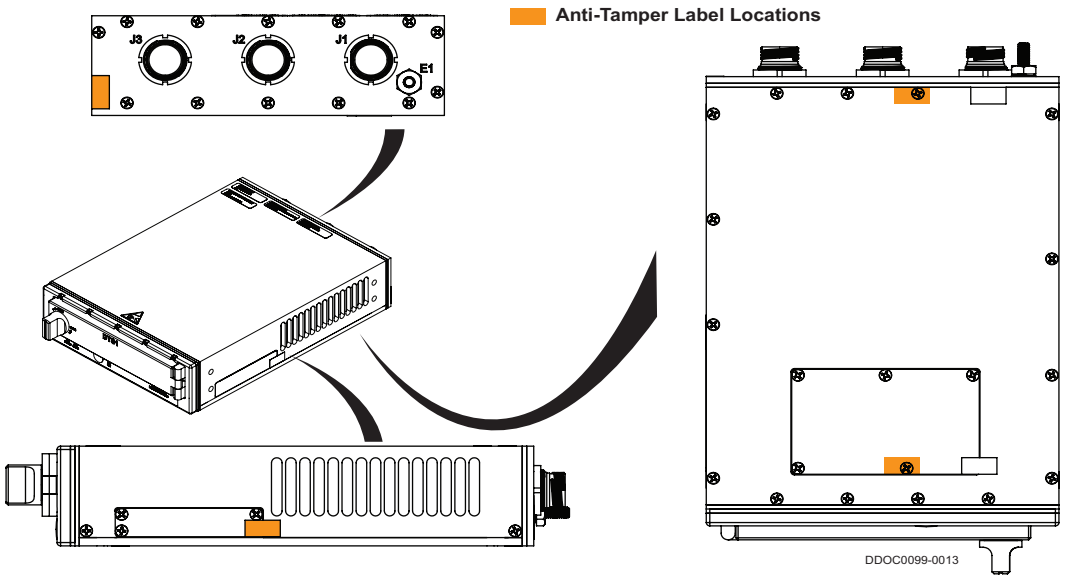

Figure 4.1 DTS1 Chassis Anti-Tamper Label Locations

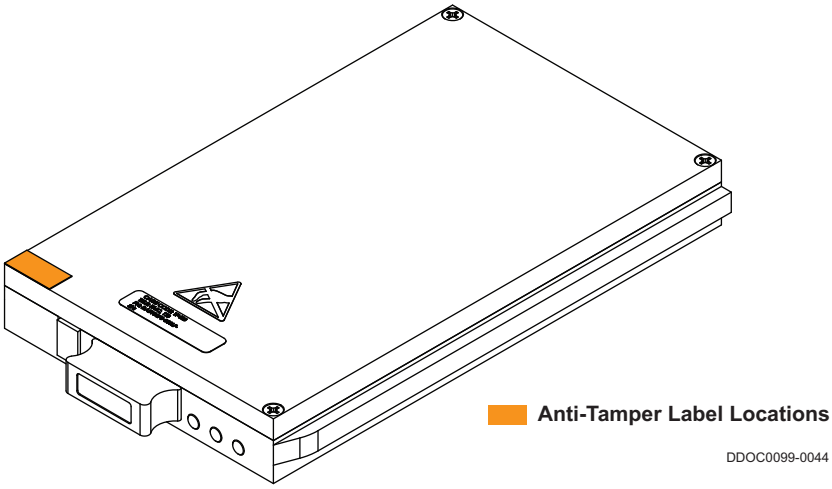

Figure 4.2 RMC Module Anti-Tamper Label Location

4.3 Mounting

Mounting environment considerations should include operating temperature limits, humidity, and vibration limits. Other considerations should include clearance for mounting hardware, cables, and safe installation or removal of the DTS1 chassis from its mounting structure. Precautions should be taken when cables are routed around structures that could cause excessive abrasion, such as around the corner of vibrating equipment.

Installation of the DTS1 can put an increased demand on cooling systems by raising ambient air temperatures. Evaluate changes in airflow obstructions and temperatures around equipment and possible detrimental surface temperatures due to conducted heat. See paragraph A.5 **Environmental, EMI, Electrical Specifications**for thermal limit specifications.

Two mounting methods (Figure 4.3) provide secure attachment to a platform: standard platform mounting brackets or a Dzus mount. This will require the acquisition of the appropriate mounting components and precise installation per the selected platforms mounting specifications. Mechanical mounting of the DTS1 with Dzus option requires compliance to MIL-STD MS25212. If installation and removal of the RMC module is desired while the DTS1 remains mounted, be sure to allow clearance (Figure 4.4) for the door to open and the RMC module to be positioned in front of the DTS1.

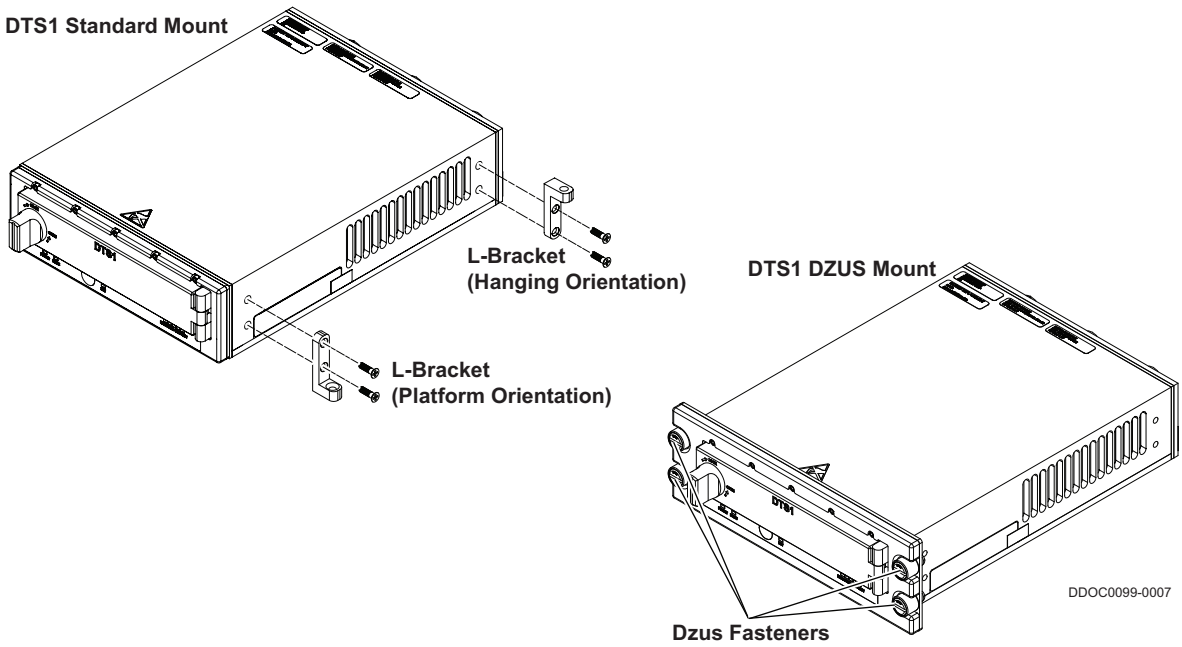

Figure 4.3 DTS1 Chassis Mounting

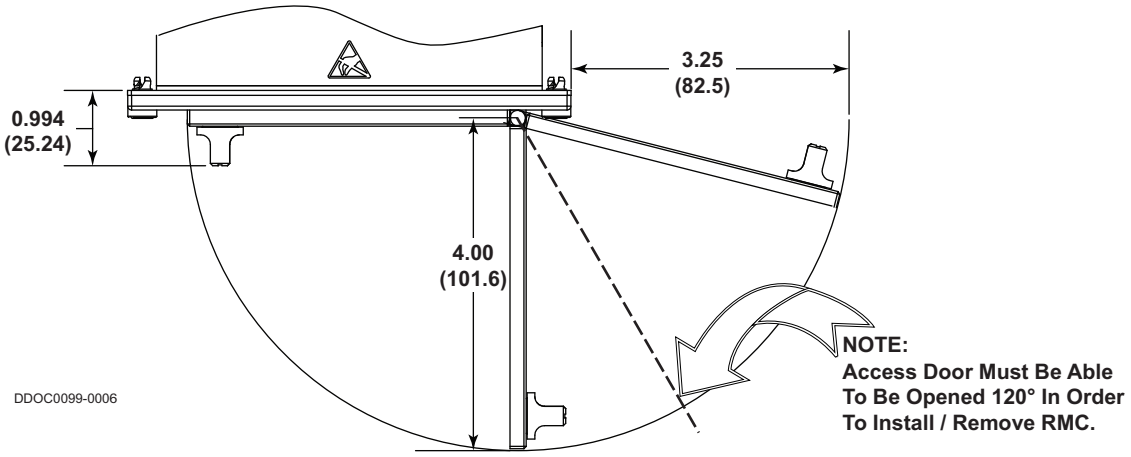

Figure 4.4 DTS1 Required Door Clearance

4.4 Cables

All connections to the DTS1 are on the rear panel (Figure 4.5). Be sure the power supply is off when making connections.

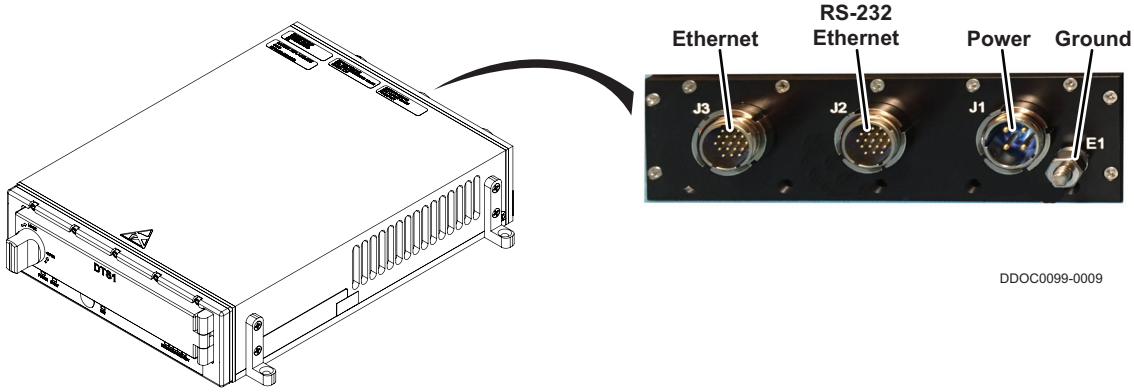

Figure 4.5 DTS1 Rear Panel Connectors

4.4.1 Power Cable

The Power Lab Cable (VS-DTS1PWRCAB-0) (Figure 4.6) is used to make power connections to the DTS1. The DTS1 requires an input power of +28 volts and ground. Refer to paragraph B.1 **Power Connector J1 / Power Lab Cable** for connector pin signal information.

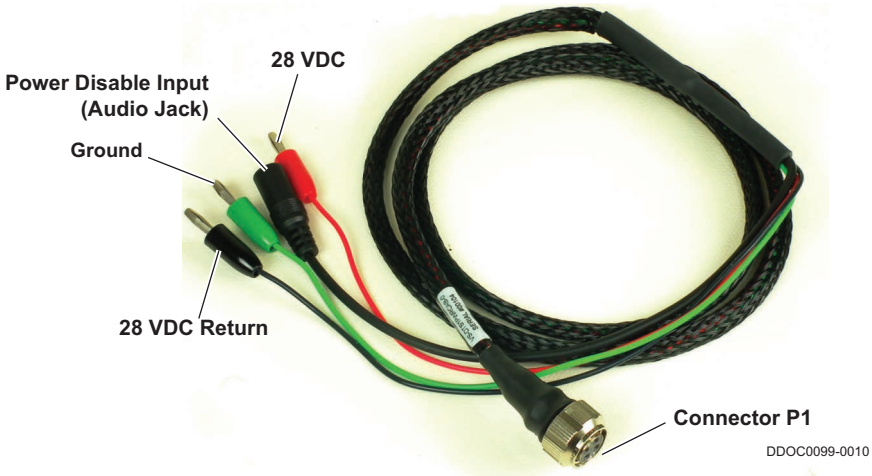

Figure 4.6 Power Lab Cable

Connections

- The 4-pin connector (P1) mates to DTS1 J1.
- The red plug connects to 28 VDC.
- The black plug connects to 28 VDC return.
- The green plug connects to chassis ground.
- The audio jack (if used) connects to a user-designed power disable switch.

4.4.2 Utility Cable

The Utility Lab Cable (VS-DTS1ETHCAB-J2) (Figure 4.7) is used for initial setup operations through RS-232 or Ethernet. Refer to paragraph B.2 **Utility Connector J2 / Utility Lab Cable** for connector pin signal information.

Connections

- The 19-pin connector (P1) mates to DTS1 J2.
- The RJ-45 plug (P2) connects to a terminal or PC Ethernet port.
- The DB-9 connector (J1) mates to a terminal or PC serial port.
- The audio jack (J2) connects to user-configured switches for zeroization and reboot.

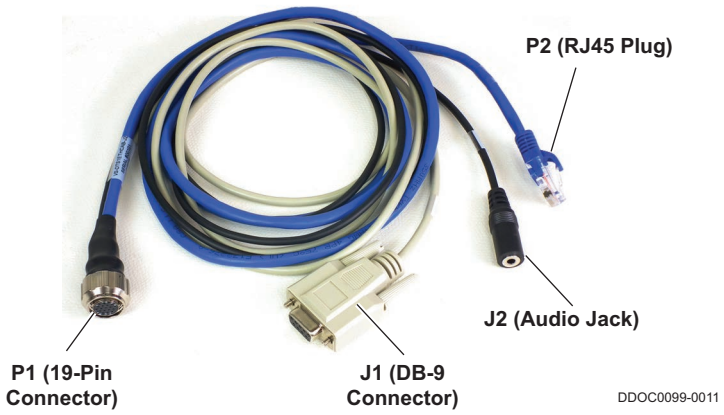

Figure 4.7 Utility Lab Cable

4.4.3 Ethernet Cable

The Ethernet Lab Cable (VS-DTS1ETHCAB-J3) (Figure 4.8) is used to make network connections to the DTS1. Refer to paragraph B.3 **Ethernet Connector J3 / Ethernet Lab Cable** for connector pin signal information.

Connections

- The 19-pin connector (P1) mates to DTS1 J3.
- The RJ-45 plug (P2) connects to the desired network outlet panel, hub, etc.

Figure 4.8 Ethernet Lab Cable

4.4.4 Ground Cable

NOTE
Do not loosen nut / washer installed on ground stud E1. Ensure nut / washer on ground stud remain properly tightened when installing / removing ground cable.

To ensure proper grounding of the DTS1, a ground cable, split lock washer, and hex nut are required, but not provided. The ground cable (Figure 4.9) terminal is installed on the DTS1 ground stud E1. Refer to paragraph B.4 **Ground Cable** for detailed installation instructions.

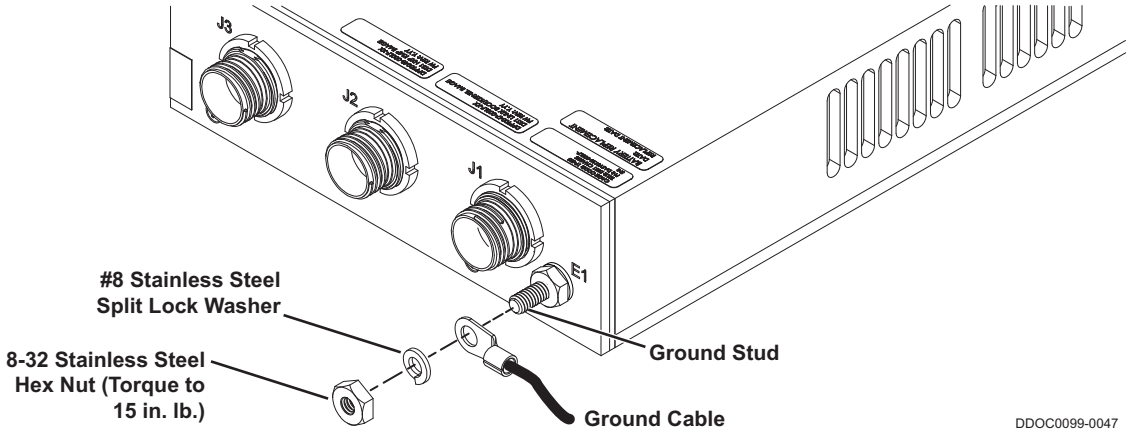

Figure 4.9 DTS1 Ground Connection

Encryption

NOTE

Throughout this section, yellow highlighted text is used to denote user-defined or software-generated inputs. Green highlighted text is used to show changes in values, settings, or responses due to implementation of a software command.

5.1 Passwords / Passphrases

5.1.1 Hardware Layer Passwords

The following is required for hardware layer passwords:

- Must be 8-64 characters in length.
- Must contain at least one number.
- Must contain at least one alpha character.
- No special characters allowed.

5.1.2 Software Layer Passwords / Passphrases

The following is required for software layer passwords / passphrases:

- Must be 15-512 characters in length.
- If using password, must pass dictionary test.
- Requires at least 1 upper case char, 1 lower case char, 1 number, and 1 special character.
- A character must not repeat more than 3 times.
- There shall be no more than 4 consecutive characters from a single character class (no more than 4 digits, lower case, upper case, or special characters in a row).

5.1.3 Incorrect Password / Passphrase Entered

Hardware Layer

The hardware layer password can be incorrectly entered two times without issue. On the third try if an incorrect password is entered, the hardware layer key will automatically zeroize. Once this occurs, the DTS1 will need to be reinitialized with the correct password.

Software Layer

The software layer password /passphrase can be incorrectly entered four times without issue. On the fifth try if an incorrect password / passphrase is entered, the DTS1 will automatically reboot. There is no limitation to the number of times an incorrect entry /reboot occurs.

5.1.4 Change Password / Passphrase

Hardware Layer

To change the hardware layer password the following must occur:

- The hardware layer must be zeroized. Refer to paragraph 5.5 **Zeroize HWE Key / Delete SWE Container / RMC Purge** for information.
- A new account must be created using the new / changed password. Refer to paragraph 5.3.1 **Initialize / Login - Crypto Module** and paragraph 5.3.3 **Access RMC Module (Plain Text DEK / Encrypted DEK)** for information.

Software Layer

To change the software layer password the following must occur:

- The software layer container(s) must be deleted. Refer to paragraph 5.5 **Zeroize HWE Key / Delete SWE Container / RMC Purge** for information.
- New software container(s) must be created using the new / changed password. Refer to paragraph 5.4.1.1 **Initialize Container (Unpartitioned Disk)** for information.

5.2 Check Hardware Layer Status

NOTE
All values listed below should equal na or 0 for a new DTS1 / RMC module.

1. Check login status

   Command:
   `cmlogin`
   - init =0 not initialized / =1 initialized
   - login =0 not logged into / =1 active login

Example:

```
cw_dts> cmlogin
 [cmlogin]
  CMLOGIN: state=uninit/init init=<0/1> login=<0/1> status=OK
 [!cmlogin] OK
```

2. Check key status

   Command:
   `cmkey`
   - init =0 not initialized / =1 initialized
   - login =0 not logged into / =1 active login
   - s0 =0 no key loaded / =1 key loaded

NOTE
In the example below id=<int> is the crypto module ID. The deks=0x0 is the location information for saved keys. See paragraph 3.2.2 **Write-Enable Switch** for information regarding key storage location.

Example

```
cw_dts> cmkey
 [cmkey]
  CMKEY: id=<int> init=<0/1>login=<0/1>s0=<0/1>s1=<0>s2=<0> deks=0x0 status=OK
 [!cmkey] OK
```

3. Check RMC module status

   Command:
   `rmcctl`
   - scryp =na / =0 no software encryption / =1 software encryption present
   - fmt =na / =0 not formatted / =1 formatted
   - mnt =na / =0 not mounted / =1 mounted

Example

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:  ins  hcryp  osdr  p#  size   serv   scryp   osdm    fmt     mnt    rem  mntpoint
  ********************************************************************************
  RMC_S0:   1     na     na   --  ----   ----  na/0/1    na    na/0/1  na/0/1   0     ----
 [!rmcctl] OK
```

5.2.1 Hardware Layer Definitions

NOTE
The cmkey command applies only to the hardware encryption layer. The software encryption layer is controlled by options associated with the rmcctl command.

The key management command cmkey provides the user the ability to compose keys, load and unload keys to the RMC module, save keys in the crypto module, delete saved keys, and set up an auto-load key feature. All of these functions are explained in the following subsections.

Before proceeding, it is helpful to have a brief description of the terms used in the subsections that follow.

Key..... This term is used in the context of the RMC module, referring to the DEK and PSK or EDEK and MAC. The singular form key applies to all keys required by the RMC module.

DEK ..... Data Encryption Key in plain text.

EDEK..... Encrypted DEK is a DEK that is encrypted or wrapped.

PSK..... Pre-Shared Key is a common key between the user workstation and the DTS1 crypto module, allowing each to read the encryption of the other.

KEK..... Key Encryption Key is the key used to create the EDEK.

MAC..... Message Authentication Code is a value used to validate messages carrying a key.

CM ..... Crypto Module is the circuitry in the DTS1 that manages encryption keys and uses them to encrypt/decrypt data.

Install ..... Sending the key from the user's workstation to the encryption chip serving a specified RMC module slot.

Save..... Store a key to the CM memory.

Load..... Move (copy) the saved key from the CM memory to the encryption chip serving a specified RMC module slot.

Unload ..... Removal of the key from the CM encryption chip.

Delete ..... Removal of the key from the CM memory.

5.3 Hardware Layer Encryption

5.3.1 Initialize / Login - Crypto Module

NOTE

`[username]` and `[password]` are selected and entered by the user.

- User name (-u) requirement is 1-15 characters in length.
- Password (-p) requirement: see paragraph 5.1.1 **Hardware Layer Passwords** for requirements.

1. Obtain user token.

   Command:

   ```
   cmlogin -u [username] -p -I
   ```

Example

```
cw_dts> cmlogin -u [username] -p -I
  [cmlogin]
   Please enter password: [password]
   Please verify password: [password]
   CMLOGIN: action=init status=OK
   USER_TOKEN=[Generated random string 128 characters (64 bytes Hex) long]
   TOKEN_HMAC=[Generated random string 96 characters (48 bytes Hex) long]
   PSK=[Curtiss-Wright provided. 64 f's will be shown in place of the actual PSK]
  [!cmlogin] OK
```

NOTE

Decrypting the user token requires a 3rd-party AES256 key-unwrapping algorithm and the PSK.

2. Decrypt user token.
3. Generate challenge.

   Command:

   ```
   cmlogin -u [username] -p -L
   ```

Example

```
cw_dts> cmlogin -u [username] -p -L
 [cmlogin]
  Please enter password: [password]
  CHALLENGE=[Generated random string 128 characters (64 bytes Hex) long]
 [!cmlogin] OK
```

NOTE
Generating the HMAC requires the decrypted user token, challenge, and a HMAC hash generator that supports the SHA-384 algorithm.

4. Generate the HMAC.
5. Login to crypto module.

   Command:
   cmlogin -M [Generated HMAC string]

Example

```
cw_dts> cmlogin -M [Generated HMAC string]
 [cmlogin]
  CMLOGIN: action=auth status=ok
 [!cmlogin] OK
```

5.3.2 Verify Successful Login

To verify a successful login type **cmlogin** and press ENTER key.

- State should show ready
- Init show 1
- Status show OK

Example

```
cw_dts> cmlogin
 [cmlogin]
  CMLOGIN: state=ready init=1 status=OK
 [!cmlogin] OK
```

5.3.3 Access RMC Module (Plain Text DEK / Encrypted DEK)

CAUTION
DATA ACCESS. Use of slot option (-s 0) is required to when entering key (DEK and PSK).

NOTE
Use of -s 0 option denotes slot 0, -F option forces an over-write of any key previously installed.

Entering a plain text DEK **or** an encrypted DEK (EDEK) is required to access the RMC. The EDEK provides additional security, but requires additional effort on the part of the user.

5.3.3.1 Access RMC Module (Plain Text DEK)

NOTE
The DEK is a user-generated 64-character string.

1. To access the RMC, enter the DEK and PSK.
2. Type **cmkey -s 0 -d -p --force** and press ENTER key.

Example

```
cw_dts> cmkey -s 0 -d -p --force
 [cmkey]
  Please enter plaintext DEK: [User-generated plain text DEK string]
  Please enter current PSK: [Curtiss-Wright provided PSK string]
  CMKEY: action=inst slot=0 status=ok
 [!cmlogin] OK
```

5.3.3.2 Access RMC Module (EDEK)

1. Generate an EDEK as follows:
   a. To obtain the KEK and associated MAC type **`cmkey --kek`** and press ENTER key.

Example

```
cw_dts> cmkey --kek
 [cmkey]
  CMKEY: kek=[KEK] mac=[MAC]
  status=OK
 [!cmkey] OK
```

   b. Using a 3rd-party HMAC SHA384 application, generate an HMAC using the KEK and Curtiss-Wright supplied PSK as the key.
      - The generated HMAC should be the same as the MAC from the example above.
   c. Using a 3rd-party application capable of performing an AES256 key-unwrapping algorithm, perform an AES key unwrap function on the KEK using the PSK. This will yield the actual/unwrapped KEK you will use to encrypt your DEK.
   d. Using a 3rd-party application capable of performing an AES256 key wrap function, encrypt the DEK using the unwrapped KEK. This will yield the wrapped/encrypted DEK (EDEK).
   e. Using a 3rd-party HMAC SHA384 application, calculate a new MAC using the HMAC SHA384 function for the EDEK using the unwrapped KEK as the key.
2. To access the RMC, enter the EDEK and MAC.
3. Type **`cmkey -s 0 -e [EDEK string] -m [MAC string] -force`** and press ENTER key.

Example

```
cw_dts> cmkey -s 0 -e [EDEK string] -m [MAC string] -force
 [cmkey]
  CMKEY: action=inst slot=0 status=ok
 [!cmlogin] OK
```

5.3.4 Hardware Encryption Key Storage

NOTE
This section is no longer applicable and has been deleted.

5.4 Software Layer Encryption

CAUTION
DATA SECURITY. Be sure to CLOSE the SSH session after initializing or entering the software encryption layer. Leaving the SSH session open can expose the passphrase to unauthorized access.

CAUTION
DATA SECURITY. Only SSH session may be used for configuring software encryption layer. The console or serial port cannot be used for setting up software encryption as the passphrase is not cleared from memory as required.

NOTE
The RMC module must have services assigned before the software encryption layer can be initialized / entered.

The rmcctl -C command allows the user to view and alter the DTS1 disk encryption options. The software encryption layer uses containers to hold the data. Creation of a container requires the use of a password or passphrase. Refer to paragraph 5.1.2 **Software Layer Passwords / Passphrases** for requirements.

5.4.1 Unpartitioned Disk

Disks cannot be partitioned after software encryption has been performed.

5.4.1.1 Initialize Container (Unpartitioned Disk)

CAUTION
DATA LOSS. Initializing SWE will overwrite / destroy any existing data on the disk. As a result the --force option must be used.

Initialize a Software Encryption (SWE) container on an RMC module as follows:

1. Type **`rmcctl --force -C`** and press ENTER key.

NOTE
After the above command has be issued, the user must acknowledge that all data on the disk will be overwritten

2. At the overwrite query prompt type **`YES`** and press ENTER key.

NOTE
Refer to paragraph 5.1.2 **Software Layer Passwords / Passphrases** for requirements.

3. Enter a password / passphrase that complies with the password / passphrase requirements and press ENTER key.
4. Reenter the password / passphrase and press ENTER key.
   - If the passphrase is entered correctly both times and meets the requirements the following message will be displayed: `RMC_C0; action=cryp status=OK`.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     --   100GB   NAS     1      0     na    na    0     rmc0
 [!rmcctl] OK
```

5.4.1.2 Open SWE Container (Unpartitioned Disk)

NOTE
The SWE container must be opened before it can be used.

Open the SWE container on an RMC module as follows:

1. Type **`rmcctl -E`** and press ENTER key.

NOTE
After five failed attempts to open the SWE container, the DTS1 will reboot and another five attempts be granted.

2. Enter the password / passphrase and press ENTER key.
   - If the passphrase is entered correctly the following message will be displayed: `RMC_C0; action=enter status=OK 'Resetting attempts to 0".`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     --   100GB   NAS     1      1      0    na    0     rmc0
 [!rmcctl] OK
```

5.4.1.3 Format / Mount SWE Container (Unpartitioned Disk)

NOTE
NTFS format is not allowed on a software encrypted RMC module.

After opening the SWE container, it can be formatted, mounted, and used.

- To format only:
  Command:
  `rmcctl -F`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     --   100GB   NAS     1       1     ext4   0     0      rmc0
 [!rmcctl] OK
```

- To format and mount:
  Command:
  `rmcctl -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     --   100GB   NAS     1       1     ext4   1     0      rmc0
 [!rmcctl] OK
```

5.4.1.4 Close SWE Container (Unpartitioned Disk)

NOTE
To close the SWE container it must be unmounted.

1. Type **`rmcctl -U`** and press ENTER key.
2. Type **`rmcctl -X`** and press ENTER key.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     --   100GB   NAS     1       0     na     na    0      rmc0
 [!rmcctl] OK
```

5.4.1.5 Delete SWE Container (Unpartitioned Disk)

CAUTION
LOSS OF CONTENT. Deletion of the SWE container will result in making the stored content unrecoverable.

