



ASTRO® 25 **INTEGRATED VOICE AND DATA**

KVL 4000 **KEY VARIABLE LOADER** **ASTRO 25 USER GUIDE**

January 2013



6871018P37-F

Copyrights

The Motorola products described in this document may include copyrighted Motorola computer programs. Laws in the United States and other countries preserve for Motorola certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola computer programs contained in the Motorola products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola.

© 2013 Motorola Solutions, Inc. All Rights Reserved

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola, except for the normal nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive



The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Document History

Version	Description	Date
6871018P37-A	Original release of the <i>KVL 4000 Key Variable Loader ASTRO 25 User Guide</i>	May 2010
6871018P37-B	Updated as follows: <ul style="list-style-type: none"> • Added the following sections: <ul style="list-style-type: none"> – “Performing the OS Hardening” – “Unlocking the Operator Account” – “Setting the PDA USB Mode” – “KVL 4000 Disaster Recovery” – “Radio Frequency Interference Requirements - European Union - EMC Directive 2004/108/EC” • Updated Figure 1-16 KVL 4000 - Charging. • Updated to include the Radio Authentication operating mode. 	November 2010
6871018P37-C	Updated as follows: <ul style="list-style-type: none"> • Changed “Motorola, Inc.” to “Motorola Solutions, Inc.” • Changed document layout. 	July 2011
6871018P37-D	Updated/added the following sections: <ul style="list-style-type: none"> • “MOTOROLA SOLUTIONS, INC. END USER LICENSE AGREEMENT” • “PUBLICLY AVAILABLE SOFTWARE LIST – KVL SOFTWARE INSTALLATION WIZARD” • “PUBLICLY AVAILABLE SOFTWARE LIST – PDA” • “Personal Digital Assistant” • “Applying Enhanced Security Settings Through the KVL Software Installation Wizard” • “Applying Transparent Security Settings Through the KVL Software Installation Wizard” • “Connecting the KVL to a Radio or Another Target Device” • “Launching the KVL Application” • “Setting Up Passwords on the KVL” 	March 2012

Version	Description	Date
	<ul style="list-style-type: none"> • “Selecting the Password Masking Mode” • “KVL 4000 – Loading Encryption Keys into Target Devices” • “Updating a Target Device” • “KVL 4000 Disaster Recovery” • “Troubleshooting KVL Application and/or VPN Software Failure” • “Motorola System Support Center and Radio Support Center” • “North America Parts Organization” • “KVL 4000 – Orderable Parts” <p>Updated the following figures:</p> <ul style="list-style-type: none"> • Figure 1-1 KVL 4000 Key Variable Loader • Figure 1-2 Personal Digital Assistant (PDA) • Figure 1-17 Today Screen 	
6871018P37-E	<p>Added/updated the following sections:</p> <ul style="list-style-type: none"> • “Applying Enhanced Security Settings Through the KVL Software Installation Wizard” • “Applying Transparent Security Settings Through the KVL Software Installation Wizard” • “Connecting the KVL to a Radio or Another Target Device” • “Connecting the KVL to the USB Modem for the KMF Communication” • “Connecting the KVL to the CRYPTR micro” • “Launching the KVL Application” • “Exiting the KVL Application” • “Entering the User-Defined System Key” • “Changing the User-Defined System Key” • “Setting Up the KVL to Use the Default System Key” • “KVL 4000 – Loading Encryption Keys into Target Devices” • “Initializing the USB Modem for KMF USB Modem Connection” • “Downloading Keys from KMF to KVL Using USB Modem Connection” 	November 2012

Version	Description	Date
	<ul style="list-style-type: none"> • “Setting the PDA USB Mode” <p>Added/updated the following figures:</p> <ul style="list-style-type: none"> • Figure 1-2 Personal Digital Assistant (PDA) • Figure 1-13 KVL and USB Modem – Connected • Figure 1-15 CRYPTR micro and KVL - Connected • “Figure 1-17 Today Screen” <p>Updated the following tables:</p> <ul style="list-style-type: none"> • Table B-5 Interface Cables • Table B-6 Optional Accessories • Table D-1 Acronyms 	
6871018P37-F	<p>Added/updated the following sections:</p> <ul style="list-style-type: none"> • “Applying Enhanced Security Settings Through the KVL Software Installation Wizard” • “Applying Transparent Security Settings Through the KVL Software Installation Wizard” • “Connecting the KVL to the USB Modem for the KMF Communication” • “Connecting the KVL to the Network for the KMF Communication” • “Exiting the KVL Application” • “Configuring VPN Settings” • “Configuring VPN Settings - KVL Directly Connected to the Firewall” • “Configuring VPN Settings - KVL Connected to the Firewall Through a Network” • “Establishing the VPN Connection” • “Terminating the VPN Connection” • “Setting Up the KVL for KMF Operations” • “Entering Main and Backup KMF Ports” • “Entering Main and Backup KMF IP Addresses” • “Downloading Keys from KMF to KVL Using Network Connection” 	January 2013

Contents

1	KVL 4000 – Introduction	1-1
1.1	MC55A0 PDA Reference	1-1
1.2	Overview of the KVL 4000	1-1
1.2.1	KVL 4000 Components	1-1
1.2.1.1	Personal Digital Assistant	1-2
1.2.1.2	Security Adapter	1-4
1.2.2	KVL 4000 Key Features	1-6
1.2.3	KVL 4000 Sounds	1-7
1.2.4	Using the KVL 4000	1-8
1.2.4.1	Types of Encryption Keys	1-8
1.2.4.2	Entering and Loading Keys – Overview	1-8
1.3	KVL 4000 User Interface	1-8
1.4	KVL 4000 – Getting Started	1-9
1.4.1	Applying Enhanced Security Settings Through the KVL Software Installation Wizard	1-9
1.4.2	Applying Transparent Security Settings Through the KVL Software Installation Wizard	1-11
1.4.3	Connecting the PDA and the Security Adapter	1-12
1.4.4	Connecting the KVL to Target Devices	1-13
1.4.4.1	Connecting the KVL to a Radio or Another Target Device	1-13
1.4.4.2	Connecting Two KVL Units	1-16
1.4.4.3	Connecting the KVL to the KMF	1-16
1.4.4.3.1	Connecting the KVL to the KMF – Direct Connection	1-16
1.4.4.3.2	Connecting the KVL to the USB Modem for the KMF Communication	1-17
1.4.4.3.3	Connecting the KVL to the Serial Modem for the KMF Communication	1-18
1.4.4.3.4	Connecting the KVL to the Network for the KMF Communication	1-19
1.4.4.4	Connecting the KVL to the CRYPTR micro	1-21
1.4.5	Charging the KVL 4000	1-21
1.4.6	Launching the KVL Application	1-23
1.4.7	Exiting the KVL Application	1-25
1.4.8	Configuring VPN Settings	1-26
1.4.8.1	Configuring VPN Settings - KVL Directly Connected to the Firewall	1-27
1.4.8.2	Configuring VPN Settings - KVL Connected to the Firewall Through a Network	1-35
1.4.9	Establishing the VPN Connection	1-43
1.4.10	Terminating the VPN Connection	1-46
2	KVL 4000 – Performing Initial Programming	2-1
2.1	KVL 4000 User Preference Parameters	2-1
2.1.1	Setting the KVL Log Off Time	2-1
2.1.2	Setting the KVL Screen Color Scheme	2-1
2.1.3	Turning Sharing On/Off	2-3
2.1.4	KVL 4000 – Managing Passwords	2-3
2.1.4.1	Setting Up Passwords on the KVL	2-4
2.1.4.1.1	Setting Up the Operator Password	2-4
2.1.4.1.2	Setting Up the Administrator Password	2-5
2.1.4.2	Changing Passwords on the KVL	2-6
2.1.4.2.1	Changing the Operator Password (Operator Access Level)	2-6
2.1.4.2.2	Changing the Operator Password (Administrator Access Level)	2-7
2.1.4.2.3	Changing the Administrator Password	2-8
2.1.4.3	Clearing KVL Passwords	2-10
2.1.4.4	Selecting the Password Masking Mode	2-11
2.2	KVL 4000 System-Dependent Parameters	2-11
2.2.1	KVL 4000 – Switching Between the Modes of Operation	2-11
2.2.2	Setting the Baud Rate for RS-232 Communication	2-12
2.2.3	Changing the FIPS Mode	2-13

2.2.4	Managing the System Key (DVI-XL Only).....	2-14
2.2.4.1	Entering the User-Defined System Key	2-15
2.2.4.2	Changing the User-Defined System Key	2-15
2.2.4.3	Setting Up the KVL to Use the Default System Key	2-16
3	KVL 4000 – Managing Encryption Keys	3-1
3.1	Entering Encryption Keys.....	3-1
3.1.1	Entering Encryption Keys Manually	3-1
3.1.2	Auto-Generating Encryption Keys	3-3
3.2	Using Key Groups	3-5
3.2.1	Creating a Group	3-5
3.2.2	Modifying Groups	3-7
3.2.2.1	Viewing Keys in a Group	3-8
3.2.2.2	Adding Keys to a Group.....	3-8
3.2.2.3	Deleting Keys from a Group	3-10
3.2.2.4	Deleting a Group	3-11
3.2.2.5	Renaming a Group	3-13
3.3	Modifying Encryption Keys.....	3-14
3.4	Deleting Encryption Keys.....	3-16
4	KVL 4000 – Loading Encryption Keys into Target Devices.....	4-1
4.1	Loading a Selected Key	4-1
4.2	Loading a Key Group	4-3
4.3	Loading All Keys	4-6
4.4	Loading All Key Groups	4-7
5	KVL 4000 – Managing Keys in Target Devices	5-1
5.1	Removing Keys from Target Devices.....	5-1
5.1.1	Removing a Key from a Target Device	5-1
5.1.2	Removing a Key Group from a Target Device	5-3
5.1.3	Removing All Keys from a Target Device	5-6
5.1.4	Removing All Key Groups from a Target Device	5-8
5.1.5	Removing All Keys and All Key Groups from a Target Device.....	5-10
5.2	Viewing Keys in Target Devices	5-12
6	KVL 4000 – Sharing Keys Between KVLs	6-1
6.1	Sharing a Single Key	6-1
6.2	Sharing a Key Group and Associated Keys	6-3
6.3	Sharing All Keys and All Groups.....	6-4
7	Using KVL 4000 in OTAR Systems	7-1
7.1	Setting Up the KVL for KMF Operations	7-1
7.1.1	Entering the UKEK.....	7-2
7.1.2	Selecting Main or Backup KMF	7-3
7.1.3	Entering Main and Backup KMF Phone Numbers	7-4
7.1.4	Entering Main and Backup KMF Ports	7-6
7.1.5	Entering Main and Backup KMF IP Addresses.....	7-7
7.1.6	Entering the KMF RSI.....	7-8
7.1.7	Entering the MNP for OTAR	7-9
7.1.8	Entering the KVL RSI for OTAR.....	7-10
7.2	Using the Store and Forward Feature	7-11
7.2.1	Downloading Keys from KMF to KVL Using Direct Connection.....	7-11
7.2.2	Downloading Keys from KMF to KVL Using Modem Connection.....	7-12
7.2.2.1	Downloading Keys from KMF to KVL Using USB Modem Connection.....	7-12
7.2.2.2	Downloading Keys from KMF to KVL Using Serial Modem Connection	7-13
7.2.3	Downloading Keys from KMF to KVL Using Network Connection	7-14
7.2.4	Updating a Target Device.....	7-15
7.2.5	Viewing the List of Received Jobs	7-16
7.2.6	Clearing the List of Received Jobs	7-17
7.3	Performing a Keyset Changeover on a Target Device.....	7-18

7.4	Managing OTAR Configuration Parameters in Target Devices	7-19
7.4.1	Viewing the Target's MNP	7-19
7.4.2	Viewing the Target's RSI and KMF RSI	7-20
7.4.3	Changing the Target's MNP	7-21
7.4.4	Changing the Target's RSI and KMF RSI	7-22
8	KVL 4000 Operations Through a Remote Control Head	8-1
8.1	Performing KVL Operations Through a Remote Control Head	8-1
8.2	Setting Up KVL for Remote Control Head Operations	8-1
8.2.1	Entering the SEK and KEK	8-2
8.2.2	Entering the MNP for Remote Control Head Operations	8-3
8.2.3	Entering the KVL RSI for Remote Control Head Operations	8-4
8.3	Provisioning a Radio for Remote Control Head Key Loading	8-5
8.4	Connecting the KVL to the Mobile Radio's Remote Control Head	8-6
9	KVL 4000 – Working with Tactical OTAR Groups	9-1
9.1	Equipment Needed For Tactical OTAR	9-1
9.2	Setting Up Tactical OTAR	9-2
9.3	Creating a New Tactical OTAR Group	9-2
9.4	Deleting an Existing Tactical OTAR Group	9-4
9.5	Viewing the Members of a Tactical OTAR Group	9-4
9.6	Adding a Member to a Tactical OTAR Group	9-5
9.7	Removing a Member from a Tactical OTAR Group	9-6
9.8	Editing the TEK of a Tactical OTAR Group	9-7
9.9	Updating a Tactical OTAR Group	9-8
10	Managing Log Records	10-1
10.1	Organization of Log Records	10-1
10.2	Accessing Log Records	10-1
10.3	Clearing Log Records	10-2
10.4	Exporting Log Records to a PC	10-4
11	KVL 4000 – Converting Encryption Keys	11-1
11.1	When to Convert Keys	11-1
11.2	Key Converting Restrictions and Guidelines	11-1
11.3	Converting a Key from ASN to ASTRO 25	11-1
11.4	Converting a Key from ASTRO 25 to ASN	11-4
12	KVL 4000 – Troubleshooting	12-1
12.1	KVL Error Messages	12-1
12.1.1	KVL User Entry Errors	12-1
12.1.2	KVL Operational Errors	12-2
12.2	Performing a System Reset	12-4
12.3	Unlocking the Operator Account	12-5
12.4	Setting the PDA USB Mode	12-5
12.5	KVL 4000 Disaster Recovery	12-6
12.6	Troubleshooting KVL Application and/or VPN Software Failure	12-6
12.7	Disassembling the Security Adapter	12-7
12.8	Assembling the Security Adapter	12-9
12.9	Contacting Motorola	12-14
12.9.1	Motorola System Support Center and Radio Support Center	12-15
12.9.2	North America Parts Organization	12-15
Appendix A	KVL 4000 - Performance Specifications	A-1
Appendix B	KVL 4000 – Orderable Parts	B-1
Appendix C	Radio Frequency Interference Requirements	C-1
C.1	Radio Frequency Interference Requirements – USA	C-1
C.2	Radio Frequency Interference Requirements – Canada	C-1
C.3	Radio Frequency Interference Requirements – European Union – EMC Directive 2004/108/EC	C-1
Appendix D	Acronyms	D-1

