

Tactical Key Management Device (TKMD)

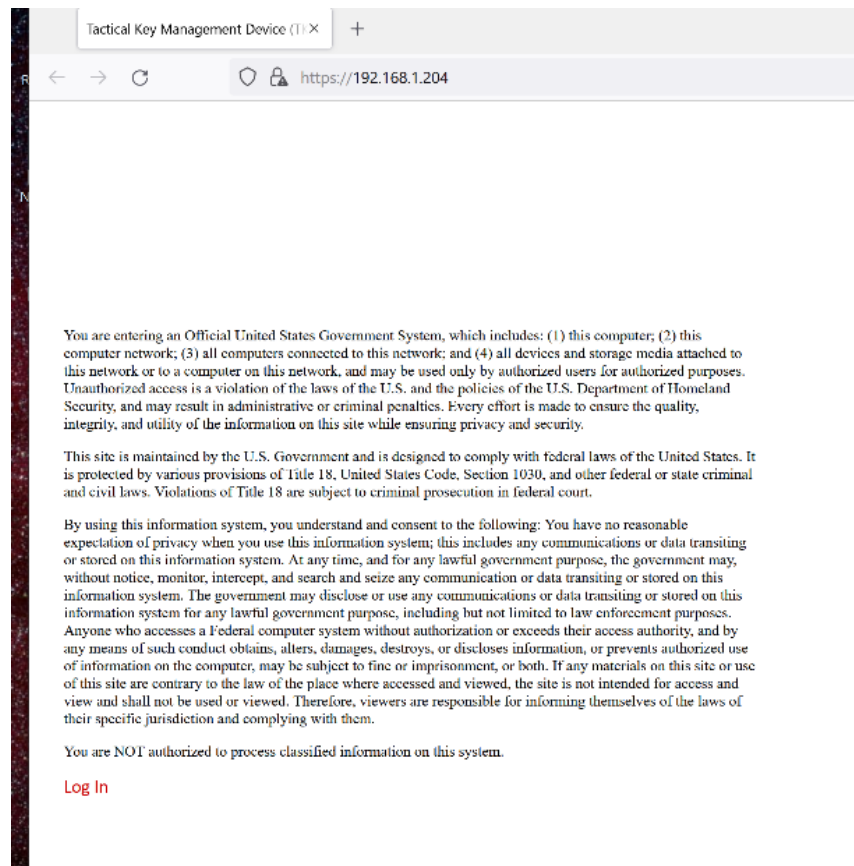
Crypto Officer Web Page Descriptions

January 17, 2022

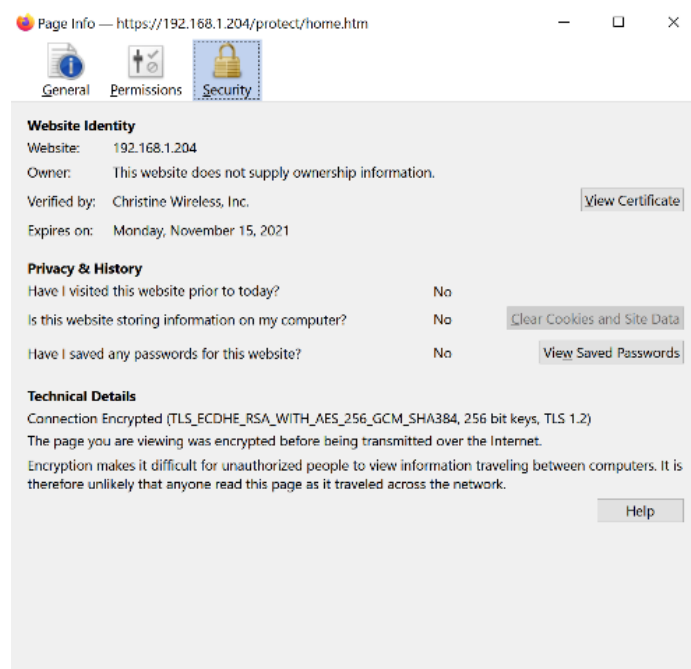
Introduction This document provides descriptions and instructions for use of each of the web pages that the Crypto Officer can access for setting up and controlling the TKMD. These are accessed over an Internet Protocol Ethernet Network connection and are secure web pages (https) using TLSv1.2 security. Access to the web pages requires the entry of the Crypto Officer username and password. When the TKMD is first powered, it runs an inventory of all Client units which can take up to several minutes depending on how many Clients are authorized for the TKMD. During this Client Inventory process, the 4 LEDs on the TKMD front panel will flash in sequence. Please wait for the Client Inventory to finish before attempting to access the TKMD web pages.

Log In To access the Log In web page open a browser on the Crypto Officer computer. In order of preference Firefox, Chrome, Edge and Internet Explorer can be used as a browser. The version of the browser may have to be updated to access the TKMD if the browser is very out-of-date. Enter the IP address for the TKMD into the browser address window for example: https://192.168.1.204. To access the IP address, it is necessary that the computer IP address and subnet mask include the IP address of the TKMD. It may be necessary to go into the Network Configuration control page on the computer and set the IPV4 configuration accordingly. If there is any question about whether the computer can reach the TKMD IP address, open a Command Prompt window and type ping 192.168.1.204(enter) for example. The TKMD will always respond to a ping.

Make sure to use the secure web page designation “https” since the web pages cannot be accessed using the non-secure web page designation “http”. The browser will attempt to do a TLS handshake with the TKMD which will result in a warning that the web site is not secure. This browser warning is a result of the TKMD not using a pre-assigned IP address or domain name and therefore using a self-signed security certificate. Click “Advanced” or whatever indication the browser uses and tell the browser to access the web page despite the security warning. The following Log In page will be produced by the browser (Firefox in this example):



If you open the security symbol in the address bar and navigate to the “More Information”, you can see the following description of the Security Certificate and TLSv1.2 connection:



The Connection Description indicates the specifics of the TLSv1.2 connection. This is the only TLSv1.2 connection type supported by the TKMD.

To access the web pages, click on the red “Log In” link at the bottom of the page and enter the Crypto Officer username and password on the Log In popup screen. If the wrong combination is entered, there is a 3 second delay before you can try again.

Overview The Overview Web Page contains a brief description of the TKMD as well as the specifics of the firmware version loaded in the TKMD:

Tactical Key Management Device

Christine Wireless, Inc.
Ellicott City Maryland
410-961-7331
www.christinewireless.com

Tactical Key Management Device

Overview

Key Data

Key Assign

Client Summary

Client Configuration

File Up/Down Load

File Share

Network Configuration

Board Configuration

Remote Configuration

Battery Monitor

View Logs

SNMP Configuration

Tactical Key Management Device

Stack Version: 7.32 - H3.2

Firmware Build Date: Jan 9 2022 08:37:37

Web Page Revision: January 09, 2022

Non-FIPS version of Tactical Key Management Device

This device includes the following capabilities:

- **OTAR KMF** - Rekey up to 3,000 radios with Project 25 compliant OTAR
 - Confirmed Data Exchanges for Individual OTAR Actions
 - Unconfirmed Data with Delayed Acknowledgements for Group OTAR Actions
- **OTAR Client** - Accept rekey from a Project 25 compliant OTAR KMF
- **Key Variable Loader** - Physically load keys into any Project 25 compliant radio
- **Key Loader Client** - Accept physical key load from a KVL-3000+ or other Project 25 compliant Key Fill Device
- **Secure File Uploads** - upload new firmware, Client Radio Configurations, web pages and key files

Control device is any PC/MAC with an Ethernet port and a web browser.

Copyright © 2012-2022 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

The vertical menu bar on the left side of the web page is used to navigate to other TKMD web pages.

Key Data Management: This page is used to view and modify the key data base common to all modes. Key data may be modified on the Key Entry Page. Use the pull-down menus to LOAD/SAVE/ERASE the desired keyset.

Selected Key Source Name: Imported Keyset 2 Selected Key Source ID: 7000

Select Key Data 9 None Enter Keyset Name Enter Keyset ID

| No. | SLN(d) | KID(h) | KSID | ALG | Name | No. | SLN(d) | KID(h) | KSID | ALG | Name |
|-----|--------|--------|------|---------|----------|-----|--------|--------|------|-----|------|
| 1 | 50 | 0003 | 1 | DES OFB | DES TEK1 | 31 | | | | | |
| 2 | 51 | 0004 | 1 | DES OFB | DES TEK2 | 32 | | | | | |
| 3 | 52 | 0001 | 1 | DES OFB | DES TEK3 | 33 | | | | | |
| 4 | 81 | 0003 | 1 | AES 256 | AES TEK1 | 34 | | | | | |
| 5 | 82 | 0004 | 1 | AES 256 | AES TEK2 | 35 | | | | | |
| 6 | 83 | 0001 | 1 | AES 256 | AES TEK3 | 36 | | | | | |
| 7 | 50 | 0003 | 2 | DES OFB | DES TEK1 | 37 | | | | | |
| 8 | 51 | 0004 | 2 | DES OFB | DES TEK2 | 38 | | | | | |
| 9 | 52 | 0001 | 2 | DES OFB | DES TEK3 | 39 | | | | | |
| 10 | 81 | 0003 | 2 | AES 256 | AES TEK1 | 40 | | | | | |
| 11 | 82 | 0004 | 2 | AES 256 | AES TEK2 | 41 | | | | | |
| 12 | 83 | 0001 | 2 | AES 256 | AES TEK3 | 42 | | | | | |
| 13 | | | | | | 43 | | | | | |
| 14 | | | | | | 44 | | | | | |
| 15 | | | | | | 45 | | | | | |
| 16 | | | | | | 46 | | | | | |
| 17 | | | | | | 47 | | | | | |
| 18 | | | | | | 48 | | | | | |
| 19 | | | | | | 49 | | | | | |
| 20 | | | | | | 50 | | | | | |
| 21 | | | | | | 51 | | | | | |
| 22 | | | | | | 52 | | | | | |
| 23 | | | | | | 53 | | | | | |
| 24 | | | | | | 54 | | | | | |
| 25 | | | | | | 55 | | | | | |
| 26 | | | | | | 56 | | | | | |
| 27 | | | | | | 57 | | | | | |
| 28 | | | | | | 58 | | | | | |
| 29 | | | | | | 59 | | | | | |
| 30 | | | | | | 60 | | | | | |

[KEY ENTRY](#) [HOME](#)

| Selected Key Source Name: Importe | | |
|-----------------------------------|-------|-------------------|
| Select Key Data 9 | | |
| No. | SLN(d | |
| 1 | 50 | None |
| 2 | 51 | Key Data 1 |
| 3 | 52 | Key Data 2 |
| 4 | 81 | Key Data 3 |
| 5 | 82 | Key Data 4 |
| 6 | 83 | Key Data 5 |
| 7 | 50 | TKMD Keys |
| 8 | 51 | Default Keys |
| 9 | 52 | Import Current SU |
| 10 | 81 | Imported Keyset 1 |
| 11 | 82 | Imported Keyset 2 |
| 12 | 83 | Imported Keyset 3 |
| 13 | | Imported Keyset 4 |
| 14 | | Imported Keyset 5 |
| 15 | | Imported Keyset 6 |
| 16 | | Imported Keyset 7 |
| 17 | | Imported Keyset 8 |
| 18 | | |

TKMD Keys Up to 60 keys assigned to Client #0, the TKMD itself.

Default Keys Hardcoded key material provided for convenience to familiarize the Crypto Officer with the use of the TKMD.

Import Current SU This selection allows the import of the up to 60 keys assigned to the Current Subscriber Unit (Client) as selected on the Client Configuration Web Page.

Imported Keyset 1 ->8 These are 8 “Key Kettles” each consisting of up to 40 keys. The Key Kettles can either be locally generated or can be imported over secure IP from other TKMDs. Key Kettle keys can be cross-referenced to those assigned to Clients allowing an easy way of automatically updating key material assigned to even a large number of Clients

Once the key source has been selected, the second pulldown menu can be used to indicate what to do with that key source.

Key Data Management: This page is used to view and modify the key data base common to all modes. Key data may be modified on the Key Entry Page. Use the pull-down menus to LOAD/SAVE/ERASE the desired keyset.