To delete software encryption layer container:

Command:
`rmcctl -D`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     --   100GB   NAS     0       na    0     na    0      rmc0
 [!rmcctl] OK
```

5.4.2 Partitions

NOTE
Refer to paragraph 5.1.2 **Software Layer Passwords / Passphrases** for requirements.

Partitions can have the same or different passwords / passphrases assigned.

5.4.2.1 Initialize SWE Containers (Partitions - Different Passphrases)

CAUTION
DATA LOSS. Initializing the software encryption layer will overwrite / destroy any existing data on the partition. As a result the **`--force`** option must be used.

1. Initialize the SWE container on partition 1 of a 100GB RMC module as follows:
   a. Type **`rmcctl -p 1 --force -C`** and press ENTER key.
   b. After the above command has be issued, the user must acknowledge that all data on the partition will be overwritten
   c. At the overwrite query prompt type **`YES`** and press ENTER key.

NOTE
Refer to paragraph 5.1.2 **Software Layer Passwords / Passphrases** for requirements.

2. Enter a password / passphrase that complies with the password / passphrase requirements and press ENTER key.
   d. Reenter the password / passphrase and press ENTER key.
      - If the passphrase is entered correctly both times and meets the requirements the following message will be displayed: `RMC_C0; action=cryp status=OK`.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   50 GB   NAS     1       0     na    na     0     rmc0p1
  RMC_S0:    1      1       1     2   50 GB   NAS     0      na     0     na     0     rmc0p2
 [!rmcctl] OK
```

3. Initialize the SWE container on partition 2 of a 100GB RMC module as follows:
   a. Type **`rmcctl -p 2 --force -C`** and press ENTER key.
   b. After the above command has be issued, the user must acknowledge that all data on the partition will be overwritten
   c. At the overwrite query prompt type **`YES`** and press ENTER key.
   d. Enter a password / passphrase than is different than the partition 1 passphrase and complies with the password / passphrase requirements.
   e. Press ENTER key.
   f. Reenter the password / passphrase and press ENTER key.
      - If the passphrase is entered correctly both times and meets the requirements the following message will be displayed: `RMC_C0; action=cryp status=OK`.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   50 GB   NAS     1       0     na    na     0     rmc0p1
  RMC_S0:    1      1       1     2   50 GB   NAS     1       0     na    na     0     rmc0p2
 [!rmcctl] OK
```

5.4.2.2 Open SWE Container (Partitions - Different Passphrases)

NOTE
The SWE containers must be opened before they can be used.

1. Open the SWE container on partition 1 of a 100GB RMC module as follows:

a. Type **`rmcctl -p1 -E`** and press ENTER key.

b. Enter the partition 1 password / passphrase and press ENTER key.

- If the passphrase is entered correctly the following message will be displayed: `RMC_C0; action=enter status=OK 'Resetting attempts to 0".`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   50 GB   NAS     1      1      0     na    0     rmc0p1
  RMC_S0:    1      1      1     2   50 GB   NAS     1      0      0     na    0     rmc0p2
 [!rmcctl] OK
```

2. Open the SWE container on partition 2 of a 100GB RMC module as follows:

a. Type **`rmcctl -p2 -E`** and press ENTER key.

b. Enter the partition 2 password / passphrase and press ENTER key.

- If the passphrase is entered correctly the following message will be displayed: `RMC_C0; action=enter status=OK 'Resetting attempts to 0".`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   50 GB   NAS     1      1      0     na    0     rmc0p1
  RMC_S0:    1      1      1     2   50 GB   NAS     1      1      0     na    0     rmc0p2
 [!rmcctl] OK
```

5.4.2.3 Initialize SWE Encryption (Partitions - Same Passphrase)

CAUTION

DATA LOSS. Initializing the software encryption layer will overwrite / destroy any existing data on the partition. As a result, the **`--force`** option must be used.

Initialize the SWE containers on all partitions of a 100GB RMC module as follows:

1. Type **`rmcctl -p all --force -C`** and press ENTER key.
2. Partition 1

a. After the above command has be issued, the user must acknowledge that all data on the partitions will be overwritten

b. At the overwrite query prompt type **`YES`** and press ENTER key.

NOTE

Refer to paragraph 5.1.2 **Software Layer Passwords / Passphrases** for requirements.

c. Enter a partition 1 password / passphrase that complies with the password / passphrase requirements and press ENTER key.

d. Reenter the password / passphrase and press ENTER key.

- If the passphrase is entered correctly both times and meets the requirements the following message will be displayed: `RMC_C0; action=cryp status=OK`.

3. Partition 2

a. At the overwrite query prompt type **`YES`** and press ENTER key.

b. Enter the same password / passphrase for partition 2 and press ENTER key.

c. Reenter the password / passphrase and press ENTER key.

- If the passphrase is entered correctly both times and meets the requirements the following message will be displayed: `RMC_C0; action=cryp status=OK`.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   50 GB   NAS     1      0     na    na     0    rmc0p1
  RMC_S0:    1      1      1     2   50 GB   NAS     1      0     na    na     0    rmc0p2
 [!rmcctl] OK
```

5.4.2.4 Open SWE Container (Partition - Same Passphrase)

NOTE
The SWE containers must be opened before they can be used.

Open the SWE containers on all partitions of a 100GB RMC module as follows:

1. Type **`rmcctl -p all -E`** and press ENTER key.
2. Partition 1: Enter the password / passphrase and press ENTER key.
3. Partition 2: Enter the password / passphrase and press ENTER key.
   - If the passphrase is entered correctly the following message will be displayed: `RMC_C0; action=enter status=OK 'Resetting attempts to 0".`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   50 GB   NAS     1      1     0    na     0    rmc0p1
  RMC_S0:    1      1      1     2   50GB    NAS     1      1     0    na     0    rmc0p2
 [!rmcctl] OK
```

5.4.2.5 Format / Mount SWE Containers (Individual Partitions)

NOTE
NTFS format is not allowed on software encrypted RMC module partitions.

After opening the SWE containers on individual partitions, they can be formatted, mounted, and used.

- To only format the SWE containers:
  Command:
  `rmcctl -p 1 -F`
- To format and mount the SWE containers:
  Command:
  `rmcctl -p 2 -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   100GB   NAS     1      1    ext4   0     0    rmc0p1
  RMC_S0:    1      1      1     2   25 GB   NAS     1      1    ext4   1     0    rmc0p2
 [!rmcctl] OK
```

5.4.2.6 Format / Mount SWE Containers (All Partitions)

NOTE
NTFS format is not allowed on software encrypted RMC module partitions.

After opening the SWE containers on individual partitions, they can be formatted, mounted, and used.

- To only format the SWE containers:
  Command:
  `rmcctl -p all -F`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     1       1     ext4   0     0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     1       1     ext4   0     0     rmc0p2
 [!rmcctl] OK
```

- To format and mount the SWE containers:
  Command:
  `rmcctl -p all -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     1       1     ext4   1     0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     1       1     ext4   1     0     rmc0p2
 [!rmcctl] OK
```

5.4.2.7 Close SWE Containers (Individual Partitions)

NOTE
To close the SWE container on a partition it must be unmounted.

1. Type **`rmcctl -p 2 -U`** and press ENTER key.
2. Type **`rmcctl -p 2 -X`** and press ENTER key.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     1       1     ext4   1     0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     1       0      na    na    0     rmc0p2
 [!rmcctl] OK
```

5.4.2.8 Close SWE Container (All Partitions)

NOTE
To close the SWE containers on the partitions they must be unmounted.

1. Type **`rmcctl -p all -U`** and press ENTER key.
2. Type **`rmcctl -p all -X`** and press ENTER key.

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     1      0     na    na    0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     1      0     na    na    0     rmc0p2
 [!rmcctl] OK
```

5.4.2.9 Delete SWE Container (Individual Partitions)

CAUTION
LOSS OF CONTENT. Deletion of a SWE container will result in making the stored content unrecoverable.

To delete a SWE container:

Command:
`rmcctl -p 2 -D`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     1      0     na    na    0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     0      na    0a    na    0     rmc0p2
 [!rmcctl] OK
```

5.4.2.10 Delete SWE Containers (All Partitions)

CAUTION
LOSS OF CONTENT. Deletion of SWE containers will result in making the stored content unrecoverable.

To delete all software encryption layer containers:

Command:
`rmcctl -p all -D`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     0      na    0a    na    0     rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS     0      na    0a    na    0     rmc0p2
 [!rmcctl] OK
```

5.5 Zeroize HWE Key / Delete SWE Container / RMC Purge

- The destruction of the HWE key(s) is accomplished via zeroization.
- The SWE passphrase(s) is /are destroyed via deleting the SWE container(s).
- The RMC module data is destroyed via the rmcpurge command.

5.5.1 Zeroize HWE Key

CAUTION
DATA LOSS. Pushing the Key Clear button will zeroize the hardware encryption layer key. It will not affect SWE passphrase(s) / data.

The goal of zeroization is to destroy the HWE key loaded in the crypto module beyond recovery by any means.

The zeroization process is accomplished by one of the following:

- Pushing the front panel KEY CLEAR button for a minimum of 5 seconds.
- Issuing a **`cmkey -zero`** command via the CLI.
- Connecting utility connector (J2) pin 1 to ground for a minimum of 5 seconds.
- Incorrectly entering the hardware layer password three times consecutively.

Zeroization affects only the crypto module HWE key. It does not affect the RMC module. The data on the RMC module is still accessible:

- If the RMC module can be placed in another DTS1 with the same DEK / EDEK loaded in its crypto module.
- If the DEK can be restored / reloaded.

5.5.2 Delete SWE Container

CAUTION
LOSS OF CONTENT. Deletion of SWE container(s) will result in making the stored content unrecoverable.

Refer to paragraph 5.4.1.5 **Delete SWE Container (Unpartitioned Disk)**, paragraph 5.4.2.9 **Delete SWE Container (Individual Partitions)**, and / or paragraph 5.4.2.10 **Delete SWE Containers (All Partitions)** for detailed instructions on how to use the SWE passphrase delete (**`rmcctl -D`**) commands.

5.5.3 RMC Purge

CAUTION
DATA SECURITY. The rmcpurge command does not affect the HWE key(s).

CAUTION
DATA SECURITY. Depending on the solid-state drive manufacturer, the rmcpurge may or may not delete the SWE passphrase(s). To be sure the passphrase has been removed, use the SWE passphrase delete (**`rmcctl -D`**) command.

To destroy the passphrase(s) and data on the RMC module, the rmcpurge command is used. There are two types of overwrite, Normal (**`-N`**) and Enhanced (**`-E`**). Refer to paragraph 12.3.26 **rmcpurge** for additional information

1. Purge RMC module in slot 0 with normal overwrite.

   Command:
   `rmcpurge -s 0 -N`

Example: Normal erase of RMC module in slot 0

```
cw_dts> rmcpurge -s 0 -N
 [rmcpurge]
  RMC_P0: status=OK
 0[!rmcpurge] OK
```

2. Purge all RMC modules with enhanced overwrite.

   Command:
   `rmcpurge -s all -E`

Example: Enhanced erase of all RMC modules

```
cw_dts> rmcpurge -s all -E
 [rmcpurge]
  RMC_P0: status=OK
  RMC_P1: status=OK
  RMC_P2: status=OK
 [!rmcpurge] OK
```

Quick Start

NOTE
Throughout this section, yellow highlighted text is used to denote user-defined or software-generated inputs. Green highlighted text is used to show changes in values, settings, or responses due to implementation of a software command.

This section provides guidance on how to quickly access the Removable Memory Cartridge (RMC) associated with the DTS1 CSfC unit. This section makes the following assumptions:

- A 28 VDC power supply is available.
- The Curtiss-Wright generated PSK is available.
- A computer with the following applications installed is available.
  - PuTTY application (www.putty.org)
  - 3rd-party AES256 key-unwrapping application ‡
  - 3rd-party HMAC hash generator application ‡

‡ Contact Curtiss-Wright for applications / source code.

6.1 Connections / Preparation

CAUTION
Make sure no power is applied to DTS1 when inserting / removing RMC.

NOTE
At a minimum, the DTS1 CSfC must have an RMC installed and be connected to both a computer and 28 VDC power source.

1. Turn door latch CCW, open door, and insert RMC into DTS1.
2. Connect lab power cable between 28 VDC source and DTS1 connector J1.
3. Connect lab utility cable between user computer Ethernet port and DTS1 connector J2.
4. Turn on 28 VDC source.
5. Log into user computer.

NOTE
If unit has been initialized, do not press front panel KEY CLEAR button.

6. Push front panel KEY CLEAR button and hold for 5 seconds.
7. Start PuTTY application and configure as follows:
   - Connection Type: **`SSH`**
   - Port: **`22`**
   - Host Name or IP Address: **`192.168.1.1`**
8. Log into DTS1:
   - User name **`admin`**
   - Password **`istrator`**

6.2 Preparation (Initialization Procedure Only)

If the DTS1 / RMC has been previously configured with both hardware (HWFDE) and software (SWFDE) encryption active, prepare the unit as follows:

1. Delete HWFDE key. Type **`cmkey --zero or`** push DTS1 front panel KEY CLEAR button and hold for 5 seconds.

NOTE
Due to code-sharing between DTS1 and DTS3 units, many CLI commands can include -s 0 (slot 0) in the command line.

2. Stop services. Type **`serv -s 0 --all 0`** and press ENTER.

3. Unmount drive: Type **`rmcctl -s 0 -U`** and press ENTER.
4. Delete SWFDE container: Type **`rmcctl -s 0 -D`** and press ENTER.
5. Wipe RMC. Type **`rmcctl -s 0 -W --force`** and press ENTER.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding **`rmcctl`** command results.

6. View RMC status. Type **`rmcctl`** and press ENTER.

Example

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins  hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1     0      0    --   -----  ----   na     na     na    na    0     -----
 [!rmcctl] OK
```

6.3 Initialization

NOTE
For DTS1 CSfC units, both HWFDE and SWFDE initialization / use is mandatory.

NOTE
In the following procedure, the PSK, DEK, HWFDE password and SWFDE password / passphrase will NOT be shown after being entered.

HWFDE / SWFDE must be initialized prior to first use and whenever changes to DEK, key storage location, password, or passphrase are desired. Refer to Figure 6.1 for an initialization overview flowchart. The numbers listed in the flowchart relate to the step numbers in the procedure.

NOTE
Username must be 1-15 characters; the HWFDE password must be 8 to 64 characters long, contain at least one number, one alpha character, and contain no special characters.

1. Obtain user token. Type **`cmlogin -u username -p -I`** and press ENTER.
   - User is prompted for password. Type **`<password>`** and press ENTER.
   - User is prompted to verify password. Type **`<password>`** and press ENTER.
     - User token and HMAC will be displayed.

NOTE
The PSK is provided on a removable label placed on top of DTS1 when shipped.

2. Using a 3rd-party application and factory supplied PSK, decrypt user token obtained in step 1. Save resulting decrypted user token for future use / logins.
3. Generate challenge. Type **`cmlogin -u username -p -L`** and press ENTER.
   - User is prompted for HWFDE password. Type **`<password>`** and press ENTER.
     - The challenge will be a random string 128 characters long.
4. Generate HMAC string using challenge generated in step 3 as input MESSAGE and unencrypted user token from step 2 as KEY.
5. Log into crypto module. Type **`cmlogin -M generated HMAC string`** and press ENTER.
6. Verify successful login. Type **`cmlogin`** and press ENTER.
   - CMLOGIN: state=login init=1 login=1 status=OK

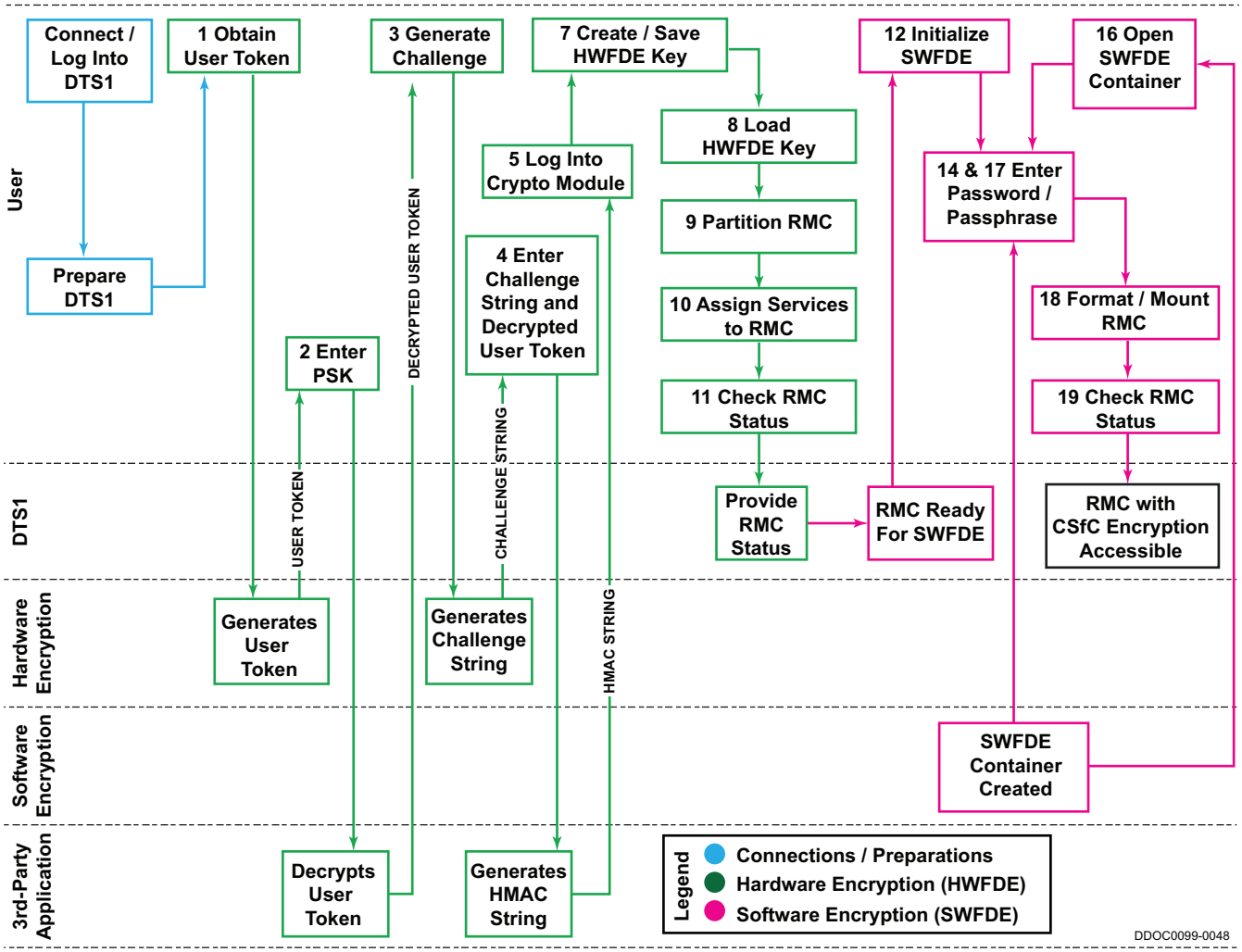

Figure 6.1 Initialization Overview Flowchart

NOTE
<loc> refers to location (0 through 31) where key will be stored.

NOTE
The DEK is a user-generated 64 character string. There are no requirements other than being able to remember it.

7. Create / save encryption key. Type **`cmkey --save <loc> -d -p`** and press ENTER.
   - User is prompted to enter user-generated DEK. Type **<User-generated `DEK string`>** and press ENTER.
   - User is prompted to enter Curtiss-Wright-provided PSK. Type **`<Curtiss-Wright provided PSK string>`** and press ENTER.
8. Load encryption key. Type **`cmkey --load <loc> -s 0`** and press ENTER.

NOTE
To partition a drive, the number of partitions (-P 1, -P 2, etc.) and their size (in either percentage or physical size [i.e 10GB, 100GB, etc.) must be contained in the command. For the purpose of this Quick Start Guide, the RMC has only 1 partition and it encompasses the entire drive.

NOTE
If any services / boot services are active, they must be turned off before partitioning / making changes to the state of the RMC. If required, type **`serv -s 0 --all 0`** and press ENTER.

9. Create partitions. Type **`rmcctl -s 0 -P 1 100% --force`** and press ENTER.

NOTE
The RMC module must have services assigned before SWFDE layer can be initialized.

10. Assign service: **`rmcctl -s 0 -p 1 --serv NAS`** and press ENTER.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding **`rmcctl`** command results.

11. View RMC status. Type **`rmcctl`** and press ENTER.

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins  hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1     1      1    1   XX GB   NAS     0     na     0     na    0     rmc0p1
 [!rmcctl] OK
```

NOTE
DTS1 CSfC units require use of SWFDE in addition to HWFDE.

NOTE
Disks cannot be partitioned after SWFDE has been performed.

12. Initialize SWFDE. Type **`rmcctl -s 0 -p 1 -C`** and press ENTER.
    - A warning will activate that SWFDE will overwrite all data.
13. When prompted about data overwrite, type: **`YES`** and press ENTER.

NOTE
SWFDE passwords / passphrases must be:

- 15 to 512 characters long
- Use at least 1 upper case, 1 lower case, 1 number, and 1 special character
- Repeat no character more than 3 times
- Have no more than 4 consecutive characters from a character class (i.e lower case, upper case, etc.)
- If using a password, it must pass dictionary test

14. When prompted, enter **`password / passphrase`** to be used for activation of SWFDE.
15. Reenter the SWFDE **`password / passphrase`** to verify it.
16. Open SWFDE container. Type: **`rmcctl -s 0 -p 1 -E`** and press ENTER.
17. When prompted, enter same SWFDE **`password / passphrase`** as previously entered.
18. Format / mount drive. Type **`rmcctl -s 0 -p 1 -F -M`** and press ENTER.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding **`rmcctl`** command results.

19. View RMC status. Type **`rmcctl`** and press ENTER.
    - DTS1 is ready to use with CSfC encryption.

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins  hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1     1      1    1   XX GB   NAS     1     1     ext4   1     0     rmc0p1
 [!rmcctl] OK
```

6.4 Login

NOTE
In the following procedure, the HWFDE password and SWFDE password / passphrase will NOT be shown after being entered.

After CSfC encryption has been initialized, subsequent use requires only following the login process. Refer to Figure 6.2 for a login overview flowchart. The numbers listed in the flowchart relate to the step numbers in the procedure.

1. Connect the user computer to the DTS1 and log in. Refer to paragraph 6.1 **Connections / Preparation** for detailed instructions.
2. Generate challenge. Type **`cmlogin -u username -p -L`** and press ENTER.
   - User is prompted for HWFDE password. Type **`<password>`** and press ENTER.
     - The challenge will be a random string 128 characters long.
3. Generate HMAC string using challenge generated in step 1 as input MESSAGE and unencrypted user token (generated during initialization) as KEY.

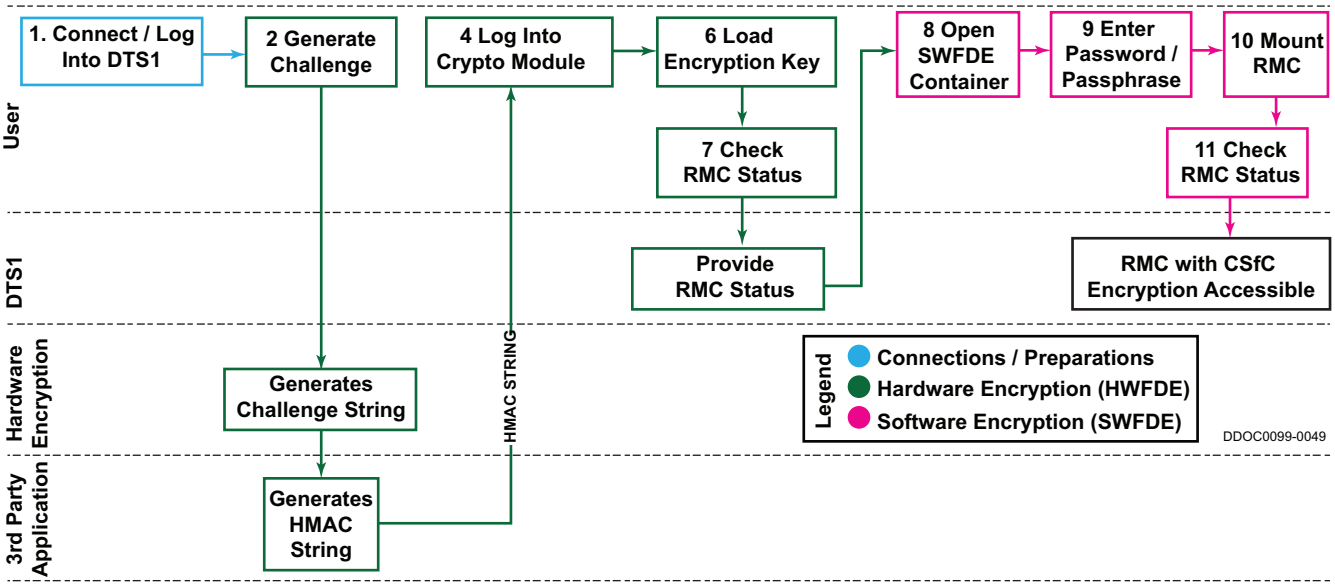

Figure 6.2 Login Overview Flowchart

4. Log into crypto module. Type **`cmlogin -M generated HMAC string`** and press ENTER.
5. Verify successful login. Type **`cmlogin`** and press ENTER.
   - CMLOGIN: state=login init=1 login=1 status=OK

NOTE
<loc> refers to location (0 through 31) where key is stored.

6. Load encryption key. Type **`cmkey --load <loc> -s 0`** and press ENTER.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding **`rmcctl`** command results.

7. View RMC status. Type **`rmcctl`** and press ENTER.

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins  hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    1   XX GB   NAS     1      0     na    na    0    rmc0p1
 [!rmcctl] OK
```

8. Open SWFDE container. Type **`rmcctl -s 0 -p 1 -E`** and press ENTER.
9. When prompted, enter same SWFDE **`password / passphrase`** as previously entered.
10. Mount drive. Type **`rmcctl -s 0 -p 1 -M`** and press ENTER.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding **`rmcctl`** command results.