List of Figures

Figure 1-1	KVL 4000 Key Variable Loader	1-2
Figure 1-2	Personal Digital Assistant (PDA)	1-3
Figure 1-3	Security Adapter	1-5
Figure 1-4	KVL 4000 Main Screen	1-9
Figure 1-5	PDA and PC – Connected	1-10
Figure 1-6	PDA and Security Adapter – Connecting	1-13
Figure 1-7	PDA and Security Adapter – Connected	1-13
Figure 1-8	KVL and Radios – Connected (Example)	1-14
Figure 1-9	KVL and KMF – Connected	1-15
Figure 1-10	KVL and MGEG – Connected (Example)	1-15
Figure 1-11	Two KVL Units – Connected	1-16
Figure 1-12	KVL and KMF – Direct Connection	1-17
Figure 1-13	KVL and USB Modem – Connected	1-18
Figure 1-14	KVL and Serial Modem – Connected (Example)	1-19
Figure 1-15	KVL and USB to Ethernet Adapter - Connected	1-20
Figure 1-16	CRYPTR micro and KVL - Connected	1-21
Figure 1-17	KVL 4000 - Charging	1-22
Figure 1-18	Today Screen	1-23
Figure 1-19	Welcome Screen	1-24
Figure 1-20	Exit Screen	1-26
Figure 1-21	Log Off Screen	1-26
Figure 1-22	NCP Entry Configuration Manager WM Window	1-28
Figure 1-23	Profile Settings Window	1-28
Figure 1-24	Assistant for New Profile – Pre-shared Key Window	1-29
Figure 1-25	Assistant for New Profile – Connection Name Window	1-29
Figure 1-26	Assistant for New Profile – Communication Medium Window	1-30
Figure 1-27	Assistant for New Profile – VPN Gateway Parameters Window	1-30
Figure 1-28	Assistant for New Profile – IPSec Configuration Window	1-31
Figure 1-29	Assistant for New Profile – Pre-shared Key	1-32
Figure 1-30	Assistant for New Profile – IPSec Configuration – IP Addresses Window	1-33
Figure 1-31	Assistant for New Profile – Firewall Settings Window	1-34
Figure 1-32	NCP Entry Configuration Manager WM Window	1-35
Figure 1-33	Profile Settings Window	1-36
Figure 1-34	Assistant for New Profile – Pre-shared Key Window	1-36
Figure 1-35	Assistant for New Profile – Connection Name Window	1-37
Figure 1-36	Assistant for New Profile – Communication Medium Window	1-37
Figure 1-37	Assistant for New Profile – VPN Gateway Parameters Window	1-38
Figure 1-38	Assistant for New Profile – IPSec Configuration Window	1-39
Figure 1-39	Assistant for New Profile – Pre-shared Key	1-40
Figure 1-40	Assistant for New Profile – IPSec Configuration – IP Addresses Window	1-41
Figure 1-41	Assistant for New Profile – Firewall Settings Window	1-42
Figure 1-42	Programs Screen	1-43
Figure 1-43	NCP Secure Client Screen – KVL 4000 at Firewall	1-44
Figure 1-44	NCP Secure Client Screen – KVL 4000 Through Network	1-44
Figure 1-45	NCP Secure Client Screen – KVL 4000 at Firewall – Connected	1-45
Figure 1-46	NCP Secure Client Screen – KVL 4000 Through Network – Connected	1-46
Figure 1-47	Programs Screen	1-47
Figure 2-1	KVL Screen in Day Time Color Scheme (Example)	2-2
Figure 2-2	KVL Screen in Night Time Color Scheme (Example)	2-2
Figure 2-3	Clear Passwords Screen	2-10
Figure 3-1	Manage Keys Screen – Entering a Key (Example)	3-1
Figure 3-2	Review Key Screen (Example)	3-3

Figure 3-3	Manage Keys Screen – Entering a Key (Example)	3-4
Figure 3-4	Manage Keys Screen – Creating a Group (Example)	3-6
Figure 3-5	Adding Keys to a Group – Example	3-7
Figure 3-6	Viewing Keys in a Group (Example)	3-8
Figure 3-7	Group with Available Keys (Example)	3-9
Figure 3-8	Deleting Keys from a Group (Example)	3-11
Figure 3-9	Deleting a Group (Example)	3-12
Figure 3-10	Group Name Field (Example)	3-13
Figure 3-11	Manage Keys Screen – Modifying a Key (Example)	3-14
Figure 3-12	Key Details Screen (Example)	3-15
Figure 3-13	Manage Keys Screen – Deleting a Key (Example)	3-17
Figure 4-1	Load Keys & Groups Screen – Example	4-2
Figure 4-2	Loading a Key (Example)	4-3
Figure 4-3	Load Keys & Groups Screen – Loading a Group (Example)	4-4
Figure 4-4	Loading a Group (Example)	4-5
Figure 4-5	Load Keys & Groups Screen – Loading All Keys (Example)	4-6
Figure 4-6	Loading a Key – Statuses (Example)	4-7
Figure 4-7	Load Keys & Groups Screen – Loading All Groups (Example)	4-8
Figure 5-1	Configure a Radio Screen	5-2
Figure 5-2	Remove Keys & Groups Screen (Example)	5-3
Figure 5-3	Configure a Radio Screen – Removing a Group	5-4
Figure 5-4	Remove Keys & Groups Screen – Removing a Group (Example)	5-5
Figure 5-5	Group Removed (Example)	5-6
Figure 5-6	Configure a Radio Screen – Removing All Keys	5-7
Figure 5-7	Remove Keys & Groups Screen – Removing All Keys (Example)	5-8
Figure 5-8	Configure a Radio Screen – Removing All Groups	5-9
Figure 5-9	Remove Keys & Groups Screen – Removing All Groups (Example)	5-10
Figure 5-10	Configure a Radio Screen – Removing All Keys and Groups	5-11
Figure 5-11	Remove All Screen	5-12
Figure 5-12	Configure a Radio Screen – Viewing Keys	5-13
Figure 6-1	Load Keys & Groups Screen – Sharing a Key (Example)	6-2
Figure 6-2	Load Keys & Groups Screen – Sharing a Group (Example)	6-3
Figure 7-1	Phone #s Screen	7-5
Figure 8-1	KVL Connected to a Mobile Radio's Remote Control Head	8-7
Figure 9-1	Tactical OTAR Equipment (Example)	9-1
Figure 10-1	Operations Log (Example)	10-2
Figure 10-2	Operations Log – Clear (Example)	10-3
Figure 10-3	Clearing Logs – Confirmation Screen	10-4
Figure 11-1	Manage Keys Screen – Converting ASN Key (Example)	11-2
Figure 11-2	Converting to ASTRO 25 (Example)	11-3
Figure 11-3	Manage Keys Screen – Converting ASTRO 25 Key (Example)	11-4
Figure 11-4	Converting to ASN (Example)	11-5
Figure 12-1	KVL System Reset Slider – Subsequent States	12-5
Figure 12-2	Security Adapter – Exploded View	12-7
Figure 12-3	Removing Back Housing	12-8
Figure 12-4	Removing Dust Covers	12-8
Figure 12-5	Removing PCB Assembly	12-9
Figure 12-6	Removing USB Clip and Foam Pad	12-9
Figure 12-7	Assembling USB Clip	12-10
Figure 12-8	Assembling Foam Pad	12-10
Figure 12-9	Assembling O-Ring	12-11
Figure 12-10	Assembling Front Housing – PCB	12-11
Figure 12-11	Assembling Front Housing – Connectors	12-12
Figure 12-12	Assembling Front Housing – PCB Placed	12-12
Figure 12-13	Assembling Dust Covers	12-13

Figure 12-14 Assembling Back Housing to Front Housing 12-13
Figure 12-15 Tightening Back Housing 12-14
Figure 12-16 Pressing Dust Covers 12-14

List of Tables

Table 1-1	PDA Controls and Ports Used in the KVL Operation.....	1-3
Table 1-2	Security Adapter Ports and Interfaces.....	1-5
Table 1-3	Sounds Played by the KVL 4000.....	1-7
Table 12-1	KVL User Entry Errors.....	12-1
Table 12-2	KVL Operational Errors.....	12-2
Table 12-3	KVL 4000 Disaster Recovery.....	12-6
Table 12-4	North America Parts Organization Telephone Numbers.....	12-15
Table A-1	Physical Characteristics.....	A-1
Table A-2	Encryption.....	A-1
Table A-3	Supported Algorithms.....	A-1
Table A-4	Electromagnetic Compatibility.....	A-2
Table A-5	Regulatory Compliance and Approvals.....	A-2
Table B-1	KVL 4000 Model.....	B-1
Table B-2	MC55 Kit.....	B-1
Table B-3	Security Adapter Super Tanapa.....	B-1
Table B-4	Front Housing Assembly – Orderable Parts.....	B-1
Table B-5	Interface Cables.....	B-2
Table B-6	Optional Accessories.....	B-2
Table D-1	Acronyms.....	D-1

List of Processes

7.1 — Setting Up the KVL for KMF Operations7-1

8.1 — Performing KVL Operations Through a Remote Control Head.....8-1

List of Procedures

1.4.1 — Applying Enhanced Security Settings Through the KVL Software Installation Wizard	1-9
1.4.2 — Applying Transparent Security Settings Through the KVL Software Installation Wizard	1-11
1.4.3 — Connecting the PDA and the Security Adapter	1-12
1.4.4.1 — Connecting the KVL to a Radio or Another Target Device.....	1-13
1.4.4.2 — Connecting Two KVL Units	1-16
1.4.4.3.1 — Connecting the KVL to the KMF – Direct Connection.....	1-16
1.4.4.3.2 — Connecting the KVL to the USB Modem for the KMF Communication.....	1-17
1.4.4.3.3 — Connecting the KVL to the Serial Modem for the KMF Communication	1-18
1.4.4.3.4 — Connecting the KVL to the Network for the KMF Communication.....	1-19
1.4.4.4 — Connecting the KVL to the CRYPTR micro	1-21
1.4.5 — Charging the KVL 4000.....	1-21
1.4.6 — Launching the KVL Application	1-23
1.4.7 — Exiting the KVL Application.....	1-25
1.4.8.1 — Configuring VPN Settings - KVL Directly Connected to the Firewall	1-27
2.1.1 — Setting the KVL Log Off Time.....	2-1
2.1.2 — Setting the KVL Screen Color Scheme	2-1
2.1.3 — Turning Sharing On/Off.....	2-3
2.1.4.1.1 — Setting Up the Operator Password.....	2-4
2.1.4.1.2 — Setting Up the Administrator Password.....	2-5
2.1.4.2.1 — Changing the Operator Password (Operator Access Level)	2-6
2.1.4.2.2 — Changing the Operator Password (Administrator Access Level).....	2-7
2.1.4.2.3 — Changing the Administrator Password	2-8
2.1.4.3 — Clearing KVL Passwords.....	2-10
2.1.4.4 — Selecting the Password Masking Mode	2-11
2.2.1 — KVL 4000 – Switching Between the Modes of Operation.....	2-11
2.2.2 — Setting the Baud Rate for RS-232 Communication.....	2-12
2.2.3 — Changing the FIPS Mode.....	2-13
2.2.4.1 — Entering the User-Defined System Key.....	2-15
2.2.4.2 — Changing the User-Defined System Key	2-15
2.2.4.3 — Setting Up the KVL to Use the Default System Key.....	2-16
3.1.1 — Entering Encryption Keys Manually	3-1
3.1.2 — Auto-Generating Encryption Keys	3-3
3.2.1 — Creating a Group.....	3-5
3.2.2.1 — Viewing Keys in a Group.....	3-8

3.2.2.2 — Adding Keys to a Group	3-8
3.2.2.3 — Deleting Keys from a Group	3-10
3.2.2.4 — Deleting a Group	3-11
3.2.2.5 — Renaming a Group	3-13
3.3 — Modifying Encryption Keys	3-14
3.4 — Deleting Encryption Keys	3-16
4.1 — Loading a Selected Key	4-1
4.2 — Loading a Key Group	4-3
4.3 — Loading All Keys	4-6
4.4 — Loading All Key Groups	4-7
5.1.1 — Removing a Key from a Target Device	5-1
5.1.2 — Removing a Key Group from a Target Device	5-3
5.1.3 — Removing All Keys from a Target Device	5-6
5.1.4 — Removing All Key Groups from a Target Device	5-8
5.1.5 — Removing All Keys and All Key Groups from a Target Device	5-10
5.2 — Viewing Keys in Target Devices	5-12
6.1 — Sharing a Single Key	6-1
6.2 — Sharing a Key Group and Associated Keys	6-3
6.3 — Sharing All Keys and All Groups	6-4
7.1.1 — Entering the UKEK	7-2
7.1.2 — Selecting Main or Backup KMF	7-3
7.1.3 — Entering Main and Backup KMF Phone Numbers	7-4
7.1.4 — Entering Main and Backup KMF Ports	7-6
7.1.5 — Entering Main and Backup KMF IP Addresses	7-7
7.1.6 — Entering the KMF RSI	7-8
7.1.7 — Entering the MNP for OTAR	7-9
7.1.8 — Entering the KVL RSI for OTAR	7-10
7.2.1 — Downloading Keys from KMF to KVL Using Direct Connection	7-11
7.2.2.1 — Downloading Keys from KMF to KVL Using USB Modem Connection	7-12
7.2.2.2 — Downloading Keys from KMF to KVL Using Serial Modem Connection	7-13
7.2.3 — Downloading Keys from KMF to KVL Using Network Connection	7-14
7.2.4 — Updating a Target Device	7-15
7.2.5 — Viewing the List of Received Jobs	7-16
7.2.6 — Clearing the List of Received Jobs	7-17
7.3 — Performing a Keyset Changeover on a Target Device	7-18
7.4.1 — Viewing the Target's MNP	7-19