Selected Key Source Name: Imported Keyset 2 **Selected Key Source ID:** 7000

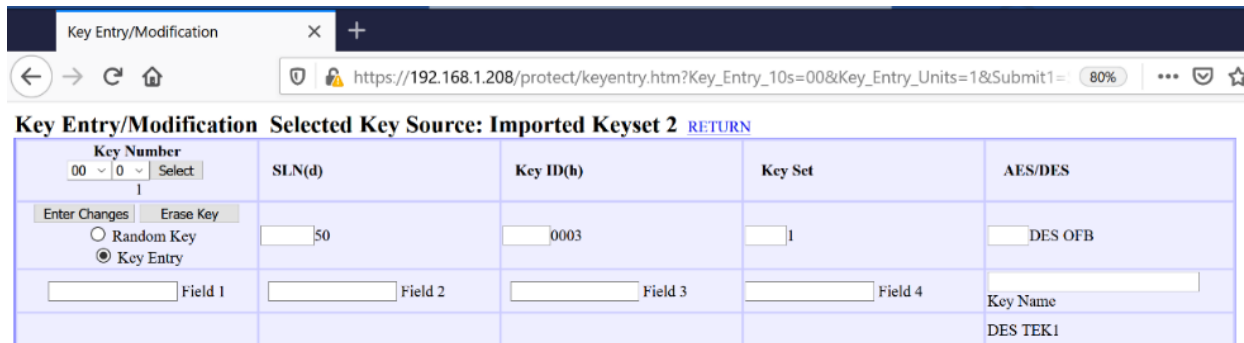
Select Key Data: 9

| No. | SLN(d) | KID(h) | KSID | Name | No. | SLN(d) | K |
|-----|--------|--------|------|-----------------|-----|--------|---|
| 1 | 50 | 0003 | 1 | Load Keyset | 31 | | |
| 2 | 51 | 0004 | 1 | Save Keyset | 32 | | |
| 3 | 52 | 0001 | 1 | Erase Keyset | 33 | | |
| 4 | 81 | 0003 | 1 | Set Keyset Name | 34 | | |
| 5 | 82 | 0004 | 1 | Set Keyset ID | 35 | | |
| 6 | 83 | 0001 | 1 | AES 256 | 36 | | |
| 7 | 50 | 0003 | 2 | DES OFB | 37 | | |
| 8 | 51 | 0004 | 2 | DES OFB | 38 | | |
| 9 | 52 | 0001 | 2 | DES OFB | 39 | | |
| 10 | 81 | 0003 | 2 | AES 256 | 40 | | |
| 11 | 82 | 0004 | 2 | AES 256 | 41 | | |
| 12 | 83 | 0001 | 2 | AES 256 | 42 | | |
| 13 | | | | | 43 | | |

If Set Keyset Name or Set Keyset ID is intended, the desired Name or ID must first be entered into one of the two adjacent data entry windows.

At the bottom of the Key Data web page is a “Home” link to go back to the TKMD Home page and a Key Entry link which will take the browser to the Key Entry web page.

Key Entry web page The Key Entry web page can be used to view or modify individual keys from the key source selected on the Key Data web page.



Key Entry/Modification Selected Key Source: Imported Keypset 2 [RETURN](#)

| Key Number | SLN(d) | Key ID(h) | Key Set | AES/DES |
|---|---------|-----------|---------|----------|
| 00 0 Select 1 | | | | |
| Enter Changes Erase Key <input type="radio"/> Random Key <input checked="" type="radio"/> Key Entry | 50 | 0003 | 1 | DES OFB |
| Field 1 | Field 2 | Field 3 | Field 4 | Key Name |
| | | | | DES TEK1 |

Key entries are not saved by this page. Use the menu on the Key Data page to save the entire keyset to Flash Memory.

Use the Key Number selection in the upper left-hand corner to select the desired key. The current settings for the selected key are displayed next to the data entry window for each parameter. Changes to any key parameter are made in the data entry window for that parameter.

If new key material is to be entered either select Random Key or Enter Key. If Enter Key is to be used, type the hexadecimal value for the key 16 digits at a time into the Field windows, Field 1 for DES and all 4 Fields for AES. Select “Enter Changes” to perform the indicated action. Note that the Key Entry changes the key values as directed, but does not save the new values. The Crypto Officer must use the “Return” link to go back to the Key Data web page and save any modifications using that page to avoid loss of any changes made on the Key Entry web page.

Key Assign The Key Assign web page allows the Crypto Officer to move key material from any location in the TKMD to any other location:

Key Assign

[←](#)
[→](#)
[↺](#)
[🏠](#)

[🔒](#)
[🔑](#)
<https://192.168.1.208/protect/keyassign.htm>

Source: Imported Keyset 2

Target: Client Number = 10

Source Client Number

Enter Keyset Name

Enter Keyset ID
 7000

Select Source Data
9
Action
None

Target Client Number

Enter Keyset Name

Client: 10
Enter Keyset ID

Client: 10

Select Target Data
24
Action
None

[KEY ENTRY](#)

[HOME](#)

Assign Key
None

Remember to SAVE changes

| Key # | ALG | KSet | SLN(d) | KID(b) | Key Name | FROM | TO | PRO | Key # | ALG | KSet | SLN(d) | KID(b) | Key Name |
|-------|---------|------|--------|--------|----------|-----------------------|-----------------------|----------------------------------|-------|---------|------|--------|--------|----------|
| 1 | DES OFB | 1 | 50 | 0003 | DES TEK1 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 1 | DES OFB | 1 | 50 | 0003 | DES TEK1 |
| 2 | DES OFB | 1 | 51 | 0004 | DES TEK2 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 2 | DES OFB | 1 | 51 | 0004 | DES TEK2 |
| 3 | DES OFB | 1 | 52 | 0001 | DES TEK3 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 3 | DES OFB | 1 | 52 | 0001 | DES TEK3 |
| 4 | AES 256 | 1 | 81 | 0003 | AES TEK1 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 4 | AES 256 | 1 | 81 | 0003 | AES TEK1 |
| 5 | AES 256 | 1 | 82 | 0004 | AES TEK2 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 5 | AES 256 | 1 | 82 | 0004 | AES TEK2 |
| 6 | AES 256 | 1 | 83 | 0001 | AES TEK3 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 6 | AES 256 | 1 | 83 | 0001 | AES TEK3 |
| 7 | DES OFB | 2 | 50 | 0003 | DES TEK1 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 7 | DES OFB | 2 | 50 | 0003 | DES TEK1 |
| 8 | DES OFB | 2 | 51 | 0004 | DES TEK2 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 8 | DES OFB | 2 | 51 | 0004 | DES TEK2 |
| 9 | DES OFB | 2 | 52 | 0001 | DES TEK3 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 9 | DES OFB | 2 | 52 | 0001 | DES TEK3 |
| 10 | AES 256 | 2 | 81 | 0003 | AES TEK1 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 10 | AES 256 | 2 | 81 | 0003 | AES TEK1 |
| 11 | AES 256 | 2 | 82 | 0004 | AES TEK2 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 11 | AES 256 | 2 | 82 | 0004 | AES TEK2 |
| 12 | AES 256 | 2 | 83 | 0001 | AES TEK3 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 12 | AES 256 | 2 | 83 | 0001 | AES TEK3 |
| 13 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 13 | DES OFB | 255 | 61440 | F5A0 | DES UKEK |
| 14 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 14 | DES OFB | 255 | 61441 | F5A1 | DES CKEK |
| 15 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 15 | AES 256 | 255 | 61442 | F5A0 | AES UKEK |
| 16 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 16 | AES 256 | 255 | 61443 | F5A1 | AES CKEK |
| 17 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 17 | | | | | |
| 18 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 18 | | | | | |
| 19 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 19 | | | | | |
| 20 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 20 | | | | | |
| 21 | | | | | | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | 21 | | | | | |

After selecting and loading a Source and Target keyset, the radio buttons in the center columns can be used to select a specific Source and Target key in the keyset. The “From” radio buttons are used to select a specific Source key and either the “To” or “Pro” radio button is used to indicate where the Source key is to be placed. Pro designates “Provisioned” which means that the key will be shown as having previously been loaded (Provisioned) in the Target Client key set. The “Pro” feature is useful to let the TKMD know that the specific key has been loaded into the designated Client by a non-TKMD means such as a Key Fill Device. Keys must be assigned one-at-a-time.

192.168.1.208/protect/keyassign.htm

ed Keyset 2 **Target: Client Nu**

ct Source Data

on

Target Client Number

Enter Keyset Name

Client: 10

Enter Keyset ID

Client: 10

OME Assign Key None

Ret

| Key Name | FROM | Key # | ALG |
|---------------|-----------------------|-------|---------|
| 0003 DES TEK1 | <input type="radio"/> | 1 | DES OFB |
| 0004 DES TEK2 | <input type="radio"/> | 2 | DES OFB |
| 0001 DES TEK3 | <input type="radio"/> | 3 | DES OFB |
| 0003 AES TIK1 | <input type="radio"/> | 4 | AES 256 |
| 0004 AES TIK2 | <input type="radio"/> | 5 | AES 256 |
| 0001 AES TIK3 | <input type="radio"/> | 6 | AES 256 |
| 0003 DES TEK1 | <input type="radio"/> | 7 | DES OFB |
| 0004 DES TEK2 | <input type="radio"/> | 8 | DES OFB |
| 0001 DES TEK3 | <input type="radio"/> | 9 | DES OFB |
| 0003 AES TIK1 | <input type="radio"/> | 10 | AES 256 |
| 0004 AES TIK2 | <input type="radio"/> | 11 | AES 256 |

Once a Source and Target Key locations are selected using the radio buttons, the Assign Key pulldown menu can be used. If it is desired to retain the current keyset for the Source key, use “Assign”. If it is desired to assign the Source key to Key Set 1 or Key Set 2 use “Assign KS1” or “Assign KS2” respectively. If it is desired to just update the UTC time stamp for an existing Target key, use Update UTC. If it is desired that the Target key be shown as Provisioned (already confirmed to be installed in the Target Client data base) use the Target radio button in the Green Pro column.

After assigning the keys to the Target file, remember to save the Target file.

Client Summary

←

→

↶

🏠

🔒

🔗

https://192.168.1.208/protect/clientsummary.htm

80%

...