11. View RMC status. Type **`rmcctl`** and press ENTER.
    - DTS1 is ready to use with CSfC encryption.

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins  hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1     1      1     1   XX GB   NAS     1      1    ext4    1     0    rmc0p1
 [!rmcctl] OK
```

Operation

CAUTION

CONFIGURATION ACCESS. Before attempting to setup or configure the DTS1, the Write-Enable switch **MUST** be in the **READ-WRITE** position.

Before attempting to configure the DTS1, set the write-enable switch to the **READ-WRITE** position. Refer to paragraph 3.2.2 **Write-Enable Switch** for detailed location information. After configuring the unit, set the write-enable switch to the **READ** position.

NOTE

Throughout this section, yellow highlighted text is used to denote user-defined or software-generated inputs. Green highlighted text is used to show changes in values, settings, or responses due to implementation of a software command.

7.1 Setup / Connections

NOTE

The DTS1 is powered by a user-supplied 28 VDC power supply and does not have a power switch of its own. The DTS1 is powered up by turning on the 28 VDC supply.

1. If not previously accomplished, connect cables to DTS1 connectors (Figure 7.1).
2. If not previously accomplished, connect cables to terminal / PC connectors.
3. Turn on 28 VDC power supply.

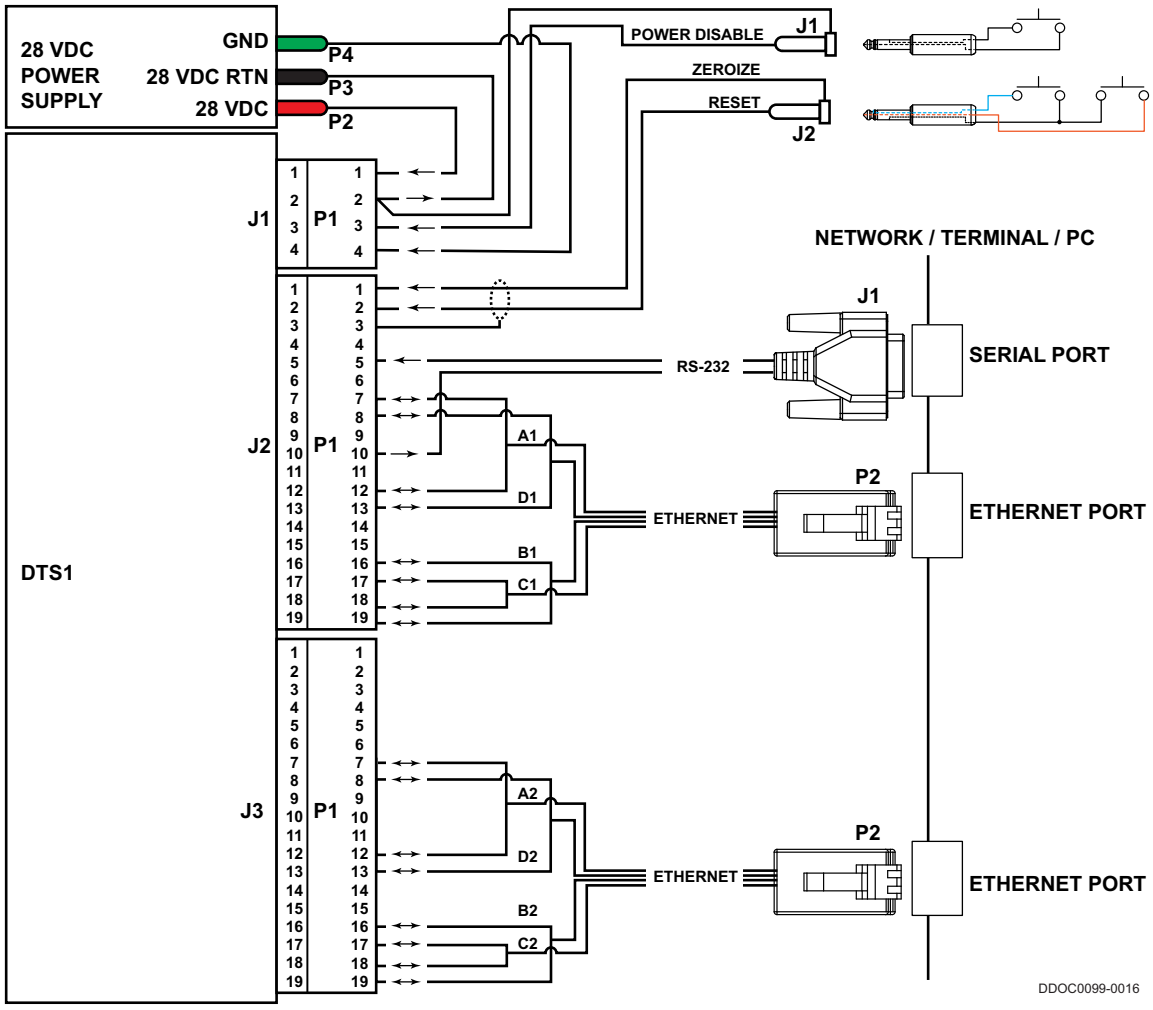

Figure 7.1 DTS1 Test Setup

7.2 Basic Operation

NOTE
Serial port access is recommended for initial configuration of the DTS1.

This topic describes how to use the DTS1 Command Line Interface (CLI) to configure the DTS1. Refer to **Command Line Interface** section for more information on the commands used in this topic. Changes to the DTS1 configuration must be performed through the admin account.

7.2.1 Communications

NOTE
The DTS1 will auto log-off after 5 minutes of communications inactivity.
A copy of the PuTTY terminal emulator can be obtained from https://www.putty.org/.

A RS-232 serial data port is provided via utility connector (J2). A terminal emulation program (PuTTY) is used to communicate with the Command Line Interface (CLI) using the RS-232 port. Serial port accesses is recommended for initial configuration of the DTS1. The terminal emulation program should be set to 9600 bps, 8 bits, no parity, one stop bit, and no flow control.

The CLI is also accessible via Ethernet using Secure Shell (SSH). The default IP addresses are shown in Table 7.1.

Table 7.1 Ethernet Interfaces

Connector	Port	Interface	IP Address	Subnet Mask
J2	Port 0	eth0	192.168.1.1	255.255.255.0
J3	Port 1	eth1	192.168.2.1	255.255.255.0

Simple Network Management Protocol (SNMP) is also available to communicate with the DTS1. See **Simple Network Management Protocol** section for details.

7.2.1.1 Terminal Emulation

This section explains setting up communications using serial communication (RS-232) and a PuTTY terminal emulator.

1. If not previously accomplished, download a copy of PuTTY terminal emulator and install on computer.
2. Open PuTTY terminal emulator (Figure 7.2).

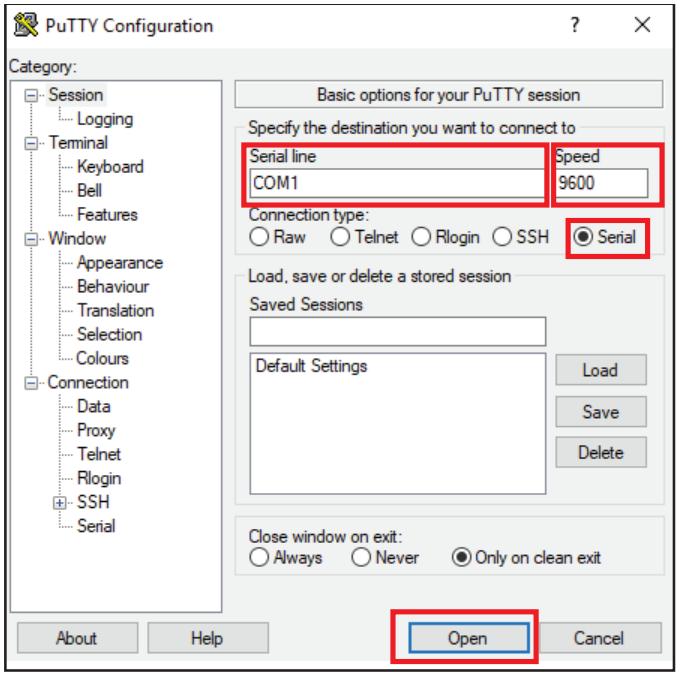

Figure 7.2 PuTTY Terminal Emulator (Serial Data)

3. Configure PuTTY as follows:
   - Connection type: Serial
   - Serial line: COM1 (example - any computer serial port can be utilized)
   - Speed: 9600
4. Click **Open** button.
   - ◆ A terminal screen should activate.
5. Click **Enter** button.
   - ◆ A login prompt should activate.
6. Log into CLI as follows:
   a. At the login prompt type **`admin.`**
   b. At the password prompt type **`istrator`**.

7.2.1.2 Ethernet

This section explains setting up communications using secure shell (SSH) and a PuTTY terminal emulator.

1. If not previously accomplished, download a copy of PuTTY terminal emulator and install on computer.
2. Open PuTTY terminal emulator (Figure 7.3).

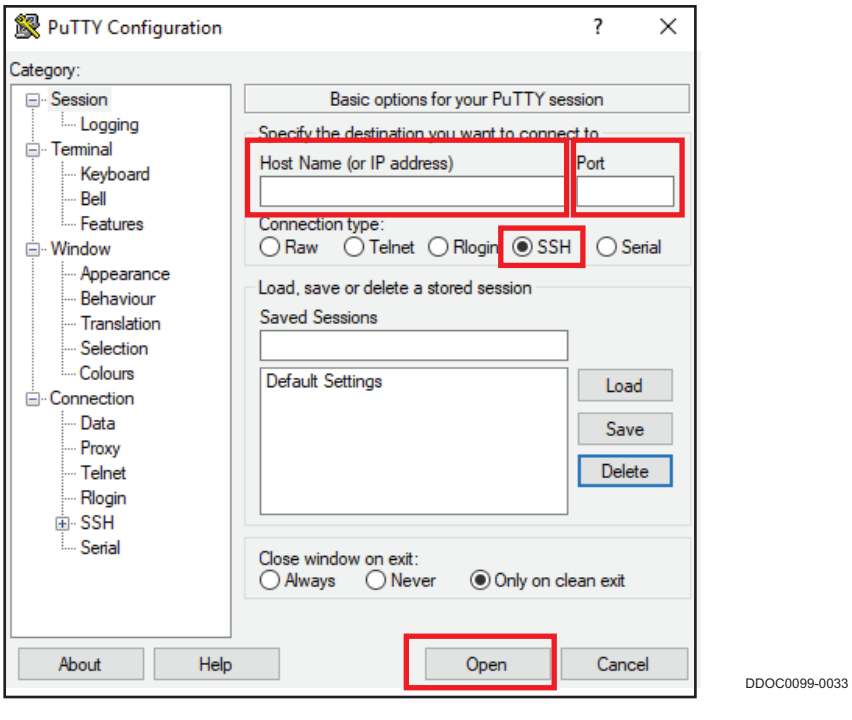

Figure 7.3 PuTTY Terminal Emulator (SSH)

3. Configure PuTTY as follows:
   - Connection Type: SSH
   - Port: 22
   - Host Name (or IP Address): see Table 7.1
4. Click **Open** button.
   - ◆ A terminal screen should activate.
5. Click **Enter** button.
   - ◆ A login prompt should activate.

6. Log into CLI as follows:
   a. At the login prompt type **admin.**
   b. At the password prompt type **istrator**.

7.2.2 IP Address

The default IP addresses can be changed if desired.

1. To change the eth0 IP address (utility connector J2), type:

```
cw_dts> ipconfig -e eth0 -i [desired IP address]
```

2. To change the eth1 IP address (Ethernet connector J3), type:

```
cw_dts> ipconfig -e eth1 -i [desired IP address]
```

3. To change the eth0 IP address and netmask, type:

```
cw_dts> ipconfig -e eth0 -i [desired IP address] -n [desired netmask]
```

NOTE
The DTS1 can be configured as a DHCP client if desired. When configured in this manner, the IP address is set remotely by a DHCP server.

4. Configure the DTS1 as a DHCP client as follows:
   a. To configure Ethernet port 0 type **ipconfig -e eth0 -D -F** and press ENTER key.
   b. To configure Ethernet port 1 type **ipconfig -e eth1 -D -F** and press ENTER key.
5. To check DHCP status, type ipconfig -V and press ENTER key.

NOTE
The green highlighted text below is assigned by the DCHP server.

Example

```
cw_dts> ipconfig -V
 [ipconfig]
  STS_ETH_0: link=1000 ip=10.19.6.64 nm=255.255.240.0 gw=10.19.1.5 status=OK
  STS_ETH_1: link=1000 ip=NA nm=NA gw=NA status=OK
  CFG_ETH_0: prot=dhcp status=OK
  CFG_ETH_1: prot=static ip=192.168.2.1 nm=255.255.255.0 gw=NA status=OK
 [!ipconfig] OK
```

7.2.3 Account Management

The DTS1 operating system has two accounts:

- admin (default password is istrator)
- user (default password is password)

The admin account is used to setup and configure the unit via the CLI. The user account can only access the RMC module and cannot change or update any operational parameters.

The Hardware Encryption (HWE) layer and Software Encryption (SWE) layer each have one account. These accounts are independent of the DTS1 accounts. Refer to paragraph 5.3 **Hardware Layer Encryption** and paragraph 5.4 **Software Layer Encryption** for additional information.

7.2.4 Passwords

NOTE
The administrator can configure the unit using the Command Line Interface (CLI).

Administrator

- Username: **admin**
- Password: **istrator**

NOTE
The user can access the drives configured as network storage. The user cannot access the CLI.

User

- Username: **user**
- Password: **password**

NOTE
The admin account has configuration privileges while the user account has access to only network storage functionality.

To change admin account password, type **password -u admin -p [desired password]** and press ENTER key.

Example

```
cw_dts> password -u admin -p [desired password]
```

To change user account password, type **password -u user -p [desired password]** and press ENTER key.

Example

```
cw_dts> password -u user -p [desired password]
```

The DTS1 software will prompt for the new password when -p command is used.

7.2.5 Time / Date

The time and date appear in some status displays and messages.

To display the current date and time, type **sysdate** and press ENTER key.

Example

```
cw_dts> sysdate
```

NOTE
The date must be entered as yyyy/mm/dd. The time must be entered as hh:mm:ss

To change the current date, type **sysdate -d yyyy/mm/dd** and press ENTER key.

Example

```
cw_dts> sysdate -d yyyy/mm/dd
```

To change the current time, type **sysdate -t hh:mm:ss** and press ENTER key.

Example

```
cw_dts> sysdate -t hh:mm:ss
```

To change the current date and time, type **sysdate -d yyyy/mm/dd -t hh:mm:ss** and press ENTER key.

Example

```
cw_dts> sysdate -d yyyy/mm/dd -t hh:mm:ss
```

7.3 Login

Logging into the DTS1 is a three-part process. Before the RMC module can be accessed or configured, the user must (in the following order):

1. Log into DTS1.
2. Initialize HWE layer.
3. Log into HWE layer.

7.4 Encryption

The DTS1 uses two layers of encryption:

- Hardware encryption layer
- Software encryption Layer

The user is required to use the CLI to issue initialization and key management commands.

7.4.1 Hardware Encryption Layer

Refer to paragraph 5.3 **Hardware Layer Encryption** for detailed instructions on how to create / log into the HWE layer.

7.4.2 Software Encryption Layer

Refer to paragraph 5.4 **Software Layer Encryption** for detailed instructions on how to create / log into the SWE layer.

7.4.3 Zeroize / Delete SWE Container / RMC Purge

CAUTION
LOSS OF CONTENT. Deletion of SWE container(s) will result in making the stored content unrecoverable.

- The destruction of the HWE layer key is accomplished via zeroization.
- The SWE layer passphrase(s) is / are destroyed via deleting the SWE container(s).
- The RMC module data is destroyed via the rmcpurge command.

Refer to paragraph paragraph 5.5 **Zeroize HWE Key / Delete SWE Container / RMC Purge** for additional information,

7.5 Storage Media

NOTE
The DTS1 must have the hardware encryption layer initialized and open before the RMC module (storage media) can be accessed.

If desired, the RMC module disk can be used without partitioning. The unpartitioned disk must have services started and assigned before formatting and mounting. Refer to paragraph 6.6 Services for additional information.

7.5.1 Preparation for Partition

The following steps must be done in sequential order.

1. Stop services.

   Commands:
   Stop services: **`serv -a 0`**
   Stop iSCSI targets: **`istarget --stop`**
   Stop PCAP recording: **`pcap --stop`**

2. Unmount drive.

   Command
   `rmcctl -U`

CAUTION
DATA LOSS. If the RMC has been previously used with full hardware and software encryption applied, erasing all partitions will delete the SWE container(s) and result in the loss of all data on the drive.

3. Erase existing partitions.

   Command:
   `rmcctl -W --force`

4. Check drive status.

NOTE
Refer to paragraph 12.3.23 **rmcctl** for information regarding the rmcctl status indications.

Command:
rmcctl

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     --  100GB  NONE    0     na     0     na    0     ----
 [!rmcctl] OK
```

7.5.2 Partition Disk

Create 1 partition on a 100GB RMC module.

Command:
rmcctl -P 1 100%

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1      1   100GB  NONE    0     na     0     na    0     ----
 [!rmcctl] OK
```

Create 2 partitions on a 100GB RMC module, each with 50%.

Command:
rmcctl -P 2 50% 50%

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1      1   50 GB  NONE    0     na     0     na    0     ----
  RMC_S0:    1      1      1      2   50 GB  NONE    0     na     0     na    0     ----
 [!rmcctl] OK
```

Create 4 partitions on a 100GB RMC module, each with 25%.

Command:
rmcctl -P 4 25% 25% 25% 25%

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1      1   25 GB  NONE    0     na     0     na    0     ----
  RMC_S0:    1      1      1      2   25 GB  NONE    0     na     0     na    0     ----
  RMC_S0:    1      1      1      3   25 GB  NONE    0     na     0     na    0     ----
  RMC_S0:    1      1      1      4   25 GB  NONE    0     na     0     na    0     ----
 [!rmcctl] OK
```

Create 4 partitions on a 100GB RMC module as follows: 10GB, 50GB, 20GB, 20GB.

NOTE
Partition must be 100MB or greater.

Command:
rmcctl -P 4 10GB 50GB 20GB 20GB

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   10 GB   NONE    0      na     0     na    0      ----
  RMC_S0:    1      1       1     2   50 GB   NONE    0      na     0     na    0      ----
  RMC_S0:    1      1       1     3   20 GB   NONE    0      na     0     na    0      ----
  RMC_S0:    1      1       1     4   20 GB   NONE    0      na     0     na    0      ----
 [!rmcctl] OK
```

7.5.3 Services

Services are not available until the drive is mounted as a NAS drive.

7.5.3.1 Assign Services

NOTE
Services can be assigned to an unpartitioned or partitioned RMC module.

Assign NAS services to an unpartitioned 100GB RMC module.

Command:
`rmcctl --serv NAS`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     0      na     0     na    0      rmc0
 [!rmcctl] OK
```

Assign NAS services to partition 1 of a 100GB RMC module with one partition.

Command:
`rmcctl -p 1 --serv NAS`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     0      na     0     na    0      rmc0p1
 [!rmcctl] OK
```

Assign NAS services to partitions 1 and 2 of a 100 GB RMC module with three partitions.

NOTE
Must be done as two separate commands.

Command:
`rmcctl -p 1 --serv NAS`
`rmcctl -p 2 --serv NAS`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   33 GB   NAS     0      na     0     na    0      rmc0p1
  RMC_S0:    1      1       1     2   33 GB   NAS     0      na     0     na    0      rmc0p2
  RMC_S0:    1      1       1     3   33 GB   NONE    0      na     0     na    0      ----
 [!rmcctl] OK
```

Assign NAS services to partitions 1 through 4 of a RMC module with four partitions.

Command:
rmcctl -p all --serv NAS

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt  mnt  rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1       1     1   25 GB   NAS    0      na     0   na   0    rmc0p1
  RMC_S0:    1      1       1     2   25 GB   NAS    0      na     0   na   0    rmc0p2
  RMC_S0:    1      1       1     3   25 GB   NAS    0      na     0   na   0    rmc0p3
  RMC_S0:    1      1       1     4   25 GB   NAS    0      na     0   na   0    rmc0p4
 [!rmcctl] OK
```

7.5.3.2 Boot Services

Set one or multiple services to start on boot-up.

Command:
serv -B --[service name] 1

Where [service] is one (or more) of the following: cifs; dhcp; ftp; http; nfs; snmp; tftp; tel.
Example Command: serv -B --cifs 1 --ftp 1 --http 1 --nfs 1

Example of Serv Status

```
cw_dts> serv -B --cifs 1 --ftp 1 --http 1 --nfs 1
 [serv]
 BOOTCFG   cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 LIVECGFG  cifs=0   nfs=0   ftp=0   http=0   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 [!serv] OK
```

Set all services to start on boot-up.

Command:
serv -B -a 1

Example of Serv Status

```
cw_dts> serv -B -a 1
 [serv]
 BOOTCFG   cifs=1   nfs=1   ftp=1   http=1   dhcp=1   tftp=1   tel=1   snmp=1   status=ok
 LIVECGFG  cifs=0   nfs=0   ftp=0   http=0   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 [!serv] OK
```

7.5.3.3 Restart Services

Restart one or multiple services.

Command:
serv --[service name] 1
Where [service] is one (or more) of the following: cifs; dhcp; ftp; http; nfs; snmp; tftp; tel.
Example Command: serv --cifs 1 --ftp 1 --http 1 --nfs 1

Example of Serv Status

```
cw_dts> serv -cifs 1 --ftp 1 --http 1 --nfs 1
 [serv]
 BOOTCFG   cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 LIVECGFG  cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 [!serv] OK
```

Restart all services.

Command:
serv -a 1

Example of Serv Status

```
cw_dts> serv -a 1
 [serv]
 BOOTCFG   cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 LIVECGFG  cifs=1   nfs=1   ftp=1   http=1   dhcp=1   tftp=1   tel=1   snmp=1   status=ok
 [!serv] OK
```

Transfer boot-up configuration to live configuration.

Command:
serv -a 2

Example of RMC Module Status

```
cw_dts> serv -a 2
 [serv]
 BOOTCFG   cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 LIVECGFG  cifs=1   nfs=1   ftp=1   http=1   dhcp=0   tftp=0   tel=0   snmp=0   status=ok
 [!serv] OK
```

7.5.4 Assign Mount Point Names

NOTE
The RMC module must be partitioned to assign mount point names. Each mount point name must be unique. Mount point names must be between 1 and 32 characters, some names might be truncated depending on CLI.

Add a mount point name to a 100GB RMC module with 1 partition.

Command:
rmcctl --mntpoint [name]

Example of RMC Module Status (Where [name]=alpha)

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   100GB   NAS     0      na     0     na    0      alpha
 [!rmcctl] OK
```

Change the mount point name of a 100GB RMC module with one partition.

Command:
rmcctl --mntpoint [name]

Example of RMC Module Status (Where [name]=aaa)

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv   scryp   osdm   fmt   mnt   rem   mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   100GB   NAS     0      na     0     na    0      aaa
 [!rmcctl] OK
```

Add a mount point name to partitions 1 and 2 of a100 GB RMC module with two partitions.

NOTE
Must be done as two separate commands.

Command:
rmcctl -p 1--mntpoint [name 1]
rmcctl -p 2--mntpoint [name 2]

Example of RMC Module Status (where partition 1 [name 1]= aaa and partition 2 [name 2]= bbb)

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:    1      1       1     1   50 GB   NAS     0      na     0     na    0      aaa
  RMC_S0:    1      1       1     2   50 GB   NAS     0      na     0     na    0      bbb
 [!rmcctl] OK
```

7.5.5 Format / Mount

7.5.5.1 Format Only

NOTE
NTFS format is not supported on an unpartitioned RMC module.

Format an unpartitioned 100GB RMC module as ext4 (default).

Command:
rmcctl -F

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:    1      1       1     1   100GB   NAS     0      na    ext4   0     0      rmc0
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from NTFS to ext4.

Format partition 1 of a 100 GB RMC module with two partitions as ext4 (default).

Command:
rmcctl -p 1 -F

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:    1      1       1     1   50 GB   NAS     0      na    ext4   0     0      rmc0p1
  RMC_S0:    1      1       1     2   50 GB   NAS     0      na     0     na    0      rmc0p2
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from ext4 to NTFS.

Format partition 2 of a 100 GB RMC module with two partitions as NTFS.

Command:
rmcctl -p 2 -F --fs NTFS

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp   osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:    1      1       1     1   50 GB   NAS     0      na    ext4   0     0      rmc0p1
  RMC_S0:    1      1       1     2   50 GB   NAS     0      na    NTFS   0     0      rmc0p2
 [!rmcctl] OK
```

Change format of partition 2 of a 100 GB RMC module with two partitions to ext4 (default).

Command:
`rmcctl -p 2 -F --force`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   50 GB   NAS     0      na    ext4    0     0     rmc0p1
  RMC_S0:    1      1      1     2   50 GB   NAS     0      na    ext4    0     0     rmc0p2
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from NTFS to ext4.

Format partitions 1 through 4 of a 100GB RMC module with four partitions to ext4 (default).

Command:
`rmcctl -p all -F`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   25 GB   NAS     0      na    ext4    0     0     rmc0p1
  RMC_S0:    1      1      1     2   25 GB   NAS     0      na    ext4    0     0     rmc0p2
  RMC_S0:    1      1      1     3   25 GB   NAS     0      na    ext4    0     0     rmc0p3
  RMC_S0:    1      1      1     4   25 GB   NAS     0      na    ext4    0     0     rmc0p4
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from ext4 to NTFS.

Format partitions 1 through 4 of a 100GB RMC module with four partitions to NTFS.

Command:
`rmcctl -p all -F -fs NTFS`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   25 GB   NAS     0      na    NTFS    0     0     rmc0p1
  RMC_S0:    1      1      1     2   25 GB   NAS     0      na    NTFS    0     0     rmc0p2
  RMC_S0:    1      1      1     3   25 GB   NAS     0      na    NTFS    0     0     rmc0p3
  RMC_S0:    1      1      1     4   25 GB   NAS     0      na    NTFS    0     0     rmc0p4
 [!rmcctl] OK
```

7.5.5.2 Format / Mount

NOTE
NTFS format is not supported on an unpartitioned RMC module.

Format (ext4) / mount an unpartitioned 100GB RMC module.

Command:
`rmcctl -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt  rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    1   100GB   NAS     0     na    ext4   1    0     rmc0
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from NTFS to ext4.

Format (ext4) / mount partition 1 of a 100GB RMC module with two partitions.

Command:
`rmcctl -p 1 -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt  rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    1   50 GB   NAS     0     na    ext4   1    0     rmc0p1
  RMC_S0:    1      1      1    2   50 GB   NAS     0     na     0     na   0     rmc0p2
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from ext4 to NTFS.

Format (NTFS) / mount partition 2 of a 100GB RMC module with two partitions.

Command:
`rmcctl -p 2 -F --fs NTFS -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt  rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    1   50 GB   NAS     0     na    ext4   1    0     rmc0p1
  RMC_S0:    1      1      1    2   50 GB   NAS     0     na    NTFS   1    0     rmc0p2
 [!rmcctl] OK
```

Change mounted partition 2 format from NTFS to ext4 of a 100GB RMC module with two partitions.

Command:
`rmcctl -p 2 -F --force`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr  p#   size   serv  scryp  osdm   fmt   mnt  rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    1   50 GB   NAS     0     na    ext4   1    0     rmc0p1
  RMC_S0:    1      1      1    2   50 GB   NAS     0     na    ext4   1    0     rmc0p2
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from NTFS to ext4.

Format (ext4) / mount partitions 1 through 4 of a 100GB RMC module.

Command:
`rmcctl -p all -F -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   25 GB   NAS     0      na    ext4    1     0    rmc0p1
  RMC_S0:    1      1      1     2   25 GB   NAS     0      na    ext4    1     0    rmc0p2
  RMC_S0:    1      1      1     3   25 GB   NAS     0      na    ext4    1     0    rmc0p3
  RMC_S0:    1      1      1     4   25 GB   NAS     0      na    ext4    1     0    rmc0p4
 [!rmcctl] OK
```

NOTE
Add the force option (---force) if changing format from ext4 to NTFS.

Format (NTFS) / mount partitions 1 through 4 of a 100GB RMC module.

Command:
`rmcctl -p all -F --fs NTFS -M`

Example of RMC Module Status

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv  scryp  osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1     1   25 GB   NAS     0      na    NTFS    1     0    rmc0p1
  RMC_S0:    1      1      1     2   25 GB   NAS     0      na    NTFS    1     0    rmc0p2
  RMC_S0:    1      1      1     3   25 GB   NAS     0      na    NTFS    1     0    rmc0p3
  RMC_S0:    1      1      1     4   25 GB   NAS     0      na    NTFS    1     0    rmc0p4
 [!rmcctl] OK
```

7.5.6 iSCSI

NOTE
The hardware encryption must be active before initiating iSCSI operation. If software encryption is going to be used, it must be active before initiating iSCSI operation as well.

The DTS1 supports use of Internet Small Computer System Interface (iSCSI). It is configured to use either Ethernet port 0 or port 1. The desired Ethernet port must have an active link before running istarget.

1. To start iSCSI services:
   a. Type **`serv -a 0`** and press ENTER key.
   b. Type **`rmcctl --serv iSCSI0 --force`** and press ENTER key.
   c. Type **`serv -a 2`** and press ENTER key.
   d. Type **`istarget --start`** and press ENTER key.

Example

```
cw_dts> istarget --start
 [istarget]
  RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=1 status=OK
 [istarget] OK
```

2. To check iSCSI status, type **`istarget`** and press ENTER key.

Example

```
cw_dts> istarget
 [istarget]
  RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=1 status=OK
 [istarget] OK
```

3. To check RMC module services, type **`rmcctl`** and press ENTER key.

Example

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:   ins   hcryp  osdr   p#   size   serv   scryp osdm   fmt   mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:    1      1      1    ---  100GB  iSCSI    na    na    na    na    0     -----
 [!rmcctl] OK
```

4. To stop iSCSI service type **`istarget --stop`** and press ENTER key.

Example

```
cw_dts> istarget --stop
 [istarget]
  RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=0 status=OK
 [!istarget] OK
```

7.6 PCAP

NOTE
The hardware encryption must be active before initiating PCAP operation. If software encryption is going to be used, it must be active before initiating PCAP operation as well.

The DTS1 supports use of the PCAP command to capture packets traveling over a network. Two data streams may be captured at any one time (Ethernet ports 0 and 1). A unique file name must be used with each recording in order to retain all recordings.

1. If not previously accomplished, type **`rmcctl --serv NAS`** and press ENTER key.
2. If not previously accomplished, type **`rmcctl -F -M`** and press ENTER key.

NOTE
Both Ethernet ports can be used simultaneously to capture packets.

3. To start capturing packets:
   a. Via Ethernet port 0, type **`pcap -i eth0 -s 0 --start [file name 1]`** and press ENTER key.

Example

```
cw_dts> pcap -i eth0 -s 0 --start [file name 1]
 [pcap]
  Start PCAP recording on eth0 to /rmc_shares/rmc0/[file name 1]
  recording started
 [!pcap] OK
```

   b. Via Ethernet port 1, type **`pcap -i eth1 -s 0 --start [file name 2]`** and press ENTER key.

Example

```
cw_dts> pcap -i eth1 -s 0 --start [file name 2]
 [pcap]
  Start PCAP recording on eth1 to /rmc_shares/rmc1/[file name 2]
  recording started
 [!pcap] OK
```

4. To get pcap status, type **`pcap --stat`** and press ENTER key.

Example

```
cw_dts> pcap --stat
 [pcap]
  PCAP recorder active
  Interface eth0: Recorded 479232 Bytes (468K) to /rmc_shares/rmc0/[file name 1]
  Interface eth1: Recorded 0 Bytes (0) to /rmc_shares/rmc0/[file name 2]
 [!pcap] OK
```

NOTE
Ethernet port captures can be stopped independently or simultaneously.

5. To stop capturing packets:
   a. from Ethernet port 0, type **pcap -i eth0 --stop** and press ENTER key.

Example

```
cw_dts> pcap -i eth0 --stop
[pcap]
Stopping active PCAP recording on eth0
[!pcap] OK
```

   b. from Ethernet port 1, type **pcap -i eth1 --stop** and press ENTER key.

Example

```
cw_dts> pcap -i eth1 --stop
[pcap]
Stopping active PCAP recording on eth0
[!pcap] OK
```

   c. from Ethernet port 0 and 1, type **pcap --stop** and press ENTER key.

Example

```
cw_dts> pcap --stop
[pcap]
Stopping active PCAP recording on eth0.
Stopping active PCAP recording on eth1.
[!pcap] OK
```

6. To start capturing packets and overwriting the previous capture, type **pcap -i eth0 -s 0 --start [file name 1]** --ov and press ENTER key.

Example

```
cw_dts> pcap -i eth0 -s 0 --start [file name 1] --ov
 [pcap]
  Start PCAP recording on eth0 to /rmc_shares/rmc0/[file name 1]
  recording started
 [!pcap] OK
```

7. To start capturing packets without overwriting the previous captures, type **pcap -i eth0 -s 0 --start [file name 3]** and press ENTER key.

Example

```
cw_dts> pcap -i eth0 -s 0 --start [file name 3]
 [pcap]
  Start PCAP recording on eth0 to /rmc_shares/rmc0/[file name 3]
  recording started
 [!pcap] OK
```

7.7 Health

The DTS1 has internal sensors that monitor critical environmental and operational parameters. The software provides this information to the user via the CLI when commanded. A FAIL status will be posted for any values that are out of tolerance.

7.7.1 Sens

To view operating voltages and temperatures and their status type **sens** and press ENTER key.

NOTE
Values provided in example are typical. As long as the sensed value is between MIN and MAX it is acceptable.

Example