7.4.2 — Viewing the Target's RSI and KMF RSI.....	7-20
7.4.3 — Changing the Target's MNP.....	7-21
7.4.4 — Changing the Target's RSI and KMF RSI.....	7-22
8.2.1 — Entering the SEK and KEK.....	8-2
8.2.2 — Entering the MNP for Remote Control Head Operations.....	8-3
8.2.3 — Entering the KVL RSI for Remote Control Head Operations.....	8-4
8.3 — Provisioning a Radio for Remote Control Head Key Loading.....	8-5
8.4 — Connecting the KVL to the Mobile Radio's Remote Control Head.....	8-6
9.2 — Setting Up Tactical OTAR.....	9-2
9.3 — Creating a New Tactical OTAR Group.....	9-2
9.4 — Deleting an Existing Tactical OTAR Group.....	9-4
9.5 — Viewing the Members of a Tactical OTAR Group.....	9-4
9.6 — Adding a Member to a Tactical OTAR Group.....	9-5
9.7 — Removing a Member from a Tactical OTAR Group.....	9-6
9.8 — Editing the TEK of a Tactical OTAR Group.....	9-7
9.9 — Updating a Tactical OTAR Group.....	9-8
10.2 — Accessing Log Records.....	10-1
10.3 — Clearing Log Records.....	10-2
10.4 — Exporting Log Records to a PC.....	10-4
11.3 — Converting a Key from ASN to ASTRO 25.....	11-1
11.4 — Converting a Key from ASTRO 25 to ASN.....	11-4
12.2 — Performing a System Reset.....	12-4
12.3 — Unlocking the Operator Account.....	12-5
12.4 — Setting the PDA USB Mode.....	12-5
12.7 — Disassembling the Security Adapter.....	12-7
12.8 — Assembling the Security Adapter.....	12-9

About the KVL 4000 Key Variable Loader ASTRO 25 User Guide

This manual provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others.

This manual is intended for use by experienced technicians familiar with similar types of equipment. Technicians should understand encryption concepts and be familiar with other types of Motorola encryption equipment.

Depending on the options ordered, the KVL has the capability of being configured to operate in the Advanced SECURENET® (ASN) mode, ASTRO® 25, and/or Radio Authentication mode. The KVL menu system, functionality, and operating characteristics are different depending which operating mode is active.

This manual describes the ASTRO® 25 operating mode.

What Is Covered in this Manual?

This manual consists of the following chapters:

- [Chapter 1 KVL 4000 – Introduction](#)
- [Chapter 2 KVL 4000 – Performing Initial Programming](#)
- [Chapter 3 KVL 4000 – Managing Encryption Keys](#)
- [Chapter 4 KVL 4000 – Loading Encryption Keys into Target Devices](#)
- [Chapter 5 KVL 4000 – Managing Keys in Target Devices](#)
- [Chapter 6 KVL 4000 – Sharing Keys Between KVLs](#)
- [Chapter 7 Using KVL 4000 in OTAR Systems](#)
- [Chapter 8 KVL 4000 Operations Through a Remote Control Head](#)
- [Chapter 9 KVL 4000 – Working with Tactical OTAR Groups](#)
- [Chapter 10 Managing Log Records](#)
- [Chapter 11 KVL 4000 – Converting Encryption Keys](#)
- [Chapter 12 KVL 4000 – Troubleshooting](#)

Helpful Background Information

Motorola offers various courses designed to assist in learning about the system. For information, go to <http://www.motorolasolutions.com/training> to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information:

Related Information	Purpose
<i>Standards and Guidelines for Communication Sites</i>	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual. This may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
<i>System Documentation Overview</i>	<p>For an overview of the ASTRO® 25 system documentation, open the graphical user interface for the ASTRO® 25 system documentation set and select the System Documentation Overview link. This opens a file that includes:</p> <ul style="list-style-type: none"> • ASTRO® 25 system release documentation descriptions • ASTRO® 25 system diagrams • ASTRO® 25 system glossary <p>For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.</p>
<i>MC55 Enterprise Digital Assistant User Guide (72E-108859)</i>	Describes how to use the MC55 EDA.
<i>MC55 Quick Start Guide (72-127603)</i>	Describes how to get the MC55 EDA up and running.
<i>KVL 4000 Quick Start Guide</i>	Provides basic information on the KVL 4000.
<i>KVL 4000 Key Variable Loader Advanced SECURENET User Guide (6871018P35)</i>	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others. This manual describes the Advanced SECURENET® operating mode.
<i>KVL 4000 Key Variable Loader Radio Authentication User Guide</i>	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store authentication keys, and then load them into Motorola radios.
<i>KVL 4000 FLASHPort Upgrade User Guide</i>	Provides instructions for upgrading the Key Variable Loader (KVL), radios, and other target devices. It also provides instructions for applying security settings on the KVL, installing and activating VPN software, as well as provides troubleshooting information.
<i>KVL 3000 Plus Key Variable Loader User's Guide (6881132E29)</i>	Provides information for the KVL 3000 Plus Key Variable Loader.

MOTOROLA SOLUTIONS, INC. END USER LICENSE AGREEMENT

Motorola Solutions, Inc. (“Motorola”) is willing to license the Motorola PDA and Security Adapter Software and the accompanying documentation to you (“Licensee” or “you”) for use with a Motorola KVL4000 only on the condition that you accept all the terms in this End User License Agreement (“Agreement”).

IMPORTANT: READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING PRODUCT.

IF YOU DO NOT AGREE TO THIS AGREEMENT, DO NOT USE THE SOFTWARE OR COPY THE SOFTWARE, INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON A KVL 4000 THAT INCLUDES MOTOROLA PDA AND SECURITY ADAPTER, WILL CONSTITUTE YOUR AGREEMENT TO THIS END USER LICENSE AGREEMENT.

1. Definitions

In this Agreement, the word “Software” refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word “Documentation” refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word “Product” refers to the specific combination of Software and Documentation that you have licensed and which has been provided to you under this Agreement.

2. Grant of License

Motorola grants you a personal, non-exclusive, non-assignable, nontransferable license to use the Products subject to the Conditions of Use set forth in Section 2 and the terms and conditions of this Agreement. Any terms or conditions appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

3. Conditions of Use

Any use of the Products outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

3.1 Only you, your employees or agents may use the Products. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

3.2 You will use the Products: (i) only for your internal business purposes; (ii) only as described in the Products; and (iii) in strict accordance with this Agreement.

3.3 You may install and use the Products on a single Motorola PDA and KVL 4000 security adapter, provided that the use is in conformance with the terms set forth in this Agreement.

3.4 Portions of the Products are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Products like any other copyrighted material (e.g., a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Products (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the

transportable part of the Products to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Motorola copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

3.5 You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

4. Title; Restrictions

If you transfer possession of any copy of the Products to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Products and any copies made by you remain with Motorola and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Motorola's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Products be equipped with such a protection device. If the Products are provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Motorola's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

5. Confidentiality

You acknowledge that all Products contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Products will result in irreparable harm to Motorola for which monetary damages would be inadequate and for which Motorola will be entitled to immediate injunctive relief. Accordingly, you will limit access to the Products to those of your employees and agents who need to use the Products for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Products, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Motorola prior to such disclosure and provide Motorola with a reasonable opportunity to respond.

6. Right to Use Motorola's Name

Except as required in Section 3.4 above, you will not, during the term of this Agreement or thereafter, use any trademark of Motorola, or any word or symbol likely to be confused with any Motorola trademark, either alone or in any combination with another word or words.

7. Payment

The rights granted hereunder are contingent upon payment for the Product. All payments are due next 30 days from the date of the invoice.

8. Transfer

In the case of Software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (i) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or (ii) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software permitted in this Agreement, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained in this Agreement. All such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy and copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without Motorola's written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the U.S. Government.

9. Upgrades and Updates

If the Products are licensed to you as an upgrade or update to a product previously licensed to you, you must destroy the Products previously licensed to you, including any copies, within 30 days of your receipt of the update or upgrade.

10. Maintenance and Support

Motorola is not responsible for maintenance or support of the Software under this Agreement. By accepting the license granted under this Agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software. Any maintenance and support of the Software and equipment on which it resides will be provided under the terms of a separate agreement.

11. Limited Warranty

All diskettes or CD-ROMS on which the Products are furnished ("Media") are warranted to be free from manufacturing and material defects for 90 days after the shipment date of the Products to you. Media that becomes defective during such period will be repaired or, at Motorola's option, replaced. This limited warranty is contingent upon proper use of the Media and does not cover Products which have been tampered with, modified, or subjected to unusual physical or electrical stress. Tampering with or removal of any factory seal or label on any Media voids this warranty and releases Motorola from any and all liability.

12. Disclaimer

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY, MOTOROLA DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. MOTOROLA SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE PRODUCTS ARE PROVIDED “AS IS”. MOTOROLA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. MOTOROLA MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

13. Remedies

The entire liability of Motorola, and your exclusive remedy under the warranty provided in this Agreement will be, at Motorola's option, to repair or replace any Media found to be defective within the warranty period, or to refund the purchase price and terminate this Agreement. To seek such a remedy, you must return the entire Product to Motorola, with a copy of the original purchase receipt, within the warranty period.

14. Limitation of Liability

THE TOTAL LIABILITY OF MOTOROLA UNDER THIS AGREEMENT FOR DAMAGES WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCT LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL MOTOROLA OR ANY OF THE LICENSORS BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIMITATIONS IN THIS PARAGRAPH WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

15. U.S. Government

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Products is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

16. Term of License

Your right to use the Products will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Motorola in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Motorola, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

17. Governing Law

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

18. Assignment

This Agreement may not be assigned by you without Motorola's prior written consent.

19. Survival of Provisions

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

20. Entire Agreement

This Agreement contains the parties' entire agreement regarding your use of the Products and may be amended only in writing signed by both parties, except that Motorola may modify this Agreement as necessary to comply with applicable laws.

21. Third-Party Software

The Software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

22. Open Source Software

The Software may contain one or more items of Open Source or other Publicly Available Software. For information regarding licenses, acknowledgements, required copyright notices, and other usage terms, see [Open Source Software Legal Notices](#), page xxxi.

Open Source Software Legal Notices

This media, or Motorola Solutions Product, may include Motorola Solutions Software, Commercial Third-Party Software, and Publicly Available Software.

The Motorola Solutions Software that may be included on this media, or included in the Motorola Solutions Product, is Copyright (c) by Motorola Solutions, Inc., and its use is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc.

The Commercial Third-Party Software that may be included on this media, or included in the Motorola Solutions Product, is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc., unless a separate Commercial Third-Party Software License is included, in which case, your use of the Commercial Third-Party Software will then be governed by the separate Commercial Third-Party License.

The Publicly Available Software that may be included on this media, or in the Motorola Solutions Product, is listed below. The use of the listed Publicly Available Software is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc., as well as the terms and conditions of the license of each Publicly Available Software package. Copies of the licenses for the listed Publicly Available Software, as well as all attributions, acknowledgements, and software information details, are included below. Motorola Solutions is required to reproduce the software licenses, acknowledgments and copyright notices as provided by the Authors and Owners, thus, all such information is provided in its native language form, without modification or translation.

The Publicly Available Software in the list below is limited to the Publicly Available Software included by Motorola Solutions. The Publicly Available Software included by Commercial Third Party Software or Products, that is used in the Motorola Solutions Product, are disclosed in the Commercial Third-Party Licenses, or via the respective Commercial Third-Party Publicly Available Software Legal Notices.

For instructions on how to obtain a copy of any source code being made publicly available by Motorola Solutions related to software used in this Motorola Solutions Product you may send your request in writing to:

MOTOROLA SOLUTIONS, INC.
Government & Public Safety Business
Publicly Available Software Management
1301 E. Algonquin Road
Schaumburg, IL 60196
USA

In your request, please include the Motorola Solutions Product Name and Version, along with the Publicly Available Software specifics, such as the Publicly Available Software Name and Version.

Note that source code for the Publicly Available Software may be resident on the Motorola Solutions Product Installation Media, or on supplemental Motorola Solutions Product Media. Please reference and review the entire Motorola Solutions Publicly Available Software Legal Notices and End User License Agreement for the details on location and methods of obtaining the source code.

Note that dependent on the license terms of the Publicly Available Software, source code may not be provided. Please reference and review the entire Motorola Solutions Publicly Available Software Legal Notices and End User License Agreement for identifying which Publicly Available Software Packages will have source code provided.

To view additional information regarding licenses, acknowledgments and required copyright notices for Publicly Available Software used in this Motorola Solutions Product, please select “Legal Notices” display from the GUI (if applicable), or review the Legal Notices and End User License Agreement File/README, on the Motorola Solutions Product Install Media, or resident in the Motorola Solutions Product.