🖨

CLIENT SUMMARY (LLID)

[VIEW CLIENT](#)
[HOME](#)

update

0-500

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|------------|------------|------------|------------|------------|------------|------------|------------|-------------|-------------|---------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| 1 N/C | 2 N/C | 3 N/C | 4 N/C | 5 N/C | 6 N/C | 7 N/C | 8 N/C | 9 N/C | 10 12345 | 11 12346 | 12 1115992 | 13 196 | 14 N/C | 15 N/C | 16 N/C | 17 N/C | 18 N/C | 19 N/C | 20 N/C | 21 N/C | 22 N/C | 23 N/C | 24 N/C | 25 N/C | 26 N/C | 27 N/C | 28 N/C | 29 N/C | 30 N/C | 31 N/C | 32 N/C |
| 33 N/C | 34 N/C | 35 N/C | 36 N/C | 37 N/C | 38 N/C | 39 N/C | 40 N/C | 41 N/C | 42 N/C | 43 N/C | 44 N/C | 45 N/C | 46 N/C | 47 N/C | 48 N/C | 49 N/C | 50 N/C | 51 N/C | 52 N/C | 53 N/C | 54 N/C | 55 N/C | 56 N/C | 57 N/C | 58 N/C | 59 N/C | 60 N/C | 61 N/C | 62 N/C | 63 N/C | 64 N/C |
| 65 N/C | 66 N/C | 67 N/C | 68 N/C | 69 N/C | 70 N/C | 71 N/C | 72 N/C | 73 N/C | 74 N/C | 75 N/C | 76 N/C | 77 N/C | 78 N/C | 79 N/C | 80 N/C | 81 N/C | 82 N/C | 83 N/C | 84 N/C | 85 N/C | 86 N/C | 87 N/C | 88 N/C | 89 N/C | 90 N/C | 91 N/C | 92 N/C | 93 N/C | 94 N/C | 95 N/C | 96 N/C |
| 97 N/C | 98 N/C | 99 N/C | 100 N/C | 101 N/C | 102 N/C | 103 N/C | 104 N/C | 105 N/C | 106 N/C | 107 N/C | 108 N/C | 109 N/C | 110 N/C | 111 N/C | 112 N/C | 113 N/C | 114 N/C | 115 N/C | 116 N/C | 117 N/C | 118 N/C | 119 N/C | 120 N/C | 121 N/C | 122 N/C | 123 N/C | 124 N/C | 125 N/C | 126 N/C | 127 N/C | 128 N/C |
| 129 N/C | 130 N/C | 131 N/C | 132 N/C | 133 N/C | 134 N/C | 135 N/C | 136 N/C | 137 N/C | 138 N/C | 139 N/C | 140 N/C | 141 N/C | 142 N/C | 143 N/C | 144 N/C | 145 N/C | 146 N/C | 147 N/C | 148 N/C | 149 N/C | 150 N/C | 151 N/C | 152 N/C | 153 N/C | 154 N/C | 155 N/C | 156 N/C | 157 N/C | 158 N/C | 159 N/C | 160 N/C |
| 161 N/C | 162 N/C | 163 N/C | 164 N/C | 165 N/C | 166 N/C | 167 N/C | 168 N/C | 169 N/C | 170 N/C | 171 N/C | 172 N/C | 173 N/C | 174 N/C | 175 N/C | 176 N/C | 177 N/C | 178 N/C | 179 N/C | 180 N/C | 181 N/C | 182 N/C | 183 N/C | 184 N/C | 185 N/C | 186 N/C | 187 N/C | 188 N/C | 189 N/C | 190 N/C | 191 N/C | 192 N/C |
| 193 N/C | 194 N/C | 195 N/C | 196 N/C | 197 N/C | 198 N/C | 199 N/C | 200 N/C | 201 N/C | 202 N/C | 203 N/C | 204 N/C | 205 N/C | 206 N/C | 207 N/C | 208 N/C | 209 N/C | 210 N/C | 211 N/C | 212 N/C | 213 N/C | 214 N/C | 215 N/C | 216 N/C | 217 N/C | 218 N/C | 219 N/C | 220 N/C | 221 N/C | 222 N/C | 223 N/C | 224 N/C |
| 225 N/C | 226 N/C | 227 N/C | 228 N/C | 229 N/C | 230 N/C | 231 N/C | 232 N/C | 233 N/C | 234 N/C | 235 N/C | 236 N/C | 237 N/C | 238 N/C | 239 N/C | 240 N/C | 241 N/C | 242 N/C | 243 N/C | 244 N/C | 245 N/C | 246 N/C | 247 N/C | 248 N/C | 249 N/C | 250 N/C | 251 N/C | 252 N/C | 253 N/C | 254 N/C | 255 N/C | 256 N/C |
| 257 N/C | 258 N/C | 259 N/C | 260 N/C | 261 N/C | 262 N/C | 263 N/C | 264 N/C | 265 N/C | 266 N/C | 267 N/C | 268 N/C | 269 N/C | 270 N/C | 271 N/C | 272 N/C | 273 N/C | 274 N/C | 275 N/C | 276 N/C | 277 N/C | 278 N/C | 279 N/C | 280 N/C | 281 N/C | 282 N/C | 283 N/C | 284 N/C | 285 N/C | 286 N/C | 287 N/C | 288 N/C |
| 289 N/C | 290 N/C | 291 N/C | 292 N/C | 293 N/C | 294 N/C | 295 N/C | 296 N/C | 297 N/C | 298 N/C | 299 N/C | 300 N/C | 301 N/C | 302 N/C | 303 N/C | 304 N/C | 305 N/C | 306 N/C | 307 N/C | 308 N/C | 309 N/C | 310 N/C | 311 N/C | 312 N/C | 313 N/C | 314 N/C | 315 N/C | 316 N/C | 317 N/C | 318 N/C | 319 N/C | 320 N/C |
| 321 N/C | 322 N/C | 323 N/C | 324 N/C | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Green The Client is currently OTAR-Registered with the TKMD and has all assigned keys.

Yellow The Client is not currently OTAR-Registered with the TKMD but has all assigned keys.

Light Blue The Client is not currently OTAR-Registered with the TKMD and does not have all assigned keys.

Dark Blue The Client is currently OTAR-Registered with the TKMD and does not have all assigned keys.

The Client Summary page is automatically refreshed once every 30 seconds.

The link to [HOME](#) can be used to go back to the introductory web page and the link to [VIEW CLIENT](#) can be used to navigate to the Client Configuration web page which is the primary TKMD web page for OTAR configuration.

Client Configuration web page The Client Configuration web page is the main configuration and operation web page for the TKMD.

Client Configuration [Client Summary](#) *Changes Must Be Saved to Client Record!* [Home](#)

| | | | | | | | |
|---|--|--|--|---|--|--|--|
| Mode = Automatic OTAR KMF Packet Data OTAR KMF DFISI Packet Data enabled Automatic OTAR KMF: ON <input type="radio"/> OFF <input type="radio"/> MON <input type="radio"/> Auto Otar Voice Lockout: None | | Client = 10 ENTER CLIENT NUMBER ENTER CLIENT LLID ENTER CLIENT RSI ACTION | | ALGORITHM: TEK KEY: WS MAC KEY: WS | | UTC: 1641914978718 Tuesday January 11 2022 10:29:38 | |
| 12345 Unit RSI MN= 0 12345 Unit ID | | 0 Group RSI MN= 0 | | 16 AES CKEK 14 DES CKEK | | Procedures Warm Start Rekey/Erase Inventory Zeroize Set MNP Change RSI Hello Message Key Summary Status Key Set Changeover Radio Enable/Disable | |
| KNG VHF 1 Name Christine Wirel Org Test Group | | 9999999 KMF RSI 0 KVL RSI | | 15 AES UKEK 13 DES UKEK | | Enter Client Data | |
| None Key Data Set: Source Key = 0 | | Key Name | | Algorithm | | SLN(d) KID(h) | |
| Client Key = 0 | | Key Name | | Algorithm | | SLN(d) KID(h) | |
| None Client Key Action | | Re-Name Key | | Key Set ID | | Re-Assign SLN Re-Assign KID(h) | |

The Client Configuration web page is organized as follows:

Yellow Background This section is for the configuration and operation of the TKMD. The first column selects the Operating mode of the TKMD, the second column selects the Client to be displayed and the third, fourth and fifth columns allow manual OTAR/Key Fill operations to be initiated by the Crypto Officer.

Green Background This section displays the parameters for the Client unit selected in the second Yellow Background column and allows for changing those parameters.

Gray Background This section allows selection of a specific key from a key source designated on the Key Data web page. The parameters for the selected key are displayed in the Gray Background section.

Blue Background This section allows selection, display and modification of specific keys in the selected Client data record.

The link to [Client Summary](#) will navigate to the Client Summary web page and the Link to [Home](#) will navigate to the introductory web page.

TKMD Operating Mode The first Yellow Background Column on the Client Configuration web page selects the operating mode for the TKMD. If desired, the operating mode on startup can be automatically configured using the Board Configuration web page.

The first three operating mode selections are for the operation of the TKMD as a Key Management Facility (KMF) with one of three Base Station selections (Quantar, SLIP and DFSI Packet Data). The next three selections are for the TKMD to behave as an OTAR Client on an external KMF using one of three Base Station type selections and the final three selections are for the TKMD to act as either a Key Fill Device (KFD) source or target. In addition, the automatic OTAR radio button can enable automatic OTAR operations in the KMF modes. The usual TKMD setup is for Automatic OTAR in one of the three KMF modes and this would be the normal start-up configuration as setup on the Board Configuration web page.

In Automatic OTAR mode, the TKMD will respond to individual Client OTAR-Registration requests. If the TKMD Client record shows that all assigned keys have been loaded in the Client, no OTAR actions other than granting the OTAR-Registration request will take place. If the TKMD Client record shows that there are assigned keys that have not been loaded in the Client, the TKMD will attempt to load those keys. If the Client sends a Rekey Request Message, the TKMD will attempt to load all assigned keys in the Client.

The Quantar Base Station mode allows use of V.24 with any compatible device (Quantar, PDR, ATAC, DIU etc.). The SLIP Base Station mode is specific to compatible portables with a Serial Line Interface Protocol transparent data mode. The DFSI Packet Data Base Station mode allows

use of a Digital Fixed Station Interface (TIA 102.BAHA-A) Base Station such as those manufactured by Codan, RF Technology and possibly others.

In the Key Fill Send mode the TKMD can be used to load key material into any Project 25 compliant Client. In the Key Fill Receive mode, any Project 25 compliant Key Fill Device can be used to load key material into Client #0, the TKMD itself.

The setting for Auto OTAR Voice Lockout allows the Crypto Officer to designate how long Auto OTAR will be inhibited after voice traffic is detected. This setting can be used to give Voice traffic priority and to attempt to avoid OTAR messaging interfering with voice traffic.

Client Selection The second Yellow Background column is for selection of a specific Client.

The Client can be selected by use of one of three Client Data parameters:

1. If the Client number (Storage location for the Client) is known, that parameter can be entered in the first data entry window.
2. If the LLID (over-the-air ID) of the Client is known, that ID can be entered in the second data entry window.
3. If the Radio Set Identifier (OTAR ID – RSI) is known, that ID can be entered into the third data entry window.

When one of the three methods of identifying which Client has been entered, the ACTION pulldown menu can be used to perform the desired action. “Load” locates the desired Client record and displays the Client parameters in the Green Background section. “Save” can be useful to retain changes made to a Client Record. “Save” is also useful to store the current Client record in another location. To use this feature, enter the new Client location in the first data entry window and use “Save” to copy the currently displayed Client parameters into the new record. Care must be taken in that this process overwrites the new storage location and also creates problems with duplicate

records. After using this copy operation it is necessary to make any changes to the new Client record to remove the duplicate record issues and “Save” it.

If a Subscriber Radio Unit (Client) has been lost or compromised, the data record for that unit can be marked for Zeroization. If the Client file is so marked, the TKMD will erase all keys in the unit in Automatic OTAR mode as soon as the unit attempts to register on the OTAR channel. This will prevent the unit from future OTAR and encrypted voice communication until new keys have been loaded into the unit using a Key Fill Device. Since data files can be optionally shared with other TKMDs, the Zeroize flag can be sent to other TKMDs preventing the unit from OTAR and Secure Voice operation. The pull-down menu can also be used to clear the Zeroize flag if desired.

Manual OTAR Operation The three right columns in the Yellow Background portion of the Client Configuration web page are devoted to Manual OTAR/Key Fill Operation under the control of the Crypto Officer. Unless otherwise noted, it is presumed that the manual OTAR/Key Fill operations are taking place with the Client selected.

The screenshot shows a web browser window with the URL `stect/clientconfig.htm?UTC=&Proc_Type=0`. The page has a yellow background and a blue border. At the top, there is a navigation bar with links: [mary](#), [Changes Must Be Saved to Client Record!](#), and [Home](#). The main content area is divided into four columns. The first column contains a form for Client configuration with the following fields: **Client = 10**, (with a dropdown arrow), **ENTER CLIENT NUMBER**, (with a dropdown arrow), **ENTER CLIENT LLID**, (with a dropdown arrow), **ENTER CLIENT RSI**, and (with a dropdown arrow) followed by **ACTION**. The second column contains two sections: **ALGORITHM:** with a dropdown menu, and **TEK KEY: 255** with a dropdown menu. Below these is **MAC KEY: 255** with a dropdown menu. The third column contains a section titled **Procedures** with a list of links: [Warm Start](#), [Rekey/Erase](#), [Inventory](#), [Zeroize](#), [Set MNP](#), [Change RSI](#), and [Hello Message](#). The fourth column contains a section titled **Key Summary** with a list of links: [Status](#), [Key Set Changeover](#), and [Radio Enable/Disable](#). The top right of the page shows the UTC time: **UTC: 1608236912485** and the date/time: **Thursday December 17 2020 15:28:32**.