```
cw_dts> sens
 [sens]
  ____________________________________VOLTAGES_____________________________________
  SENSOR              VALUE          MIN          MAX       STATUS
  V_ETH_CORE           1.04         1.00         1.10       Pass
  V_ETH_VDDa           1.86         1.70         2.10       Pass
  V_ETH_VDDd           1.90         1.70         2.10       Pass
  V_ETH_VDD            1.81         1.60         2.00       Pass
  V_MAIN_12V          11.98        11.00        13.00       Pass
  V_V5.0               4.89         4.50         5.50       Pass
  V_V3.3               3.31         3.00         3.60       Pass
  V_RMC0_12           12.02        11.00        13.00       Pass
  V_RMC0_5             5.03         4.50         5.50       Pass
  V_RMC0_3             3.30         3.00         3.60       Pass
  CAP_OK                  1            -            -       Pass
  V_CRYPT              3.67         3.40         3.90       Pass
  ___________________________TEMPERATURES___________________________________
  SENSOR              VALUE          MIN          MAX       STATUS
  T_COMF                 37          -45           90       Pass
  T_COMM                 42          -45           90       Pass
  T_COMR                 38          -45           90       Pass
  T_VREG                 43          -45           90       Pass
  T_PSUT                 38          -45           90       Pass
  T_PSUB                 38          -45           90       Pass
  T_RMC0_DR              35          -45           90       Pass
  T_RMC0_DF              38          -45           90       Pass
  T_CRYPT                40          -45           90       Pass
  ____________________ADVANTECH HWMON SENSORS_____________________________
  SENSOR              VALUE          MIN          MAX       STATUS
  V_12                11.79        11.00            1       Pass
  CORE0                  46            0          110       Pass
  CORE1                  46            0          110       Pass
  CORE2                  46            0          110       Pass
  CORE3                  46            0          110       Pass
 [!sens] OK
```

7.8 Built In Test

7.8.1 IBIT (Initiated BIT)

NOTE

Results will be provided as 1 (Pass), 0 (Fail), and NA (function not active)

The ibit command provides a snap-shot of the DTS1 status. To view status, type **`ibit`** and press ENTER key.

- IBIT_MON line provides results for system monitor subsystem.
- IBIT_ETH line provides results for Ethernet subsystem.
- IBIT_RMC# line provides results for RMC module in slot #

Example

```
cw_dts> ibit
 [ibit]
  IBIT_MON: mcu=1/0 i2c=1/0 volt=1/0 status=OK/ERR
  IBIT_ETH: eth0=1/0 eth1=1/0
  IBIT_RMC0: volt=1/0/NA ata=1/0/NA smart=1/0/NA status=OK/ERR
 [!ibit] <summary>
```

7.8.2 MBIT (Maintenance BIT)

The mbit command is used with various options to perform maintenance built-in tests. Several of these tests either destroy or may destroy data on the RMC module. As a result, to perform these tests use of a **`--go`** option along with command option is required.

CAUTION
DATA LOSS. Use of following command options may / will destroy data on the RMC module.

Use --disk option to run disk test on the RMC module or on a partition.
Use --fsck option to run file system check on the RMC module on a partition.
Use --fsckauto option to fix simple problems without intervention.
Use --fsckyes to auto-repair problems by assuming yes to all repair prompts.

For additional information refer to paragraph 12.3.17 **mbit**.

7.9 Update Software / Firmware

7.9.1 Update Operating System Software

CAUTION
UPDATE ERROR / FAILURE. Before attempting to update the DTS1, the Write-Enable switch **MUST** be in the **READ-WRITE** position.

CAUTION
UPDATE ERROR / FAILURE. Before attempting any software / firmware updates, ensure the RMC module has been removed. Failure to remove the RMC module may result in update errors / failure.

NOTE
All updates to software / firmware should be accomplished using RS-232 serial data protocol.

NOTE
Contact Curtiss-Wright to obtain any available / applicable update files.

Before attempting to update the DTS1, set the write-enable switch to the **READ-WRITE** position. Refer to paragraph 3.2.2 **Write-Enable Switch** for detailed location information. After updating the unit, set the write-enable switch to the **READ** position.

The update files should be received from Curtiss-Wright as a tarball (compressed files package). The tarball will have to be uncompressed and the digital signature verified before loading the files into the DTS1 flash memory.

The fupdate command boots the DTS1 system into a RAM disk image where the user can install a new disk image onto the system. Upon logging into the new RAM disk image, a menu of operations to restore and verify the restoration of a new disk image activates.

NOTE
The fupdate command loads an image into memory to allow the user to update the boot image on the unit.

1. Type **`fupdate`** and press ENTER key.
   - The update utility will start.
2. If using Linux OS, save the operating system image to the DTS1 as follows:
   a. Type **`ip addr`** and press ENTER.
   b. DTS1 IP address will be shown.
   c. Type **`scp dts1_image_`*`year_month_day`*`-ver_#_##.tar root@IP_ADDRESS:/updates`** and press ENTER.
3. If using Windows OS, save the operating system image to the DTS1 updates folder via a utility such as Win SCP.
4. Typically, the update file name should appear above the displayed menu (Figure 7.4) (e.g.,dts1_image_*year_month_day*-ver_#_##.tar).
5. Select **3) Verify digital signature, md5sum and program image into DTS1 flash** and press ENTER key.
6. The DTS1 examines the digital signature to determine if the tarball has been compromised.
   - If tarball is uncompromised the update process will begin. If the tarball has been changed for any reason, the update process aborts.

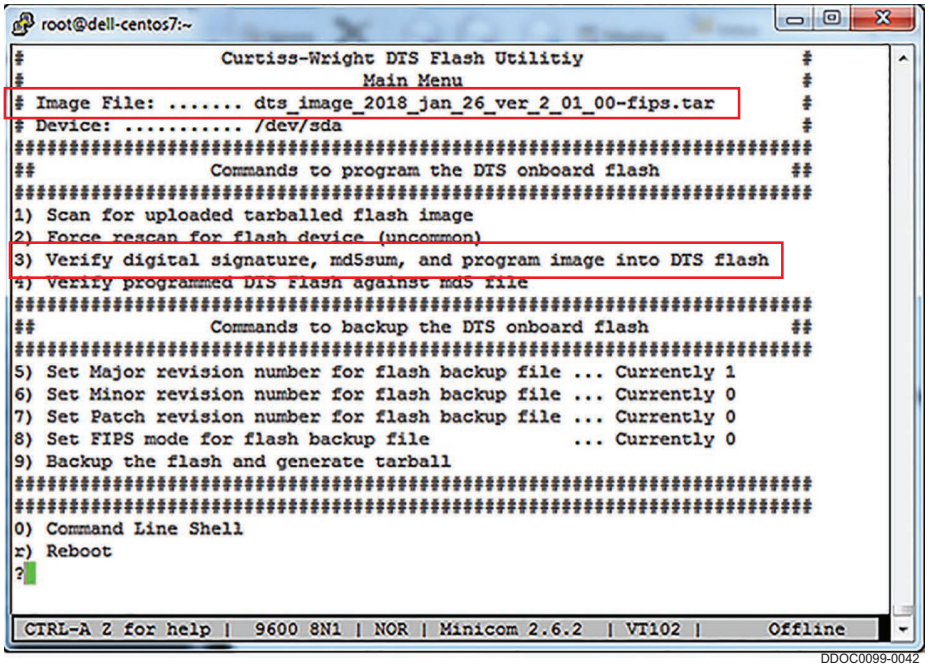

Figure 7.4 DTS1 Update Utility

7. The update process will continue for approximately 3 to 5 minutes.
8. Power unit OFF and back ON to boot the new image.

7.9.2 Update Crypto Firmware

CAUTION
RENDER INOPERABLE. Once the crypto firmware update is started, it must not be interrupted. If the update is interrupted, the DTS1 will be rendered inoperable.

NOTE
For DTS1 units with operating software version prior to 3.00.00, the crypto firmware update will take approximately 90 minutes. For unit with operating system software 3.00.00 or later, the crypto firmware update will take approximately 10 minutes

Before updating crypto firmware:

- Ensure you are logged into the crypto module.
- Ensure an RMC is installed in the DTS1.

1. Copy crypto firmware update files to mounted RMC via NFS/CIFS/FTP/etc. to /rmc_shares/rmc0p1.
2. Type **`cmfwupdate -f DTS_v5.x_CSfC.bin -s DTS_v5.x_CSfC_signature.bin`** and press Y.
   - ◆ Crypto firmware update begins.
3. After update is complete, wait 10 seconds and then power unit OFF and back ON.

Example

```
cw_dts> cmfwupdate -f DTS_v5.2_CSfC.bin -s DTS_v5.2_CSfC_signature.bin
 [cmfwupdate]
  The Trusted Firmware Update takes approximately 10 minutes to complete.
  During the process you shall not operate or powerdown the device.
  Interrupting this process can brick the device leaving it inoperable.
  Proceed?  y/n: y
  STATUS: Activity[.....................................................
  ....................................................................
  ....................................................................]
  Update Complete. Please wait 10 seconds to power cycle the unit.
 status=OK
[!cmfwupdate] OK
```

7.10 Access from Windows as NAS Device

NOTE
When the partitions are formatted and mounted, they can be accessed from a PC running Windows.

1. Log into the DTS1 via SSH. Refer to paragraph 7.2.1.2 **Ethernet**.
2. Type **`rmcctl`** and press ENTER key.
   - The RMC module must have NAS services assigned, be formatted (fmt=ext4 or NTFS). and mounted (mnt=1). See Example.

Example

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:  ins  hcryp  osdr  p#  size   serv   scryp   osdm    fmt     mnt   rem  mntpoint
  ********************************************************************************
  RMC_S0:   1     1     1    --  100GB   NAS     0      na     ext4     1     0     rmc0
 [!rmcctl] OK
```

3. If required, format and mount RMC module as follows:
   a. Type **`rmcctl --serv NAS`** and press ENTER key
   b. Type **`rmcctl -F -M`** and press ENTER key.
4. Type **`serv`** and press ENTER key to see if CIFS and NFS is enabled.
   - NFS enabled: `nfs=1` NFS disabled: `nfs=0`
   - CIFS enabled: `cifs=1` CIFS disabled: `cifs=0`
5. If NFS is disabled type **`serv --nfs 1`** and press ENTER key.
6. If CIFS is disabled type **`serv --cifs 1`** and press ENTER key.
7. Open a File Explorer window.
8. Enter the IP address of the DTS1 in the address bar.

Example `\\192.168.1.1\`

9. Login as user:
   a. Type **`user`** at user name prompt.
   b. Type **`password`** at password prompt.

7.11 Access from Linux as NAS Device

NOTE
When the partitions are formatted and mounted, they can be accessed from a PC running Linux.

NOTE
This procedure is performed via Ethernet connected to DTS1 port 0.

1. Open a terminal window
2. Type **`ssh admin@192.168.1.1.`**
3. Press ENTER key.
4. Type **`istrator`** for password.
5. Press ENTER key.
6. Type **`serv`** and press ENTER key to see if NFS is enabled.
   - NFS enabled: `nfs=1` NFS disabled: `nfs=0`
7. If NFS is disabled type **`serv --nfs 1`**.

8. In the terminal window on the Linux PC:
   a. Create a mount point.
   b. Mount to the storage device.

Example

```
mkdir /rmc0
mount -t nfs 192.168.1.1:/rmc_shares/rmc_nas0 /fs
```

System Configuration

The commands below are used to configure the crypto module, DTS1, and associated RMC module.

8.1 Crypto Module

The cmlogin command allows for initialization of / logging into the Hardware Encryption (HWE) crypto module. For status information, issue cmlogin without options. Refer to paragraph 12.3.5 **cmlogin** for detailed information about initializing /logging into the HWE crypto module.

The cmkey command allows for management of keys on the HWE crypto module. For status information, issue cmkey without options. Refer to paragraph 12.3.3 **cmkey** for detailed information about configuring the crypto module.

8.1.1 Initialize / Log In

NOTE

`[username]` and `[password]` are selected and entered by the user.

`cmlogin -u [username] -p [password] -I` .....Initialize HWE crypto module.
`cmlogin -u [username] -p [password]` .....Log into HWE crypto module.
`cmlogin -M`.....Authorize HWE crypto module password.

8.1.2 Key Load / Unload

`cmkey --auto` .....Auto-load the saved key for RMC module.
`cmkey --load` .....Load a saved key for RMC module.
`cmkey --unload`.....Unload/zeroize key from RMC module.

8.1.3 Key Removal / Zeroize

`cmkey --del` .....Delete/zeroize a saved key.
`cmkey -Z`.....Zeroize crypto module. Clears any saved / loaded key.
`cmkey --zpsk` .....Zeroize the crypto unit PSK.

8.1.4 Key Commands

`cmkey --save` .....Save key to non-volatile memory location (0-31).
`cmkey -e`.....Encrypted DEK (data encryption key) 40 byte value represented by 80 hex characters.
`cmkey -m`.....MAC (message authentication code) 32 byte value represented by 64 hex characters.
`cmkey -p`.....Plain Text PSK (pre-shared key) 32 byte value represented by 64 hex characters.
`cmkey -d`.....Plain Text DEK (data encryption key) 32 byte value represented by 64 hex characters.
`cmkey -k`.....Generates KEK (key encryption key.
`cmkey -u`.....User defined plain text PSK (pre-shared key) 32 byte value represented by 64 hex characters.

8.2 DTS1

CAUTION

CONFIGURATION ACCESS. Before attempting to setup or configure the DTS1, the Write-Enable switch **MUST** be in the **READ-WRITE** position.

Before attempting to configure the DTS1, set the write-enable switch to the **READ-WRITE** position. Refer to paragraph 3.2.2 **Write-Enable Switch** for detailed location information. After configuring the unit, set the write-enable switch to the **READ** position.

Refer to paragraph 12.3.12 **info** and paragraph 12.3.13 **ipconfig** for detailed information about configuring the DTS1.

8.2.1 Versions

The info command displays DTS hardware and software information, such as versions.

info -A.....Alternate short-form display.
info -M.....Show the media type(s) supported by each slot.
info -R.....Generate a status report of info useful for tech support.

8.2.2 Configure

The ipconfig command allows for configuration of an IP interface. By default, changes take effect on the next bootup.

ipconfig -d .....Use DHCP.
ipconfig -e .....Ethernet device: eth0, eth1. Default is 'all' when viewing status (see -V), otherwise eth0.
ipconfig -g .....Assign static gateway address. Use '.' to clear.
ipconfig -i .....Assign static IP address.
ipconfig -m .....View MAC address.
ipconfig -n .....Assign static IP netmask. Use '.' to clear.
ipconfig -V .....View interface status and configuration settings. Default action when other options absent.

8.3 RMC Module

NOTE
The DTS1 has only 1 RMC module slot. As a result, the -s option is always -s 0.

Refer to paragraph 12.3.23 **rmcctl** and paragraph 12.3.29 **serv** for detailed information about configuring the RMC module.

The rmcctl command without options applied returns the RMC module status. When options are applied, the rmcctl command performs control tasks on the RMC modules, such as partitioning, formatting, mounting, and requesting removal.

8.3.1 RMCCTL Definitions

The rmcctl command without options is used to determine status. The response will be similar to that shown in the examples below.

Example - New RMC

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:  ins  hcryp  osdr  p#  size   serv   scryp   osdm    fmt     mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:   1     na     na   --  ----   ----    na      na      na      na     0     ----
 [!rmcctl] OK
```

Example -HWE Active, 4 Partitions, SWE Active, formatted and Mounted

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#:  ins  hcryp  osdr  p#  size   serv   scryp   osdm    fmt     mnt   rem  mntpoint
  ************************************************************************************
  RMC_S0:   1     1      1    1  25 GB  NAS      1       1     ext4     1     0    rmc0p1
  RMC_S0:   1     1      1    2  25 GB  NAS      1       1     ext4     1     0    rmc0p2
  RMC_S0:   1     1      1    3  25 GB  NAS      1       1     ext4     1     0    rmc0p3
  RMC_S0:   1     1      1    4  25 GB  NAS      1       1     ext4     1     0    rmc0p4
 [!rmcctl] OK
```

RMC_S# .....RMC module slot number: DTS1 will always be 0.
ins.....RMC module insertion status: 0 if no RMC module inserted; 1 if RMC module is inserted.
hcryp .....Hardware encryption: 0 if not ready; 1 if ready; na if not detected.
osdr.....Operating system raw block device detection status: 0 if raw device not detected; 1 if raw device detected.

`p#` ..... Partition number: number of partitions present. Can be 0 to 128
`size` ..... Size of partitions: can be listed in MiB, MB, GiB, GB, TiB or TB. The minimum size allowed is 100MB.
`serv` ..... Services: can be none, iSCSI, NAS, or PCAP recording.
`scryp` ..... Software encryption: 0 if no software encryption applied; 1 if software encryption is present
`osdm` ..... Operating system mapped block device detection status: 0 if software container is closed; 1 if software container is open
`fmt` ..... Format: na / 0 if RMC module is unformatted; ext4 if RMC module is formatted ext4; ntfs if formatted ntfs
`mnt` ..... Mount: na / 0 if RMC module is unmounted; 1 if RMC module is mounted; ro is mounted read-only.
`rem` ..... Removal request status: 0 if not requested; RQ if requested; OK if ready for removal.
`mtpoint` ..... Mount point: Assign a mount point <name> to a partition. Limited to 32 characters, and may wrap or truncate depending on CLI terminal type

8.3.2 Configure

`rmcctl -F` ..... Format RMC module / partition. May take several minutes.
`rmcctl -M` ..... Mount RMC module / partition.
`rmcctl -P` ..... Create partition(s) on the RMC module disk. Size of partitions can be specified as percent of disk or sizes in MiB, MB, GiB, GB, TiB or TB. The minimum size allowed is 100MB. NAS services, iSCSI targets, and PCAP recordings need to be inactive, and the RMC module disk / partitions need to be unmounted to run this command.
`rmcctl --serv` ..... Assign a service name to partition. Valid names are NONE, NAS, iSCSI, and iSCSI0/1.
`rmcctl -U` ..... Unmount RMC module / partition.
`rmcctl -W` ..... Destructively clean the disk and any partitions. Must be used with the --force option.

8.3.3 Encrypt / Decrypt

`rmcctl -C` ..... Software encrypt RMC module. Passphrase is entered interactively.
`rmcctl -D` ..... Destructively overwrite S/W encryption information.
`rmcctl -E` ..... Gain entry to S/W encrypted RMC module. Passphrase is entered interactively.
`rmcctl -X` ..... Exit from S/W encrypted RMC module.

8.3.4 Insert / Remove

`rmcctl -I` ..... Undo request for removal (-R).
`rmcctl -R` ..... Request RMC module removal.

8.3.5 Service

The serv command allows the user to set the boot configuration for DTS services and to manually start/stop services. When no options are given, the current boot configuration and active status is displayed for all the services.

`serv` -a ..... All Services.
`serv -B` ..... Apply the settings to the boot-time configuration.
`serv` -c ..... CIFS Service.
`serv` -d ..... DHCP Service.
`serv` -f ..... FTP Service.
`serv` -n ..... NFS Service.
`serv` -s ..... SNMP Service.
`serv` -t ..... TFTP Service.
`serv` -z ..... Telnet Service.
`serv` -w ..... HTTP Read Service.

Troubleshooting

The ibit command is able to detect many problems. While some problems may not have a user remedy, the problem(s) reported by the **ibit** CLI command should be recorded and discussed with a Curtiss-Wright service representative. The **mbit** CLI command can resolve some problems, but it will destroy stored data and formatting of the RMC module. The user should see **ibit** CLI command and **mbit** CLI command for additional information before using the commands.

The chart below provides a basic failure analysis by observing status indicators. If any one of the LEDs exhibits the failure status, the DTS1 may not function properly. The investigative/remedial actions offered should only be tried one or two times. Refer to paragraph 3.1 **Chassis Indicators** for information regarding front panel LEDs.

9.1 Chassis LED Fault Indicators

NOTE
If problems persist, contact Curtiss-Wright Defense Solutions Customer Support. Refer to paragraph 1.6 **Technical Support** for contact information.

Refer to Table 9.1 for chassis fault information.

Table 9.1 Chassis LED Fault Indications

Symptoms/Condition	Meaning	Investigative/Remedial Action
DTS1 red Fault LED on.	Periodic Built In Test (PBIT) failed Encryptor module failed one or more of the tests in the Error Codes table or a listed error has occurred.	1. Run **ibit** CLI command. If the problem can be associated with the RMC module, run **mbit** CLI command. 2. Cycle power and reinitialize the system. 3. Run **cmkey** CLI command for an error report and reference Table 9.3.
DTS1 green Power LED off	Boot failed. Power not applied.	1. Verify power is actually applied and at the correct level. 2. Run **ibit** CLI command.
DTS1 yellow Key Loaded LED off.	Encryption key not loaded or Zeroize button was pushed.	1. Load encryption key. 2. Run **cmkey** CLI command for an error report and reference Table 9.3.

9.2 RMC Module LED Fault Indications

CAUTION
DATA LOSS. Improper use of the **mbit** CLI command can destroy stored data and formatting of the RMC module

NOTE
If problems persist, contact Curtiss-Wright Defense Solutions Customer Support. Refer to paragraph 1.6 **Technical Support** for contact information.

The ibit command is able to detect many problems. While some problems may not have a user remedy, the problem(s) reported by the **ibit** CLI command should be recorded and discussed with a Curtiss-Wright service representative. The **mbit** CLI command can resolve some problems, but it will destroy stored data and formatting of the RMC module. The user should see **ibit** CLI command and **mbit** CLI command for additional information before using the commands.

Table 9.2 RMC Module LED Fault Indications

Symptoms/Condition	Meaning	Investigative/Remedial Action
RMC module red Fault LED on.	Self-test failed	1. Run **ibit** CLI command. If the problem can be associated with the RMC module, run **mbit** CLI command. 2. Reseat RMC module and cycle power.
Cannot store data.	RMC module may be full.	Run **rmcfree** CLI command.
No access to RMC module.	Cannot login to RMC module.	Encryptor battery dead. Replace battery. Refer to paragraph 10.2 **Battery** for detailed instructions.

9.3 Encryptor Error Codes

NOTE
If problems persist, contact Curtiss-Wright Defense Solutions Customer Support. Refer to paragraph 1.6 **Technical Support** for contact information.

Refer to Table 9.3 for fault information.RMC module

Table 9.3 Encryptor Error Codes

Symptoms/Condition	Meaning	Investigative/Remedial Action
0x0103	AES	Memory allocation error
0x0109	AES	KAT (known answer test) failed
0x0203	KEY_WRAP	Memory allocation error
0x0209	KEY_WRAP	KAT (known answer test) failed
0x0210	KEY_WRAP	Initialization vector error
0x0303	SHA	Memory allocation error
0x0309	SHA	KAT (known answer test) failed
0x0403	HMAC	Memory allocation error
0x0409	HMAC	KAT (known answer test) failed
0x0503	DRBG	Memory allocation error
0x0509	DRBG	KAT (known answer test) failed
0x0603	RNG	Memory allocation error
0x0609	RNG	KAT (known answer test) or continual test failed
0x0720	encryptor	3.3Vpower supply error
0x0730	encryptor	2.5Vpower supply error
0x0740	encryptor	1.8Vpower supply error
0x0709	encryptor	KAT (known answer test) failed
0x0810	I2C	Interrupt handler error
0x0901	SATA_P_CTRL	Initialization error
0x0904	SATA_P_CTRL	Write error
0x0905	SATA_P_CTRL	Read error
0x0A10	ENCRYPTION	Chip_A BIST error
0x0A20	ENCRYPTION	Chip_B BIST error
0x0A30	ENCRYPTION	Chip_C BIST error

Table 9.3 Encryptor Error Codes

Symptoms/Condition	Meaning	Investigative/Remedial Action
0x0A40	ENCRYPTION	Chip_D BIST error
0x0A50	ENCRYPTION	Chip_A POST error
0x0A60	ENCRYPTION	Chip_B POST error
0x0A70	ENCRYPTION	Chip_C POST error
0x0A80	ENCRYPTION	Chip_D POST error
0x0A01	ENCRYPTION	Key Load error
0x0D04	SRAM	Write error
0x0D05	SRAM	Read error
0x0E03	E2PROM	Memory allocation error
0x0E04	E2PROM	Write error
0x0E05	E2PROM	Read error
0x0F03	STORAGE	Memory allocation error
0x0F04	STORAGE	Write error
0x0F05	STORAGE	Read error
0x2002	PBKDF2	Invalid input length

Remove / Replace

10.1 RMC Module

CAUTION
EQUIPMENT DAMAGE. Exercise ESD precautions when installing, removing, or handling the RMC module.

10.1.1 Install

CAUTION
EQUIPMENT DAMAGE. The RMC is hot-swappable (remove / install with power applied), however, extreme caution must be used to ensure all ESD handling precautions are followed. Failure to properly handle the RMC will result in equipment damage.

1. Rotate the door latch (Figure 10.1) a quarter turn and open the door.
2. Orient the RMC module with the status LEDs closest to the DTS's door hinge.
3. Align the RMC module rails with the chassis slides and push the RMC module in until the connector makes contact.
4. Apply pressure on the RMC module handle to seat the connector into the backplane connector.
5. Close and latch the DTS1 door.
6. If the door will not latch
   a. Remove the RMC module and inspect the connector contacts on the RMC module and the DTS1 backplane.
   b. If no problem is found with the connectors, reinstall the RMC module and try latching the door again.
   c. If the problem persists, contact Curtiss-Wright Defense Solutions.
7. Open the DTS1 door and observe the RMC module STATUS LED. When green LED turns ON, RMC module is ready.

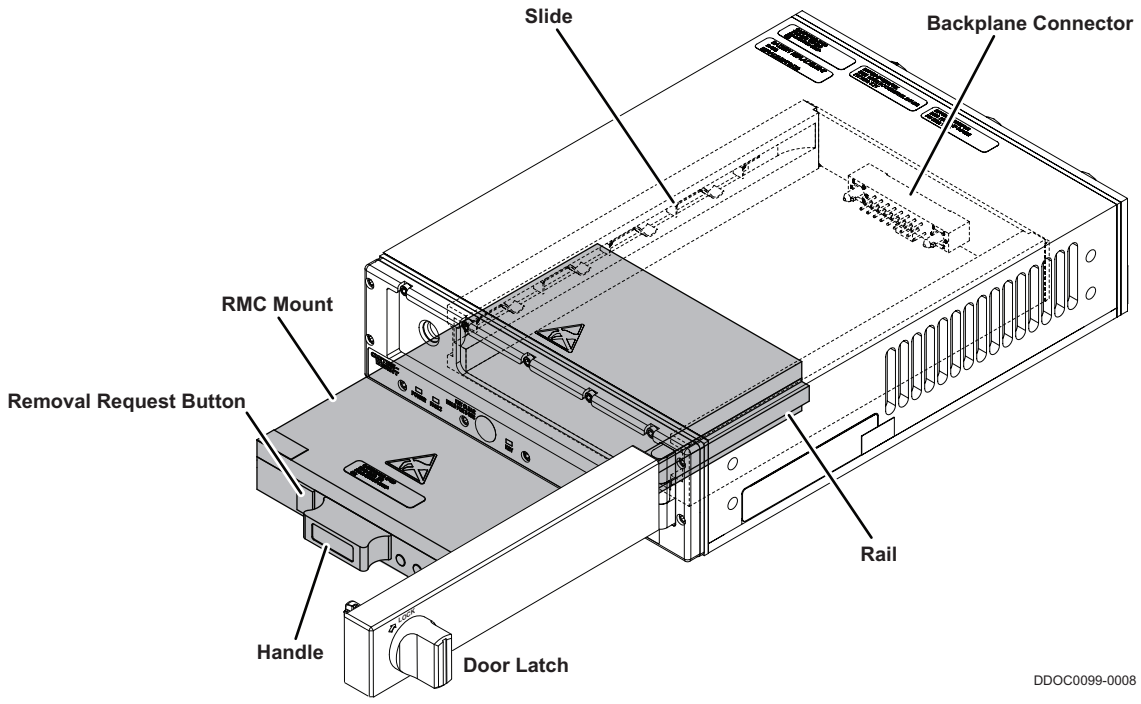

Figure 10.1 RMC Module Install / Remove

10.1.2 Remove

CAUTION
EQUIPMENT DAMAGE. The RMC is hot-swappable (remove / install with power applied), however, extreme caution must be used to ensure all ESD handling precautions are followed. Failure to properly handle the RMC will result in equipment damage.

1. Rotate the door latch a quarter turn and open the door.

NOTE
Removal may also be requested with the CLI command rmcctl.

2. Press and hold the removal request button for three to five seconds to request removal of the RMC module.
   - The STATUS LED will blink at 5Hz for two seconds to acknowledge the request. After acknowledgment, the system will unmount and prepare the RMC module for removal.
   - When the RMC module is ready for removal, the STATUS LED will blink one time every five seconds.
3. Grasp the RMC module handle and pull the unit straight out.

10.2 Battery

CAUTION
EQUIPMENT DAMAGE. Extreme caution must be used to ensure all ESD handling precautions are followed when replacing the battery. Failure to properly handle the DTS1 / battery will result in equipment damage.

CAUTION
UNIT ZEROIZATION. Removal / replacement of the battery assembly will result in zeroization of the unit. Ensure all encryption keys are known and recorded before battery module is removed.

NOTE
Battery life is estimated to be approximately 5 years. As a result, Curtiss-Wright recommends replacing it every 5 years.

The DTS1 encryptor module uses a battery assembly to maintain the encryption key. The status can be checked by initiating the sens command and looking at V_CRYPT response. The battery should be replaced if the V-CRYPT reading is outside of the normal response (3.4 < x < 3.9 Vdc).

Refer to Table 10.1 for possible consumable materials required to replace battery. Refer to **Ordering Information** section for battery assembly part number

Table 10.1 Consumable Materials

Qty	U/M	Description	Curtiss-Wright P/N	OEM P/N	OEM
6	EA	Screw, Sealing Flat Head 2-56 x 0.25	D700058-R00-LF	98070A079	McMaster-Carr
4	EA	Screw, BSHC, 1-64 x 0.125	D700272-R00-LF	92949A314	McMaster-Carr

NOTE
O-rings are integral to sealing screws.

1. Remove six sealing screws, o-rings, and the battery access panel (Figure 10.2).
2. Remove four screws and battery assembly. Discard battery assembly in accordance with local regulations.
3. Align replacement battery assembly connector pins with DTS1 connector sockets.
4. Install the battery assembly in the DTS1. Make sure the pins/sockets properly engage.
5. Use four screws to secure the battery assembly in place. Tighten the screws to 1.7 in. lb.