PUBLICLY AVAILABLE SOFTWARE LIST – KVL SOFTWARE INSTALLATION WIZARD

Name: RAPI2
Version: 1.2
Description: A managed wrapper to access the features exposed by the COM interfaces for the Remote API 2. These classes allow the developer to access information, files, and the registry on a device connected through ActiveSync from desktop applications.
Software Site: <http://rapi2.codeplex.com>
Source Code: No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License: MIT Type of License

Copyright (c) 2008 David Hall

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS“, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Credits: See License

Name: NLOG
Version: 2.0
Description: NLog is a logging platform for .NET with rich log routing and management capabilities. It makes it easy to produce and manage high-quality logs for application.
Software Site: <http://nlog.codeplex.com>
Site: <http://nlog-project.org>
Source Code: No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License: BSD Type of License

Copyright (c) 2004-2009, Jaroslaw Kowalski
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Jaroslaw Kowalski nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Credits: See License

PUBLICLY AVAILABLE SOFTWARE LIST – PDA

Name: NLOG
Version: 2.0
Description: NLog is a logging platform for .NET with rich log routing and management capabilities. It makes it easy to produce and manage high-quality logs for application.
Software Site: <http://nlog.codeplex.com>
<http://nlog-project.org>
Source Code: No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License: BSD Type of License

Copyright (c) 2004-2009, Jaroslaw Kowalski
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Jaroslaw Kowalski nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Credits: See License

Name: Smart Device Framework - Community Edition
Version: 2.3.0.39
Description: Extensions, to the NET Compact Framework core libraries, which enables calls to OS services.
Software Site: <http://www.opennetcf.com/Products/SmartDeviceFramework.aspx>
Source Code: No Source Code Distribution Obligations. The Community Edition of the Smart Device Framework is only provided in Binary form from the Software Authors. Source Code can be obtained via commercially licensing the Software.
License: OpenNETCF Shared Source License

NOTICE

This license governs use of the accompanying software (“Software”), and your use of the Software constitutes acceptance of this license.

Subject to the restrictions below, you may use the Software for any commercial or noncommercial purpose, including distributing derivative works.

SECTION 1: DEFINITIONS

- A. “OpenNETCF” refers to OpenNETCF Consulting, LLC, a limited liability corporation organized and operating under the laws of the state of Maryland.
- B. “SDF” refers to the OpenNETCF Smart Device Framework, which is an OpenNETCF software product.
- C. “SOFTWARE” refers to the source code, compiled binaries, installation files documentation and any other materials provided by OpenNETCF.

SECTION 2: LICENSE

You agree that:

- A. You are NOT allowed to combine or distribute the SOFTWARE with other software that is licensed under terms that seek to require that the SOFTWARE (or any intellectual property in it) be provided in source code form, licensed to others to allow the creation or distribution of derivative works, or distributed without charge.
- B. You may NOT distribute the SOFTWARE in source code form to any other person, company, government, group or entity.

- C. You may NOT decompile, disassemble, reverse engineer or otherwise attempt to extract, generate or retrieve source code from any compiled binary provided in the SOFTWARE.
- D. You will (a) NOT use OpenNETCF's name, logo, or trademarks in association with distribution of the SOFTWARE or derivative works unless otherwise permitted in writing; and (b) you WILL indemnify, hold harmless, and defend OpenNETCF from and against any claims or lawsuits, including attorneys fees, that arise or result from the use or distribution of your modifications to the SOFTWARE and any additional software you distribute along with the SOFTWARE.
- E. The SOFTWARE comes “as is”, with no warranties. None whatsoever. This means no express, implied or statutory warranty, including without limitation, warranties of merchantability or fitness for a particular purpose or any warranty of title or non-infringement.
- F. Neither OpenNETCF nor its suppliers will be liable for any of those types of damages known as indirect, special, consequential, or incidental related to the SOFTWARE or this license, to the maximum extent the law permits, no matter what legal theory its based on. Also, you must pass this limitation of liability on whenever you distribute the SOFTWARE or derivative works.
- G. If you sue anyone over patents that you think may apply to the SOFTWARE for a person's use of the SOFTWARE, your license to the SOFTWARE ends automatically.
- H. The patent rights, if any, granted in this license only apply to the SOFTWARE, not to any derivative works you make.
- I. The SOFTWARE is subject to U.S. export jurisdiction at the time it is licensed to you, and it may be subject to additional export or import laws in other places. You agree to comply with all such laws and regulations that may apply to the SOFTWARE after delivery of the SOFTWARE to you.
- J. If you are an agency of the U.S. Government, (i) the SOFTWARE is provided pursuant to a solicitation issued on or after December 1, 1995, is provided with the commercial license rights set forth in this license, and (ii) the SOFTWARE is provided pursuant to a solicitation issued prior to December 1, 1995, is provided with Restricted Rights as set forth in FAR, 48 C.F.R. 52.227-14 (June 1987) or DFAR, 48 C.F.R. 252.227-7013 (Oct 1988), as applicable.
- K. Your rights under this license end automatically if you breach it in any way.
- L. This license contains the only rights associated with the SOFTWARE and OpenNETCF reserves all rights not expressly granted to you in this license. © 2006 OpenNETCF Consulting, LLC. All rights reserved.

Credits: See License Above

PUBLICLY AVAILABLE SOFTWARE LIST – SECURITY ADAPTER

Name: Buffer Management Source Code from OpenBSD Operating System, as well as, OpenSSH Project.

Version: N/A

Description: This Package was included by Commercial Third Party Software Development Kit, from WindRiver-Interpeak, within the Motorola Product.

Copyright 2000-2005 Interpeak AB (<http://www.interpeak.se>).
All rights reserved.

Software Site: <http://www.openbsd.org>

License: The utilized Code is under BSD Type of License

Author: Tatu Ylonen <ylo@cs.hut.fi>

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved.

Functions for manipulating fifo buffers (that can grow if needed).

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Credits: OpenBSD Project, <http://www.openbsd.org>
Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

Name: C Support Libraries and Headers

Version: N/A

Description: The Packages were included by Commercial Third Party Software Development Kit, from Blunk Microsystems, within the Motorola Product.

Copyright 2009, Blunk Microsystems, ALL RIGHTS RESERVED

Software Site: <http://www.blunkmicro.com>

Source Code: No Source Code Distribution Obligations
License: The utilized Code is under BSD and MIT Type of Licenses

sccl.c, vscanf.c

Copyright (c) 1990 The Regents of the University of California.
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms, and that any documentation related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

xscanf.c

Copyright (c) 1990, 2006 The Regents of the University of California.
All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

stdint.h

Copyright (c) 2004, 2005 by Ralf Corsepius, Ulm/Germany.
All rights reserved.

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

Credits: N/A

PUBLICLY AVAILABLE SOFTWARE COMMON LICENSES

No Common Licenses included.

Commercial Warranty and Service Limited Warranty

MOTOROLA COMMUNICATION PRODUCTS

I. WHAT THIS WARRANTY COVERS AND FOR HOW LONG:

MOTOROLA SOLUTIONS, INC. (“MOTOROLA”) warrants the MOTOROLA manufactured Communication Products listed below (“Product”) against defects in material and workmanship under normal use and service for a period of time from the date of purchase as scheduled below:

KVL 4000 Key Variable Loader	One (1) Year
Product Accessories	One (1) Year

MOTOROLA, at its option, will at no charge either repair the Product (with new or reconditioned parts), replace it (with a new or reconditioned Product), or refund the purchase price of the Product during the warranty period provided it is returned in accordance with the terms of this warranty. Replaced parts or boards are warranted for the balance of the original applicable warranty period. All replaced parts of Product shall become the property of MOTOROLA.

This express limited warranty is extended by MOTOROLA to the original end user purchaser only and is not assignable or transferable to any other party. This is the complete warranty for the Product manufactured by MOTOROLA. MOTOROLA assumes no obligations or liability for additions or modifications to this warranty unless made in writing and signed by an officer of MOTOROLA. Unless made in a separate agreement between MOTOROLA and the original end user purchaser, MOTOROLA does not warrant the installation, maintenance or service of the Product.

MOTOROLA cannot be responsible in any way for any ancillary equipment not furnished by MOTOROLA which is attached to or used in connection with the Product, or for operation of the Product with any ancillary equipment, and all such equipment is expressly excluded from this warranty. Because each system which may use the Product is unique, MOTOROLA disclaims liability for range, coverage, or operation of the system as a whole under this warranty.

II. GENERAL PROVISIONS:

This warranty sets forth the full extent of MOTOROLA's responsibilities regarding the Product. Repair, replacement or refund of the purchase price, at MOTOROLA's option, is the exclusive remedy.

THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED TO THE DURATION OF THIS LIMITED WARRANTY. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW.

III. STATE LAW RIGHTS:

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION OR EXCLUSIONS MAY NOT APPLY.

This warranty gives specific legal rights, and there may be other rights which may vary from state to state.

IV. HOW TO GET WARRANTY SERVICE:

You must provide proof of purchase (bearing the date of purchase and Product item serial number) in order to receive warranty service and, also, deliver or send the Product item, transportation and insurance prepaid, to an authorized warranty service location. Warranty service will be provided by MOTOROLA through one of its authorized warranty service locations. If you first contact the company which sold you the Product (e.g., dealer or communication service provider), it can facilitate your obtaining warranty service. You can also call MOTOROLA at 1-800-927-2744 in the US/Canada.

V. WHAT THIS WARRANTY DOES NOT COVER:

1. Defects or damage resulting from use of the Product in other than its normal, customary or authorized manner.
2. Defects or damage from misuse, accident, water, neglect or act of God.
3. Defects or damage from improper testing, operation, maintenance, installation, alteration, modification, or adjustment not provided or authorized in writing by MOTOROLA.
4. Breakage or damage to antennas unless caused directly by defects in material workmanship.
5. A Product subjected to unauthorized Product modifications, disassembles or repairs (including, without limitation, the addition to the Product of non-MOTOROLA supplied equipment) which adversely affect performance of the Product or interfere with MOTOROLA's normal warranty inspection and testing of the Product to verify any warranty claim.
6. Product which has had the serial number removed or made illegible.
7. Rechargeable batteries if:
 - any of the seals on the battery enclosure of cells are broken or show evidence of tampering.
 - the damage or defect is caused by charging or using the battery in equipment or service other than the Product for which it is specified.
8. Freight costs to the repair depot.
9. A Product which, due to illegal or unauthorized alteration of the software/firmware in the Product, does not function in accordance with MOTOROLA's published specifications or the FCC type acceptance labeling in effect for the Product at the time the Product was initially distributed from MOTOROLA.
10. Scratches or other cosmetic damage to Product surfaces that does not affect the operation of the Product.
11. Normal and customary wear and tear.

VI. PATENT AND SOFTWARE PROVISIONS:

MOTOROLA will defend, at its own expense, any suit brought against the end user purchaser to the extent that it is based on a claim that the Product or parts infringe a United States patent, and MOTOROLA will pay those costs and damages finally awarded against the end user purchaser in any such suit which are attributable to any such claim, but such defense and payments are conditioned on the following:

1. that MOTOROLA will be notified promptly in writing by such purchaser of any notice of such claim;
2. that MOTOROLA will have sole control of the defense of such suit and all negotiations for its settlement or compromise; and
3. should the Product or parts become, or in MOTOROLA's opinion be likely to become, the subject of a claim of infringement of a United States patent, that such purchaser will permit MOTOROLA, at its option and expense, either to procure for such purchaser the right to continue using the Product or parts or to replace or modify the same so that it becomes non-infringing or to grant such purchaser a credit for the Product or parts as depreciated and accept its return. The depreciation will be an equal amount per year over the lifetime of the Product or parts as established by MOTOROLA.

MOTOROLA will have no liability with respect to any claim of patent infringement which is based upon the combination of the Product or parts furnished hereunder with software, apparatus or devices not furnished by MOTOROLA, nor will MOTOROLA have any liability for the use of ancillary equipment or software not furnished by MOTOROLA which is attached to or used in connection with the Product. The foregoing states the entire liability of MOTOROLA with respect to infringement of patents by the Product or any parts thereof.

Laws in the United States and other countries preserve for MOTOROLA certain exclusive rights for copyrighted MOTOROLA software such as the exclusive rights to reproduce in copies and distribute copies of such MOTOROLA software. MOTOROLA software may be used in only the Product in which the software was originally embodied and such software in such Product may not be replaced, copied, distributed, modified in any way, or used to produce any derivative thereof. No other use including, without limitation, alteration, modification, reproduction, distribution, or reverse engineering of such MOTOROLA software or exercise of rights in such MOTOROLA software is permitted. No license is granted by implication, estoppel or otherwise under MOTOROLA patent rights or copyrights.

VII. GOVERNING LAW:

This Warranty is governed by the laws of the State of Illinois, U.S.A.

SERVICE

Proper repair and maintenance procedures will assure efficient operation and long life for this product. A Motorola maintenance agreement will provide expert service to keep this and all other communication equipment in perfect operating condition. A nationwide service organization is provided by Motorola to support maintenance services. Through its maintenance and installation program, Motorola makes available the finest service to those desiring reliable, continuous communications on a contract basis. For a contract service agreement, please contact your nearest Motorola service or sales representative, or an authorized Motorola dealer.

Repair Service Advantage (RSA) Service Agreements is a post-warranty service offering that provides for the repair of this product. The service agreement is renewable annually for as long as Motorola supports the equipment. For more information about RSA Service Agreements, contact the Motorola Radio Support Center at 800-247-2346 or your Customer Support Manager.

1 KVL 4000 – Introduction

1.1 MC55A0 PDA Reference

See the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at <http://www.motorola.com/enterprisemobility/manuals>) for the following information:

- Inserting/replacing the battery
- Charging the battery (Security Adapter disconnected)
- Changing the power settings (setting the timeout for turning off the display to conserve battery power)



SUGGESTION

Set up the PDA so that it turns itself off when it is not in use to preserve the KVL 4000 battery life.

- Changing the backlight settings:
 - Setting the display backlight time-out
 - Adjusting brightness
- Setting date and time for timestamping logs
- Turning KVL sounds on/off
- Troubleshooting the MC55
- MC55 performance specifications

1.2 Overview of the KVL 4000

The KVL 4000 Key Variable Loader is a portable, handheld, rugged device whose most basic function is to transfer encryption keys to a target device. Encryption keys can be entered manually by the KVL user, auto-generated by the KVL, obtained from or shared with another KVL, or downloaded from a Key Management Facility (KMF). Keys can be transferred to secure mobile and portable radios, infrastructure devices, and system test equipment.