Procedures Overview The following Procedures/Status Windows can be selected from the fourth and fifth columns of the Yellow Background section of the Client Configuration web page:

- 1. Warm Start** This link will bring up a popup window that can be used to initiate a Warm Start procedure with the designated Client. It is first necessary to select the Cryptographic algorithm AES or DES. Use of DES is strongly discouraged in that it provides only illusionary security.
- 2. Rekey/Erase** This link will bring up a popup window that can be used to send keys to the designated Client. In the Key Fill modes, it is not necessary to set the TEK mod MAC key windows. For OTAR it is necessary to set both the TEK and MAC Keys as well as the algorithm. The two keys can be set to a key that it is known that the designated Client possesses. For the first rekey after a successful Warm Start, the Warm Start key can be used. The Warm Start key can only be use once.

3. Inventory This link will bring up a popup window that can be used to run a number of Inventory types primarily in the Keyfill Send mode. Many major radio types only support a very limited number of Inventory types. If Inventory is used for OTAR, both the TEK and MAC keys must be set as well as the algorithm.

4. Zeroize Zeroize can be used to erase all Cryptographic keys in the designated Client. If Zeroize is used for OTAR, both the TEK and MAC keys must be set as well as the algorithm. Zeroizing using one algorithm will result in erasure of all keys from both algorithms.

5. Set MNP This link will bring up a popup window that can be used to set the Message Number Period for OTAR operations in the designated Client. If Set MNP is used for OTAR, both the TEK and MAC keys must be set as well as the algorithm.

6. Change RSI This link will bring up a popup window that can be used to change the Radio Set Identifier for the designated Client. If Change RSI is used for OTAR, both the TEK and KEY keys must be set as well as the algorithm.

7. Hello Message This link will bring up a popup window that can be used to send a Hello Message the designated Client. Both the TEK and MAC keys must be set as well as the algorithm.

8. Key Summary This link will bring up a popup window that shows the current status of all keys assigned to the designated Client.

9. Status This link will bring up a popup window that shows the current status of all Key Fill and OTAR actions with the designated Client. This window is overwritten at the completion of each operation and therefor only display the most recent completed operation.

10. Key Set Changeover This link will bring up a popup window to send a command to change the active key set in the designated Client. If Key Set Changeover is used for OTAR, both the TEK and MAC keys must be set as well as the algorithm.

11. Radio Enable/Disable This is a placeholder for an OTAR encrypted Radio Enable/Disable function that is planned for addition to the TKMD in the future.

Detailed Manual OTAR/Key Fill Descriptions The following sections describe use of the Manual OTAR/Key Fill features of the TKMD. It is highly recommended that the Crypto Officer open the “Status” window and leave it open on the computer Desktop. The “Status” Window will provide the confirmation messages for the Crypto Officer to use in executing Manual OTAR/Key Fill operations. For a more detailed view of what is transpiring in Manual OTAR/Key Fill (and other) operations, the Crypto Officer can enable the RS-232 port to be “Debug” on the Board Configuration web page, connect a RS-232 Terminal emulation (Example RS-232 -> USB adapter with the baud rate set to 115,200 with Tera Term) and view step-by-step status Debug messages.

Warm Start Details The following view shows the result of an AES Warm Start with Client 10.

OTAR Subscriber Configuration

Warm Start Subscriber Unit
TKMD is about to send a Warm Start Traffic Key to the Client Unit.
AES 256
Confirm Cancel

Client Summary *Changes Must Be Saved to Client Record!* [Home](#)

| | | | | | |
|-----------------------------------|---------------|--------------------|------------------------------|--|----------------------------------|
| OTAR KMF Packet | | Client = 10 | ALGORITHM: AES 256 | UTC: 1608301475804 | Friday December 18 2020 09:24:35 |
| ENTER CLIENT NUMBER | | ENTER CLIENT LLID | TEK KEY: WS | Procedures | |
| ENTER CLIENT RSI | | ACTION | MAC KEY: WS | Key Summary Warm Start Rekey/Erase Inventory Zeroize Set MNP Change RSI Hello Message | |
| 12345 Unit RSI MN= 42 | 12345 Unit ID | 0 Group RSI MN= 0 | 16 AES CKEK | 14 DES CKEK | |
| KNG VHF 1 Name | | 9999999 KMF RSI | 15 AES UKER | | |
| Christine Wirel Org | | 0 KVL RSI | | | |
| Test Group | | | | | |
| None Key Data Set: Source Key = 0 | | Key Name | Algorithm | | |
| Client Key = 0 | | Key Name | Algorithm | | |
| None Client Key Action | | Re-Name Key | Key Set ID | | |

Status — Mozilla Firefox

KMF/KFD Status [Close](#)

Rekey Ack to Msg = 32

1 ALG= AES 256 KID(h)FEDC Stat= 0 KS= 1 WS Key Found = 0

The steps involved in achieving this result are:

1. Set the TKMD Operating mode in KMF mode consistent with the Base Station to be used, in this case a Codan DFSI Packet Data unit. Use of Automatic OTAR is recommended.
2. Select the Client to be used in the Client Configuration Yellow Background second column.
3. Open the “Status” popup window and place it at a convenient location on the Desktop.
4. Turn on the Client radio so that it can OTAR-Register with the TKMD KMF.
5. Select the desired algorithm in the Yellow Background third column.
6. Open the Warm Stop popup window.
7. Click Confirm on the Warm Start popup window to initiate Warm Start.
8. If the Warm Start procedure is successful, the Client radio will send back a message encrypted with the random number key sent to the Client in the Warm Start message. If this return message

Rekey/Erase Details Using a Warm Start Key in OTAR KMF Mode To utilize the Warm Start key established in the previous example, the Crypto Officer must select the Warm Start key for both the TEK and MAC.

Select Auto Select in the TEK Key menu. Then select Warm Start Key in the TEK Key menu. Repeat these two steps in the MAC Key menu. Use the Rekey/Erase link in the Yellow Background column 4 to open the Key Selection popup menu shown below.

The pulldown menu is used to select which keyset to use and the individual actions desired for that key set are selected using the radio buttons for each key. In this example three AES keys from Key Set 1 have been selected for rekey.

OTAR Subscriber Configuration

Key Selection — Mozilla Firefox

https://192.168.1.208/protect/keyselect.htm

None

AES 256

Select Keys: Key Set = 1

KS = 1 Key = AES-TEK1---- ☒ None ☐ Rekey ☐ Erase

KS = 1 Key = AES-TEK2---- ☒ None ☐ Rekey ☐ Erase

KS = 1 Key = AES-TEK3---- ☒ None ☐ Rekey ☐ Erase

Select Keys Cancel

IC_No=0 90%

Home

UTC: 1608304399193 Friday December 18 2020 10:13:19

Procedures

Warm Start
Rekey/Erase
Inventory
Zeroize
Set MNP
Change RSI
Hello Message

Key Summary
Status
Key Set Changeover
Radio Enable/Disable

16 AES CKEK 14 DES CKEK

15 AES UKER 13

Status — Mozilla Firefox

https://192.168.1.208/protect/status_msg.htm

KMF/KFD Status Close

Rekey Ack to Msg = 19

1 ALG= AES 256 KID(h)0003 Stat= 0 KS= 1 Item Found 4
2 ALG= AES 256 KID(h)0004 Stat= 0 KS= 1 Item Found 5
3 ALG= AES 256 KID(h)0001 Stat= 0 KS= 1 Item Found 6

From the “Status” window it can be confirmed that the Client replied back that the Rekey was successfully completed with all three keys for Key Set 1 having been updated.

If an OTAR Rekey operation not using a Warm Start key was to be performed, the TEK and MAC keys must be set. The TEK and MAC key selection menus show which keys of the selected algorithm are known to have been previously loaded in the selected Client radio and are therefore available for OTAR Rekey use. The TEK and MAC keys may be set the same key, but this is not a requirement.

If Rekey is to be performed in Key Fill mode, change the TKMD Operation Mode to Key Fill Send and connect the Client radio to the TKMD Key Fill port with an appropriate cable. For Rekey and other operations in Key Fill Send mode it is not necessary to set the TEK or MAC Keys.

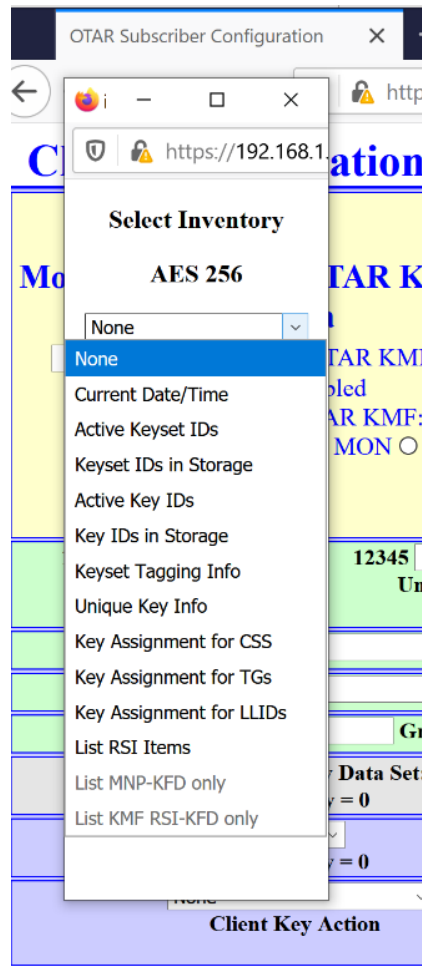
Key Summary The link in the Yellow Background fifth column can be used to bring up the Client Key Summary popup web page for the selected Client:

Client Key Summary Client = 10 [Close](#)

| Key Expired | Key Established | Key Provisioned | Key Erased |
|----------------------|-----------------|-----------------|------------|
| Key CRC Error | | | |
| Key Reference Error | | | |
| Key Number | Alg | Keyset No. | Key ID(h) |
| Key #1 | DES OFB | 1 | 50 |
| Key #2 | DES OFB | 1 | 51 |
| Key #3 | DES OFB | 1 | 52 |
| Key #4 | AES 256 | 1 | 81 |
| Key #5 | AES 256 | 1 | 82 |
| Key #6 | AES 256 | 1 | 83 |
| Key #7 | DES OFB | 2 | 50 |
| Key #8 | DES OFB | 2 | 51 |
| Key #9 | DES OFB | 2 | 52 |
| Key #10 | AES 256 | 2 | 81 |
| Key #11 | AES 256 | 2 | 82 |
| Key #12 | AES 256 | 2 | 83 |
| Key #13 | DES OFB | 255 | 61440 |
| Key #14 | DES OFB | 255 | 61441 |
| Key #15 | AES 256 | 255 | 61442 |
| Key #16 | AES 256 | 255 | 61443 |

This page will display the key parameters for all keys (up to 60) assigned to the selected Client. The displayed color of the individual key changes with the current key status as denoted in the legend near the top of the page. In this case, all 16 assigned keys are Green which means that all 16 keys have been loaded as confirmed by the selected Client. After a Rekey or other OTAR/Key Fill operation it may be useful to view the Client Key Summary web page to confirm that the intended actions have taken place. If the page is open, the contents of the popup page are automatically updated once every 30 seconds to ensure the page displays the current status of the Client keys.

Inventory Details Use the link to Inventory to bring up a popup window for Inventory.



The above list shows all possible Inventory requests supported by the TKMD. Be aware that, depending on the manufacturer, Project 25 Client Radios may only support a small subset of this list and therefore a specific Inventory request may fail on a given radio type.