NOTE
If an integral o-ring is damaged, replace sealing screw.

6. Use six sealing screws and o-rings to secure the battery access cover in place. Tighten the screws to 2.2 in. lb. using the pattern shown in Figure 10.3.

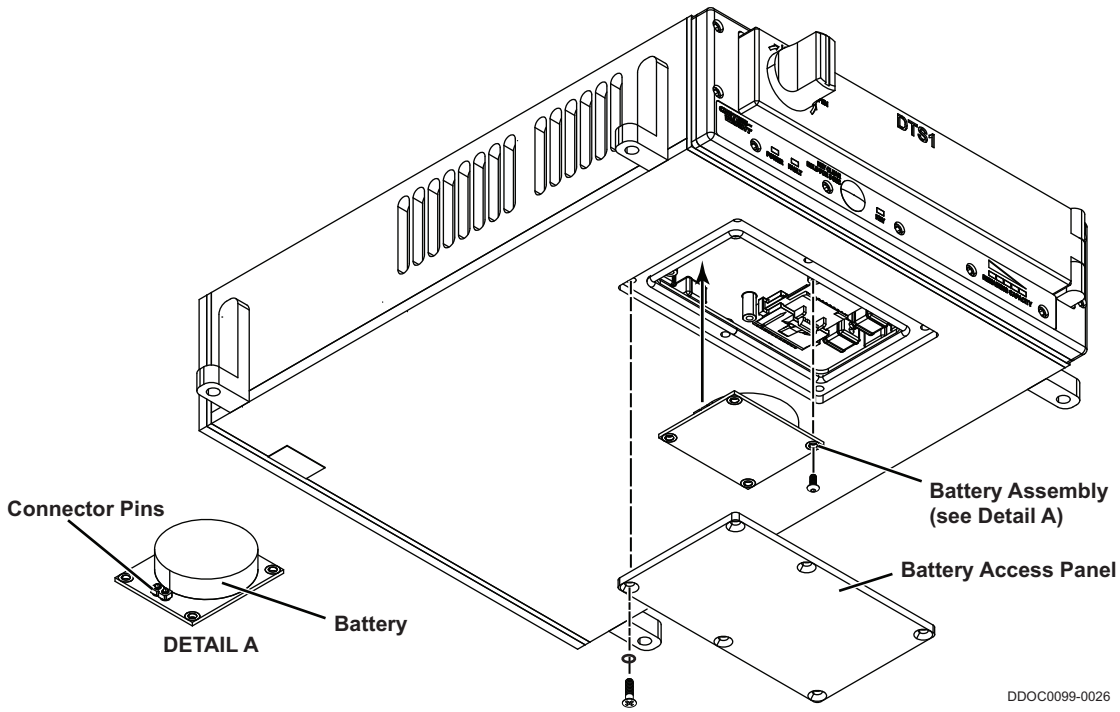

Figure 10.2 Battery Assembly Replacement

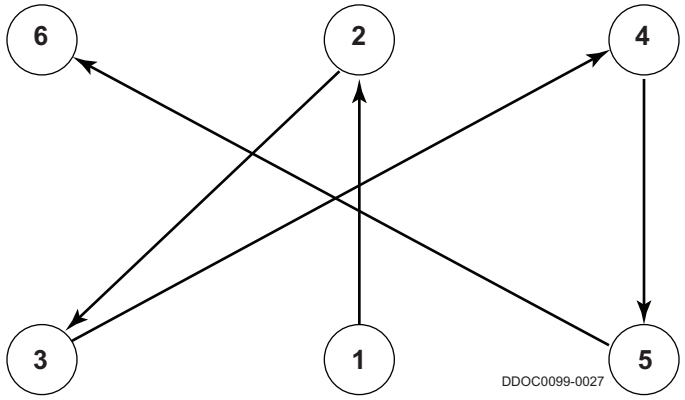

Figure 10.3 Battery Access Panel Screws Tightening Sequence

Simple Network Management Protocol

11.1 SNMP MIB

The DTS1 supports Simple Network Management Protocol (SNMP). The user may configure SNMP for a Windows workstation via the Windows Control Panel. The user should consult with their network administrator for details on configuration and utilization of the SNMP traps and other data capture programs.

DTS1 SNMP Management Information Basis (MIB) Definitions are as follows:

```
CWCDS-DTS-MIB DEFINITIONS ::= BEGIN

--
-- MIB for CWCDS DTS.
--

IMPORTS
   MODULE-IDENTITY, OBJECT-TYPE, Integer32, enterprises,
   NOTIFICATION-TYPE                    FROM SNMPv2-SMI
   OBJECT-GROUP, NOTIFICATION-GROUP       FROM SNMPv2-CONF
;

dtsSnmp MODULE-IDENTITY
   LAST-UPDATED "201206250000Z"
   ORGANIZATION "www.cwcontrols.com"
   CONTACT-INFO
       "email: support@curtisswright.com"
   DESCRIPTION
      "MIB for CWCDS DTS."
   REVISION     "201206250000Z"
   DESCRIPTION
      "version 1.0"
   ::= { enterprises 27675 }

--
-- top level structure
--
dtsSnmpValues      OBJECT IDENTIFIER ::= { dtsSnmp 1 }

dtsSnmpValuesGroup OBJECT-GROUP
   OBJECTS { dtsINFO,
             dtsSERV,
             dtsIPCONFIG,
             dtsRMCFREE,
             dtsRMCCTL,
             dtsRMCINFO,
             dtsLEDCTRL,
             dtsSENS,
             dtsSYSDATE,
             dtsIBIT,
             dtsCMLOGIN,
             dtsCMKEY }

   STATUS current
   DESCRIPTION
         "Group of all DTS variables."
   ::= { dtsSnmp 4 }

--
```

```
-- Values
--

dtsINFO OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..4096))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: info"
   ::= { dtsSnmpValues 1 }

dtsSERV OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..4096))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: serv"
   ::= { dtsSnmpValues 2 }

dtsIPCONFIG OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..8192))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: ipconfig"
   ::= { dtsSnmpValues 3 }

dtsRMCFREE OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..4096))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: rmcfree"
   ::= { dtsSnmpValues 4 }


dtsRMCCTL OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..4096))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: rmcctl"
   ::= { dtsSnmpValues 5 }

dtsRMCINFO OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..8192))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: rmcinfo"
   ::= { dtsSnmpValues 6 }

dtsLEDCTRL OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..8192))
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Output of command: ledctrl"
   ::= { dtsSnmpValues 7 }

dtsSENS OBJECT-TYPE
   SYNTAX      OCTET STRING (SIZE(1..8192))
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Output of command: sens"
    ::= { dtsSnmpValues 8 }

dtsSYSDATE OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..8192))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Output of command: sysdate"
    ::= { dtsSnmpValues 9 }

dtsIBIT OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..65536))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Output of command: ibit"
    ::= { dtsSnmpValues 10 }

dtsCMLOGIN OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..8192))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Output of command: cmlogin"
    ::= { dtsSnmpValues 11 }

dtsCMKEY OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..8192))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Output of command: cmkey"
    ::= { dtsSnmpValues 12 }

END
```

Command Line Interface

The Command Line Interface (CLI) is the primary method of communicating with and configuring the DTS1 and / or RMC module.

12.1 DTS1

amnt ..... Auto mounter/starter control utility
cmfwupdate ..... Update DTS security processor
cmkey ..... Manage key on encryptor
cmlog ..... Read / clear crypto module error log
cmlogin ..... Login, Logout, initialize crypto module
dhcpconfig ..... Configure DHCP services
fdefaults ..... Load factory default values
fupdate ..... Boot into RAM disk image to perform field update
fwall ..... Firewall control utility
help ..... Display commands available to DTS1 admin user
ibit* ..... Perform initiated built-in test (IBIT).
info* ..... View DTS1 system information
ipconfig* ..... Configure IP interfaces
istarget ..... Control iSCSI target services
ledctrl* ..... Set/get duty cycle and status for DTS LEDs
log ..... View DTS1 log files
mbit ..... Perform maintenance built-in tests (MBIT)
nfsctl ..... Change NFS options
ntpdate ..... Retrieve system time and date from ntp server
password ..... Change login password for an account
pcap ..... Perform packet capture (PCAP) recording to capture network traffic
rtp ..... RTP video stream recording control and status.
reboot ..... Reboot the DTS1
sens* ..... View DTS1 sensor readings
serv* ..... DTS1 service control and status utility
shutdown ..... Halt the DTS1
sysdate* ..... Configure system time and date

12.2 RMC Module

rmcctl* ..... RMC control utility
rmcfree* ..... Display file system free/used info for RMC storage devices
rmcinfo* ..... View and set RMC identification information
rmcpurge ..... Purge all data on the drives of RMC

* Commands with SNMP service

12.3 Commands

Refer to following paragraphs for detailed information regarding CLI commands.

12.3.1 amnt

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The amnt command is used to determine the configuration of the RMC auto mounter/starter daemon. The conditions that allow auto-mounting of NAS RMCs, and the auto-starting of iSCSI targets can be configured. When an action is not requested, the current state is reported. The default operation for NAS RMCs / partitions to auto mount at POR or the first insertion. The default operation for iSCSI RMCs to NOT auto-start the iSCSI targets. Configuring an RMC/partition to be NAS or iSCSI is done with the **--serv** command.

Syntax
amnt [**-h** | **--help** | **--version**]
amnt [**-s** slotnum] [**--off**] [**--on**] [**--key**] [**--nas**] [**--iscsi**] [**--por**] [**--fin**] [**--sin**] [**--can**] [**--ro**] [**--restart**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, **--slot** <slotnum> .....Slot number where the RMC is located(0,1,2,A). For all slots, use A or all. Omission will select slot 0.
--off, off, 0 .....Disable an option, or the auto mounter/starter capability as a whole.
--on, on, 1.....Enable an option, or the auto mounter/starter capability as a whole.
--key, key.....Configure auto key loading of the crypto unit
--nas, nas.....Configure the auto mounting of NAS file systems on the RMC described by --slot.
--iscsi, iscsi .....Configure the auto starting of iSCSI targets on the RMC described by --slot.
--por, por .....Configure the operation at POR of the RMC described by --slot.
--fin, fin.....Configure the operation at the first insertion of the RMC described by --slot.
--sin, sin.....Configure the operation at subsequent insertions of the RMC described by --slot.
--can, can.....Configure the operation at canceled removals of the RMC described by --slot.
--ro, ro .....Make the RMC mount read only, or the iSCSI target start read only. An RMC that is write-protected will automatically use this option.
--blk, blk <blk size>.....Configure the auto starting of iSCSI targets with this block size. Valid sizes are 512, 1024, 2048, and 4096. The default block size is 4096, the same as the istarget CLI command.
--restart, restart.....Restart the auto mounter/starter daemon for the RMC described by --slot.

Example: Status display

```
cw_dts> amnt
 [amnt]
   AMT_S#: AMNT KEY iPOR iFIN iSIN iCAN iRO iBLK nPOR nFIN nSIN nCAN nRO
   ***********************************************************************
   AMT_S0:  1    0    1   0     0    0    0  512   1    0    0    0   0
 [!amnt] <summary>
```

Line Identifier
AMT_S# .....Current automounter status of RMC in slot "#"

Enumerated types
<summary> .....Command status summary (OK, ERR)

Example: Turn off auto-mounting on slot 0 completely

```
amnt -s 0 --off
```

Example: Turn on H/W encryption auto key loading. A subsequent load of a H/W encryption key will attempt to auto-mount

```
amnt -s 0 --key --on
```

Example: Turn off auto-mounting of NAS RMC / partitions

```
amnt -s 0 --nas --off
```

Example: Turn off auto-mounting of NAS RMC / partitions at POR

```
amnt -s 0 --nas --por --off
```

Example: Turn off auto-mounting of NAS RMC / partitions at first insertion

```
amnt -s 0 --nas --fin --off
```

Example: Turn off auto-mounting of NAS RMC / partitions at subsequent insertion

```
amnt -s 0 --nas --sin --off
```

Example: Turn off auto-mounting of NAS RMC / partitions at canceled removal

```
amnt -s 0 --nas --can --off
```

Example: Turn on read only mounting option for NAS RMC / partitions. Allowed during auto-mounting only. Doesn't affect CLI mounting.

```
amnt -s 0 --nas --ro --on
```

Example: Turn off auto-starting of iSCSI target RMC

```
amnt -s 0 --iscsi --off
```

Example: Turn off auto-starting of iSCSI RMC at POR

```
amnt -s 0 --iscsi --por --off
```

Example: Turn off auto-starting of iSCSI RMC at first insertion

```
amnt -s 0 --iscsi --fin --off
```

Example: Turn off auto-starting of iSCSI RMC at subsequent insertion

```
amnt -s 0 --iscsi --sin --off
```

Example: Turn off auto-starting of iSCSI RMC at canceled removal

```
amnt -s 0 --iscsi --can --off
```

Example: Turn on read only option for iSCSI RMC. Valid during auto-mounting only. Doesn't affect CLI iSCSI target starting.

```
amnt -s 0 --iscsi --ro --on
```

Example: Configure the block size for the auto started iSCSI targets.

```
amnt -s 0 --iscsi --blk 512
```

Example: Restart the auto mounter/starter daemon for the RMC described by --slot.

```
amnt -s 0 --restart
```

12.3.2 cmfwupdate

Description:
The cmfwupdate command provides the user the ability to update the firmware within the DTS security processor. The update is a trusted update that requires a binary image paired with its associated signature. This update file and signature will be verified during the transfer and will generate a failure if verification is unsuccessful.

NOTE
Place the provided files in the root of the NAS folder (/rmc_shares/rmc0p1).

NOTE
Curtiss-Wright will be the only entity who provides a firmware update

Syntax:
```
cmfwupdate [-h | --help | -v | --version]
cmfwupdate [-f <str>] [-s <str>]
cmfwupdate - [options]
```

Options:
-h, --help.....Print help message.
-v, --version.....Report application version.
-f, --filename.....Filename (example: filename.bin).
-s, --signature.....signature (exmaple: signature.bin).

Returns:
0 on success, else error

Example:. Update crypto firmware.

```
cw_dts> cmfwupdate -f dts_crypto_csfc.bin -s dts_crypto_csfc_signature.bin
 [!cmfwupdate] ERR
```

12.3.3 cmkey

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The cmkey command allows for management of keys on the crypto module. For status information, issue cmkey without options.

Syntax
cmkey [**-h** | **--help** | **--version**]
cmkey -e KEY -m MAC [**-s** SLOT] [**--save** LOC] [**-F**]
cmkey -p PSK -d DEK [**-s** SLOT] [**--save** LOC] [**-F**]
cmkey -s SLOT [**--load** LOC | **--auto** | **--unload**] [**-F**]
cmkey --del LOC
cmkey --kek
cmkey --zero [**--nowait**]

Options
-h, **--help**.....Print help message
--version.....Print program version
--auto.....Auto-load the saved key for RMC selected by -s.
--save <loc>.....Save key to non-volatile memory location (0-31).
--del <loc>.....Delete/zeroize a saved key.
--load <loc>.....Load a saved key for RMC selected by -s.
--unload.....Unload/zeroize key from RMC selected by -s.
-s, **--slot** <num>.....RMC slot number (0, all) for which to load/install a key.
-e, **--ekey** <hex>.....Encrypted DEK (data encryption key) 40 byte value represented by 80 hex characters.
-m, **--mac** <hex>.....MAC (message authentication code) 48 byte value represented by 96 hex characters.
-p, **--psk**.....Plain Text PSK (pre-shared key) 32 byte value represented by 64 hex characters.
-d, **--dek**.....Plain Text DEK (data encryption key) 32 byte value represented by 64 hex characters.
-k, --kek .....Generates KEK (key encryption key).
-r, --resetkek.....Reset the key used to encrypt the KEK to the PSK.

NOTE
Must provide existing PSK (-p option) when using this option.

-u, **--userpsk**.....User defined plain text PSK (pre-shared key) 32 byte value represented by 64 hex characters.

NOTE
The --zpsk option will restore the unit back to a state prior to assignment of the PSK making the unit inoperable. Will prompt user prior to performing the erase.

--zpsk.....Zeroize the crypto unit PSK.
-Z, **--zero**.....Zeroize crypto module. Clears all saved/loaded keys.
--nowait.....Do not wait until zeroization is complete before returning.
-F, **--force**.....Force key load to RMC if key mismatch is detected.

NOTE
Options **--save, --del**, and **--load** operate on 32 non-volatile memory locations for key storage. These locations are within the crypto module. For security, the saved keys cannot be retrieved or viewed. Use of these memory locations is not required, and must be explicitly requested with option **--save** when entering a key. By default, keys are directly loaded/installed for the RMC selected with option **-s**.

Example: Get status regarding keys

```
cw_dts> cmkey
 [cmkey]
  CMKEY: id=<int> init=<b> login=<b> s0=<b> s1=<b> s2=<b> deks=<mask> status=<sts>
 [!cmkey] <summary>
```

Line Identifier
CMKEY .....Status line

Fields
`id=<int>`.....Unique crypto module identifier
`init=<b>`.....Initialization indicator
`login=<b>`.....Login indicator
`s0=<b>` .....Key-loaded indicator for RMC slot 0
`s1=<b>` .....Key-loaded indicator for RMC slot 1
`s2=<b>` .....Key-loaded indicator for RMC slot 2
`deks=<int>`.....Saved key locations
`status=<sts>` .....Summary status for the line

Enumerated types (See above examples in fields)
<int> .....An integer value
<b> .....Boolean status value (1=true, 0=false)
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

Example: Pass encrypted key, save to location 4, load for RMC..

```
cw_dts> cmkey --save 4 -s 0 -F -e [edek string] -m [mac string]
 [cmkey]
  CMKEY: action=inst slot=<int> status=<sts>
 [!cmkey] <summary>
```

Where
`[edek string]` = 40 byte value represented by 80 hex characters
`[mac string]` = 32 byte value represented by 64 hex characters

Line Identifier
CMKEY .....Status line

Fields
`action=`<act> .....Action being performed
`slot=`<int> .....RMC slot number
`status=`<sts> .....Summary status for the line

Enumerated types (See above examples in fields)
<int> .....An integer value
<act> .....Action (zero, auto, save, inst, load, unload, delete)
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

Example: Pass plain text key, load for RMC

```
cw_dts> cmkey -s 0 -d -p
 [cmkey]
  Please enter plaintext DEK: [User-generated plain text DEK string]
  Please enter current PSK: [Curtiss-Wright provided PSK string]
  CMKEY: action=inst slot=<int> status=<sts>
 [!cmkey] <summary>
```

Where
`[dek string]` = 32 byte value represented by 64 hex characters
`[psk string]` = 32 byte value represented by 64 hex characters

Example: Pass plain text key, save to location 3.

```
cw_dts> cmkey --save 3 -d -p
 [cmkey]
  Please enter plaintext DEK: [User-generated plain text DEK string]
  Please enter current PSK: [Curtiss-Wright provided PSK string]
  CMKEY: action=save status=<sts>
 [!cmkey] <summary>
```

Example: Load key from memory location 5 for RMC.

```
cw_dts> cmkey --load 5 -s 0
 [cmkey]
  CMKEY: action=inst slot=<int> status=<sts>
 [!cmkey] <summary>
```

Example: Unload key for RMC.

```
cw_dts> cmkey --unload -s 0
 [cmkey]
  CMKEY: action=unload slot=<int> status=<sts>
 [!cmkey] <summary>
```

Example: Delete key in memory location 3.

```
cw_dts> cmkey --del 3
 [cmkey]
  CMKEY: action=delete status=<sts>
 [!cmkey] <summary>
```

Example: Zeroize crypto module

```
cw_dts> cmkey --zero
 [cmkey]
 CMKEY: action=zero status=<sts>
 [!cmkey] <summary>
```

Example: Auto load keys for RMC

```
cw_dts> cmkey --auto -s all
 [cmkey]
  CMKEY: action=auto slot=<int> status=<sts>
 [!cmkey] <summary>
```

Example: Generate KEK (key encryption key)

```
cw_dts> cmkey --kek
 [cmkey]
  CMKEY: kek=<str> mac=<str> status=<sts>
 [!cmkey] <summary>
```

Example: Assign user defined PSK

```
cw_dts> cmkey -p -u
 cmkey]
  Please enter current PSK: [current psk string]
  Please enter new PSK: [new psk string]
  CMKEY: action=psk status=OK
 [!cmkey] OK
```

Where

`[current psk string]` = current 32-bit plain-text PSK represented by 64 hex characters
`[new psk string]` = new 32-bit plain-text PSK represented by 64 hex characters

Line Identifier

CMKEY:.....Crypto init status line

Fields

`kek=<str>`.....Wrapped Key Encryption Key
`mac=<str>`.....Message Authentication Code
`status=<sts>` .....Summary status for the line

Enumerated types (See above examples in fields)

<str> .....String
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

12.3.4 cmlog

Description:
The cmlog command allows a user to view the error log of the DTS crypto module. Only the crypto officer has permission to clear the error log

Syntax:
`cmlog [-h | --help | -v | --version]`
`cmlog [-c | --clear]`
`cmlog`
`cmlog - [options]`

Options:
`-h, --help`: .....Print help message.
`-v, --version`: .....Report application version.
`-c, --clear`: .....Clear error log.

Returns:
0 on success, else error

Example: View crypto module error log

```
cw_dts> cmlog
  [cmlog]
   CMLOG: Currently Logged Errors
   (0x0c20):[SECURITY] - tamper event: T1
   status=OK
  [!cmlog] OK
```

Example: Clear crypto module error log

```
cw_dts> cmlog-c
  [cmlog]
   CMLOG: status=OK
   status=OK
  [!cmlog] OK
```

12.3.5 cmlogin

Description
The cmlogin command allows the user to initialize and manage the login state of the crypto module. Initialization is required before crypto keys can be loaded and RMC formatted and mounted as storage. Initialization state is maintained across power cycles as long as a zeroization event has not occurred.

Login is required after each power up or initialization. Login state is not maintained across power cycles.

Syntax
```
cmlogin [-h | --help | --version]
cmlogin -I -u username -p password [-F]
cmlogin [-L] -u username -p password
cmlogin -O
```

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-u, **--user** <str>.....Username for CM login. 1-15 characters.
-p, **--pass** <str>.....Password for CM login. 8-15 characters, must contains at least one letter and one number (no special characters).
-M, **--auth**.....HMAC used for password authorization. Must be completed after providing username/password to enter login state. The HMAC must be 96-ascii hex characters.
-I, **--init** .....Initialize crypto module
-F, **--force** .....Force reinitialization if module already initialized or RMC mounted. Re-init zeroizes a previously initialized crypto module.
-L, **--login**.....Login to crypto module. Default operation when credentials are supplied.
-O, **--logout**.....Logout of crypto module. (Undo login)

Example: Initialize crypto module.

```
cw_dts> cmlogin -u [user name] -p -I
 [cmlogin]
  Please enter password: [password]
  Please verify password: [password]
  CMLOGIN: action=save status=<sts>
 [!cmlogin] <summary>
```

Where
[user name] = 1-15 characters
[password] = 8-15 characters, Contains at least one letter, one number and no special characters

Line Identifier
CMLOGIN .....Command status line

Fields
action=<act> .....Action being performed
status=<sts> .....Summary status for the line

Enumerated types (See above examples in fields)
<act> .....Action (init, login, logout, auto, save, clear)
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

Example: Login to crypto module.

```
cw_dts> cmlogin -u [user name] -p
 [cmlogin]
  Please enter password: [password]
  CMLOGIN: action=save status=<sts>
 [!cmlogin] <summary>
```

Where
[user name] = 1-15 characters
[password] = 8-15 characters, Contains at least one letter, one number and no special characters

Example: Display current state.

```
cw_dts> cmlogin
 cmlogin]
  CMLOGIN: state=<desc> init=<bool> login=<bool> status=<sts>
 [!cmlogin] <summary>
```

Line Identifier
CMLOGIN ..... Command status line

Fields
`state=<desc>` ..... State description
`init=<bool>` ..... Initialization indicator
`login=<bool>` ..... Login indicator
`status=<sts>` ..... Summary status for the line

Enumerated types (See above examples in fields)
<desc> ..... Description of crypto module state:
- uninit ..... Not initialized
- init ..... Initialized
- ready ..... Initialized, Login complete
- error ..... Error state
- unknown ..... Invalid state

<bool> ..... Boolean status value (1=true, 0=false)
<sts> ..... Status message (OK, ERR "<str>")
<summary> ..... Command status summary (OK, ERR)

12.3.6 dhcpconfig

Description

The dhcpconfig command allows the user to configure DHCP services on the DTS unit.

Syntax
dhcpconfig [**-h** | **--help** | **--version**]
dhcpconfig -A -s IP NM [**-r** val] [**-n** val] [**-g** val] [**-d** val] [**-t** val]
dhcpconfig -D -s IP NM
dhcpconfig -A -b NAME [**-m** val | **-c** val] [**-t** val] [**-f** val] [**-n** val] [**-g** val] [**-d** val]
dhcpconfig -D -b NAME

Options for subnet and BOOTP declarations
-h, **--help**.....Print help message.
--version.....Print program version.
-A, **--add**.....Add/Update subnet or bootp entry
-D, **--delete**.....Delete subnet or bootp entry
-n, **--netmask** <ip> .....Netmask to assign to subnet clients
-g, **--gateway** <ip> .....Gateway to assign to clients in subnet
-i, **--domainserver** <ip>...IP of Domain Name Server to assign to clients
-d, **--domain** <str> .....Domain Name to assign to clients
-o, **--offset** <str> .....Time offset from UTC in seconds

Options specific to subnet declarations
-s, **--subnet** <ip> <nm> ..... IP and netmask for DHCP Subnet entry (Required)
-r, **--range** <ip> <ip>.....Low to high range of IP addresses to provide

Options specific to BOOTP declarations
-b, **--bootp** <str>.....Name for bootp entry (Required)
-m, **--mac** <str>.....Ethernet MAC to identify bootp client
-c, **--clientid** <str> .....Alternative bootp client identifier value
-t, **--tftpfile** <str> .....TFTP file for bootp client to download/boot
-f, **--fixedip** <ip> .....Fixed IP for bootp client

To start and stop the DHCP service, use command 'serv'.

Example: View configuration (enumerated)

```
cw_dts> dhcpconfig
 [dhcpconfig]
  SUBNET: subnet=<net> rn=<ip>-<ip> gw=<ip> dns=<ip> nm=<nm> dmn=<str> toff=<int>
  status=<sts>
  BOOTP: host=<str> mac=<mac> id=<str> tftp=<file> ip=<ip> nm=<nm> gw=<ip>
  dmn=<str> dns=<ip> toff=<int> status=<sts>
 [!dhcpconfig] <summary>
```

Line Identifier
SUBNET.....Reports a DHCP subnet declaration
HOST .....Reports a BOOTP client declaration

Fields (only fields defined for the entry are displayed)

`subnet=<net>` .....Reports subnet on which to assign addresses
`rn=<ip>-<ip>` .....Reports range of addresses to assign to clients
`gw=<ip>` .....Reports gateway address passed to clients
`dns=<ip>` .....Reports DNS server address passed to clients
`nm=<nm>` .....Reports netmask passed to clients
`dmn=<str>` .....Reports domain name passed to clients
`toff=<int>` .....Reports time offset passed to clients
`host=<str>` .....Reports name of BOOTP entry / hostname of client
`mac=<mac>` .....Reports MAC address of BOOTP client
`id=<str>` .....Reports client ID of BOOTP client
`tftp=<file>` .....Reports BOOTP file name
`ip=<ip>` .....Reports IP address to assign to client
`status=``<sts>` .....Summary status for the given line.

Enumerated types:
<net> .....IPv4 dotted-decimal subnet address (Ex: 192.168.1.0)
<ip> .....IPv4 dotted-decimal address (Ex: 192.168.1.1)
<nm> .....IPv4 dotted-decimal netmask (Ex: 255.255.255.0)
<int> .....An integer value (Ex: -28800, 7200)
<mac> .....MAC address (Ex: 00:11:22:33:44:55)
<file> .....File name for BOOTP client (Ex: "/rmc0/bootimage")
<str> .....Text string
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

Example: View configuration (sample command output)

```
cw_dts> dhcpconfig
[dhcpconfig]
SUBNET: subnet=192.168.1.0 rn=192.168.1.1-192.168.1.10 gw=192.168.1.1
dns=192.168.1.1 nm=255.255.255.0 dmn="CWNAS" toff=-8 status=OK
BOOTP: host=target mac=00:1b:ac:70:10:42 tftp="/rmc0/bootfile" status=OK
[!dhcpconfig] OK
```

Example: Add subnet configuration

```
cw_dts> dhcpconfig -A -s 192.168.3.0 255.255.255.0 -g 192.168.3.5 -r 192.168.3.10
192.168.3.20 -i 192.168.3.10 -o -8
 [dhcpconfig]
  SUBNET: status=<sts>
 [!dhcpconfig] <summary>
```

Example: Delete subnet configuration

```
cw_dts> dhcpconfig -D -s 192.168.3.0 255.255.255.0
 [dhcpconfig]
  SUBNET: status=<sts>
 [!dhcpconfig] <summary>
```

Example: Add BOOTP client

```
cw_dts> dhcpconfig -A -b mypc -m 20:50:A4:FC:6B:B5 -f 192.168.3.55 -t /rmc0/bootfile
 [dhcpconfig]
  BOOTP: status=<sts>
 [!dhcpconfig] <summary>
```

Example: Delete BOOTP client

```
cw_dts> dhcpconfig -D -b mypc
 [dhcpconfig]
  BOOTP: status=<sts>
 [!dhcpconfig] <summary>
```

12.3.7 fdefaults

Description
The fdefaults command set passwords, IP addresses, NAS configuration, etc. to factory default values and clears out saved crypto credentials, command history and saved ssh authorized keys.