The KVL 4000 provides a User Interface for entering encryption keys, downloading them from an external source, and transferring them to target devices. It also provides internal processing and memory for secure key storage, as well as interfaces for data communication.

1.2.1 KVL 4000 Components

The KVL 4000 consists of the two main components:

- **Personal Digital Assistant (PDA)**
- **Security Adapter**

Figure 1-1 KVL 4000 Key Variable Loader



1.2.1.1 Personal Digital Assistant

The Personal Digital Assistant (PDA) is the host component of the KVL 4000, responsible for controlling all operations of the device. It is a Motorola rugged handheld computer operating Windows Mobile 6.5. The PDA model used as part of the KVL 4000 is MC55A0.

Figure 1-2 Personal Digital Assistant (PDA)**Table 1-1 PDA Controls and Ports Used in the KVL Operation**

Callout Number	Item	Description
1	Charging/Battery Status LED	Blinks when the battery is charging; solid when the battery is charged.
2	Touch screen	Navigate through the UI by tapping or dragging items on the screen.
3	Volume Up Key	Press to turn the volume of the KVL sounds up.
4	Volume Down Key	Press to turn the volume of the KVL sounds down.
5	Action Button	You can use it instead of your finger to initiate an action.
6	End Key	Press to return to the KVL main screen.
7	Side Up Navigation Key	You can use it instead of your finger to scroll up a list.
8	Side Down Navigation Key	You can use it instead of your finger to scroll down a list.
9	Backspace Key	Press to delete digits entered with the PDA keypad.

Table 1-1 PDA Controls and Ports Used in the KVL Operation (cont'd.)

Callout Number	Item	Description
10	Shift Key	Press twice to access and lock capital letters.
11	PDA Keypad	Use it for all cases when alphanumeric text entry is required.
12	Orange Key	Press twice to access and lock the secondary layer of characters.
13	Power Button	Press to power on or suspend the KVL; press and hold for 5 seconds to reboot.
14	I/O Connector	Use to connect the PDA to the Security Adapter or to a PC through the USB Programming Cable.
15	Stylus	You can use it instead of your finger to tap and drag items on the screen.

**NOTE**

For more information on the PDA, see the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at <http://www.motorola.com/enterprisemobility/manuals>).

1.2.1.2 Security Adapter

The Security Adapter is an integral component of the KVL 4000, providing secure storage of encryption keys, cryptographic operations, and port access for the KVL 4000.

**CAUTION**

Always make sure to exit the KVL application on the PDA before disconnecting the Security Adapter. Otherwise, you may lose any unsaved work or cause data corruption.

Figure 1-3 Security Adapter**Table 1-2 Security Adapter Ports and Interfaces**

Callout Number	Item	Description
1	Key load Port	Serves as the interface to all target devices for key loading and upgrade operations.
2	Tricolored LED	Serves as the diagnostic status indicator for the KVL. The available states are: <ul style="list-style-type: none"> • Momentary Red – before security adapter self tests • Fast Flashing Amber – during security adapter self tests (power up) • Solid Green – after successful security adapter self tests • Solid Red – fatal error / hardware failure
3	Charging Port	Connect the charger to charge the PDA battery.

Table 1-2 Security Adapter Ports and Interfaces (cont'd.)

Callout Number	Item	Description
4	DB9 Port (RS-232)	Serves as the interface to: <ul style="list-style-type: none"> • a PC for transferring log records • a radio for Tactical OTAR key management • a mobile radio's Remote Control Head • a KMF (serial modem connection) • a KMF (direct connection)
5	USB Port	Serves as the interface to all expansion adapters used by the KVL, such as a USB modem for KMF communication.
6	Locking Tabs	Attach the Security Adapter to the PDA and slide the two locking tabs up until they both lock into position.
7	PDA Interface Port	Serves as the interface to any attached host (the primary host for the Security Adapter is the PDA).

1.2.2 KVL 4000 Key Features

The KVL 4000 offers the following features:

- Manual and automatic generation of encryption keys
- Password protection (Administrator and Operator security levels)
- Secure storage of encryption keys
- Configuration of system- and user-specific settings
- Support of the KVL and Crypto Module upgrades
- Support of the following encryption algorithms:
 - ADP
 - AES-256
 - DES-XL
 - DES-OFB
 - DVI-XL
 - DVP-XL
- Key Management Support for the following encryption protocols:
 - 9.6 kbps Secure ASTRO® (VSELP Vocoder)
 - 9.6 kbps Secure APCO Project 25 (IMBE Vocoder)
- Support of the following encryption standards:
 - FIPS 46-3
 - FIPS 140-2

– FIPS 197

- USB, DB9 (RS-232), and key load ports
- Support of modem connectivity
- Sharing encryption keys between two KVLs
- Maintenance of log records of KVL activities
- Transferring keys from a Key Management Facility (KMF) using the Store and Forward feature
- Keyset changeover on a target radio



NOTE

The KVL supports any combination of algorithms.



NOTE

ADP does not support the following features related to OTAR:

- Store & Forward
- KEK Key loading
- Tactical OTAR
- Remote Control Head key loading

1.2.3 KVL 4000 Sounds

Table 1-3 Sounds Played by the KVL 4000

Sound name	Description
attention	Played for any case when your attention is needed.
bad bonk	Played when you enter an invalid digit when entering a value.
completed	Played when an action or a process (such as loading keys) is completed.
connected	Played when you connect an external device (such as a radio) to the KVL.



NOTE

For information on how to turn the sounds on or off, see the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at <http://www.motorola.com/enterprisemobility/manuals>).

1.2.4 Using the KVL 4000

Secure communications systems are designed to provide coded (encrypted) voice and data signals between some or all links in the system (including RF links and network links). In order to do this, each device, such as a radio or fixed encryption unit, is loaded with a multi-digit encryption variable (a key). This key is used by the encryption algorithm, such as AES-256 or DES-XL, built into the device to mathematically encrypt all transmitted voice and data signals, and decode all encrypted received voice and data signals.

Only devices in the system with the same algorithm and encryption key can decode the encrypted signal and carry on communications with each other. Talkgroups can therefore be created by controlling the assignment of encryption keys to specific groups of radios.

1.2.4.1 Types of Encryption Keys

The KVL stores two basic types of encryption keys:

- **Traffic Encryption Keys (TEK)** – Used by subscriber units to encrypt/decrypt voice and data communications.
- **Key Encryption Keys (KEK)** – Used by the KVL to provide an additional level of encryption to the encryption keys when transferring keys directly to the KMF or over the air to secure subscriber devices.

Both types of keys are stored in the KVL memory in an encrypted format and are protected from tampering.

1.2.4.2 Entering and Loading Keys – Overview

Encryption keys are entered into the KVL memory locations (slots). The keys may then be transferred (loaded) to a target device, such as a secure radio.

A two-step process is required for most encryption keys:

- Create (enter) the multi-digit encryption key into the KVL memory. See [3.1 Entering Encryption Keys, page 3-1](#).
- Connect the KVL to a target device, such as a radio, and transfer the key to the target device. See [1.4.4 Connecting the KVL to Target Devices, page 1-13](#) and [Chapter 4 KVL 4000 – Loading Encryption Keys into Target Devices](#).

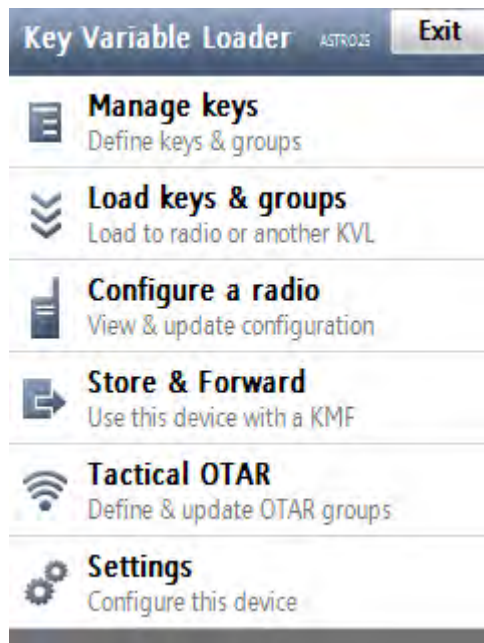
1.3 KVL 4000 User Interface

You navigate through the KVL User Interface and perform operations by:

- Selecting list items, buttons, and tabs
- Entering data
- Dragging sliders
- Scrolling through lists

You can navigate through the KVL UI using your finger. Alternatively, you can use the stylus attached to the side of the PDA, or press hard controls on the PDA.

Figure 1-4 KVL 4000 Main Screen



1.4 KVL 4000 – Getting Started

1.4.1 Applying Enhanced Security Settings Through the KVL Software Installation Wizard

Prerequisites:

- Ensure that you have the USB Programming Cable.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.

When and where to use:

By default, the KVL uses Transparent Security Settings. If required by your organization's policies, follow this procedure to apply Enhanced Security Settings.



Applying Enhanced Security Settings causes the KVL to:

- prevent installation and launching of any unsigned applications
- disable the use of wireless modem (Bluetooth and WiFi are disabled)
- require you to set a password on the Operating System

Procedure Steps

- 1 If the KVL Application software is running, exit or log out of the KVL.
 - 2 Disconnect the Security Adapter from the PDA.
 - 3 Connect the PDA to a PC using the USB Programming Cable.
-

Figure 1-5 PDA and PC – Connected



Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.



NOTE

If ActiveSync or Windows Mobile Device Center do not start automatically, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Client** or **USB OTG** mode.

-
- 4 Insert the CD provided by Motorola and run the Setup.exe file to start the KVL Software Installation Wizard.
Step result: The End User License Agreement screen appears.
 - 5 Click **Accept**.
-

- 6 In the window that appears, select the check box next to **Your device is using Transparent Security Settings (default)**, and click **Next**. The Enhanced Security Settings will be applied after the KVL application reinstallation/upgrade.

**NOTE**

During the process, the PDA may restart several times.

Step result: When the process is completed, a message appears, asking you to configure your device according to the security policy.

- 7 Check your PDA screen and follow the instructions to renew your password settings.
 - 8 When you have entered and confirmed the password on your PDA, click **OK** on the message on your PC.
Step result: The Enhanced Security Settings are applied successfully.
-

- 9 Click **Next** → **Exit** to close the KVL Software Installation Wizard.
-

- 10 Disconnect the USB Programming Cable from the PDA.
-

- 11 Connect the Security Adapter to the PDA.

**NOTE**

If the Security Adapter is not detected automatically, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.2 Applying Transparent Security Settings Through the KVL Software Installation Wizard

Prerequisites:

- Ensure that you have the USB Programming Cable.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.

Procedure Steps

- 1 If the KVL Application software is running, exit or log out of the KVL.
 - 2 Disconnect the Security Adapter from the PDA.
-

- 3 Connect the PDA to a PC using the USB Programming Cable.

Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.

**NOTE**

If ActiveSync or Windows Mobile Device Center do not start automatically, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Client** or **USB OTG** mode.

- 4 Insert the CD provided by Motorola and run the Setup.exe file to start the KVL Software Installation Wizard.

Step result: The End User License Agreement screen appears.

- 5 Click **Accept**.
-

- 6 In the window that appears, clear the check box next to **Your device is using Enhanced Security Settings**, and click **Next**. The Transparent Security Settings will be applied after the KVL application reinstallation/upgrade.

**NOTE**

During the installation process, the PDA may restart several times.

- 7 When the process is completed, click **Next** → **Exit** to close the KVL Software Installation Wizard.

Step result: The Transparent Security Settings are applied successfully.

- 8 Disconnect the USB Programming Cable from the PDA.
-

- 9 Connect the Security Adapter to the PDA.

**NOTE**

If the Security Adapter is not detected automatically, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.3 Connecting the PDA and the Security Adapter

Procedure Steps

- 1 Connect the PDA and the Security Adapter.

Figure 1-6 PDA and Security Adapter – Connecting



- 2 To secure the Adapter, slide the locking tabs up fully until a click is felt indicating they are in the locked position. If either slide is not in the locked position, an orange dot is visible.

Figure 1-7 PDA and Security Adapter – Connected



- 3 If the Security Adapter is not detected automatically after powering on the PDA, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.4 Connecting the KVL to Target Devices

1.4.4.1 Connecting the KVL to a Radio or Another Target Device

You can load encryption keys into the following devices:

- Secure ASTRO® 25 Single Key Target Radio

- Secure ASTRO® 25 Multiple Key Target Radio
- Another KVL unit (see [1.4.4.2 Connecting Two KVL Units, page 1-16](#))
- Radio Network Controller (RNC)
- Digital Interface Unit (DIU)
- Motorola Gold Elite Gateway (MGEG)
- MCC 7500 Dispatch Console
- PDEG Encryption Unit
- CAI Data Encryption Module (CDEM)
- Key Management Facility (KMF) (see [1.4.4.3 Connecting the KVL to the KMF, page 1-16](#))
- KMF CryptR
- CRYPTR micro (used with MCC 7100 IP Dispatch Console and AME 1500/2000) (see [1.4.4.4 Connecting the KVL to the CRYPTR micro, page 1-21](#))

Procedure Steps

- 1 For information on what cables/adaptors to use with particular target devices, see [Table B-5 Interface Cables in B KVL 4000 – Orderable Parts, page B-1](#).
-
- 2 Connect the KVL and the Target Device using an appropriate key load cable and an adaptor (if required).