As an example, Client 10 did not respond to an OTAR Inventory Active Key IDs but did respond to Inventory List RSI Items:

OTAR Subscriber Configuration

https://192.168.1.208/protect/clientconfig.htm?Sel_MAC_No=1

Client Summary *Changes Must Be Saved to Client Record!* Home

Select Inventory

AES 256

List RSI Items

Run Inventory

Close

Client = 10

ENTER CLIENT NUMBER

ENTER CLIENT LLID

ENTER CLIENT RSI

ACTION

ALGORITHM: AES 256

TEK KEY: 4

MAC KEY: 4

UTC: 1608307829678

Friday December 18 2020 11:10:29

Procedures

Key Summary Status

Key Set Changeover

Radio Enable/Disable

Warm Start

Rekey/Erase

Inventory

Zeroize

Set MNP

Change RSI

Hello Message

12345 Unit ID

Group RSI MN= 0

Name

Org

Group

Data Set: = 0

Key Name

Key Name

Re-Name Key

Client Key Action

Status — Mozilla Firefox

https://192.168.1.208/protect/status_msg.htm

KMF/KFD Status Close

Message Rx-Client = 10 List RSI Items Resp

RSI Inv-Client = 12345 Indiv. MN = 57

In general, Client radios will respond to more Inventory request types in Key Fill Send mode than in OTAR mode.

Zeroize The link in the Yellow Background section fourth column can be used to bring up the Zeroize popup window.

The screenshot shows the 'OTAR Subscriber Configuration' web interface. A 'Zeroize Subscriber Unit' popup is displayed, asking for confirmation to zeroize the client unit. The main interface includes a 'Client Summary' section with a yellow background, a 'Procedures' section with a yellow background, and a 'Key Summary' section with a yellow background. The 'Client Summary' section contains fields for 'Client = 10', 'ENTER CLIENT NUMBER', 'ENTER CLIENT LLID', 'ENTER CLIENT RSI', and 'ACTION'. The 'Procedures' section contains links for 'Warm Start', 'Rekey/Erase', 'Inventory', 'Zeroize', 'Set MNP', 'Change RSI', and 'Hello Message'. The 'Key Summary' section contains links for 'Key Summary', 'Status', 'Key Set Changeover', and 'Radio Enable/Disable'. A status message at the bottom right indicates 'Message Rx-Client = 10 Zeroize Resp'.

Zeroize Subscriber Unit
TKMD is about to completely zeroize the Client Unit.
Are You sure?
AES 256
[Confirm](#) [Cancel](#)

Client Summary *Changes Must Be Saved to Client Record!* [Home](#)

Client = 10
ENTER CLIENT NUMBER
ENTER CLIENT LLID
ENTER CLIENT RSI
ACTION

Procedures
[Warm Start](#)
[Rekey/Erase](#)
[Inventory](#)
[Zeroize](#)
[Set MNP](#)
[Change RSI](#)
[Hello Message](#)

Key Summary
[Key Summary](#)
[Status](#)
[Key Set Changeover](#)
[Radio Enable/Disable](#)

UTC: 1608388671104
Saturday December 19 2020 09:37:51

Unit RSI MN= 57
Unit ID 12345
Group RSI MN= 8
KMG VHF 1 Name
Christine Wirel Org
Test Group
Key Data Set: Source Key = 0
Client Key = 0
Client Key Action

Key Name
Key Name
Re-Name Key

KMF/KFD Status [Close](#)
Message Rx-Client = 10 Zeroize Resp

After Client Zeroization all keys assigned to the Client will be Red on the Client Key Summary.

The screenshot shows the 'Client Key Summary' web interface for Client = 10. The table displays a list of keys with columns for Key Number, ALG, Keyset No., SLN(d), Key ID(h), and Key Name. The keys are categorized by status: Key Expired (yellow), Key Established (green), Key Provisioned (green), and Key Erased (red). The table shows 16 keys, with the first 12 keys being Key Erased (red) and the last 4 keys being Key Established (green).

| Key Number | ALG | Keyset No. | SLN(d) | Key ID(h) | Key Name |
|------------|---------|------------|--------|-----------|----------|
| Key #1 | DES OFB | 1 | 50 | 0003 | DES TEK1 |
| Key #2 | DES OFB | 1 | 51 | 0004 | DES TEK2 |
| Key #3 | DES OFB | 1 | 52 | 0001 | DES TEK3 |
| Key #4 | AES 256 | 1 | 81 | 0003 | AES TEK1 |
| Key #5 | AES 256 | 1 | 82 | 0004 | AES TEK2 |
| Key #6 | AES 256 | 1 | 83 | 0001 | AES TEK3 |
| Key #7 | DES OFB | 2 | 50 | 0003 | DES TEK1 |
| Key #8 | DES OFB | 2 | 51 | 0004 | DES TEK2 |
| Key #9 | DES OFB | 2 | 52 | 0001 | DES TEK3 |
| Key #10 | AES 256 | 2 | 81 | 0003 | AES TEK1 |
| Key #11 | AES 256 | 2 | 82 | 0004 | AES TEK2 |
| Key #12 | AES 256 | 2 | 83 | 0001 | AES TEK3 |
| Key #13 | DES OFB | 255 | 61440 | F5A0 | DES UKEK |
| Key #14 | DES OFB | 255 | 61441 | F5A1 | DES CKEK |
| Key #15 | AES 256 | 255 | 61442 | F5A0 | AES UKEK |
| Key #16 | AES 256 | 255 | 61443 | F5A1 | AES CKEK |

Set MNP (Message Number Period) The link in the Yellow Background section fourth column can be used to bring up a popup window to set the select Client MNP. As noted on the popup menu, this feature is only applicable to Key Fill Send operation.

Tactical Key Management Device x OTAR Subscriber Configuration x +

https://192.168.1.208/protect/clientconfig.htm?UTC=1608393114780 90%

Client Configuration

[Client Summary](#) *Changes Must Be Saved to Client Record!* [Home](#)

| | | | | |
|---|---|------------------------------------|--|---------------------------------------|
| Mode = Keyfill Send <input type="text"/> SLIP Mode off-UART enabled for debug Automatic OTAR KMF: ON <input type="radio"/> OFF <input type="radio"/> MON <input type="radio"/> | Client = 10 ENTER CLIENT NUMBER <input type="text"/> ENTER CLIENT LLID <input type="text"/> ENTER CLIENT RSI <input type="text"/> ACTION <input type="button"/> | ALGORITHM: AES 256 | UTC: 1608393335752 | Saturday December 19 2020 10:55:35 |
| | | TEK KEY: 4 <input type="text"/> | Procedures Warm Start Rekey/Erase Inventory Zeroize Set MNP Change RSI Hello Message | |
| | | MAC KEY: 4 <input type="text"/> | | |

| | | | |
|------------------|-------------------------|----------------|----------------|
| 12345 Unit ID | 0 Group RSI MN= 8 | 16 AES CKEK | 14 DES CKEK |
|------------------|-------------------------|----------------|----------------|

Reset Message Number Period
TKMD is about to reset the MNP on the Client Unit.
Key Fill Send Only
500 Confirm
Message Number Period
[Cancel](#)

| | |
|--------------------------------|----------------------------------|
| <input type="text"/> Name | 9999999 KMF RSI |
| <input type="text"/> Org | 0 KVL RSI |
| <input type="text"/> Group | |
| <input type="text"/> Data Set: | <input type="text"/> Key Name |
| 0 | <input type="text"/> Key Name |
| 0 | <input type="text"/> Re-Name Key |
| <input type="text"/> | |

KMF/KFD Status [Close](#)
Message Rx-Client = 10 KFD Load Config Response:
KMF RSI = 9999999 MNP = 500 Status = 0

Change RSI The link in the Yellow Background section fourth column can be used to bring up a popup window to change the Radio Set Identifier of the selected Client. This may be done in Key Fill Send or in OTAR modes.

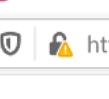
The screenshot displays the 'OTAR Subscriber Configuration' web interface. A 'Change Radio Set Identifiers' popup window is open, showing fields for 'Indiv', 'Select RSI Type', 'Client Group RSI = 0', 'Client Indiv RSI = 12345', 'Client KMF RSI = 9999999', and 'Enter New RSI'. The main interface has a yellow background and contains several sections:

- Client Summary:** Includes 'Client = 10', 'ENTER CLIENT NUMBER', 'ENTER CLIENT LLID', 'ENTER CLIENT RSI', and an 'ACTION' button.
- Procedures:** A list of links including 'Warm Start', 'Rekey/Trase', 'Inventory', 'Zeroize', 'Set MNP', 'Change RSI', and 'Hello Message'.
- Key Data Set:** A table with columns for 'Unit RSI', 'Unit ID', 'Group RSI', 'Key Name', and 'Re-Name Key'.
- Key Data Set:** A table with columns for 'Unit RSI', 'Unit ID', 'Group RSI', 'Key Name', and 'Re-Name Key'.

A 'Status' window is also open, showing 'KMF/KFD Status' and 'Message Rx-Client = 10'.

In this example a change from the currently assigned RSI to the same RSI value was done to demonstrate the process. Changing a Client RSI to a new value could prove to be disruptive to the OTAR operation for the Client if corresponding changes to the Client TKMD data record are not manually applied by the Crypto Officer.

Hello Message The link in the Yellow Background section fourth column can be used to bring up a popup window to send a Hello Message to the KMF when the TKMD is operating as a Client for that KMF. This is generally used to request a full rekey from the KMF.



Key Set Changeover The link in the Yellow Background section fourth column can be used to bring up a popup window to change the active Key Set in the selected Client.

Chang... — □ ×

OTAR Subscriber Configuration × +

https://192.168.1.208/protect/clientconfig.htm?UTC=1608393542837 90%

Client Summary *Changes Must Be Saved to Client Record!* [Home](#)

| | | | | | | | |
|--|--|---|--|---|--|--|--|
| Key Set Changeover KS1 to KS2 <input type="button" value="submit"/> | | Client = 10 ENTER CLIENT NUMBER <input type="text"/> ENTER CLIENT LLID <input type="text"/> ENTER CLIENT RSI <input type="text"/> ACTION | | ALGORITHM: <input type="text"/> AES 256 | | UTC: 1608397437891 Saturday December 19 2020 12:03:57 | |
| R KMF Packet | | | | TEK KEY: 4 <input type="text"/> | | Procedures Warm Start Rekey/Erase Inventory Zeroize Set MNP Change RSI Hello Message | |
| R KMF DFSI Packet | | | | MAC KEY: 4 <input type="text"/> | | Key Summary Status Key Set Changeover Radio Enable/Disable | |
| KMF: ON <input type="radio"/> | | | | | | | |
| 12345 <input type="text"/> Unit RSI MN= 0 | 12345 <input type="text"/> Unit ID | 0 <input type="text"/> Group RSI MN= 8 | 16 <input type="text"/> AES CKEK | 14 <input type="text"/> DES CKEK | | | |
| KNG VHF 1 <input type="text"/> Name | | 9999999 <input type="text"/> KMF RSI | | | | | |
| Christine Wirel <input type="text"/> Org | | 0 <input type="text"/> KVL RSI | | | | | |
| Test <input type="text"/> Group | | | | | | | |
| None <input type="button" value="Key Data Set: Source Key = 0"/> | | Key Name | | | | | |
| <input type="text"/> Client Key = 0 | | Key Name | | | | | |
| None <input type="button" value="Client Key Action"/> | | Re-Name Key | | | | | |

Status — Mozilla Firefox

https://192.168.1.208/protect/status_msg.htm

KMF/KFD Status [Close](#)

Message Rx-Client = 10 Changeover Response

Changeover Item = 0 Supercd KS = 0 Activ KS = 1
 Changeover Item = 1 Supercd KS = 1 Activ KS = 2

Key Fill Send If the TKMD Operational Mode is set to Key Fill Send, the TKMD can be used to configure and send key Material to any Project 25 compliant Client. Fill is done by connecting an appropriate cable to the Key Fill Connector on the front panel of the TKMD.