Syntax
`fdefaults` [**`-h`** | **`--help`** | **`--version`** | **`--go`**]

Options
`-h`, **`--help`**.....Print help message.
`--version`.....Print program version.
`--go`.....Proceed with restoration to factory defaults

12.3.8 fupdate

Descripton:
The fupdate command boots the DTS system into a RAM disk image where the user can install a new DTS disk image onto the system. By default the new image file to be updated is uploaded via FTP or SCP into memory.

See paragraph 7.9 **Update Software / Firmware** for detailed instructions.

12.3.9 fwall

Description

The fwall command is used to determine the configuration of the firewall. This command does not start or stop DTS services, but only allows the firewall to pass or block traffic for them. The default zone used is the public zone. The default configuration of the firewall is ON. The boot flash needs to be writeable to make changes to the firewall configuration permanent. There is a way to pass a user defined command straight through (no error checking) to the underlying firewall-cmd utility.

Syntax

fwall [**-h** | **--help** | **--version**]
fwall [**--status**] [**--start**] [**--stop**] [**--restart**]

Options

-h, **--help**.....Print help message.
--version.....Print program version.
--status.....Show the firewall status
--unmask.....Unmask the firewall
--start.....Start the firewall
--enable.....Enable the firewall at boot
--stop.....Stop the firewall
--disable.....Disable the firewall at boot
--mask.....Mask the firewall
--restart.....Restart the firewall
--reload.....Reload the firewalls permanent rules
--perm.....Make action permanent
--dhcp.....Add/remove dhcp
--ftp, ...Add/remove ftp
--http.....Add/remove http
--iscsi.....Add/remove iscsi targets
--nfs.....Add/remove nfs
--telnet.....Add/remove telnet
--cifs.....Add/remove cifs
--ssh.....Add/remove ssh
--snmp.....Add/remove snmp
--tftp.....Add/remove tftp
--all.....Add/remove all DTSx services
--add.....Add a port, service, or interface
--rem.....Remove a port, service or interface
--port.....Port number to add/remove
--iface.....Interface to add/remove: eth0, etc.
--udp.....Define a port as udp
--tcp.....Define a port as tcp
--cmd "options".....Pass "options" to firewall-cmd

Example: Status display

```
cw_dts> fwall
 [fwall]
  FIREWALL: status=OK "The firewall IS running"
  public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: dhcp ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
 [!fwall] <summary>
```

Line Identifier
FIREWALL .....Current fireWall status

Enumerated types
<summary> .....Command status summary (OK, ERR)

Example: Display firewall status

```
fwall --status
```

Example: Unmask firewall

```
fwall --unmask
```

Example: Start firewall

```
fwall --start
```

Example: Enable firewall at boot

```
fwall --enable
```

Example: Stop firewall

```
fwall --stop
```

Example: Disable firewall at boot

```
fwall --disable
```

Example: Mask firewall

```
fwall --mask
```

Example: Restart firewall

```
fwall --restart
```

Example: Reload firewall permanent rules

```
fwall --reload
```

Example: Add eth0 to firewall

```
fwall --add --iface --eth0
```

Example: Add ftp service to firewall

```
fwall --add ftp
```

Example: Remove ftp service from firewall

```
fwall --rem ftp
```

Example: Add udp port 7777 to firewall permanently

```
fwall --add --perm --port 7777 udp
```

Example: Remove udp port 7777 from firewall permanently

```
fwall --rem --perm --port 7777 udp
```

Example: Pass command to firewall-cmd

```
fwall --cmd  "--list-services"
```

12.3.10 help

Description
The help command displays a list of commands available to the DTS admin user if no arguments are supplied. For help information for a specific command, use help [command]. For example: help ipconfig. Alternatively, run the command with -h or --help as an argument.

Syntax
`help`
`help` [**`-h`** | **`--help`** | **`--version`**]
help command

Options
`-h`, **`--help`**.....Print help message.
`--version`.....Print program version.

Examples
```
ipconfing -h
help
```

12.3.11 ibit

Description
The ibit command performs the initiated built-in test.

Syntax
`ibit` [**`-h`** | **`--help`** | **`--version`**]

Options
`-h`, **`--help`**.....Print help message.
`--version`.....Print program version.
`-v`.....Verbose mode. Print more info regarding tests.
`-vf`.....Verbose-on-failure. Print more info about failures.

NOTE
Additional output for -v an -vf is not formalized. Non-verbose IBIT output is at the end of the response.

Example: IBIT execution

```
cw_dts> ibit
 [ibit]
  IBIT_MON: mcu=<s> i2c=<s> volt=<s> status=<sts>
  IBIT_ETH: eth0=<s> eth1=<s>
  IBIT_RMC0: volt=<s> ata=<s> smart=<s> status=<sts>
 [!ibit] <summary>
```

Line Identifier
IBIT_MON .....Results for system monitor subsystem.
IBIT_ETH .....Results for Ethernet subsystem.
IBIT_RMC# .....Results for RMC in slot '#'.

Fields
`mcu=``<s>` .....Result for sysmon microcontroller
`i2c=<s>` .....Result for I2C bus
`volt=<s>` .....Result for voltage regulator monitors
`eth#=<s>` .....Result for Ethernet device eth# (eth0, eth1, ...)
`ata=<s>` .....Result for ATA driver log check
`smart=<s>` .....Result for disk S.M.A.R.T. self assessment
`status=<sts>` .....Summary status for the line.

Enumerated types
<s> .....Subtest status. 1=pass, 0=fail
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

12.3.12 info

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The info command displays DTS hardware and software information, such as versions.

Syntax
`info [-h | --help | --version | -R | -M | -A ]`
`info`

Options
`-h`, **`--help`** ..... Print help message.
`--version` ..... Print program version.
`-A` ..... Alternate short-form display.
`-M` ..... Show the media type(s) supported by each slot.
`-R` ..... Generate a status report of info useful for tech support. Output not formalized. With optional SLOT, export report to RMC.

Example: Long-form output

```
cw_dts> info
 [info]
  Manufacturer: Curtiss-Wright Controls
  Cage Code: 1P423
  System firmware: <ver>
  Sysmon firmware: <ver>
  Crypto firmware: <ver>
  Media slots: <num>
 [!info] <summary>
```

Fields
`System firmware` ..... Operating system firmware version
`Sysmon firmware` ..... System monitor firmware version
`Crypto firmware` ..... Encryption module firmware version
`Media slots` ..... RMC/media slot count

Enumerated types:
<ver> ..... Version string. 'ERR' on error, or 'na' for "not applicable"
<num> ..... Number of slots (integer)
<summary> ..... Command status summary (OK, ERR)

Example: Short-form output

```
cw_dts> info -A
 [info]
  DTS_INFO: system=<ver> sysmon=<ver> crypto=<ver> slots=<num> status=<sts>
 [!info] <summary>
```

Line Identifier
DTS_INFO ..... Firmware versions and slot count data.

Fields
`system=<ver>` ..... Operating system firmware version
`sysmon=<ver>` ..... System monitor firmware version
`crypto=`**<ver>** ..... Encryption module firmware version
`slots=<num>` ..... RMC/media slot count
`status=<sts>` ..... Summary status for the line

Enumerated types (See above examples in fields)

<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string

Example: Media types

```
cw_dts> info -M
 [info]
  DTS_MEDIA: slots=<num> type0=<t> type1=<t> type2=<t> status=<sts>
 [!info] <summary>
```

Line Identifier
DTS_MEDIA.....Media types supported by the media/RMC slot

Fields
`slots=<num>` .....RMC/media slot count
`type#=<t>`.....RMC/media types supported by slot '#'.

Enumerated types (See above examples in fields)
<num>.....Number of slots (integer)
<t> Media type options. A hexadecimal value as follows:

Bit	Mask	Description
0	1	RMC
-	E	Reserved

NOTE
The following error examples for phony example command 'cmd' are applicable to all commands supported by the CLI.

Example: Invalid parameters / Command errors

```
cw_dts> cmd --badoption
[cmd]
INVALID: status=ERR "<errstr>"
[!cmd] ERR
```

```
cw_dts> cmd --valid --options
 [cmd]
  ERROR: status=ERR "<errstr>"
 [!cmd] ERR
```

Line Identifier
INVALID .....Command parameter(s) invalid
ERROR .....Critical error. Command did not complete.

Enumerated types
<errstr>.....Text string describing the error.

12.3.13 ipconfig

Description
The ipconfig command allows for configuration of an IP interface. By default, changes take effect on the next bootup.

Syntax
ipconfig [**-h** | **--help** | **--version**]
ipconfig [**-e** device] **-V**
ipconfig [**-e** device] **-D** [**-F**]
ipconfig [**-e** device] [**-i** address] [**-n** netmask] [**-g** gateway] [**-F**]
ipconfig [**-e** device] **-D6** [**-F**]
ipconfig [**-e** device] [**-i6** address] [**-g6** gateway] [**-F**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-e, **--eth** <str>.....Ethernet device: eth0, eth1....eth[n] Default is 'all' when viewing status (see -V), otherwise eth0.
-i, **--ip** <str>.....Assign static IPv4 address.
-n, **--net** <str>.....Assign static IPv4 netmask. Use '.' to clear.
-g, **--gate** <str>.....Assign static IPv4 gateway address. Use '.' to clear.
-D, **--dhcp**.....Use DHCP with IPv4 addressing.
-i6, **--ip6** <str>.....Assign static IPv6 address. Use '.' to clear.
-D6, **--dhcp6**.....Use DHCP with IPv4 and IPv6 Addressing.
-A6, **--slaac**.....Use StateLess Address AutoConfiguration method for IPv6.
-O,--onboot .....Configure interface to come up on boot

NOTE
This will cause termination of active connections.

-F, **--force**.....Force reconfiguration without reboot.
-V, **--view**.....View interface status and IPv4 configuration settings. Default action when other options absent.
-V6, **--view6**.....View interface status and IPv6 configuration settings.
-M, **--mac**.....View MAC addresses.
-S.....Like -V, but status only.
-S6.....Like -V6, but status only.

Example: Status/config display

```
cw_dts> ipconfig -V
 [ipconfig]
  STS_ETH_0: link=<lnk> ip=<ip> nm=<ip> gw=<ip> status=<sts>
  STS_ETH_1: link=<lnk> ip=<ip> nm=<ip> gw=<ip> status=<sts>
  CFG_ETH_0: prot=<prot> ip=<ip> nm=<ip> gw=<ip> status=<sts>
  CFG_ETH_1: prot=<prot> ip=<ip> nm=<ip> gw=<ip> status=<sts>
 [!ipconfig] <summary>
```

NOTE
Command 'ipconfig -S' reports only the STS_ETH_# lines as above.

Line Identifier
STS_ETH_#:.....Current status for Ethernet device eth#.
CFG_ETH_#:.....Configuration settings for Ethernet device eth#.

Fields
link=<lnk>.....Link speed / link down indicator
ip=<ipv4>.....IPv4 address
nm=<ipv4>.....IPv4 subnet mask (netmask)
gw=<ipv4>.....IPv4 gateway address
ip6=<ipv6>.....IPv6 address
gw6=<ipv6>.....IPv6 gateway address
prot=<prot>.....Identifies protocol/method of assigning IP parameters.
status=<sts>.....Summary status for the given line.

Enumerated types

<lnk> ..... Link speed (10, 100, 1000, down)
<ipv4> ..... IPv4 dotted-decimal address (Ex: 10.19.6.6), netmask (Ex: 255.255.255.0), gateway (Ex: 10.19.0.0), or 'NA' for "Not available"
<ipv6> ..... IPv6 colon-hexadecimal address (Ex: fd01::1) or 'NA' for "Not available"
<prot> ..... "dhcp" for DHCP assignment (ip, nm, gw fields absent) "static" for static assignment (ip, nm, gw fields follow)
<sts> ..... Status message (OK, ERR "<str>")
<str> ..... Text string
<summary> ..... Command status summary (OK, ERR)

Example: MAC display

```
cw_dts> ipconfig -M
 [ipconfig]
  MAC_ETH_0: mac=<mac> link=<lnk> status=<sts>
  MAC_ETH_1: mac=<mac> link=<lnk> status=OK
 [!ipconfig] <summary>
```

Line Identifier

MAC_ETH_# ..... MAC address / current status for Ethernet device eth#.

Fields

mac=<mac> ..... Interface MAC address
link=<lnk> ..... Link speed / link down indicator
status=<sts> ..... Summary status for the given line.

Enumerated types (See above examples in fields)

<mac> ..... MAC address (Ex format: 00:11:22:33:44:55)
<summary> ..... Command status summary (OK, ERR)

Example: Set static IPv4 and netmask on interface eth1

```
cw_dts> ipconfig -e eth1 -i 192.168.1.5 -n 255.255.255.0
 [ipconfig]
  IP: status=<sts>
 [!ipconfig] <summary>
```

Example: Set static IPv6 on interface eth0

```
cw_dts> ipconfig -e eth0 -i6 fd01::1/64
 [ipconfig]
  IP: status=<sts>
 [!ipconfig] <summary>
```

Example: Set DHCP config / force reconfiguration on interface eth1

```
cw_dts> ipconfig -e eth1 -D -F
 [ipconfig]
  IP: status=<sts>
 [!ipconfig] <summary>
```

Example: Configure (enable) boot configuration of eth1

```
cw_dts> ipconfig -e eth1 -O yes
 [ipconfig]
  IP: status=<sts>
 [!ipconfig] <summary>
```

Line Identifier

IP ..... Configuration status line

Fields

status=<sts> ..... Summary status for the given line.

12.3.14 istarget

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The istarget command starts, stops, and reports the status of the iSCSI target server.

Syntax
istarget [**-h** | **--help** | **--version**]
istarget [**--start** | **--stop** | **--status** | **--setTargetName** <rmc idx> <part idx> <iqn name>]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, --slot <slotnum>.....Specify RMC slot to use. 0,1,2 or 'all' for all slots
--start.....Start iSCSI Target service.
--stop.....Stop iSCSI Target service.
--status.....Status of iSCSI Target service (default).
--setTargetName <rmc idx> <part idx> <iqn name>: Set iSCSI qualified name (iqn)
<rmc idx>.....rmc index 0,1, 2 ,etc
<part idx>.....part index 1,2,etc 0 for whole disk
<iqn name>.....iSCSI Qualified Name (IQN)
--getTargetNames.....Get iSCSI iqn target names
--clrTargetNames.....Clear saved iSCSI iqn target names
--blk <blksize>.....Sets blocksize. Only 512, 1024, 2048, and 4096 blocks are supported. The default blocksize is 4096
--ro.....Start iSCSI Targets as read only.

The IQN format takes the form 'iqn.yyyy-mm.naming-authority:unique name', where:

- 'yyyy-mm' is the year and month when the naming authority was established. 'naming-authority' is usually reverse syntax of the Internet domain name of the naming authority.
- 'unique name' is any name you want to use, for example, the name of your host.
- The information following the colon must be unique, such as:
  - iqn.2015-05.net.cwnas.iscsi:1
  - iqn.2015-05.net.cwnas.iscsi:2

Responses
ISCSI#.....<idevY> [is_tgt_en] <status>
idevY.....ISCSI target device iqn.2015-05.net.cwnas.iscsi:Y (Y=ISCSI target disk 0,1, or 2)
[is_tgt_en].....iSCSI Target Enabled <bool> (0,1)
<status>.....Status <enum> (OK, ERR "<str>")
INVALID.....<status>
INVALID.....Command parameter(s) invalid
<status>.....Status <str> (ERR "<str>")
ERROR.....<status>
ERROR.....Critical error has occurred
<status>.....Status <str> (ERR "<str>")

Example: Determine the iSCSI target status

```
cw_dts> istarget
  [istarget]
   RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=1 status=OK
   RMC_S0_P2_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p2 is_tgt_en=1 status=OK
  [!istarget] OK
```

NOTE
See **`rmcctl --serv`** command for information on controlling Ethernet interfaces targets will be available on.

Example: Start all the iSCSI targets on the RMC in slot 0.

```
cw_dts> istarget --start -s 0
 [istarget]
  RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=1 status=OK
  RMC_S0_P2_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p2 is_tgt_en=1 status=OK
 [!istarget] OK
```

Example: Stop all the iSCSI targets on the RMC in slot 0.

```
cw_dts> istarget --stop -s 0
 [istarget]
  RMC_S0_P1_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p1 is_tgt_en=0 status=OK
  RMC_S0_P2_L0: iqn.2015-05.net.cwnas.iscsi:rmc0p2 is_tgt_en=0 status=OK
 [!istarget] OK
```

12.3.15 ledctrl

Description
The ledctrl command allows the user to set the duty cycle (brightness) of the DTS LEDs. When the duty cycle option is not provided, current duty cycle and on/off state of LEDs is reported. LED 0 is the POWER LED, other LEDs are reserved.

Syntax
`ledctrl` [**`-h`** | **`--help`** | **`--versio`**n]
`ledctrl` [**`-l`** ledNum] [**`-d`** dutyCycle]

Options
`-h`, **`--help`**.....Print help message.
`--version`.....Print program version.
`-d`, **`--duty`** <num>.....Set LED duty cycle (0 - 100%). Duty cycle of 0 will prevent the LED from lighting.
`-l`, **`--led`** <str>.....LED number ('A' for all LEDS: 0,1,2,3,4,5,6,7)

Example: Status display

```
cw_dts> ledctrl
 [ledctrl]
  LED: s0=<s> d0=<d> s1=<s> d1=<d> s2=<s> d2=<d> s3=<s> d3=<d> s4=<s> d4=<d> s5=<s>
  d5=<d> status=<sts>
 [!ledctrl] <summary>
```

NOTE
Line wrap above simulated for viewability

Line Identifier
LED .....LED status line

Fields
`s#=<s>` .....State of LED number #
`d#=<d>` .....Duty cycle setting of LED number #
`status=<sts>` .....Summary status for the line

Enumerated types (See above examples in fields)
<s> .....State of LED. Integer: 0 for off, 1 for on.
<d> .....Duty cycle. Integer: 0 to 100
<sts> .....Status message (OK, ERR <str>)
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

Example: Set duty cycle of all LEDs to 75%

```
cw_dts> ledctrl -l A -d 75
 [ledctrl]
  LED: status=<sts>
 [!ledctrl] <summary>
```

12.3.16 log

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The log command provides access to the DTS log files. Without options, a list of log files is printed. Without a filename, will list log files that are available for viewing. With filename, will display text of the log file. By default, only the last 100 are shown, but viewing mode can be modified with options.

Syntax
`log` [**`-h`** | **`--help`** | **`--version`**]
`log` [**`-m`** MODE] FILENAME

Options
`-h`, **`--help`** ..... Print help message.
`--version` ..... Print program version. List log files.
`-M` ..... Paged using 'more' utility. 'q' to quit.
`-L` ..... Paged using 'less' utility. 'q' to quit.
`-A` ..... All. Unpaged full text dump.
`-F` ..... Follow output with 'tail -f'. Ctrl-C to quit.
`--export` ..... Export log files to an RMC selected by -s.
`--archive` ..... Like --export, but package files in a .tar.gz file.
`-s` ..... Selects RMC used by --export or --archive.

Example: View list of log files

```
cw_dts> log
 [log]
 <filename>
  <filename>
 [!log] <summary>
```

Enumerated types
<filename> ..... Name of a log file
<summary> ..... Command status summary (OK, ERR)

Example: View log file pbit.log using paged viewer

```
cw_dts> log -M pbit.log
<file contents>
```

NOTE
Output of viewer(s) not formalized.

Example: Export an archive of log files to RMC

```
cw_dts> log --archive -s 1
 [log]
  LOG: status=<sts>
 [!log] <summary>
```

Line Identifier
LOG: Log export status line

Fields
`status=<sts>` ..... Summary status for the line

Enumerated types
<sts> ..... Status message (OK, ERR "<str>")
<str> ..... Text string
<summary> ..... Command status summary (OK, ERR)

12.3.17 mbit

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The mbit command executes maintenance built-in tests.

Syntax
mbit [**-h** | **--help** | **--version**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, **--slot**.....Slot number where the RMC unit is located. Operations on all slots is prohibited.
-p, **--pnum**.....Partition number. Ranges from 1-128. Operations on all partitions is prohibited.
--go.....Required for destructive/disruptive tests.

CAUTION
DATA LOSS. Use of --disk option will destroy data on the disk

--disk .....Run disk test on RMC in slot <slotNum> or on partition <partnum>.
--smart.....View SMART stats for RMC in slot <slotNum>.
--eth DEVICE .....Run Ethernet self-tests on DEVICE. DEVICE is one of: eth0, eth1. The interface will be taken offline for this test. Do not perform test on the interface used for the CLI.

CAUTION
DATA LOSS. Use of --fsck option may destroy data on the disk

--fsck .....Run file system check on RMC in slot <slotNum> or on partition <partnum> on RMC <slotNum>. All --fsck* options will unmount the RMC/partition.
--fsckro.....Read-only version of --fsck.

CAUTION
DATA LOSS. Use of --fsckauto option may destroy data on the disk

--fsckauto.....Auto-repair version of --fsck. Fixes simple problems without intervention.

CAUTION
DATA LOSS. Use of --fsckyes option may destroy data on the disk

--fsckyes.....Auto-repair version of --fsck, assuming 'yes' to all repair prompts.

NOTE
Output of this command is not formalized. For interactive use.

Example: Full disk test output data

```
cw_dts> mbit --disk -s 0 --go
   [mbit]
   ====== File is a block device
   ====== File corresponds to whole disk
   dT=14 p=0 Tx=700 Rx=645 tM=141.86 rM=87.49 M=110.24 Ex2=0 Ex=0 LgB=-98.87
  [!mbit] OK
```

Example: Disk partition test output data

```
cw_dts> mbit --disk -s 0 -p 1 --go
  [mbit]
   ====== File is a block device
   ====== File corresponds to partition 1 on disk 2
   dT=14 p=0 Tx=700 Rx=645 tM=141.86 rM=87.49 M=110.24 Ex2=0 Ex=0 LgB=-98.87
  [!mbit] OK
```

Fields

dT	Elapsed time in seconds
p	Pass count. Number of times the full disk has been verified.
Tx	Count of transmitted (written) buffers
Rx	Count of received (read) buffers
tM	Cumulative Tx throughput (timed during write phase only)
rM	Cumulative Rx throughput (timed during read/verify phase only)
M	Cumulative total throughput (read/write combined)
Ex2	Errors other than data errors
Ex	Data verification errors
LgB	ROUGH representation of the byte error rate exponent

Example: Disk file system check on RMC 0

```
cw_dts> mbit --fsckro -s 0 --go
 [mbit]
  e2fsck 1.42.9 (28-Dec-2013) /dev/rmc0: clean, 11/30531584 files, 1967964/
  122094592 blocks
 S!mbit] OK
```

Example: Disk file system check on RMC 0 partition 1

```
cw_dts> mbit --fsckro -s 0 -p 1 --go
 [mbit]
  e2fsck 1.42.9 (28-Dec-2013) /dev/rmc0p1: clean, 11/30531584 files, 1967964/
  122094592 blocks
 [!mbit] OK
```

12.3.18 nfsctl

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description:
The nfsctl command is used to determine the configuration of the NFS exports for both the static / etc/exports file, and the flags for the exportfs command used to dynamically create NFS exports. Those exports are created in two cases. The first is when the NFS server is running, and an RMC/ partition is mounted. The second is when an RMC/partition is already mounted, and the NFS server is started,

The default /etc/exports file is:

`/rmc_shares *(rw, fsid=0,sync, no_root_squash, no_all_squash)`

This is meant to export the top level directory at /rmc_shares. RMCs/partitions will be created underneath this top level directory, with these default options:

`rw,fsid=0,sync,no_root_squash,no_all_squash`

The default options used for the exportfs command are:

`rw, async, wdelay, root_squash, all_squash,no_subtree_check, anonuid=1000, anongid=1000`

This is meant to export the RMC/partitions so they belong the user on the DTS1 and the files can be seen can be seen from other services, such as HTTP, FTP, CIFS, etc. that user has access too. Other configurations may be more appropriate, depending on the users intent for the DTS1.

CAUTION
INCORRECT OPERATION. Be careful to provide a correctly formed string for <nfsString>. No error checking is done on it.

NOTE
If an RMC/partition is mounted read only, the corresponding export will also be read only, regardless of the options set here.

NOTE
The NFS server needs to be restarted for a new /etc/exports file to take effect.

Syntax:
nfsctl [-h | --help | --version]
nfsctl [--exports] <phr>
nfsctl [--exportfs] <phr>

Options:
-h, --help.....Print help message.
--version .....Print program version.
--exports, exports <nfsString> .....Use <nfsString> as the options to the/etc/exports file.
--exportfs, exportfs <nfsString>.....Use <nfsString> as the options to the exportfs command.

Example: Status command

```
cw_dts> nfsctl
 [nfsctl]
  exports:"rw,fsid=0,sync,no_root_squash,no_all_squash"
  exportfs:"rw,async,wdelay,root_squash,all_squash,no_subtree_check,anonuid=1000,a
  nongid=1000"
 [!nfsctl] <summary>
```

Example: Turn off root_squash command

```
nfsctl --exportfs "rw,async,wdelay,all_squash,no_subtree_check,anonuid=1000,
anongid=1000"
```

Example: Turn off autmounting on slot 0 completely command

```
nfsctl --exports "rw,async,wdelay,root_squash,no_subtree_check"
```

12.3.19 ntpdate

Description
The ntpdate command allows for configuration and retrieval of the time and date from specified list of ntp servers.

Syntax
ntpdate [**-h** | **--help** | **--version**]
ntpdate [**--ip** <ip>] | [--ip6 <ip>] | **--name** <str>]
ntpdate [**--clear** | **--list**]

Options>
-h, **--help**.....Print help message.
--version.....Print program version.
-s, **--setdate** .....Set the local time and date via NTP
-i, **--ip** <str>.....IPv4 address of ntp server to add to list
-i6, **--ip6** <str>.....IPv6 address of ntp server to add to list
-n, **--name** <str> .....Host name of ntp server to add to list
-c, **--clear**.....Clear stored ntp server values
-l, **--list**.....List stored ntp server values
-p, **--poll** <sec>.....Poll for time from ntp server
-q, **--quitpoll** .....Quit polling for time from ntp server
--status.....Print server list and polling status

Example: Set current time and date via NTP

```
cw_dts> ntpdate --setdate
  [ntpdate]
   SETDATE: date=<date> time=<time> status=<sts>
  [!ntpdate] <summary>
```

Line Identifier
SETDATE.....Reports date/time configuration status

Fields
date=<date> .....Reports system date
time=<time> .....Reports system time
status=<sts> .....Summary status for the given line.

Enumerated types:
<str> .....Text string
<date> .....System date as month day year (Ex: Aug 2 2014)
<time> .....24-hour system time as Hour:Minute:Second (Ex: 23:05:06)
<sts> .....Status message (OK, ERR "<str>")
<summary> .....Command status summary (OK, ERR)

NOTE
See 'help info' for format of parser and critical execution errors.

Example: Store ntp server address

```
cw_dts> ntpdate --ip <ip>
  [ntpdate]
   STORE: status=<sts>
  [!ntpdate] <summary>
```

Line Identifier
STORE..... Reports NTP server list config update status

Fields
<ip>..... IPv4 dotted-decimal address (Ex: 10.19.6.6) to be added to NTP server(s) list

Enumerated types (See above examples in fields)

Example: Store ntp server name

```
cw_dts> ntpdate --name <str>
 [ntpdate]
  STORE: status=<sts>
 [!ntpdate] <summary>
```

Line Identifier
STORE ..... Reports NTP server list config update status

Fields
<str> ..... host name of NTP server to be added to NTP server(s) list

Enumerated types (See above examples in fields)

Example: Clear ntp server list

```
cw_dts> ntpdate --clear
 [ntpdate]
  CLEAR: status=<sts>
 [!ntpdate] <summary>
```

Line Identifier
CLEAR ..... clearing entries from NTP servers list

Enumerated types (See above examples in fields)

Example: List ntp server entries

```
cw_dts> ntpdate --list
 [ntpdate]
  LIST_SERVERS:
  <ip>
  <name>
 [!ntpdate] <summary>
```

Fields
<name> ..... host name of NTP server
<ip> ..... IP address of NTP server

Example: configuration status

```
cw_dts> ntpdate [--status]
 [ntpdate]
  STATUS: <sts>
  servers:
  <name>
  <ip>
  Polling for time every <sec> seconds.
 [!ntpdate] <summary>
```

Line Identifier
STATUS ..... Configuration status

Fields
<name> ..... Host name of NTP server
<ip> ..... IP address of NTP server
<sec> ..... Number of seconds to wait before polling NTP server

Enumerated types (See above examples in fields)

12.3.20 password

Description
The password command allows the admin to change the login password. The optional -u option can be provided to change the password for a different login account.

Syntax
password [**-h** | **--help** | **--version**]
password [**-u** userName] [**-p** userPass]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-u, **--user** <str>.....Username of account (admin, user)
-p, **--pass** <str>.....New password.

Example: Password change

```
cw_dts> password -u admin -p password
  [password]
   PASS: status=<sts>
  [!password] <summary>
```

Line Identifier
PASS.....Password change status line

Fields
status=<sts> .....Summary status for the line

Enumerated types (See above examples in fields)
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

12.3.21 pcap

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The pcap command controls PCAP recording functions.

Syntax
pcap [**-s**] **-i interface --start** filename [**--ov**][**--filter** filters]
pcap --stop [-i interface]
pcap [**-h** | **--help** | **--version**]
pcap --peek -i interface
pcap --stat
pcap

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, --slot <num>.....Slot number for RMC unit to record to, default 0
-p, --pnum <partnum>....Partition number for RMC unit within a given slot number
--peek -i <interface>..Show snippet of traffic from interface.
--start <filename> .....Start PCAP recording into file. Must be accompanied by --ov if file already exists.
--stop [<interface>] ....Stop PCAP recording on select interface if specified or all if not specified.
--stat .....Get PCAP recorder status. Default action when invoked with no parameters.
-i <interface>.....Name of interface to capture data from ex. eth0, eth1, etc.
--ov.....Overwrite file if file exists.
--filter <filters> .....TCP data filter. Selects which packets will be dumped. If no filter is given all packets on the net will be dumped into the file. Filter parameter follow standard PCAP format. See PCAP-filter for exact syntax.