Figure 1-8 KVL and Radios – Connected (Example)



Figure 1-9 KVL and KMF – Connected

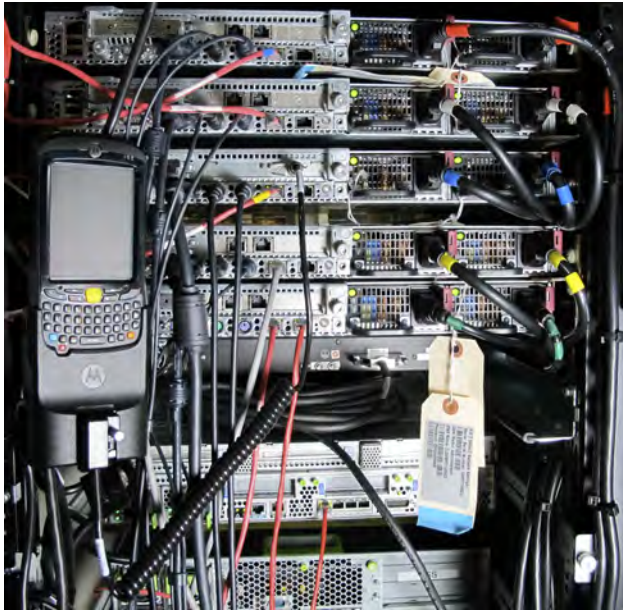


Figure 1-10 KVL and MEGEG – Connected (Example)



1.4.4.2 Connecting Two KVL Units

Prerequisites:

Ensure you have the KVL to KVL cable.

Procedure Steps

- 1 Take the KVL to KVL cable (TKN8209).
 - 2 Connect two KVLs through their key load ports.
-

Figure 1-11 Two KVL Units – Connected



NOTE

The KVL 4000 is also compatible with the previous models of the KVL.

1.4.4.3 Connecting the KVL to the KMF

1.4.4.3.1 Connecting the KVL to the KMF – Direct Connection

Prerequisites:

Ensure you have a Null Modem Cable.

When and where to use:

Use these steps to directly connect the KVL to the KMF.

Procedure Steps

- 1 Take a Null Modem Cable.
- 2 Connect the KVL to the KMF through the DB9 Port (RS-232).



NOTE

Depending on the cable type, you may need to use a DB9 Gender Changer.

Figure 1-12 KVL and KMF – Direct Connection



1.4.4.3.2 Connecting the KVL to the USB Modem for the KMF Communication

Prerequisites:

Ensure that:

- You have the power supply.
- You have the USB modem.

Procedure Steps

- 1 Connect the power supply to the KVL.



IMPORTANT

It is recommended that you keep the power supply connected to the KVL during the operation.

- 2 Connect the KVL to the USB modem.



NOTE

Use the MultiMobile™ USB modem.

Figure 1-13 KVL and USB Modem – Connected



- 3 Connect the USB modem to the telephone line.
-

1.4.4.3.3 Connecting the KVL to the Serial Modem for the KMF Communication

Prerequisites:

Ensure you have:

- serial modem
- serial cable

Procedure Steps

- 1 Take a serial cable (CKN6324).
 - 2 Connect the KVL to the serial modem through the KVL DB9 (RS-232) Port.
-

Figure 1-14 KVL and Serial Modem – Connected (Example)



IMPORTANT

Since the KVL 4000 has no flow control, you need to configure any attached external modem to:

- Override the modem's Data Terminal Ready signal.
 - Turn off the echo of offline commands.
-

1.4.4.3.4 Connecting the KVL to the Network for the KMF Communication

Prerequisites:

Ensure that you have:

- USB to Ethernet Adapter
- MINI-B to Type-A USB Cable
- Ethernet cable

Procedure Steps

- 1 Connect the KVL to the power supply.



IMPORTANT

It is recommended that you keep the power supply connected to the KVL during the operation.

- 2 Connect the USB to Ethernet Adapter to the USB Port on the KVL using the MINI-B to Type-A USB Cable.



NOTE

Use the CradlePoint Technology® Ethernet adapter.

- 3 Connect the USB to Ethernet Adapter to the network, using the Ethernet cable.

Figure 1-15 KVL and USB to Ethernet Adapter - Connected



1.4.4.4 Connecting the KVL to the CRYPTR micro

Prerequisites:

Ensure you have the CRYPTR micro key load cable.

Procedure Steps

- 1 Connect the CRYPTR micro key load cable to the key load port on the KVL.
- 2 Insert the CRYPTR micro into the Cable Connector.

Figure 1-16 CRYPTR micro and KVL - Connected



1.4.5 Charging the KVL 4000

Prerequisites:

Ensure that you have:

- Power Supply
- AC Line Cord (See [B KVL 4000 – Orderable Parts, page B-1](#) for the list of compatible AC Line Cords.)

Procedure Steps

- 1 Connect one end of the AC Line Cord to the power source.
- 2 Connect the other end of the AC Line Cord to the power supply.
- 3 Connect the power supply to the KVL through the Charging Port on the Security Adapter.

Step result: The KVL starts charging. The middle LED on the PDA is blinking to indicate the KVL is being charged. Once the device is fully charged, the LED becomes solid.

Figure 1-17 KVL 4000 - Charging



1.4.6 Launching the KVL Application

Procedure Steps

- 1 If the device is not already powered on, press the **Power** button on the PDA.

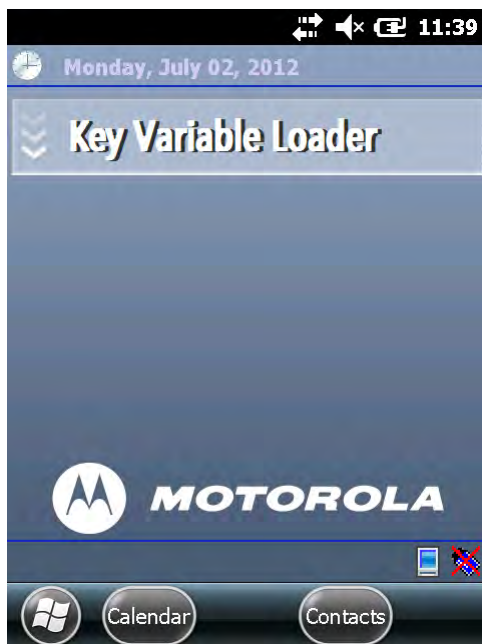


NOTE

If you reboot the device, the KVL application launches automatically.

Step result: The KVL powers on and the **Today** screen appears.

Figure 1-18 Today Screen



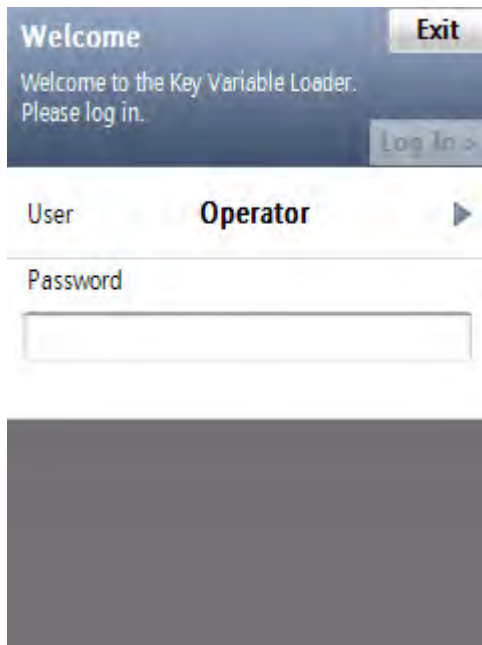
- 2 Tap the **Key Variable Loader** button.

**NOTE**

If the PDA and the Security Adapter are not compatible, a notification appears.

Step result: If there are no passwords defined for your KVL, the KVL application launches and the KVL main screen appears. Otherwise, the **Welcome** screen appears.

Figure 1-19 Welcome Screen

**NOTE**

- To change the user level, tap **User** (the current user level is presented). The available values are **Operator** and **Administrator**.
- To exit the KVL application, tap **Exit**.

**NOTE**

If you launch the KVL first time after reinstalling/upgrading the KVL application, upgrading Security Adapter software, or applying Security Settings on the KVL, the End User License Agreement screen appears. To continue, select **Accept >**.

- 3 In the **Password** field, type your password using the keypad and tap **Log In >**.

Step result: The KVL main screen appears.

**NOTE**

If you log on as an Administrator and there are upgrades available for the Security Adapter or a target device, the **Upgrades available** screen appears. For more information on upgrades, see the *KVL 4000 FLASHPort Upgrade User Guide*.

**NOTE**

If you log on as an Operator and enter an incorrect password 3 times, your account is locked. Wait 15 minutes to try again, or contact an Administrator to unlock your account (see [12.3 Unlocking the Operator Account, page 12-5](#)).

1.4.7 Exiting the KVL Application

When and where to use:

Use these steps to exit the KVL application.

**IMPORTANT**

To avoid unnecessary drain on the battery, always exit the KVL application before turning off the unit with the **Power** button.

Procedure Steps

- 1 Navigate to the KVL main screen.

**NOTE**

You can do it by pressing the End Key on the PDA (see [1.2.1.1 Personal Digital Assistant, page 1-2](#)).

- 2 Tap **Exit**.

**NOTE**

If you have passwords defined for your KVL, the button says **Log Off** instead.

Step result: Depending on whether you have passwords defined or not, the **Exit** or the **Log off** screen appears.

Figure 1-20 Exit Screen

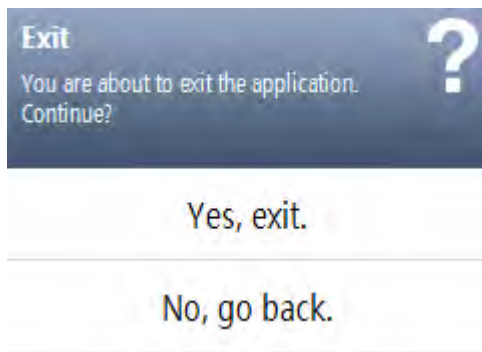
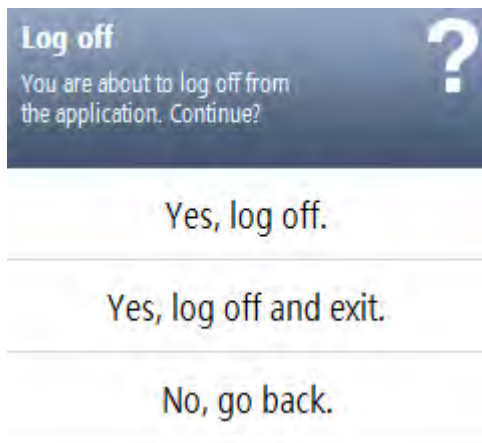


Figure 1-21 Log Off Screen



- 3 Select **Yes, exit** or **Yes, log off and exit**.

Step result: You exit the application and the **Today** screen appears.

1.4.8 Configuring VPN Settings

The KVL can use an Ethernet connection to communicate with the KMF. If applicable, you can establish this connection within your organization's trusted network, or you can use the VPN client provided by Motorola. To be able to use the VPN client, configure the VPN settings on the PDA.

There are configuration profiles for two scenarios:

- When the KVL is directly connected to the Firewall (see [1.4.8.1 Configuring VPN Settings - KVL Directly Connected to the Firewall, page 1-27](#)).
- When the KVL is connected to the Firewall through a network (see [1.4.8.2 Configuring VPN Settings - KVL Connected to the Firewall Through a Network, page 1-35](#)).

**NOTE**

It is recommended that you create both profiles.

1.4.8.1 Configuring VPN Settings - KVL Directly Connected to the Firewall

Prerequisites:

- Obtain the VPN gateway IP address from the system administrator.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.
- Ensure that NCP Entry Configuration Manager WM is installed on your PC. NCP Entry Configuration Manager WM is available at <http://www.ncp-e.com/en/downloads/software.html>.
- Ensure that you have the USB Programming Cable.

When and where to use:

If you are going to establish the KVL to KMF Ethernet connection using the VPN client provided by Motorola, use these steps to create a configuration profile for a scenario when the KVL is going to be directly connected to the Firewall.

Procedure Steps

- 1 On the desktop, select **Start** → **Programs** → **NCP Secure Client** → **NCP Entry Configuration Manager WM**.

Step result: The NCP Entry Configuration Manager WM launches.

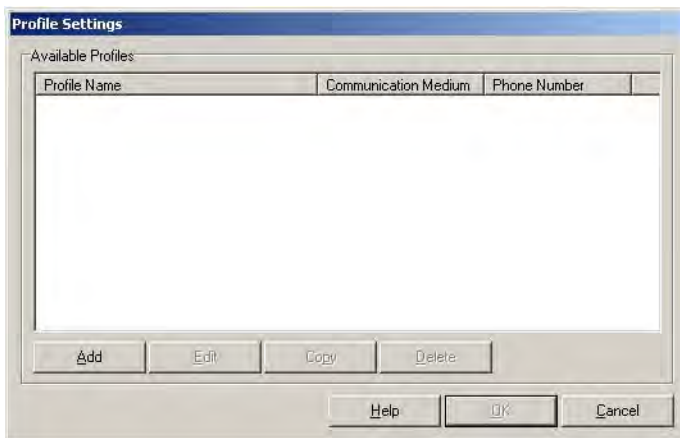
Figure 1-22 NCP Entry Configuration Manager WM Window



- 2 On the NCP Entry Configuration Manager WM window, select **Configuration** → **Profile Settings**.

Step result: The Profile Settings window appears.

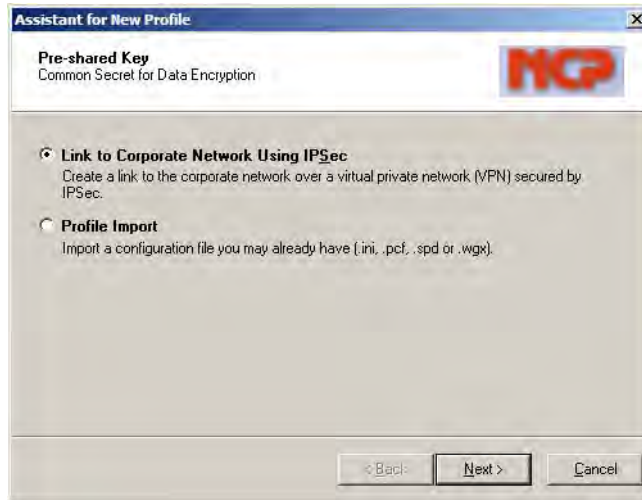
Figure 1-23 Profile Settings Window



- 3 On the Profile Settings window, click **Add**.