OTAR Subscriber Configuration

Client Configuration Client Summary Changes Must Be Saved to Client Record! Home

Mode = Keyfill Send
SLIP Mode off-UART
enabled for debug
Automatic OTAR KMF:
ON OFF MON

Client = 10
ENTER CLIENT NUMBER
ENTER CLIENT LLID
ENTER CLIENT RSI
ACTION

12345 Unit RSI MN= 1
12345 Unit ID
0 Group RSI MN= 8
16 AES CKEK
14 DES CKEK
KMG VHF 1 Name
Christine Wirel Org
Test Group
None Key Data Set: Source Key = 0
Client Key = 0
None Client Key Action
9999999 KMF RSI
0 KVL RSI
15 AES UKEK
13 DES UKEK
Enter Client Data
Key Name Algorithm SLN(d) KID(h)
Key Name Algorithm SLN(d) KID(h) FEDC
Re-Name Key Key Set ID Re-Assign SLN Re-Assign KID(h)

ALGORITHM: UTC: 1608585061755
Monday December 21 2020 16:11:01
Procedures
Warm Start
Rekey/Erase
Inventory
Zeroize
Set MNP
Change RSI
Hello Message
Key Summary
Status
Key Set Changeover
Radio Enable/Disable

In Key Fill modes it is not necessary to set the TEK or MAC key in that Key Fill is done unencrypted. The following several examples demonstrate some of the Key Fill Send procedures.

Inventory The following shows the result of Key Fill Send: Inventory: Active Key IDs.

OTAR Subscriber Configuration

Client Configuration Client Summary Changes Must Be Saved to Client Record! Home

Mode = Keyfill Send
SLIP Mode off-UART
enabled for debug
Automatic OTAR KMF:
ON OFF MON

Client = 10
ENTER CLIENT NUMBER
ENTER CLIENT LLID
ENTER CLIENT RSI
ACTION

12345 Unit RSI MN= 1
12345 Unit ID
0 Group RSI MN= 8
16 AES CKEK
14 DES CKEK
KMG VHF 1 Name
Christine Wirel Org
Test Group
None Key Data Set: Source Key = 0
Client Key = 0
None Client Key Action
9999999 KMF RSI
0 KVL RSI
15 AES UKEK
13 DES UKEK
Enter Client Data
Key Name Algorithm SLN(d) KID(h)
Key Name Algorithm SLN(d) KID(h) FEDC
Re-Name Key Key Set ID Re-Assign SLN Re-Assign KID(h)

ALGORITHM: UTC: 1608585868022
Monday December 21 2020 16:24:28
Procedures
Warm Start
Rekey/Erase
Inventory
Zeroize
Set MNP
Change RSI
Hello Message
Key Summary
Status
Key Set Changeover
Radio Enable/Disable

Select Inventory
Active Key IDs
Run Inventory
Close

Status - Mozilla Firefox
https://192.168.1.208/protect/status_msg.htm
KMF/KFD Status Close
Message Rx-Client = 10 KFD Key Inv Resp
1 KS 255 SLN(d) 61442 ALG AES 256 KID(h) F5A0
2 KS 255 SLN(d) 61443 ALG AES 256 KID(h) F5A1
3 KS 255 SLN(d) 61440 ALG DES OFB KID(h) F5A0
4 KS 255 SLN(d) 61441 ALG DES OFB KID(h) F5A1
5 KS 1 SLN(d) 50 ALG DES OFB KID(h) 0003
6 KS 1 SLN(d) 51 ALG DES OFB KID(h) 0004
7 KS 1 SLN(d) 52 ALG DES OFB KID(h) 0001
8 KS 1 SLN(d) 81 ALG AES 256 KID(h) 0003
9 KS 1 SLN(d) 82 ALG AES 256 KID(h) 0004
10KS 1 SLN(d) 83 ALG AES 256 KID(h) 0001

Note that only keys in the Active Key Set (Key Set 1) and KEKs are returned. There are keys in Key Set 2 but the Active Key Set must be changed to 2 for them to be displayed.

Rekey The following shows the result of a Key Fill Send: Rekey: Rekey all Key Set 1 AES Keys.

OTAR Subscriber Configuration

https://192.168.1.208/protect/clientconfig.htm?Sel_ENC_Al

Client Configuration

[Client Summary](#) *Changes Must Be Saved to Client Record!* [Home](#)

| | | | | |
|--|--|-----------------------|--|---|
| Mode = Keyfill Send <div>SLIP Mode off-UART enabled for debug Automatic OTAR KMF: ON <input type="radio"/> OFF <input type="radio"/> MON <input type="radio"/></div> | Client = 10 ENTER CLIENT NUMBER ENTER CLIENT LLID ENTER CLIENT RSI | ALGORITHM: AES 256 | UTC: 1608586861723 | Monday December 21 2020 16:41:01 |
| | | TEK KEY: 255 | Procedures Warm Start Rekey/Erase Inventory Zeroize Set MNP Change RSI Hello Message | Key Summary Status Key Set Changeover Radio Enable/Disable |
| | | MAC KEY: 255 | | |
| | | AES CKEK | 14 | DES CKEK |
| | | AES UKFK | 13 | DES UKFK |

Key Selection — Mozilla Firefox

https://192.168.1.208/protect/keyselect.htm

None AES 256

Select Keys: Key Set = 1

KS = 1 Key = AES-TEK1---- ☐ None ☒ Rekey ☐ Erase

KS = 1 Key = AES-TEK2---- ☐ None ☒ Rekey ☐ Erase

KS = 1 Key = AES-TEK3---- ☐ None ☒ Rekey ☐ Erase

Select Keys Cancel

Status — Mozilla Firefox

https://192.168.1.208/protect/status_msg.htm

KMF/KFD Status [Close](#)

Rekey Ack to Msg = 19

1 ALG= AES 256 KID(h)0003 Stat= 0 KS= 1 Item Found 4
2 ALG= AES 256 KID(h)0004 Stat= 0 KS= 1 Item Found 5
3 ALG= AES 256 KID(h)0001 Stat= 0 KS= 1 Item Found 6

Key Fill Receive In Key Fill Receive mode, a Project 25 Key Fill Device can be connected to the TKMD Key Fill Connector to load key material from the KFD into Client 0, the TKMD. In this example, a KVL-3000+ is used to load 4 keys into the TKMD.

The screenshot displays three overlapping web browser windows from the OTAR Subscriber Configuration system.

Client Configuration Window: The main window shows configuration for Client = TKMD. It includes fields for Mode (Keyfill Receive), Client Number, LLID, and RSI. It also displays the Algorithm (AES 256), TEK Key (255), and MAC Key (255). A list of procedures is available, including Warm Start, Rekey/Erase, Inventory, Zeroize, Set MNP, Change RSI, and Hello Message.

Client Key Summary Window: This window shows a table of keys loaded into the client. The table has columns for Key Number, ALG, Keyset No, SLN(d), Key ID(h), and Key Name.

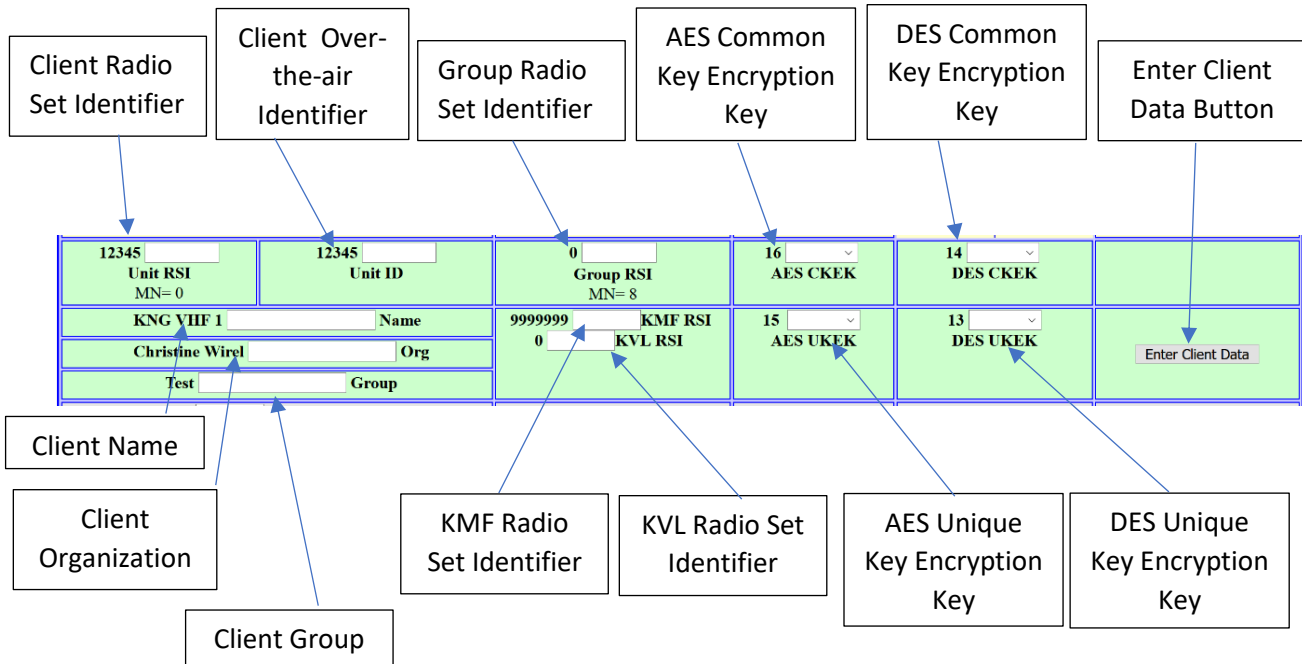
| Key Number | ALG | Keyset No | SLN(d) | Key ID(h) | Key Name |
|------------|---------|-----------|--------|-----------|----------|
| Key #1 | AES 256 | 2 | 1 | 0001 | |
| Key #2 | AES 256 | 2 | 2 | 0002 | |
| Key #3 | AES 256 | 2 | 777 | 0036 | |
| Key #4 | AES 256 | 255 | 62001 | 1003 | |

Status Window: This window displays the KMF/KFD Status, showing incoming messages and actions. The status indicates that the client has been updated with AES Modify Key CMD Key Set ID = 255.

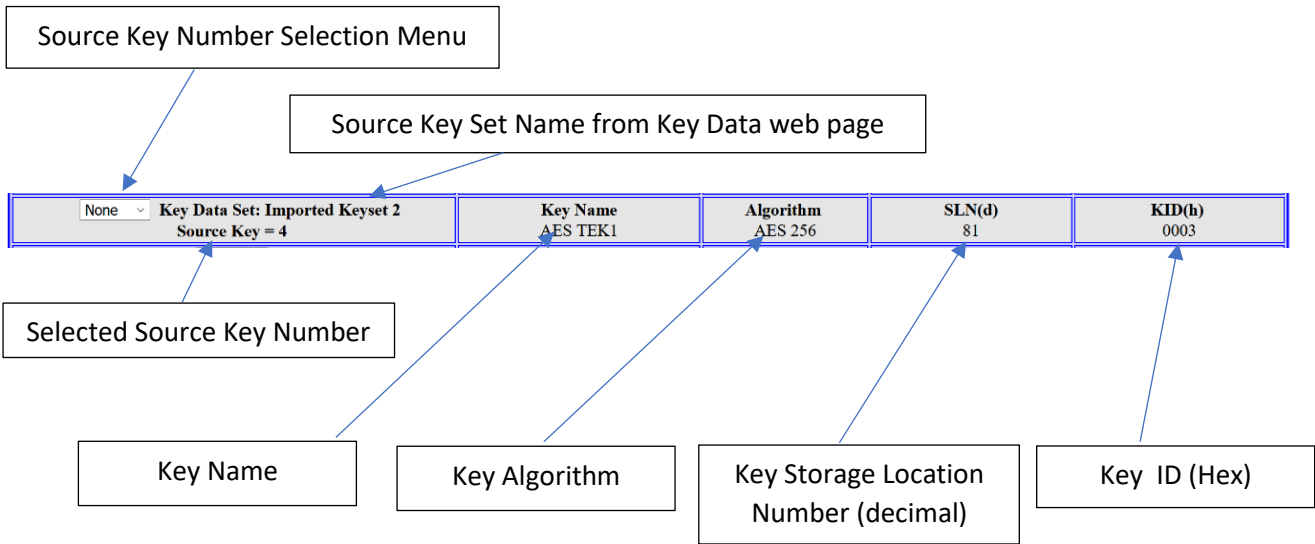
Item= 1 SLN(d)= 62001 KID(h)= 1003 Action= R

Since the “Status” window only displays the last Client response and the KFD sends the keys one at a time, only the last key sent appears in this window.