Example: PCAP recording

```
cw_dts> pcap
 [pcap]
  No PCAP recorder active
 [!pcap]
```

```
cw_dts> pcap -i eth0 -s 0 --start ch0.pcap
 [pcap]
  Start recording on interface eth0 to file /rmc_shares/rmc0/ch0.pcap
  recording started
 [!pcap]
```

```
cw_dts> pcap --stat
 [pcap]
  PCAP recorder active
  Interface eth0: Recorded 24576 Bytes. (24K) to /rmc_shares/rmc0/ch0.pcap
 [!pcap]
```

```
cw_dts> pcap --stop
 [pcap]
  Stopping active PCAP recording.
 [!pcap]
```

12.3.22 reboot

Description
The reboot performs a soft reset of the hardware.

Syntax
`reboot` [**`-h`** | **`--help`** | **`--version`**]

Options
`-h`, **`--help`**.....Print help message.
`--version`.....Print program version.
`--now` .....Require option to avoid accidental reboot.

Example: Rebooting the DTS

```
cw_dts> reboot --now
  [reboot]
    REBOOT: status=<sts>
  [!reboot] <summary>
```

Line Identifier
REBOOT .....Reboot status line

Fields
`status=`<sts> .....Summary status for the line

Enumerated types (See above examples in fields)
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

12.3.23 rmcctl

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The rmcctl command performs control tasks on the RMCs, such as partitioning, formatting, mounting, and requesting removal. When an action is not requested, the current state is reported.

Syntax
rmcctl [**-h** | **--help** | **--version**]
rmcctl [**-s**] [**-p**] [**-M**] [**-U**] [**-F**] [**-C**]

Options
-h, **--help** ..... Print help message.
--version ..... Print program version.
-s, **--slot** ..... slot number where the RMC unit is located(0). For all slots, use "A" or "all".
-p, **--pnum** ..... Partition number. Ranges from 1-128. Some operations on all partitions is prohibited.
-P, **--part** ..... Create 1-n partition(s) on the RMC described with --slot.
<num parts> Number of partitions on the disk.
<part sizes> Size of partitions can be specified as percent of disk or sizes in MiB, MB, GiB, GB, TiB or TB. The minimum size allowed is 100MB. NAS services, iSCSI targets, and PCAP recordings need to be inactive, and the RMC / partitions need to be unmounted to run this command.
--force ..... Necessary due to the destructive nature of --part. All services, iSCSI targets, and PCAP recordings need to be inactive, and the RMC / partitions need to be unmounted to run this command.
-W, **--wipe** ..... Destructively clean the disk and any partitions.
--force ..... Necessary due to the destructive nature of --wipe. All services, iSCSI targets, and PCAP recordings need to be inactive, and the RMC/partitions need to be unmounted to run this command.
-C, **--cryp** ..... Software encrypt RMC. Passphrase is entered interactively
-D, **--dcryp** ..... Destructively overwrite S/W encryption information.
-E, **--enter** ..... Gain entry to S/W encrypted RMC. Passphrase is entered interactively.
-X, **--exit** ..... Exit from S/W encrypted RMC.
-F, **--format** ..... Format RMC/partition. May take several minutes.
--force ..... Force reformatting of a formatted RMC / partition.
--fs ..... Choose either EXT4 (default) or NTFS. NTFS can only be used with partitions and RMC USB adapter to provide compatibility with Windows. This option can only be used with the -F option.
-M, **--mount** ..... Mount RMC/partition.
--ro ..... Mount file system. This option can only be used with the -M option.
-U, **--unmount** ..... Unmount RMC/partition.
-S, **--scan** ..... Scan for undetected RMCs.

CAUTION
EQUIPMENT DAMAGE. The RMC is hot-swappable (remove / install with power applied), however, extreme caution must be used to ensure all ESD handling precautions are followed. Failure to properly handle the RMC will result in equipment damage.

-R, **--remove** ..... Request RMC removal.
-I, **--insert** ..... Undo request for removal (-R).
--status ..... Display current state of RMCs.

--serv ..... Assign a service name to partition. Valid names are NONE, NAS, iSCSI, and iSCSI0/1.

NOTE
Each partition in the system needs to have a unique (mntpoint) <name>.

--mntpoint..... Assign a mount point <name> to a partition. Limited to 32 characters, and may wrap or truncate depending on CLI terminal type.

Example: Status display (multi-partition)

```
cw_dts> rmcctl
 [rmcctl]
  RMC_S#: ins hcryp osdr p#  size  serv   scryp osdm fmt mnt rem mntpoint
  ************************************************************************
  RMC_S0:  1    1    1   1  16.0GB NONE     0     na  0   na  0   rmc0p1
  RMC_S0:  1    1    1   2  16.0GB NONE     0     na  0   na  0   rmc0p2
  RMC_S0:  1    1    1   3  16.0GB NONE     0     na  0   na  0   rmc0p3
  RMC_S0:  1    1    1   4  6.40GB NONE     0     na  0   na  0   rmc0p4
 [!rmcctl] <summary>
```

Example: Status display (no partitioning))

```
cw_dts> rmcctl
 [rmcctl]
 RMC_S#: ins hcryp osdr p#  size  serv   scryp osdm fmt mnt rem mntpoint
  ************************************************************************
  RMC_S0:  1    1    1  --  64.0GB -----    0    na  1   1   0   rmc0
 [!rmcctl] <summary>
```

Line Identifier
RMC_S#:.....Current status of RMC in slot "#"

Fields /Columns
ins.....Reports insertion status of RMC (default). 0 = not inserted, 1 = inserted
hcryp .....Reports H/W encryption status 0 = not ready, 1 = ready, na = not detected
osdr.....Reports raw block device detection status 0 = Raw device not detected, 1 = detected
p#.....Partition number
size.....Size of partition
serv.....Service type
scryp .....Reports S/W encryption mode0 = not encrypted, 1 = encrypted
osdm.....Reports mapped block device detection status 0 = Mapped device not detected, 1 = detected
fmt.....Reports file system format status 0 = not formatted, ext4 = formatted ext4, ntfs = formatted ntfs
mnt.....Reports file system mount status 0 = not mounted, 1 = mounted, ro = mounted read only
rem.....Reports removal request status 0 = not requested, RQ = requested, OK = ready for removal

Enumerated types:
<summary> .....Command status summary (OK, ERR)

Example: Create 2 partitions of size 100Gib and 900Gib.

```
rmcctl --part 2 100Gib 900Gib --force
```

Example: Create 3 partitions, using disk percentages: 35, 35, and 20.

```
rmcctl -P 3 35% 35% 20% --force
```

Example: Format partition 1 of the RMC.

```
rmcctl -p 1 -F
```

NOTE
RMC / partition must be formatted before mounting.

Example: Mount partition 1 of the RMC0.

```
rmcctl -p 1 -M
```

Example: Unmount RMC/partition 1 of the RMC in slot 0.

```
rmcctl -s 0 -U
rmcctl -s 0 -p 1 -U
```

Example: Software encrypt RMC in slot 0.

```
rmcctl -s 0 -C
```

Example: Access S/W encrypted RMC in slot 0.

```
rmcctl -s 0 -E
```

Example: Exit from S/W encrypted RMC mode in slot 0.

```
rmcctl -s 0 -X
```

Example: Destructively overwrite S/W encryption info on RMC in slot 0.

```
rmcctl -s 0 -D
```

Example: Associate RMC slot 0 partition 1 with general NAS use.

```
mcctl -s 0 -p 1 --serv NAS
```

Example: Associate RMC slot 0 partition 1 with an iSCSI target available on all the Ethernet interfaces.

```
rmcctl -s 0 -p 1 --serv iSCSI
```

Example: Associate RMC slot 0 partition 1 with an iSCSI target available only on Ethernet interface eth0.

```
rmcctl -s 0 -p 1 --serv iSCSI0
```

Example: Name the mount point for RMC 0 partition 1 "/rmc_shares/lancer".

```
rmcctl -s 0 -p 1 --mntpoint lancer
```

Example: Perform wipe operation on RMC in slot 0.

```
rmcctl -s 0 --wipe --force
```

12.3.24 rmcfree

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

NOTE
The rmcfree information displayed in the CLI help is incorrect. It will be updated in the next DTS software release.

Description
The rmcfree command displays RMC storage status and usage.

Syntax
rmcfree [**-h** | **--help** | **--version**]
rmcfree [**-s**]

Options
-h, **--help**..... Print help message.
--version..... Print program version.
-s, **--slot**..... Slot number of an RMC (0, A, all). Default is 'A' for all slots.
-p, **--pnum**..... Partition number (1-128, A, all). Default is 'A' for all partitions.

Example: Status display

```
cw_dts> rmcfree
 [rmcfree]
  RMC_F#:      det   p#    fmt   mnt   size  used  free  used
  ************************************************************************
  RMC_F0:       1     1    ext4   1    252G  63M   252G    1
 [!rmcfree] <summary>
```

Line Identifier
RMC_F#:..... Current disk utilization status of RMC in slot "#"

Fields
det=<d> ..... Reports if RMC is detected
p=<#>..... Number of partitions
fmt=<f> ..... File system format
mnt=<d> ..... Reports if RMC is mounted
size=<sz>..... Size of RMC
used=<sz>..... Amount of file system used
free=<sz>..... Amount of file system available
used=<p> ..... Percentage

Enumerated types:
<#> ..... Integer showing numerical value
<d> ..... Status. 0 = not detected / not mounted, 1 = detected / mounted
<f> ..... File system type (ext4, NA)
<p> ..... Percentage used. Integer from 0 to 100, or "na".
<summary> ..... Command status summary (OK, ERR)
<sz> ..... Disk space with unit indicators as powers of 1000. (G - Gigabytes, M - Megabytes, K - Kilobytes). Examples: 46G, 180M. Also, "NA" for not available

Example: Display storage status and usage of RMC in slot 0 .

```
rmcfree -s 0
```

Example: Display RMC storage status and usage of partition 1 of the RMC in slot 0..

```
rmcfree -s 0 -p 1
```

12.3.25 rmcinfo

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The rmcinfo command displays RMC identification and manufacturing data.

Syntax
rmcinfo [**-h** | **--help** | **--version**]
rmcinfo [**-s**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, **--slot**.....Slot number of the target RMC. For all slots, use "A" or "all" (default).
-F.....Force retrieval of info data from RMC. By default, will display from a cached copy.
-n, **--name STRING**.....Set the volume name to STRING.

Example: Information display (RMC installed)

```
cw_dts> rmcinfo -s 0
 [rmcinfo]
 RMC_I0:
  Manufacturer: Curtiss-Wright Controls
  Cage Code: 1P423
  RMC Assembly P/N: <str>
  RMC Assembly S/N: <str>
  RMC Assembly Rev: <str>
  Assembly Date: <str>
  Drive Vendor Name: <str>
  Drive Vendor P/N: <str>
  Drive Vendor S/N: <str>
  Drive Capacity: <str>
  Drive Media Type: <str>
  Volume Name: <str>
 [!rmcinfo] <summary>
```

Enumerated types:
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

Example: Information display (RMC not installed)

```
cw_dts> rmcinfo -s 2
 [rmcinfo]
  RMC_I2:
  RMC not installed
 [!rmcinfo] OK
```

Example: Set volume name

```
cw_dts> rmcinfo -s 0 -n "Mission Data"
 [rmcinfo]
  RMC_I0: action=setname status=<sts>
 [!rmcinfo] <summary>
```

Line Identifier
RMC_I#..... Reports status of request for RMC in slot "#"

Fields
status=<sts> .....Summary status for the given line.

Enumerated types:

<sts> ..... Status message (OK, ERR "<str>")
<str> ..... Text string
<summary> ..... Command status summary (OK, ERR)

12.3.26 rmcpurge

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The rmcpurge command allows the user to purge all data on a selected RMC by issuing an ATA Security Erase or ATA Security Enhanced Erase command to the selected storage device.

Syntax
rmcpurge [**-h** | **--help** | **--version**]
rmcpurge [**-s**] [**-E** | **-N**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-s, --slot.....Slot number of the target RMC (0, A,all). For all slots, use "A" or "all" (default).
-N, **--normal**.....Issue ATA Security Erase Command.
-E, **--enhanced**.....Issue ATA Security Enhanced Erase Command.

Example: Enhanced erase of RMC

```
cw_dts> rmcpurge -s A -E
 [rmcpurge]
  RMC_P0: status=<sts>
  RMC_P1: status=<sts>
  RMC_P2: status=<sts>
 [!rmcpurge] <summary>
```

Line Identifier
RMC_P#.....Reports status of purge request for RMC in slot "#"

Fields
status=<sts> .....Summary status for the given line.

Enumerated types
<sts> .....Status message (OK, NA, ERR "<str>")
<str> .....Text string
<summary> ..... Command status summary (OK, ERR)

Example: Normal erase of RMC in slot 1

```
cw_dts> rmcpurge -s 1 -N
 [rmcpurge]
  RMC_P1: status=<sts>
 [!rmcpurge] <summary>
```

12.3.27 rtp

Description

The rtp command provides controls for starting, stopping and reporting status of RTP video stream recordings. Supports recording of RTP video streams with H.264 encoding and MPEGTS formatting.

Syntax

```
rtp [-h | --help | --version]
rtp --start [-s <slot>][-p <part>][-m <dir>][-i <ip>][-P <port>]
    [-S <sdp>] -f <file> [--ov] [-t <sec>]
rtp --stop [-i <ip>][-P <port>][-c <str>][-f <str>]
rtp --stat
```

Options

-h, --help.....Print help message.
--version.....Print program version.
-s, --slot <num>.....Slot number for RMC unit to record to, default 0.
-p, --pnum <partnum>....Partition number to indicate RMC partition to record to, default 1.
-m, --mntpt <dirname>..Alternate mount point where the recording file is to be stored.
-f, --filename <str>....String indicating the filename to record to.
--ov.....Overwrite file if file exists.
-i, --ip <str>.....IPv4 address of network interface to listen on.
-i6, --ip6 <str>.....IPv6 address of network interface to listen on.
-P, --port <str>.....Interface port to listen on.
-S, --sdp <str>.....String indicating the RTP Session Description Protocol filename.
-t, --segtime <num>.....Time in seconds to record to the filename before creating a new file. Each file will be appended with an integer indicating the index of the file.
--start .....Start RTP recording into file. Must be accompanied by --ov if file already exists.
--stop .....Stop RTP recording on select interface or filename if specified or all if not specified.
--stat.....Get RTP recording status. Default action when invoked with no parameters.

Example: Start video stream capture with IPv4 address and port

```
cw_dts> rtp --start -i 192.168.1.1 -P 1234 -f videoFile
 [rtp]
  RTP: action=start status=OK
 [!rtp] OK
```

Example: Start video stream capture with IPv6 address and port

```
cw_dts> rtp --start -i6 fd01::1 -P 5004 -f videoFile
 [rtp]
  RTP: action=start status=OK
 [!rtp] OK
```

Example: Start video stream capture using sdp file

```
cw_dts> rtp --start -S rtpChan1.sdp -f videoFile
 [rtp]
  RTP: action=start status=OK
 [!rtp] OK
```

Example: Stop specified video using start parameters

```
cw_dts> rtp --stop -i6 fd01::1 -P 5004 -f videoFile
 [rtp]
  RTP: action=stop status=OK
 [!rtp] OK
```

Example: Stop all video stream capture processes

```
cw_dts> rtp --stop
  [rtp]
   RTP: action=stop status=OK
  [!rtp] OK
```

Example: Status example

```
cw_dts> rtp --stat
  [rtp]
   RTP: action=stat instances=2 status=OK
   RTP_1: ip=fd01::1 port=1234 filename=videoFile1 state=started
   RTP_2: ip=fd01::1 port=5004 filename=videoFile2 state=capturing
  [!rtp] OK
```

12.3.28 sens

Description
The sens command displays DTS voltage and temperature sensor readings.

Syntax
sens [**-h** | **--help** | **--version**]
sens [**-S**] [**-T**] [**-V**] [**-p PERIOD**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-p PERIOD.....Refresh display every PERIOD milliseconds. Ctrl-C to exit.
-S.....View Advantech subset of sensors only
-T.....View Temperature subset of sensors only
-V.....View Voltage subset of sensors only

12.3.29 serv

NOTE
The DTS1 has only 1 RMC slot. As a result, the -s option is always -s 0.

Description
The serv command allows the user to set the boot configuration for DTS services and to manually start/stop services. When no options are given, the current boot configuration and active status is displayed for all the services.

Syntax
serv [**-h** | **--help** | **--version**]
serv [**-a**] [**-n**] [**-w**] [**-h**] [**-f**] [**-d**] [**-t**]
serv **--boot** [**-a**] [**-n**] [**-w**] [**-h**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-B, **--boot**..... Apply the settings to the boot-time configuration.
-a, **--all** **<num>**.....All Services
-c, **--cifs** **<num>** .....CIFS Service
-n, **--nfs** **<num>**.....NFS Service
-f, **--ftp** **<num>**.....FTP Service
-w, **--http** **<num>**.....HTTP Read Service
-d, **--dhcp** **<num>**.....DHCP Service
-t, **--tftp** **<num>**.....TFTP Service
-z, **--tel** **<num>**.....Telnet Service
-s, **--snmp** **<num>**.....SNMP Service

Enumerated type:
<num>.....Selects server state. 0=Disable, 1=Enable, 2=Use boot setting

Example: Status/configuration display

```
cw_dts> serv
 [serv]
  BOOTCFG: cifs=<s> nfs=<s> ftp=<s> http=<s> dhcp=<s> tftp=<s> tel=<s> snmp=<s>
  status=<sts>
  LIVECFG: cifs=<s> nfs=<s> ftp=<s> http=<s> dhcp=<s> tftp=<s> tel=<s> snmp=<s>
  status=<sts>
 [!serv] <summary>
```

Line Identifier
BOOTCFG .....Reports of service states to be applied at boot-up.
LIVECFG.....Reports the current operation state of each service.

Fields
`cifs=`**<s>** .....Common Internet File System service state
`nfs=`**<s>**.....Network File System service state
`ftp=`**<s>**.....File Transfer Protocol service state
`http=`**<s>** .....Hypertext Transfer Protocol service state
`dhcp=`**<s>** .....Dynamic Host Configuration Protocol service state
`tftp=`**<s>** .....Trivial File Transfer Protocol service state
`tel=`**<s>**.....Telnet service state
`snmp=`**<s>** .....Simple Network Management Protocol service state
`status=`**<sts>** .....Summary status for the line

NOTE
The 'status' field appears on the same line as the others. The example output above is line wrapped for clarity.

Enumerated types:

<s> ..... Configuration state. 0=Disabled, 1=Enabled, ERR=Unknown
<sts> ..... Status (OK, NA, ERR "<str>")
<str> ..... Text string
<summary> ..... Command status summary (OK, ERR)

Example: Boot configuration

```
cw_dts> serv --boot --cifs 1 --nfs 0
 [serv]
  BOOTSET: status=<sts>
 [!serv] OK
```

Line Identifier
BOOTSET ..... Indicates boot configuration update performed

Fields
status=<sts> ..... Summary status for the line

Example: Start/stop servers

```
cw_dts> serv --cifs 1 --nfs 0 --ftp 1
 [serv]
  LIVESET: cifs=1 status=OK
  LIVESET: nfs=0 status=OK
  LIVESET: ftp=1 status=ERR "Failed to start server"
 [!serv] ERR
```

Line Identifier
LIVESET ..... Indicates change to operational state of server.

Fields
<serv>=<s> ..... Indicator of which server is being started/stopped
status=<sts> ..... Status for action (OK, ERR "<str>")

12.3.30 shutdown

Description
Shutdown halts the DTS operating system.

Syntax
shutdown [**-h** | **--help** | **--version**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
--now .....Require option to avoid accidental shutdown.

Example: Rebooting the DTS

```
cw_dts> shutdown now
  [shutdown]
   SHUTDOWN: status=<sts>
  [!shutdown] <summary>
```

Line Identifier
SHUTDOWN.....Shutdown status line

Fields
status=<sts> .....Summary status for the line

Enumerated types (See above examples in fields)
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

12.3.31 sysdate

Description
The sysdate command allows for configuration and retrieval of the time and date. When no options are given, the current date is printed.

Syntax
sysdate [**-h** | **--help** | **--version**]
sysdate [**-d**] [**-t**]

Options
-h, **--help**.....Print help message.
--version.....Print program version.
-d, **--date**.....Set date. (Year/Month/Day)
-t, **--time**.....Set time. (Hour:Minute:Second)

Example: View current time and date

```
cw_dts> sysdate
 [sysdate]
  DATE: date=<date> time=<time> status=<sts>
 [!sysdate] <summary>
```

Line Identifier
DATE.....Reports the current date and time

Fields
date=<date> .....Reports system date
time=<time> .....Reports system time
status=<sts> .....Summary status for the given line.

Enumerated types:
<date> .....System date as year/month/day (Ex: 2012/01/07)
<time> .....24-hour system time as Hour:Minute:Second (Ex: 23:05:06)
<sts> .....Status message (OK, ERR "<str>")
<str> .....Text string
<summary> .....Command status summary (OK, ERR)

Example: Set current time and date

```
cw_dts> sysdate -d 2018/04/01 -t 00:00:01
 [sysdate]
  SETDATE: status=<sts>
 [!sysdate] <summary>
```

Line Identifier
SETDATE.....Reports date/time configuration status

Fields
status=<sts> .....Summary status for the given line.

Enumerated types: (See above examples in fields)

Specifications

A.1 Envelope / Mounting Dimensions

A.1.1 RMC Module

NOTE
Dimensions are in inches and (millimeters).

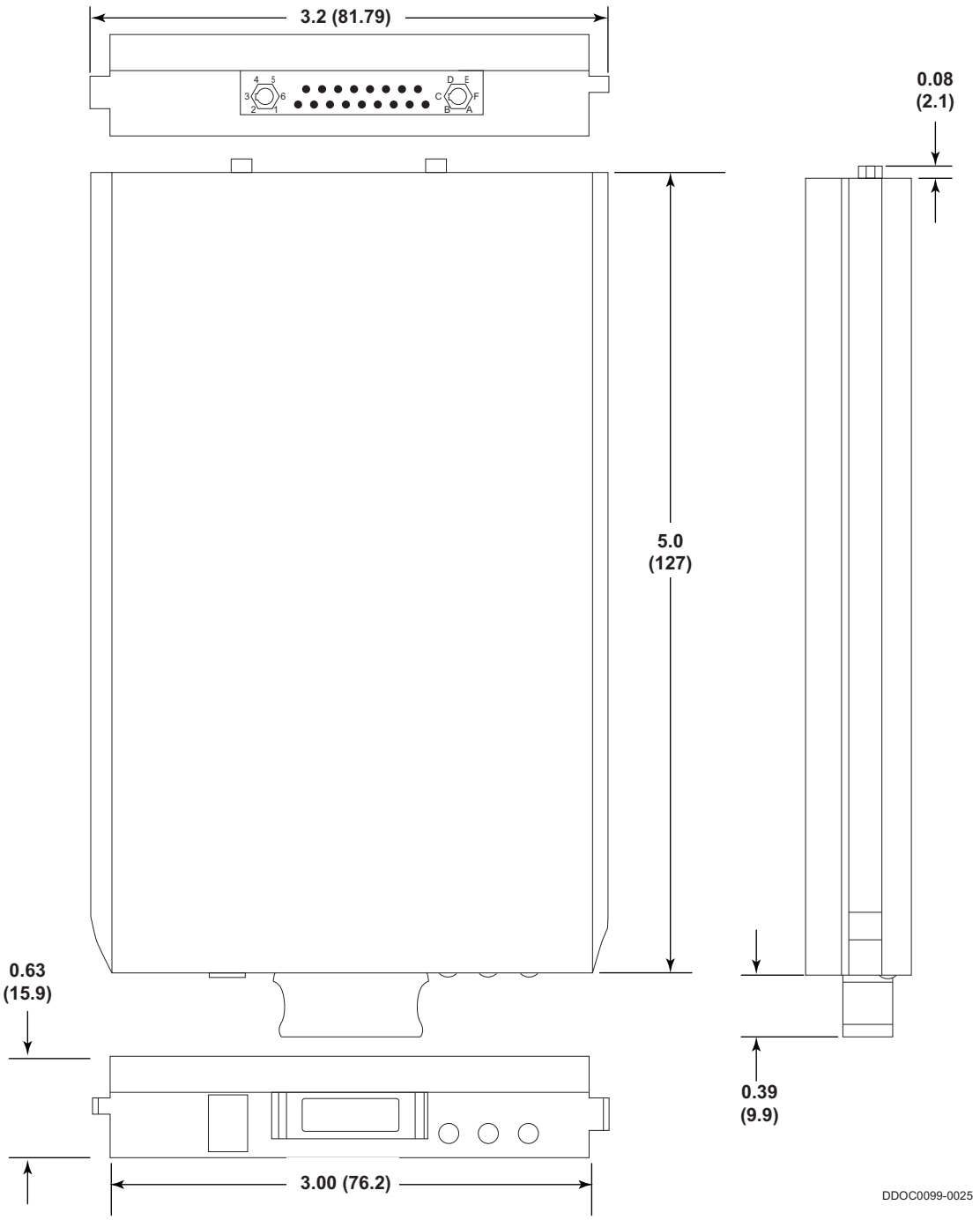

Figure A.1 RMC Module

A.1.2 Panel Mount

NOTE
Dimensions are in inches and (millimeters).

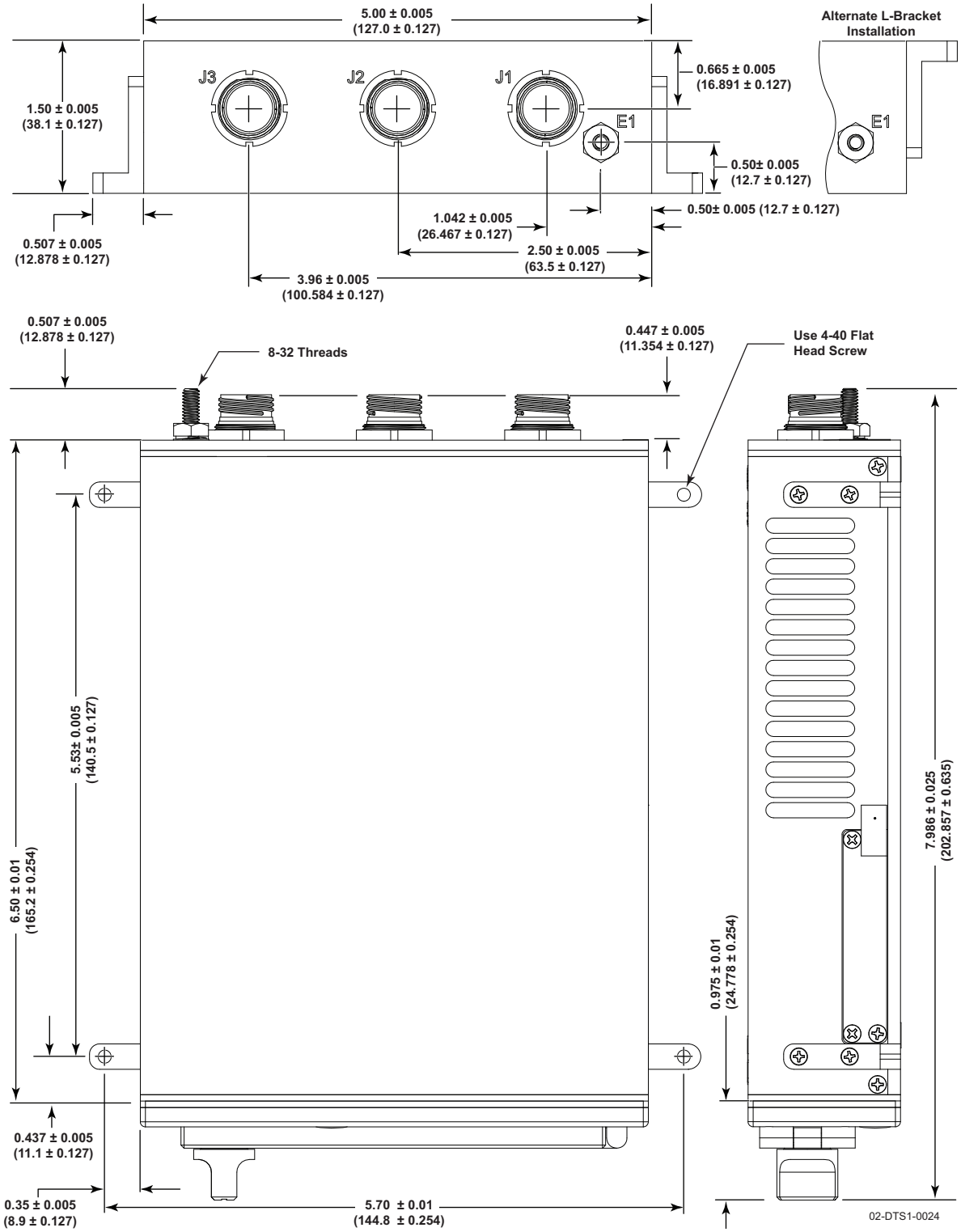

Figure A.2 DTS1 (Panel Mount)

A.1.3 DZUS Fastener Mount

NOTE
Dimensions are in inches and (millimeters).