Step result: The Assistant for New Profile – Pre-shared Key window appears.

Figure 1-24 Assistant for New Profile – Pre-shared Key Window



- 4 Select **Link to Corporate Network Using IPsec**, and click **Next**.

Step result: The Assistant for New Profile – Connection Name window appears.

Figure 1-25 Assistant for New Profile – Connection Name Window



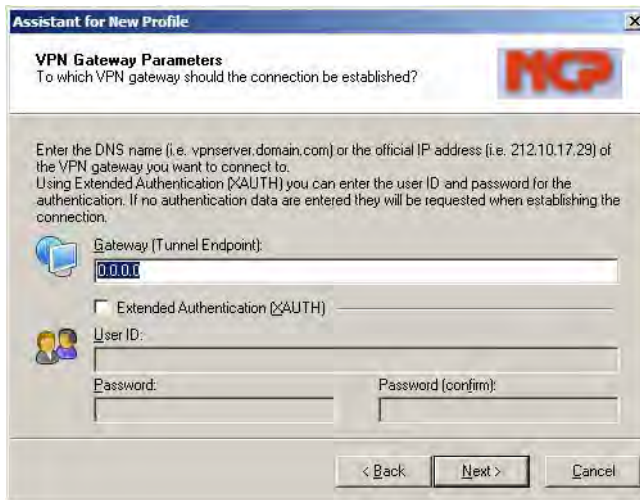
- 5 In the Name of the connection field, type **KVL4000 at Firewall**, and click **Next**.
Step result: The Assistant for New Profile – Communication Medium window appears.

Figure 1-26 Assistant for New Profile – Communication Medium Window



- 6 From the Communication Media drop-down list, select **LAN (over IP)**, and then click **Next**.
Step result: The Assistant for New Profile – VPN Gateway Parameters window appears.

Figure 1-27 Assistant for New Profile – VPN Gateway Parameters Window



- 7 On the VPN Gateway Parameters window, perform the following actions:
 - a. In the Gateway (Tunnel Endpoint) field, enter the IP address you obtained from the system administrator.

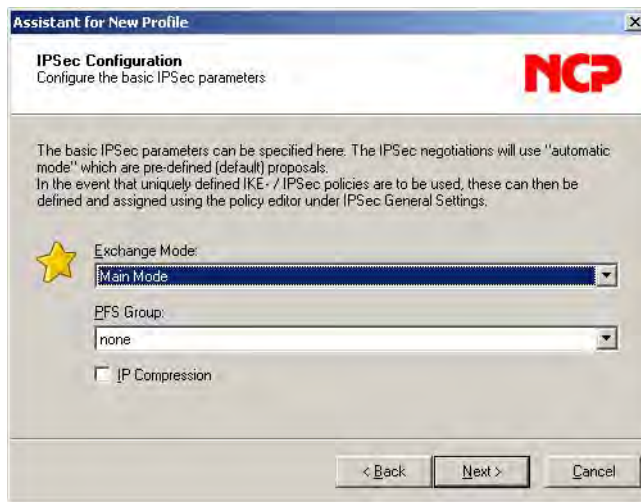
**NOTE**

For systems with the Dynamic System Resilience (DSR) feature, in case of a switchover, you will need to change the IP address to be able to contact the backup Gateway.

- b. Click **Next**.

Step result: The Assistant for New Profile – IPSec Configuration window appears.

Figure 1-28 Assistant for New Profile – IPSec Configuration Window



- 8 On the IPSec Configuration window, click **Next**.

Step result: The Assistant for New Profile – Pre-shared Key window appears.

Figure 1-29 Assistant for New Profile – Pre-shared Key

Assistant for New Profile

Pre-shared Key
Common Secret for Data Encryption

A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VPN client and VPN gateway).

Enter the appropriate value for the IKE ID according to the selected ID type.

Pre-shared Key

Shared Secret: Confirm Secret:

Local Identity (IKE)

Type: IP Address

ID:

< Back Next > Cancel

- 9 In the Pre-shared Key window, perform the following actions:
 - a. In the appropriate fields, enter and reenter the Shared Secret.



NOTE

The Pre-shared key that you enter here must match the Pre-shared key on the Firewall. For more information, see the *Firewall* manual.

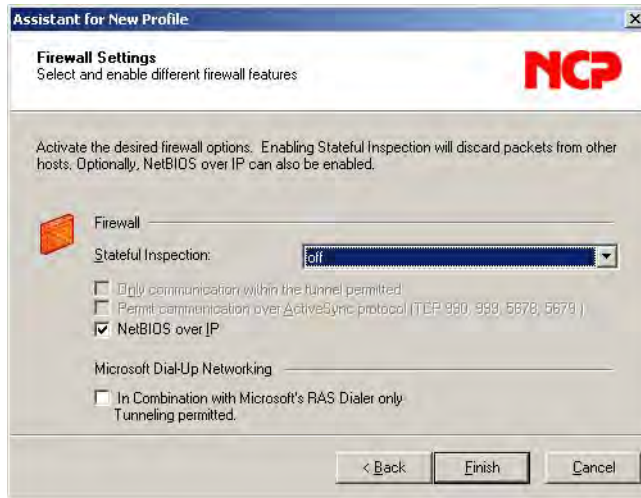
- b. From the Type drop-down list, select **Fully Qualified Domain Name**.
- c. In the ID field, enter the ID.
- d. Click **Next**.

Step result: The Assistant for New Profile – IPSec Configuration – IP Addresses window appears.

Figure 1-30 Assistant for New Profile – IPSec Configuration – IP Addresses Window

- 10 From the IP Address Assignment drop-down list, select **Local IP Address**, and then click **Next**.
Step result: The Assistant for New Profile – Firewall Settings window appears.

Figure 1-31 Assistant for New Profile – Firewall Settings Window



- 11 On the Firewall Settings window, click **Finish**.
Step result: The window closes.
- 12 On the Profile Settings window, click **OK**.
Step result: The window closes.
- 13 Connect the PDA to the PC using the USB Programming Cable.
Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.



NOTE

If ActiveSync or Windows Mobile Device Center do not start, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Client** or **USB OTG** mode.

- 14 Click **Upload** on the NCP Entry Configuration Manager WM window.
Step result: The upload process starts, followed by a confirmation message.

1.4.8.2 Configuring VPN Settings - KVL Connected to the Firewall Through a Network

Prerequisites:

- Obtain the VPN gateway IP address from the system administrator.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.
- Ensure that NCP Entry Configuration Manager WM is installed on your PC. NCP Entry Configuration Manager WM is available at <http://www.ncp-e.com/en/downloads/software.html>.
- Ensure that you have the USB Programming Cable.

When and where to use:

If you are going to establish the KVL to KMF Ethernet connection using the VPN client provided by Motorola, use these steps to create a configuration profile for a scenario when the KVL is going to be connected to the Firewall through a network.

Procedure Steps

- 1 On the desktop, select **Start** → **Programs** → **NCP Secure Client** → **NCP Entry Configuration Manager WM**.

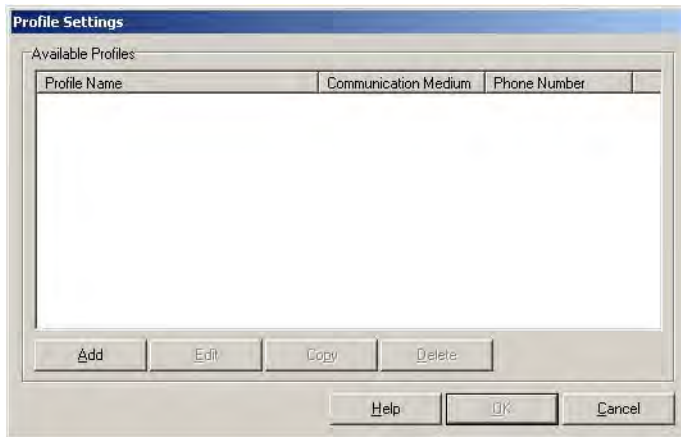
Step result: The NCP Entry Configuration Manager WM launches.

Figure 1-32 NCP Entry Configuration Manager WM Window



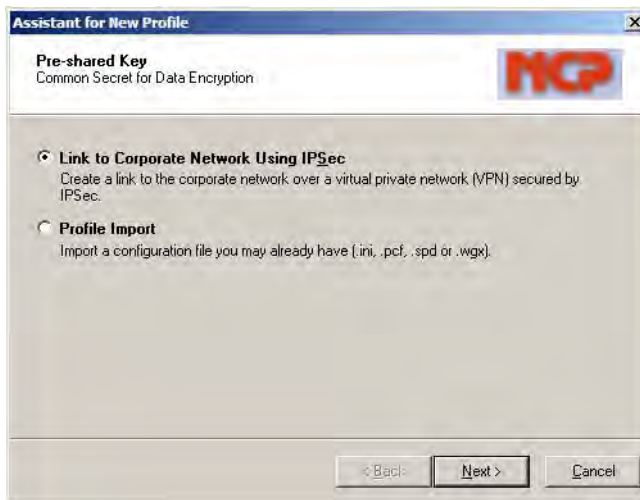
- 2 On the NCP Entry Configuration Manager WM window, select **Configuration** → **Profile Settings**.
Step result: The Profile Settings window appears.

Figure 1-33 Profile Settings Window



- 3 On the Profile Settings window, click **Add**.
Step result: The Assistant for New Profile – Pre-shared Key window appears.

Figure 1-34 Assistant for New Profile – Pre-shared Key Window



- 4 Select **Link to Corporate Network Using IPSec**, and click **Next**.

Step result: The Assistant for New Profile – Connection Name window appears.

Figure 1-35 Assistant for New Profile – Connection Name Window



- 5 In the Name of the connection field, type **KVL4000 through Network**, and click **Next**.

Step result: The Assistant for New Profile – Communication Medium window appears.

Figure 1-36 Assistant for New Profile – Communication Medium Window



- 6 From the Communication Media drop-down list, select **LAN (over IP)**, and then click **Next**.
Step result: The Assistant for New Profile – VPN Gateway Parameters window appears.

Figure 1-37 Assistant for New Profile – VPN Gateway Parameters Window

Assistant for New Profile

VPN Gateway Parameters
To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.
Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint):
0.0.0.0

Extended Authentication (XAUTH)

User ID:
Password:
Password (confirm):

< Back Next > Cancel

- 7 On the VPN Gateway Parameters window, perform the following actions:
 - a. In the Gateway (Tunnel Endpoint) field, enter the IP address you obtained from the system administrator.

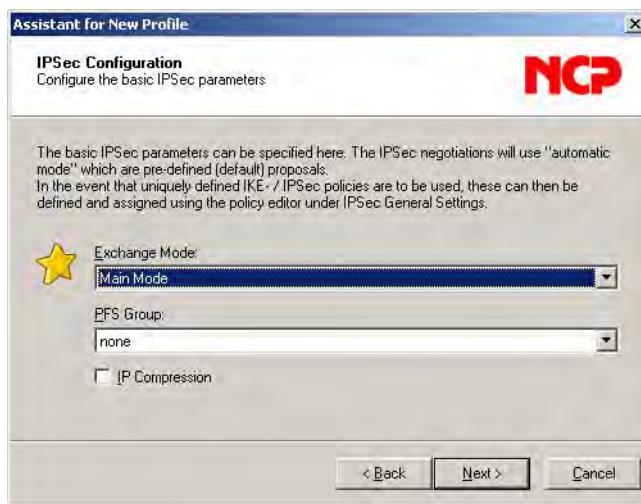
**NOTE**

For systems with the Dynamic System Resilience (DSR) feature, in case of a switchover, you will need to change the IP address to be able to contact the backup Gateway.

- b. Click **Next**.

Step result: The Assistant for New Profile – IPSec Configuration window appears.

Figure 1-38 Assistant for New Profile – IPSec Configuration Window



- 8 On the IPSec Configuration window, click **Next**.

Step result: The Assistant for New Profile – Pre-shared Key window appears.

Figure 1-39 Assistant for New Profile – Pre-shared Key



- 9 In the Pre-shared Key window, perform the following actions:
 - a. In the appropriate fields, enter and reenter the Shared Secret.



NOTE

The Pre-shared key that you enter here must match the Pre-shared key on the Firewall. For more information, see the *Firewall* manual.

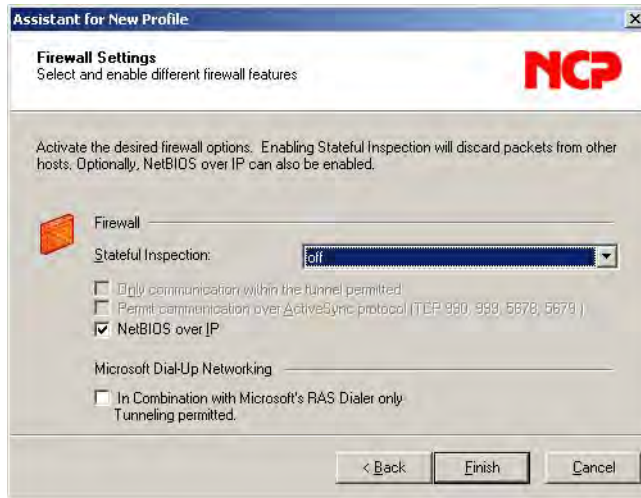
- b. From the Type drop-down list, select **Fully Qualified Domain Name**.
- c. In the ID field, enter the ID.
- d. Click **Next**.

Step result: The Assistant for New Profile – IPSec Configuration – IP Addresses window appears.

Figure 1-40 Assistant for New Profile – IPSec Configuration – IP Addresses Window

- From the IP Address Assignment drop-down list, select **Local IP Address**, and then click **Next**.
Step result: The Assistant for New Profile – Firewall Settings window appears.