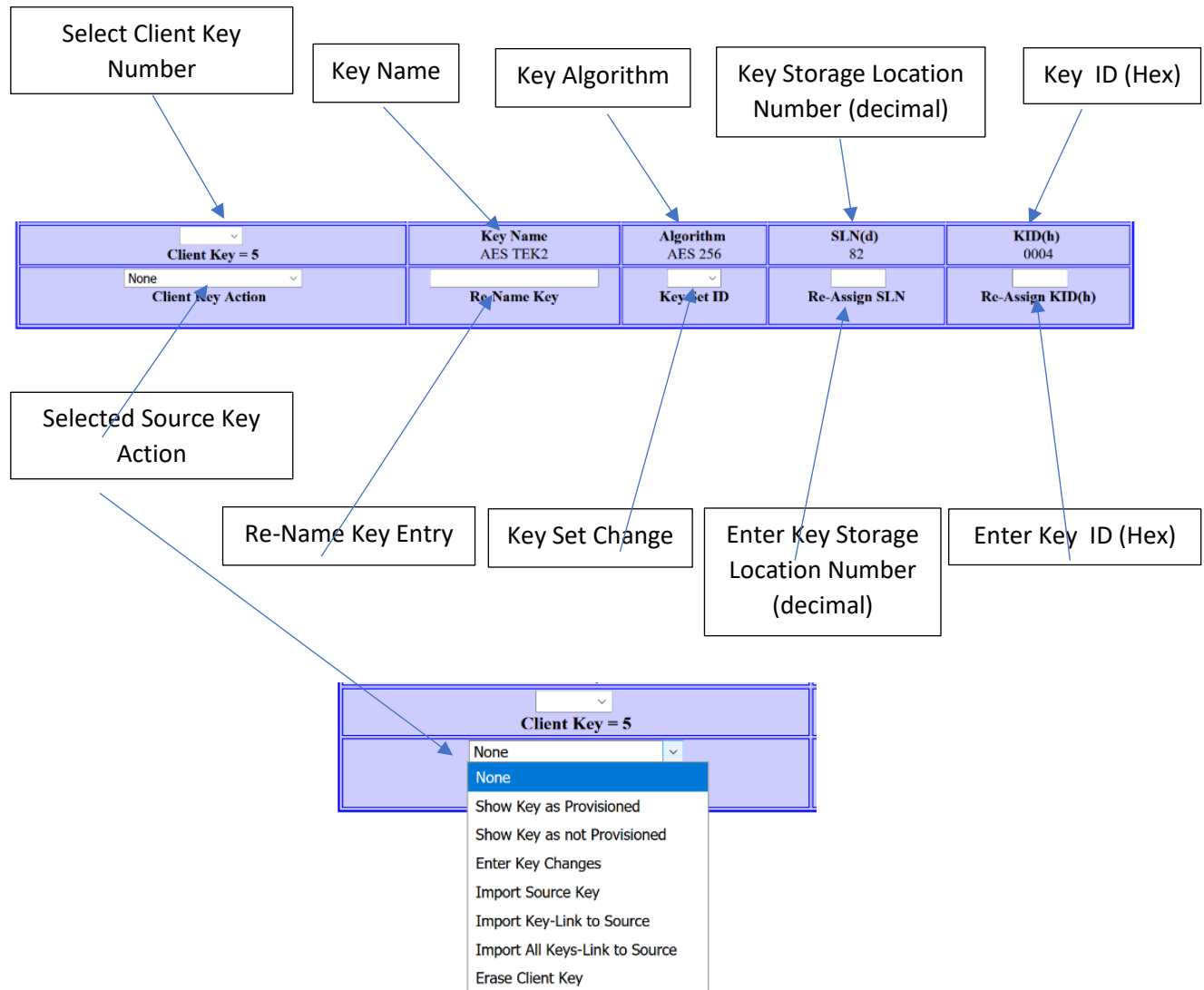
Selected Client Configuration The Green Background section of the Client Configuration web page is for the display and entry of parameters specific to the selected Client.



Source Key Selection The Gray Background section of the Client Configuration web page allows for the selection and display of Source Key parameters for a selected key from the key set selected on the Key Data web page.



Client Key The Blue Background section allows the selection modification and transfer of specific key parameters/key material for the selected Client.



The Actions that can be selected are:

1. Show Key as Provisioned tells the TKMD that it should mark that key as having been loaded in the selected Client.
2. Show Key as not Provisioned tells the TKMD that it should mark that key as not yet loaded in the selected Client.
3. Enter Key Changes instructs the TKMD to enter the changes to the key as determined by the entry windows.
4. Import Source Key copies the Source key and any entered changes into the selected Client key location.
5. Import Key-Link to Source imports the key along with any external key reference.
6. Import All Keys-Link to Source is a placeholder for a future capability.
7. Erase Client Key completely erases the Client key.

File Up/Down Load The File Up/Down Load web page is used to upload firmware as well as uploading configuration files. It is also used to download configuration and log files.

Tactical Key Management Device

Christine Wireless, Inc
Ellicott City Maryland
410-961-7331
www.christinewireless.com

Tactical Key Management Device

File Upload/Download

File Type:

File: No file selected.

No File Type Selected Restart TKMD after successful Message Digest Upload to complete firmware update

Export File Enable:

Enable download of current TKMD Log or Client CSV File over USB and Download to export.

LLID File Request

Firmware updates are uploaded to the TKMD using this page. First select the file type from the menu then locate the file using the "Browse" button. When the file to be uploaded is selected, use the "Upload" button to initiate the upload. The status of the upload will be displayed above the Message Digest browse box.

A Message Digest (MD) file must be uploaded after uploading the Firmware file. The Message Digest file extension must be "mdh" and the file name must match the name of the previously uploaded file. If the MD File does not match the MD calculated using the content of the Firmware File, the update will not be executed.

WARNING: Do not navigate away from the Upload page during the upload process as this will disrupt the upload requiring starting over. Please wait for the TKMD to complete the reprogramming of the internal flash memory before disconnecting power to the TKMD. Failure to heed this warning may result in damaging the internal firmware and require returning the TKMD to the manufacturer for reprogramming.

Copyright © 2012-2021 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

Upload File Type Selection TKMD Firmware and Message Digest are used to upload and install new TKMD firmware and Client CSV is used to upload a Client Configuration as an Excel Comma Separated Variable file.

File Type:

File:

No File Type Selected

Export File

Enable download of current

Firmware Upload/Installation The following steps are required to upload and install new firmware in the TKMD:

1. Select “TKMD Firmware” in the File Type menu. “File Type Selected” will appear below the “Browse” button.
2. Click Browse and locate and select the TKMD Firmware to be installed. The name of the firmware will appear to the right of the “Browse” button. The file name extension on TKMD Firmware is hex.
3. Click the “Upload” button to start the file upload. The upload will take less than a minute but the Crypto Officer must be patient at this point and wait for the file upload to finish.
4. When the upload is finished the message “MD Calculated-Enter Correct MD” will appear below the “Browse” button. In the event that a “501” error message appears use the browser left arrow button to return to the previous web page view and click on the File Up/Down Load button on the left side of the web page. The “MD Calculated-Enter Correct MD” message should now appear below the “Browse” button.
5. Use the File Type menu and select Message Digest. The message “MD Selected, upload matching name file with .mdh extension” will appear below the “Browse” button.
6. Click the “Browse” button and navigate to and select the file with the extension mdh.
7. The name of the Message Digest file will appear to the right of the “Browse” button. The file name will be the same as the TKMD Firmware file name except for the extension being mdh instead of hex.
8. Click the “Upload” button to upload the Message Digest file.
9. The message “MD Checks-Update Enabled” will appear below the “Browse” button. In the event that a “501” error message appears use the browser left arrow button to return to the previous view and click on the File Up/Down Load button on the left side of the web page. The “MD Checks-Update Enabled” message should now appear below the “Browse” button.
10. Click the “Restart TKMD” button to complete the firmware installation. At this point the Red LED on the TKMD will flash periodically until the TKMD is done installing the new firmware. The TKMD will then restart using the newly installed firmware.

Client CSV Upload To upload a Client CSV file:

1. Use the File Select menu and select Client CSV.
2. “File Type Selected” will appear below the “Browse” button.
3. Use the “Browse” button to navigate to the client configuration csv file.
4. The name of the csv file will appear to the right of the “Browse” button.
5. Click upload to upload the csv file.

The csv file will be stored in flash memory in the TKMD. On the next startup of the TKMD, the Client configuration contained in the csv file will be installed. Care must be taken in constructing the csv file in that the TKMD will overwrite existing Client files if that action is indicated in the csv file.

File Export The File Type to be exported is selected in the middle part of the File Up/Down Load web page.

| | |
|-----------------------|--|
| Client Configuration | Export File Enable: Download_Disabled |
| File Up/Down Load | Enable download of: Download_Disabled |
| File Share | Request: <input type="text"/> |
| Network Configuration | Firmware updates: Download Latest Client CSV |
| Board Configuration | locate the file using: Download 2nd Oldest Client CSV |
| Remote Configuration | button to initiate the: Download 3rd Oldest Client CSV |
| | box. Download 4th Oldest Client CSV |
| | A Message Digest (MD): Download 5th Oldest Client CSV |
| | extension must be: Download 6th Oldest Client CSV |
| | MD File does not match: Erase All Client CSV |
| | executed. |

All Downloads are done to through the TKMD USB port. If is a good idea to disable other use of the USB port using the Board Configuration web page. This will prevent the presence of unwanted V.24 I/O etc. data in the Download file. Open a Tera Term window with the TKMD USB port connected and enable log in the Tera Term controls prior to initiating a Download.

Download Log will set up the Download of a Log File which is a cumulative summary of all significant events on the TKMD. The next 6 Download selections allow picking which version of the Client csv file is desired. On each restart of the TKMD, a new copy of the csv Client file is created and stored. Erase All Client CSV erases all stored copies.

Click the “Download” button to initiate the USB Download of the selected file or csv file erasure.

After the Download is completed, save the Tera Term log file as a .csv or .txt file to preserve the Download contents.

LLID Request The final feature of the File Up/Down Load web page is the ability to locate a specific LLID (over-the-air Client ID) locally or in a network of TKMDs. This feature is used automatically if a Client with an unknown LLID attempts to OTAR-register with the TKMD KMF. In both the manual mode and automatic mode, if a LLID request is received (entered) into a TKMD, the TKMD will search its Client data base for that LLID. In the TKMD network case if that LLID is found, the file will be encrypted and sent over a TLSv1.2 secure IP connection back to the requesting TKMD.

Request LLID File Request

In the case of a manual LLID request, a message will appear under the Request LLID window indicating whether or not the LLID was found in the local Client data base.

Request LLID File Request
Client Found = 12

File Share The File Share web page is used to setup the sharing of Key Kettle files or Client files on a network of TKMDs.

TKMD
Christine Wireless, Inc.
Ellicott City Maryland
410-961-7331
www.christinewireless.com

Tactical Key Management Device

File Share

| Item | IP Address | MAC Address | Enable Share | Key File # | Key File ID | Export | Client Share |
|------|---------------|-------------------|----------------------------------|------------|-----------------|----------------------------------|-------------------------------|
| 1 | 192.168.1.204 | 04:91:62:2d:d1:e2 | <input checked="" type="radio"/> | 1 | 8000 | <input checked="" type="radio"/> | Start Client 10 Invalid Entry |
| 2 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 2 | 7000 | <input checked="" type="radio"/> | End Client 13 Invalid Entry |
| 3 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 3 | Not Set | <input type="radio"/> | Share Client Files |
| 4 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 4 | Not Set | <input type="radio"/> | |
| 5 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 5 | Not Set | <input type="radio"/> | |
| 6 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 6 | Not Set | <input type="radio"/> | |
| 7 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 7 | Not Set | <input type="radio"/> | |
| 8 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | 8 | Not Set | <input type="radio"/> | |
| 9 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | | Share Key Files | | |
| 10 | 0.0.0.0 | 00:00:00:00:00:00 | <input type="radio"/> | | | | |

Clear

Copyright © 2012-2021 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

In this example the TKMD is setup to share with one other TKMD located at 192.168.1.204. The TKMDs that are involved in the file share are set on the Network Configuration web page. If the share TKMD has been found on the IP network, the MAC Address for the remote TKMD will appear in the third column of the table. Radio buttons are used to enable which TKMD(s) to share with and also to designate which Key Kettle files to share. If it is desired to share Client files, the range of Client numbers is entered in the final column of the File Share table.