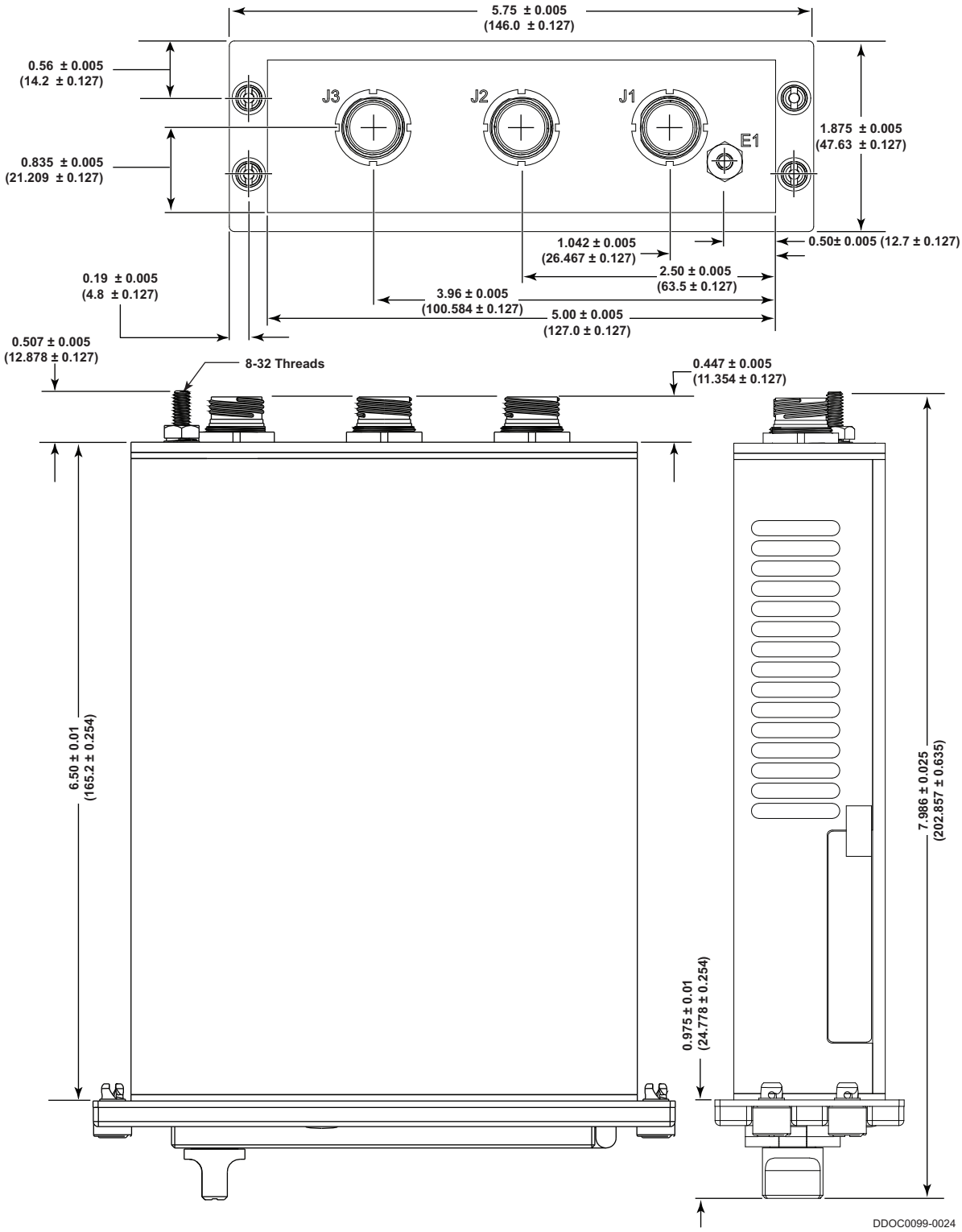

Figure A.3 DTS1 (Dzus Mount)

A.2 DTS1 Specifications

Physical Dimensions

Height ..... 1.50 In. (38.1 mm) chassis
Width ..... 5.00 In. (127.0 mm) chassis
Depth ..... 7.99 In. (202.9mm) knob to GND lug.

Weight:

Without RMC Module ..... 2.60 lb. (1.18 kg)

Power

Input Power ..... 28 VDC (MIL-STD 704E)
Power Dissipation ..... 14 Watts average with RMC
Peak Inrush Current ..... 1.3 Amps

A.3 RMC Module Specifications

RMC Module Physical Dimensions

Height ..... 0.66 In. (16.76 mm)
Width ..... 3.000 + 0.22 In.rails (76.20 mm +5.59 mm rails)
Depth ..... 5.000 + 0.390 In. knob (27.0mm +9.9 mm knob)
Weight ..... 0.7 lb. (0.317kg)

* RMC module weight dependent on configuration. Weight provided is maximum weight for any RMC module configuration.

Reliability

Data Reliability ..... <1 non-recoverable error in 10^{14} bits read
Data Retention ..... >10 years
SSD Endurance ..... >100,000 writes

Capacity

256 GB (unformatted) ..... 235 GB (formatted)
1 TB (Unformatted) ..... 931 GB (formatted)
2 TB (Unformatted) ..... 1.862 TB (formatted)
4 TB (Unformatted) ..... 3,725 TB (formatted)
8 TB (Unformatted) ..... 7,496 TB (formatted)

A.4 Mean Time Between Failures

These Mean Time Between Failure (MTBF) values (provided in hours) are calculated using Windchill Quality Solutions Relex 2011 software with MIL-HDBK- 217 FN2 with parts screening / de-rating based on ANSI/VITA 51.1-2008 specifications.

Table A.1 DTS1 / RMC Calculated Mean Time Between Failures

Order Number	MTBF
VS-DTS1SL-F (L-Bracket Mounting)	
VS-DTS1SL-FD (DZUS Panel Mounting)	
Ground Benign / Controlled @ 30°C	132,906
Ground Mobile @ 30°C	65,687
Naval Sheltered @ 30°C	95,464
Airborne Uninhabited Cargo @ 30°C	55,900
Airborne Uninhabited Fighter @ 30°C	46,984
Airborne Rotary Wing @ 30°C	40,956
VS-RMC8192M-00 (8 TB SSD) and VS-RMC4096M-00 (4 TB SSD)	

Table A.1 DTS1 / RMC Calculated Mean Time Between Failures

Order Number	MTBF
Ground Benign / Controlled @ 30°C	625,644
Ground Mobile @ 30°C	146,503
Naval Sheltered @ 30°C	230,992
Airborne Uninhabited Cargo @ 30°C	98,205
Airborne Uninhabited Fighter @ 30°C	85,131
Airborne Rotary Wing @ 30°C	69,000
VS-RMC2048M-00 (2TB SSD) VS-RMC1024M-00 (1TB SSD)	
Ground Benign / Controlled @ 30°C	698,477
Ground Mobile @ 30°C	166,876
Naval Sheltered @ 30°C	264,999
Airborne Uninhabited Cargo @ 30°C	117,425
Airborne Uninhabited Fighter @ 30°C	99,206
Airborne Rotary Wing @ 30°C	77,966
VS-RMC256M-00 (256GB SSD)	
Ground Benign / Controlled @ 30°C	517,682
Ground Mobile @ 30°C	117,751
Naval Sheltered @ 30°C	183,815
Airborne Uninhabited Cargo @ 30°C	73,986
Airborne Uninhabited Fighter @ 30°C	66,313
Airborne Rotary Wing @ 30°C	56,097
VS-RMC0000-00 (No SSD)	
Ground Benign / Controlled @ 30°C	1,073,322
Ground Mobile @ 30°C	286,330
Naval Sheltered @ 30°C	474,625
Airborne Uninhabited Cargo @ 30°C	284,406
Airborne Uninhabited Fighter @ 30°C	196,851
Airborne Rotary Wing @ 30°C	127,777

A.5 Environmental, EMI, Electrical Specifications

The DTS1 CSfC has been tested to the following environmental conditions using the standards, test procedures, and methods indicated below (test reports are available from Curtiss-Wright on request):

- High Temperature - Storage (Non-operational) per MIL-STD-810G, Method 501.5 Procedure I
  - 7 cycles: from 35C 7% RH to 85C 1% RH within 7 hours, maintain 85C 1% RH for 3 hours, to 35C 7% RH within 7 hours and maintain 35C 7% RH for 7 hours. Total of 7 24 hour cycles.
- High Temperature - Operational per MIL-STD-810G, Method 501.5 Procedure II
  - 3 cycles: +71C for 2 hours, +55C for 3 hours, +35C for 3 hours. Total 24 hours.
- Low Temperature - Storage (Non-operational) per MIL-STD-810G, Method 502.5 Procedure I
  - -45C, maintain for 24 hours following temperature stabilization of the test item, rate of temperature change not exceeding 3C per minute.

- Low Temperature - Operational per MIL-STD-810G, Method 502.5 Procedure II
  - -45C for 4 hours
- Temperature Shock per MIL-STD-810G, Method 503.5 Procedure I, Non-operational
  - -45C to +85C, 3 cycles, less than 5 minute transition time
- Temperature Variation per RTCA/DO-160E, Section 5, Category B, Operational
  - -45C to +55C, 10 cycles, no power cycling, > 5degC/min
- Humidity Tropical Exposure per MIL-STD-810G, Method 507.5, Operational
  - 24 hr baseline, 95% Humidity for 48 hrs, +20 to +55C, 5 cycles
- Altitude per MIL-STD-810G, Method 500.5 Procedure II, Operational
  - 0 ft to 20,000 ft, 5000 feet per minute, no hold time required
- Rapid decompression per MIL-STD-810G, Method 500.5 Procedure III, Operational
  - Ambient temperature, pressure at 8,000 feet (10.9 PSIA) then reduce pressure to 40,000 feet (2.73 PSIA) within (15) fifteen seconds. Hold ambient temperature and pressure at 40,000 feet for a period of (10) ten minutes.
- Vibration - Narrowband Random over Broadband Random per MIL-STD-810G, Method 514.6 Procedure I, Operational
  - Category 13 - Aircraft, Propeller, Installed Material vibration environment, Figure 514.6D-2 and Table 514.6D-II, 1 hour per axis
    - 0 = 68 Hz @ L0 = 0.3 g2/Hz
    - 1 = 136 Hz @ 0.15 g2/Hz
    - 2 = 272 Hz @ 0.075 g2/Hz
    - 3 = 544 Hz @ 0.0375 g2/Hz
- Vibration Endurance Frequency Sweep per DEF STAN 0035, Part 3, Chapter 2-01, Operational
  - 1 hr frequency sweep (Curve N) at 1 octave per minute in 3 directions
- Crash Landing per MIL-STD-810G, Method 513.6 Procedure III, Pre-Test: Operational, Test: Non-operational, Post-Test: Operational
  - 20g in all directions > 10 seconds
- Acceleration per MIL-STD-810G, Method 513.6, Procedure II, Pre-Test: Operational, Test: Non-operational, Post-Test: Operational
  - Linear 3 seconds from 0g to 5g, remain at 5g for 10 seconds, linear fall back to 0 in 3 seconds. 3 directions
- Operational Shock per MIL-STD-810G, Method 516.6, Procedure I
  - 20g peak, 11 ms wide, 3 shocks in each direction per each axis
- Crash Safety per MIL-STD-810G, Method 516.6, Procedure V, Non-operational
  - 40g peak, 11 ms wide, 2 shocks in each direction per each axis
- Bench Handling per MIL-STD-810G, Method 516.6, Procedure VI, Pre-Test: Operational, Test: Non-operational, Post-Test: Operational
- Salt Fog (Mist) per MIL-STD-810G, Method 509.5 Procedure I, Pre-Test: Operational, Test: Non-operational, Post-Test: Operational
- Explosion Proofness per MIL-STD-810G, Method 511.5, Procedure I, Operational
  - 15,000 feet
- EMI/EMC per MIL-STD-461G
  - CE101 - Conducted Emissions, Power Leads, 30 Hz to 10 kHz
  - CE102 - Conducted Emissions, Power Leads, 10 kHz to 10 MHz
  - RE101- Radiated Emissions, Magnetic Field, 30 Hz to 100 kHz
  - RE102 - Radiated Emissions, Electric Fields, 2 MHz to 18 GHz
  - CS101 - Conducted Susceptibility, Power Leads, 30 Hz to 150 kHz
  - CS114 - Conducted Susceptibility, Bulk Cable Injection, 10 kHz to 200 MHz, Curve 5
  - CS115 - Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation

    - CS116 - Conducted Susceptibility, Damped Sinusoid Transients, Cables and Power Leads, 10 kHz to 100 MHz
    - RS101 - Radiated Susceptibility, Magnetic Fields, 30 Hz to 100 kHz
    - RS103 - Radiated Susceptibility, Electric Fields, 2 MHz to 18 GHz, 200 Volts/meter
- Electrical Power per MIL-STD-704F
    - Normal, Aircraft Electrical Operation
        - LDC101 Load Measurements
        - LDC102 Steady State Limits for Voltage
        - LDC103 Voltage Distortion Spectrum
        - LDC104 Total Ripple
        - LDC105 Normal Voltage Transients
    - Transfer, Aircraft Electrical Operation
        - LDC201 Power Interrupt Abnormal, Aircraft Electrical Operation
        - LDC301 Abnormal Steady State Limits for Voltage
        - LDC302 Abnormal Voltage Transients (Overvoltage/Undervoltage)
    - Emergency, Aircraft Electrical Operation
        - LDC401 Emergency Limits for Voltage Starting, Aircraft Electrical Operation
        - LDC501 Starting Voltage Transients
    - Power Failure, Aircraft Electrical Operation
        - LDC601 Power Failure
        - LDC602 Polarity Reversal
- ESD per RTCA/DO-160E, Section 25
    - 10 ESD discharges of +15000V and -15000V at each knob or connector (4 places) Operational

The DTS1 has been designed to meet the following environmental conditions:

- Water Proofness per MIL-STD-810G, Method 506.5, Procedure III
- Mold Growth (Fungus) per MIL-STD-810F, Method 508.5
- Contamination by Fluids per MIL-STD-810F, Method 504.1
- Blowing Dust per MIL-STD-810F, Method 510.5, Procedure I
- Ice Formation per MIL-STD-810G, Method 521.3
- Flammability per RTCA/DO-160E, Section 26, Fire, Category C

Connectors / Cables

The Glenair Series 801 Mighty Mouse Connectors feature double-start ACME threads with anti-decoupling spring or ratchet and provide fast mating requiring only 1-½ turns to fully engage.

B.1 Power Connector J1 / Power Lab Cable

NOTE
The EMI / safety ground on J1 pin 4 is isolated from the +28VDC_RTN line within the DTS1. This isolation should be maintained. All +28VDC power return current must be carried on +28VDC_RTN line and not the EMI / safety ground.

Table B.1 provides DTS1 bulkhead J1 connector pin signals. Figure B.1 show the DTS1 bulkhead J1 connector pinout. Table B.2 shows the DTS1 power lab cable connection pin signals. Figure B.1 show the power lab cable wiring diagram.

Connector ManufacturerGlenair
Connector Reference Designator.J1
Connector.....PN 801-023-07M9-4PA
Mating Connector PN 801-007-16M9-4SA

Table B.1 Power Connector J1 Signals

Connector Pin	Signal Name	Signal Type	Direction	Description / Functions
1	28V DC	Analog	In	Main 28VDC Power Input
2	28 VDC RTN	Analog	Out	Main 28VDC Power RTN
3	Power Disable	Analog	In	DTS1 power off control. Short to +28VDC_RTN to turn off the DTS1
4	EMI GND	Analog		EMI / Safety Ground

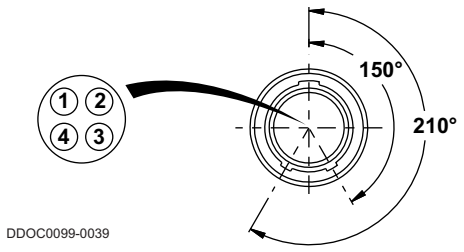

Figure B.1 Power Connector J1

Table B.2 Power Lab Cable (VS-DTS1PWRCAB-0)

Connector Description	Mates With / Signal Name
P1	DTS1 J1
P2 Banana Plug - Red	28 VDC
P3 Banana Plug - Black	28 VDC RTN
P4 Banana Plug - Green	Chassis Ground
J1 3.5mm Audio Jack Tip	28VDC RTN
J1 3.5mm Audio Jack Ring	PWR DISABLE – Short to +28 VDC RTN to power off DTS1

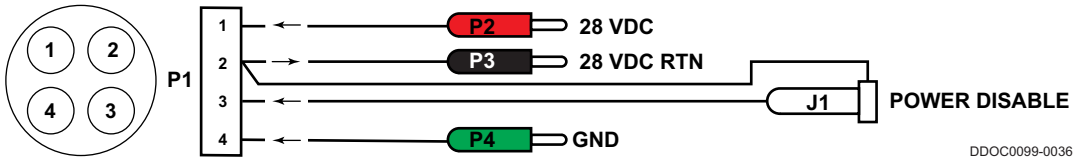

Figure B.2 Power Lab Cable Diagram

B.2 Utility Connector J2 / Utility Lab Cable

Table B.3 provides DTS1 bulkhead J2 connector pin signals. Figure B.3 show the DTS1 bulkhead J2 connector pinout. Table B.4 shows the DTS1 utility lab cable connection pin signals. Figure B.4 show the utility lab cable wiring diagram.

Connector Manufacturer Glenair
Connector Reference DesignatorJ2
Connector.....PN 801-023-07M9-19PA
Mating ConnectorPN 801-007-16M9-19SA

Table B.3 Utility Connector J2 Signals

Connector Pin	Signal Name	Signal Type	Direction	Description / Functions
1	ZEROIZE_N	Analog	In	Active low open collector/switch closure to induce Zeroization of DTS. This signal must be active for a minimum of 5 seconds for the zeroization process to take affect.
2	RST_IN_N	Analog	In	Active low external reset input. Short to GND to invoke DTS reset.
3	GND	Analog		Signal return/GND for ZEROIZE_N and RST_IN_N
4	GND	Analog		NC
5	NASP_RXD	RS-232	In	NAS Processor Serial Port Receive I/F
6	GND	Analog		Signal return/GND for NASP_RXD and NASP_TXD
7	BI_DA1-	GbE	In / Out	Gigabit Ethernet Bi-directional pair A1+/-
8	BI_DD1+	GbE	In / Out	Gigabit Ethernet Bi-directional pair D1+/-
9	GND	Analog		NC
10	NASP_TXD	RS-232	Out	NAS Processor Serial Port Transmit I/F
11	GND	Analog		NC
12	BI_DA1+	GbE	In / Out	Gigabit Ethernet Bi-directional pair A1+/-
13	BI_DD1-	GbE	In / Out	Gigabit Ethernet Bi-directional pair D1+/-
14	GND	Analog		NC
15	GND	Analog		NC
16	BI_DB1-	GbE	In / Out	Gigabit Ethernet Bi-directional pair B1+/-
17	BI_DC1+	GbE	In / Out	Gigabit Ethernet Bi-directional pair C1+/-
18	BI_DC1-	GbE	In / Out	Gigabit Ethernet Bi-directional pair C1+/-
19	BI_DB1+	GbE	In / Out	Gigabit Ethernet Bi-directional pair B1+/-

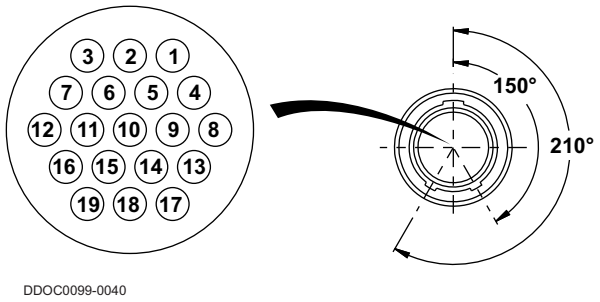

Figure B.3 Utility Connector J2

Table B.4 Utility Lab Cable (VS-DTS1ETHCAB-J2)

Connector Description	Mates With / Signal Name
P1	DTS1 J2
P2 TIA/EIA-568B Modular Plug	Gigabit Ethernet TIA/EIA-568B Modular Jack
J1 D-sub DE-9 Female/Socket	RS-232 Pin 2: DTS1 transmit Pin 3: DTS1 receive Pin 5: GND
J2 3.5mm Audio Jack Tip	ZEROIZE – Short to GND to ZEROIZE Crypto Keys. This signal must be active for a minimum of 5 seconds for the zeroization process to take affect.
J2 3.5mm Audio Jack Ring	RESET – Short to GND to reset DTS1
J2 3.5mm Audio Jack Shield	GND

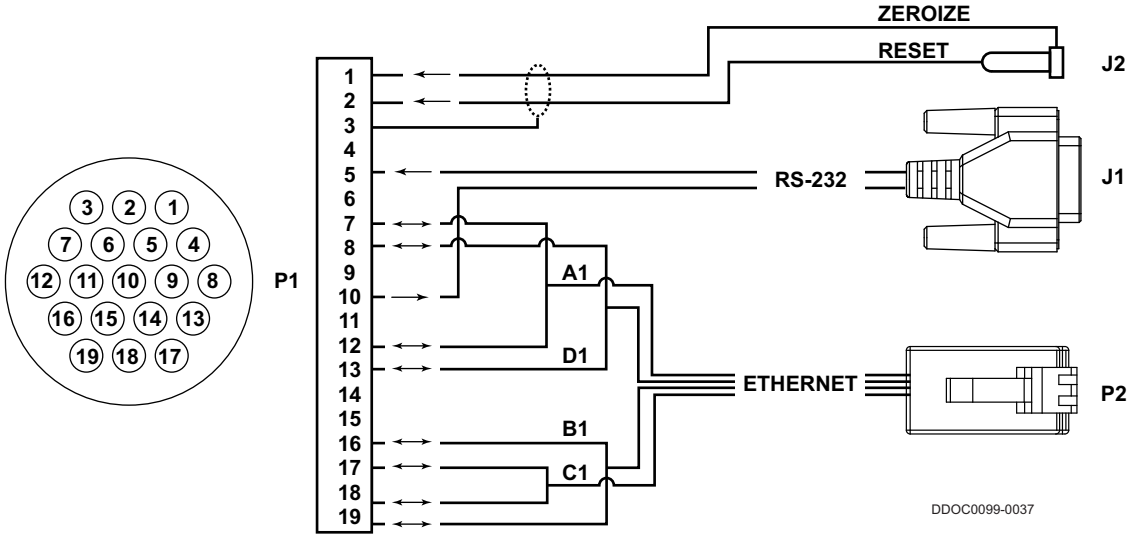

Figure B.4 Utility Lab Cable Diagram

B.3 Ethernet Connector J3 / Ethernet Lab Cable

Table B.5 provides DTS1 bulkhead J3 connector pin signals. Figure B.5 show the DTS1 bulkhead J3 connector pinout. Table B.6 shows the DTS1 Ethernet lab cable connection pin signals. Figure B.6 show the utility lab cable wiring diagram.

Connector Manufacturer Glenair
Connector Reference DesignatorJ3
Connector.....PN 801-023-07M9-19PB
Mating ConnectorPN 801-007-16M9-19SB

Table B.5 Ethernet Connector J3 Signals

Connector Pin	Signal Name	Signal Type	Direction	Description / Functions
1				
2				
3	GND	Analog		NC
4	GND	Analog		NC
5				
6	GND	Analog		NC
7	BI_DA2-	GbE	In / Out	Gigabit Ethernet Bi-directional pair A2+/-
8	BI_DD2+	GbE	In / Out	Gigabit Ethernet Bi-directional pair D2+/-
9	GND	Analog		NC
10				
11	GND	Analog		NC
12	BI_DA2+	GbE	In / Out	Gigabit Ethernet Bi-directional pair A2+/-
13	BI_DD2-	GbE	In / Out	Gigabit Ethernet Bi-directional pair D2+/-
14	GND	Analog		NC
15	GND	Analog		NC
16	BI_DB2-	GbE	In / Out	Gigabit Ethernet Bi-directional pair B2+/-
17	BI_DC2+	GbE	In / Out	Gigabit Ethernet Bi-directional pair C2+/-
18	BI_DC2-	GbE	In / Out	Gigabit Ethernet Bi-directional pair C2+/-
19	BI_DB2+	GbE	In / Out	Gigabit Ethernet Bi-directional pair B2+/-

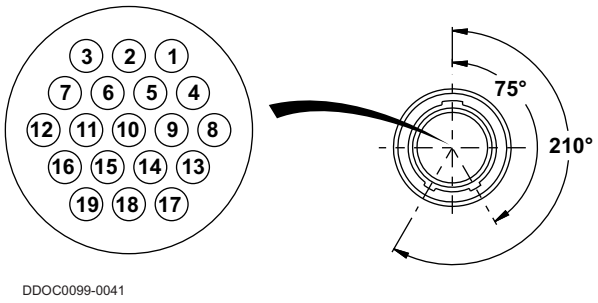

Figure B.5 Ethernet Connector J3

Table B.6 Ethernet Lab Cable (VS-DTS1ETHCAB-J3)

Connector Description	Mates With / Signal Name
P1	DTS1 J3
P2 – TIA/EIA-568B Modular Plug	Gigabit Ethernet TIA/EIA-568B Modular Jack

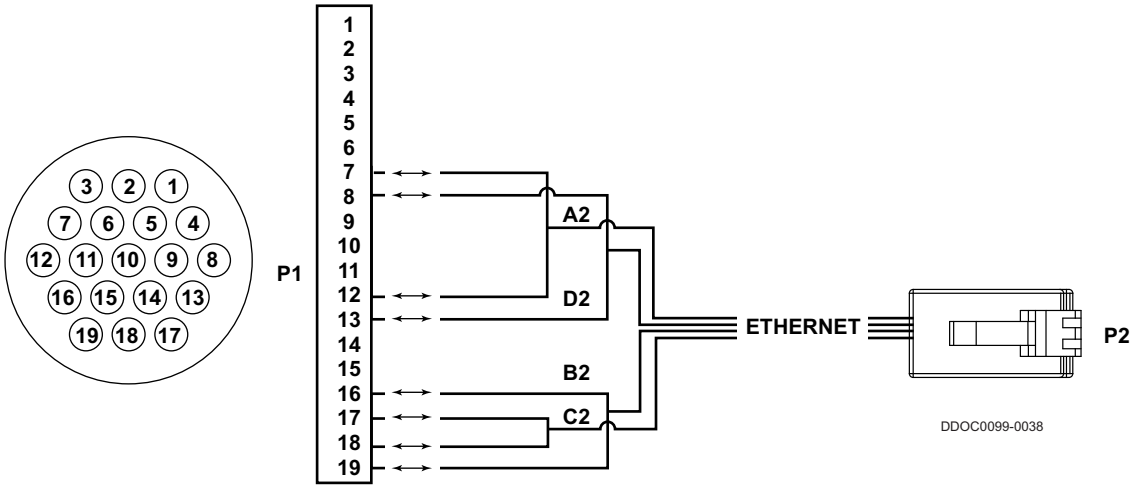

Figure B.6 Ethernet Lab Cable Wiring Diagram

B.4 Ground Cable

NOTE
Do not loosen nut / washer installed on ground stud E1. Ensure nut / washer on ground stud remain properly tightened when installing / removing ground cable.

NOTE
It is recommended that the grounding cable used be a flat, braided, low impedance cable and be as short as possible.

To ensure proper grounding of the DTS1, a ground cable, split lock washer, and hex nut are required, but not provided. The ground cable (Figure B.7) terminal is installed on the DTS1 ground stud E1. The hex nut and split lock washer used to secure the ground cable terminal to ground stud E1 should be torqued to 15 in. lb. to ensure proper connection.

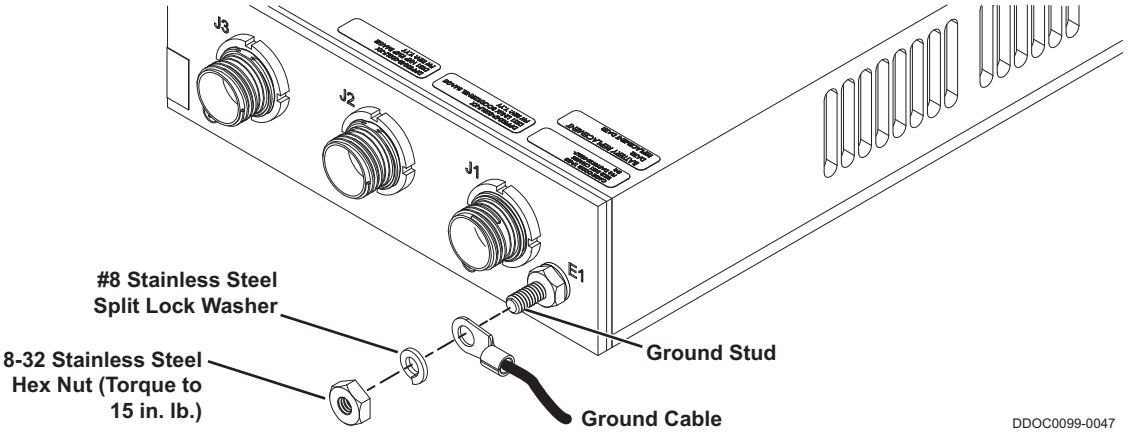

Figure B.7 DTS1 Ground Connection

Ordering Information

C.1 DTS1 / RMC Module / Lab Cables

This appendix contains the ordering numbers for the DTS1 CSfC chassis (Table C.1), RMC module (Table C.2), lab cables (Table C.3), and crypto battery (Table C.4). For an up to date list, or for inquiries about these products, contact Curtiss-Wright Defense Solutions Sales at http:/www.cwcdefensesolutions.com/sales.html.

Table C.1 DTS1 CSfC Chassis

Order Number	Description
VS-DTS1SL-F	DTS1 Chassis Without RMC Module (L Bracket Mount)
VS-DTS1SL-FD	DTS1 Chassis Without RMC Module (DZUS Panel Mount)

Table C.2 RMC Module

Order Number	Description
VS-RMC8192M-00	RMC, 8 TB
VS-RMC4096M-00	RMC, 4 TB
VS-RMC2048M-00	RMC, 2 TB
VS-RMC1024M-00	RMC, 1 TB
VS-RMC256M-00	RMC, 256 GB
VS-RMC0000-00	RMC, empty cartridge

Table C.3 DTS1 Lab Cables

Order Number	Description
VS-DTS1PWRCAB-0	DTS1 Power Lab Cable
VS-DTS1ETHCAB-J2	DTS1 Utility Lab Cable
VS-DTS1ETHCAB-J3	DTS1 Ethernet Lab Cable

Table C.4 DTS1 Battery

Order Number	Description
VS-DTS1SL-Battery	DTS1 Battery Module