After setting up the File Share, click on “Share Key Files” or “Share Client Files” to initiate the file sharing.

Entries in the File Share can be cleared by clicking “Clear”

Network Configuration The TKMD IP Network and Share configuration is set using the Network Configuration web page.

Tactical Key Management Device

←

→

↺

🏠

🔒

https://192.168.1.208/protect/config.ht

80%

⋮

🔒

☆

TKMD

Christine Wireless, Inc.

Ellicott City Maryland

410-961-7331

www.christinewireless.com

Tactical Key Management Device

Network Configuration

Overview

Key Data

Key Assign

Client Summary

Client Configuration

File Up/Down Load

File Share

Network Configuration

Board Configuration

Remote Configuration

Battery Monitor

SNMP Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity.

| | | | | | | |
|----------------------|------------------------|----------------------------|----------------------------------|-----------------------|-----------------------|----------------------------------|
| Local TKMD | | | | | | |
| MAC Address: | 04:91:62:2d:d2:33 | | | | | |
| IP Address: | 192.168.1.208 | | | | | |
| Subnet Mask: | 255.255.255.0 | | | | | |
| Gateway: | 192.168.1.1 | | | | | |
| External IP Address: | 0.0.0.0 | Set to 0.0.0.0 if not used | | | | |
| Control DSCP: | 34 | | | | | |
| Voice DSCP: | 46 | | | | | |
| Data DSCP: | 46 | | | | | |
| Set Key | Remote TKMD IP Address | Remote TKMD MAC Address | NONE | TX | RX | TX/RX |
| 1 | 192.168.1.204 | 04:91:62:2d:d1:e2 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| 2 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10 | 0.0.0.0 | 00:00:00:00:00:00 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Saving an IP address change will cause the TKMD to restart

Save Config

Copyright © 2012-2021 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

The IP address, Subnet Mask and Gateway IP address used by the TKMD are entered on this page. Care must be taken with these entries since the IP Address and Gateway must be within the Subnet Mask and will be rejected if not. The MAC Address shown is read from the TKMD microprocessor chip and cannot be changed.

Up to 10 Remote TKMD IP Addresses can be entered in the Network Configuration web page. Radio buttons are used to set how the Remote TKMDs are allowed to share with the local TKMD. If the Remote TKMD IP Address has been found on the connected IP network, the Remote TKMD MAC Address value will be displayed.

The Red link to the Set Key page is for a future capability for a customer to uniquely set the File Share Base Key. Files to be shared are AES encrypted using a key derived from this File Share Base Key, the name of the file and the type of a file. To be able to decrypt a shared file, the File Share Base Key must be the same on both the source and destination TKMDs. Currently this File Share Base Key is a fixed value in TKMD firmware, but in the future it will be customer-set to enhance file share security.

Board Configuration The basic board settings for the TKMD are set on the Board Configuration web page.

| Navigation | Board Configuration |
|-----------------------|--|
| Overview | Preset Select: All User Data Erased |
| Key Data | Crypto Officer Name: Password: |
| Key Assign | Virtual Com Port Option: Not Set Port: 23 |
| Client Summary | Virtual Com Port User Name: Password: |
| Client Configuration | Debug Enable: USB: USB V.24 I/O Enable RS-232: Debug Enabled |
| File Up/Down Load | TKMD Start Up Option: None Auto OTAR: ON |
| File Share | TKMD Options: No Share at Start Key Validity (1,000's Seconds) 32000 |
| Network Configuration | Connection Option: No Quantar Latency 14 |
| Board Configuration | TKMD Behavior Option: DIU Emulation Voice/Data Transport: UDP |
| Remote Configuration | RTP Option: Standard RTP |
| Battery Monitor | Output Site Number: 2 |
| SNMP Configuration | DFSI NAC (decimal): 659 |
| | V.24 Clock: INPUT: External Clock OUTPUT: Internal Clock |
| | V.24 Connection: V.24 Board |
| | Board Temp: 357 (tenths of a degree C) |
| | Save Board Config Apply Changes |

- Options applied after board reset, Gain settings applied real-time.
 - Enhanced RTP should not be used when connecting to a Dispatch Console.
 - Be careful when changing the TKMD Crypto Officer Name and/or Password.
- If you forget them you will not be able to return to any of the protected setup pages.

Copyright © 2012-2021 Christine Wireless, Inc. Including RIC-M under license from DHS
Science and Technology

The above settings are typical and may be customized to meet individual setup requirements as noted in the following sections.

Presets The Presets pulldown allows selection of several pre-loaded preset board configuration settings. This menu also allows erasure of all settings and return to the Factory Default values.

Crypto Officer The Crypto Officer user name and password can be entered in this section. The password must contain an upper case letter, a lower case letter, a number and a special character and must be 8-10 characters long.

Virtual Com Port Option This section is used to set up the Virtual Com Port which is useful to connect a Quantar or ATAC Radio Service Software RS-232 port to a remote location through the TKMD.

Virtual Com Port User This section is used to set the user name and password for the Virtual Com Port.

Debug Enable This section is to set the use of the RS-232 and USB ports on the TKMD. Recommended settings are Debug for the RS-232 port and V.24 I/O for the USB port. If a file export is planned, the USB port should be set to None to keep from introducing extraneous USB output characters in the desired export text.

TKMD Startup Option This section is used to set the startup operational mode for the TKMD. Usual settings are for Packet Data KMF or Quantar KMF with Automatic OTAR enabled. Setting this option will ensure that the TKMD returns to an appropriate Operating Mode if power is interrupted without requiring Crypto Officer intervention.

Connection Option This setting controls how the V.24 connection enables/disables the IP connection. To prevent unexpected behavior, this should be set to No Quantar to prevent the interaction.

TKMD Behavior Option This setting is used to change the TKMD from appearing to be a Quantar or a DIU on the V.24. This setting will depend on which type of equipment to which the V.24 is connected.

Latency This setting controls how many V.24 20 millisecond voice frames are stored prior to beginning to output the V.24 voice to the connected equipment. A larger value introduces what may be a noticeable delay in voice traffic. A lower latency may prevent the TKMD from correcting out-of-order voice packets or packets with unexpected or highly variable delays.

RPT Option This setting defines how the TKMD handles the DFSI Voice/Data connection. The options are:

- **Standard RTP** This is the most usual operation and is consistent with the relevant TIA DFSI standards.
- **Enhanced RTP** This is similar to above except for some manufacturer specific enhancements to assist in V.24 fidelity.
- **HDLC Server/Client Tunnel** These modes are used to transport V.24 in a “Tunnel” mode on IP. One device is set to Server and the connected device is set to Client. This provides 100% fidelity for V.24 transport over IP.

- **HDLC DTLS Server/Client Tunnel** These modes are used to transport V.24 in a DTLS encrypted “Tunnel” mode on IP. One device is set to Server and the connected device is set to Client. This provides 100% fidelity for V.24 transport over IP with the added security of DTLS encryption of the V.24 packets.

Voice/Data Transport Mode This setting is used to send each V.24 packet once, four times or eight times. The repeat packets are spaced in time and interleaved which provides a great deal of immunity for transport on networks with poor packet delivery reliability. Repeated packets are deleted by the receiver once one good copy of each packet has been received.

Output Site Number This allows setting of the “Quantar Site Number” included in the V.24 frames.

DFSI NAC This setting allows selection of the Network Access Code used in the DFSI messaging.

V.24 Settings This section allows the setting of the clock directions for the V.24 input and output. The V.24 board connections must be used since the TKMD does not have ribbon cable connection implemented.

After making any changes to the settings on the Board Configuration web page click on the Save Board Config” button then click on “Apply Changes” button to make the changes. This will cause a restart of the TKMD.

Remote Configuration The Remote Configuration web page is used to setup the DFSI IP connection for the TKMD. In this example, the connection is to a Codan DFSI Packet Data Base Station. Settings for connection to a RF Technology or other DFSI Packet Data capable base Station would be similar.



Christine Wireless, Inc.
Ellicott City Maryland
410-961-7331
www.christinewireless.com

Tactical Key Management Device

Remote Configuration

| Overview | Remote Configuration | | | |
|-----------------------|--|-----------------------------|-------------------|-------------------|
| Key Data | Remote Connect Mode Voice, Data and Control Select | | | |
| Key Assign | | Control | Voice | Data |
| Client Summary | Local IP | 192.168.1.208 | 192.168.1.208 | 192.168.1.208 |
| Client Configuration | Remote IP | 192.168.1.66 | 192.168.1.66 | 192.168.1.66 |
| File Up/Down Load | Local UDP Port | 50000 | 50020 | 50010 |
| File Share | Remote UDP Port | 50000 | 50020 | 60947 |
| Network Configuration | Remote MAC Address | f8:dc:7a:10:9e:89 | f8:dc:7a:10:9e:89 | f8:dc:7a:10:9e:89 |
| Board Configuration | Status | Connected | Connected | Connected |
| Remote Configuration | SSRC | 0x3e6eb37b | | |
| Battery Monitor | RTP Count In | 6199 | RTP Count Out | 0 |
| SNMP Configuration | V.24 Count In | 0 | V.24 Count Out | 16928 |
| | | Reset Counters | | |
| | | Local | Remote | |
| | Heartbeat Period | 255 | 255 | |
| | Channel Number | 255 | 255 | |
| | Operating Mode | Base Station | Base Station | |
| | Monitor Mode | Monitor Off | Monitor Off | |
| | | Apply Changes | | |

Battery Monitor The status of the TKMD internal Lithium Ion battery is displayed on the Battery Monitor web page.

Tactical Key Management Device

← → ↻ 🏠 🔒 https://192.168.1.208/protect/battery.h 80% ⋮

TKMD

Christine Wireless, Inc.
Ellicott City Maryland
410-961-7331
www.christinewireless.com

Tactical Key Management Device

Battery Monitor

(milliVolts)

| | | | |
|-----------------------|--------------|------|-------------------|
| Overview | Current | 4135 | |
| Key Data | 1 Hour Ago | 4135 | 17 Hours Ago 4138 |
| Key Assign | 2 Hours Ago | 4136 | 18 Hours Ago 4138 |
| Client Summary | 3 Hours Ago | 4136 | 19 Hours Ago |
| Client Configuration | 4 Hours Ago | 4136 | 20 Hours Ago |
| File Up/Down Load | 5 Hours Ago | 4136 | 21 Hours Ago |
| File Share | 6 Hours Ago | 4136 | 22 Hours Ago |
| Network Configuration | 7 Hours Ago | 4136 | 23 Hours Ago |
| Board Configuration | 8 Hours Ago | 4136 | 24 Hours Ago |
| Remote Configuration | 9 Hours Ago | 4136 | 25 Hours Ago |
| Battery Monitor | 10 Hours Ago | 4136 | 26 Hours Ago |
| SNMP Configuration | 11 Hours Ago | 4136 | 27 Hours Ago |
| | 12 Hours Ago | 4136 | 28 Hours Ago |
| | 13 Hours Ago | 4136 | 29 Hours Ago |
| | 14 Hours Ago | 4136 | 30 Hours Ago |
| | 15 Hours Ago | 4136 | 31 Hours Ago |
| | 16 Hours Ago | 4136 | 32 Hours Ago |

Copyright © 2012-2021 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

The current battery voltage (in millivolts) is displayed along with the stored battery voltage values for the previous 32 hours of operation. The displayed voltage value will be Red if the battery is being charged and in Green if the battery is not being charged. If the TKMD is not connected to external power, the battery will support the retention of critical parameters for as long as several weeks. If the battery has been discharged, it may take several days for the battery charging circuitry to return the battery to full charge. Complete discharge of the battery will result in the erasure of all Client files and other parameters and therefore must be avoided.