Figure 1-41 Assistant for New Profile – Firewall Settings Window



- On the Profile Settings window, click **OK**.
Step result: The window closes.
- On the Profile Settings window, click **OK**.
Step result: The window closes.
- Connect the PDA to the PC using the USB Programming Cable.
Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.



If ActiveSync or Windows Mobile Device Center do not start, perform [12.4 Setting the PDA USB Mode, page 12-5](#) to put the PDA into the **USB Client** or **USB OTG** mode.

- Click **Upload** on the NCP Entry Configuration Manager WM window.
Step result: The upload process starts, followed by a confirmation message.

1.4.9 Establishing the VPN Connection

Prerequisites:

- For the VPN connection to work, the NCP Client Service must be running. On the PDA screen, select **Start** → **Programs** → **NCP Client Service**, and run the service if it is not already running.
- Obtain the VPN Username and VPN Password from your system administrator.

When and where to use:

Use these steps if you want to establish the KVL to KMF Ethernet connection using the VPN client provided by Motorola.

Procedure Steps

- 1 In the upper left corner of the PDA screen, select **Start** → **Programs**.

Step result: The Programs screen appears.

Figure 1-42 Programs Screen



- 2 Select the **NCP Secure Client** icon.

Step result: The NCP Secure Client screen appears.

Figure 1-43 NCP Secure Client Screen – KVL 4000 at Firewall



Figure 1-44 NCP Secure Client Screen – KVL 4000 Through Network



- 3 From the drop-down list, select one of the following options:

If...	Then...
Your KVL is connected directly to the Firewall...	Select KVL4000 at Firewall .
Your KVL is connected to the Firewall through a network...	Select KVL4000 through Network .

- 4 Select **Connect**.

Step result: You are prompted to enter your VPN Username.

- 5 Type in your VPN Username and select **OK**.

Step result: You are prompted to enter your VPN Password.

- 6 Type in your VPN Password and select **OK**.

Step result: The **Connecting** animation appears, followed by the Connected screen. The VPN connection is established.

Figure 1-45 NCP Secure Client Screen – KVL 4000 at Firewall – Connected



Figure 1-46 NCP Secure Client Screen – KVL 4000 Through Network – Connected



1.4.10 Terminating the VPN Connection

When and where to use:

Use these steps if you established the KVL to KMF Ethernet connection using the VPN client provided by Motorola.

Procedure Steps

- 1 In the upper left corner of the PDA screen, select **Start** → **Programs**.

Step result: The Programs screen appears.

Figure 1-47 Programs Screen



- 2 Select the **NCP Secure Client** icon.

Step result: The NCP Secure Client screen appears.

- 3 Select **Disconnect**.

Step result: The **Disconnecting** animation appears, and then the NCP Secure Client screen comes back. The VPN connection is terminated.

Postrequisites:

Before provisioning radios with authentication keys, ensure the NCP Client Service is stopped. On the PDA screen, select **Start** → **Programs** → **NCP Client Service**, and stop the service.

2 KVL 4000 – Performing Initial Programming

Before using your KVL to enter and load encryption keys, set several parameters that determine how the KVL operates.

2.1 KVL 4000 User Preference Parameters

The user preference parameters and settings are not required for operation of the KVL, but instead provide a way of customizing certain functions to suit your individual needs.

2.1.1 Setting the KVL Log Off Time

For security reasons, you can set the period of inactivity after which you are logged off from the KVL.

Prerequisites:

This option is only available if you have set passwords on your KVL. Only an Administrator can set or change the KVL log off time.

Procedure Steps

1 Log on to the KVL application as an Administrator.

2 On the KVL main screen, select **Settings** → **Security** → **Inactivity**.

Step result: The list of available duration appears, with the currently set duration highlighted.



NOTE

To return to the previous screen without changing the current duration, tap **Cancel**.

3 Tap the desired duration.

Step result: The duration is changed.

4 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.2 Setting the KVL Screen Color Scheme

You can set the KVL screen to one of the two color schemes: Day Time, or Night Time. These schemes define the text and background colors of the KVL screen. By default, the KVL screen is set to the Day Time scheme.

When and where to use:

Use these steps to set the KVL screen color scheme.

Figure 2-1 KVL Screen in Day Time Color Scheme (Example)

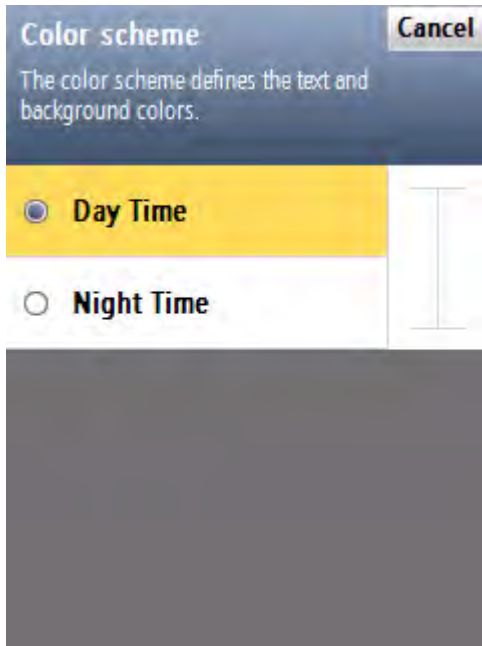
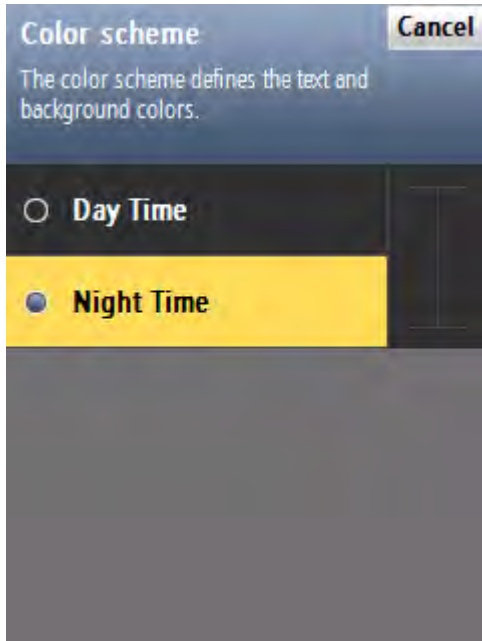


Figure 2-2 KVL Screen in Night Time Color Scheme (Example)



Procedure Steps

- 1 On the KVL main screen, select **Settings** → **General** → **Color scheme**.

Step result: The list of color scheme options appears, with the one currently used highlighted.



NOTE

Tap **Cancel** to return to the previous screen without changing the current mode.

- 2 Tap the desired color scheme.

Step result: The color scheme is changed.

- 3 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.3 Turning Sharing On/Off

In addition to loading keys into target devices, the KVL can also share its keys with another KVL. In order to share keys, the sharing feature must be turned on in both the source and target KVL.

Prerequisites:

Only an Administrator can turn sharing on or off.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **Sharing**.

Step result: A list of available values appears (On/Off), with the currently set value highlighted.

- 2 Select the desired value.
-

- 3 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.4 KVL 4000 – Managing Passwords

The KVL provides two levels of security access:

- **Administrator**
- **Operator**

The Administrator has access to all functions and features. The Operator does **NOT** have access to the following functions and features:

- performing KVL and radio's Crypto Module upgrades
- adding, deleting, and editing keys and groups

- adding and deleting keys in a group
- converting keys
- adding, deleting, and editing Tactical OTAR groups
- entering and changing Tactical OTAR MNP
- entering and changing KVL RSI
- setting and changing the KVL inactivity timeout
- changing FIPS mode
- changing System Key
- changing Sharing mode
- changing Administrator password
- clearing passwords
- entering and changing KMF RSI
- entering and changing KMF MNP
- selecting Main and Backup KMF
- entering and changing KMF phone numbers
- changing UKEK for KMF operation
- clearing the list of received jobs
- clearing log records

Without password protection, all users have access to all of the KVL functions.

2.1.4.1 Setting Up Passwords on the KVL

This section covers the following topics:

- [2.1.4.1.1 Setting Up the Operator Password, page 2-4](#)
- [2.1.4.1.2 Setting Up the Administrator Password, page 2-5](#)

2.1.4.1.1 Setting Up the Operator Password

When and where to use:

Use these steps to set up the Operator password.



NOTE

You cannot set just Administrator or Operator passwords, but must set both, if the password feature is desired.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **Passwords** → **Define passwords** → **Operator**.

Step result: The **New password** and **Repeat password** entry fields appear.

- 2 In the **New password** entry field, type the password of your choice using the PDA keypad.



NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~



NOTE

As you type the password, dynamic hints about password rules appear.

- 3 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.



NOTE

To abort the operation at any time, tap **Cancel**.

- 4 Tap **Done**.

Step result: The password has been set up.

- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.



IMPORTANT

If the Operator password is forgotten, the Administrator can assign a new Operator password.

2.1.4.1.2 Setting Up the Administrator Password

When and where to use:

Use these steps to set up the Administrator password.



NOTE

You cannot set just Administrator or Operator passwords, but must set both, if the password feature is desired.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **Passwords** → **Define passwords** → **Administrator**.
Step result: The **New password** and **Repeat password** entry fields appear.
-

- 2 In the **New password** entry field, type the password of your choice using the PDA keypad.



NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~



NOTE

As you type the password, dynamic hints about password rules appear.

- 3 In the **Repeat password** entry field, type the password again.
Step result: If the passwords match, the **Done** button is enabled.



NOTE

To abort the operation at any time, tap **Cancel**.

- 4 Tap **Done**.
Step result: The password has been set up.
-

- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.4.2 Changing Passwords on the KVL

This section covers the following topics:

- [2.1.4.2.1 Changing the Operator Password \(Operator Access Level\), page 2-6](#)
- [2.1.4.2.2 Changing the Operator Password \(Administrator Access Level\), page 2-7](#)
- [2.1.4.2.3 Changing the Administrator Password, page 2-8](#)

2.1.4.2.1 Changing the Operator Password (Operator Access Level)

When and where to use:

Use this procedure if you have the Operator level of access.

Procedure Steps

- 1 Log on as an Operator.

Step result: The KVL main screen appears.

- 2 Select **Settings** → **Security** → **Password**.

Step result: The **Operator** screen appears, with the **Current password**, **New password**, and **Repeat password** entry fields.

- 3 In the **Current password** entry field, type the current password using the PDA keypad.
-

- 4 In the **New password** entry field, type the password of your choice using the PDA keypad.



NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~



NOTE

As you type the password, dynamic hints about password rules appear.

- 5 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.



NOTE

To abort the operation at any time, tap **Cancel**.

- 6 Tap **Done**.

Step result: The password has been changed.

- 7 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.4.2.2 Changing the Operator Password (Administrator Access Level)

When and where to use:

Use this procedure if you have the Administrator level of access.

Procedure Steps

- 1 Log on as an Administrator.



NOTE

If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

- 2 Select **Settings** → **Security** → **Passwords** → **Update passwords** → **Operator**.

Step result: The **Current password**, **New password**, and **Repeat password** entry fields appear.

- 3 In the **Current password** entry field, type the current password using the PDA keypad.
-

- 4 In the **New password** entry field, type the password of your choice using the PDA keypad.



NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~



NOTE

As you type the password, dynamic hints about password rules appear.

- 5 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.



NOTE

To abort the operation at any time, tap **Cancel**.

- 6 Tap **Done**.

Step result: The password has been changed.

- 7 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.4.2.3 Changing the Administrator Password

Prerequisites:

Only an Administrator can change the Administrator password.

Procedure Steps

- 1 Log on as an Administrator.



NOTE

If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

- 2 Select **Settings** → **Security** → **Passwords** → **Update passwordsAdministrator**.

Step result: The **Current password**, **New password**, and **Repeat password** entry fields.

- 3 In the **Current password** entry field, type the current password using the PDA keypad.
-

- 4 In the **New password** entry field, type the new password.



NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~



NOTE

As you type the password, dynamic hints about password rules appear.

- 5 In the **Repeat password** entry field, type the new password again.

Step result: If the passwords match, the **Done** button is enabled.



NOTE

To abort the operation at any time, tap **Cancel**.

- 6 Tap **Done**.

Step result: The password has been changed.

- 7 Tap **Done** on the consecutive screens to return to the KVL main screen.



IMPORTANT

If you forget the Administrator password, you must perform a system reset before the KVL can be used again. Since a system reset erases all stored keys and returns the KVL settings to the factory defaults, you must enter all keys again.

2.1.4.3 Clearing KVL Passwords

Prerequisites:

Only an Administrator can clear passwords.

Procedure Steps

- 1 Log on as an Administrator.



NOTE

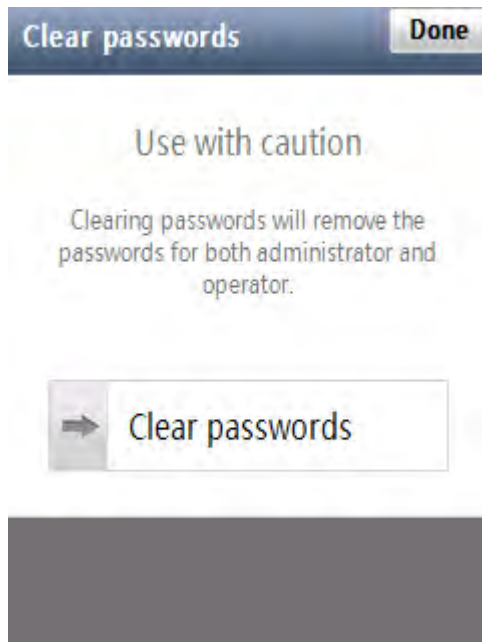
If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

- 2 Select **Settings** → **Security** → **Passwords** → **Clear passwords**.

Step result: A screen with the **Clear passwords** slider appears.

Figure 2-3 Clear Passwords Screen



- 3 Touch the slider and drag it from left to right. Alternatively, highlight the slider, and use the navigation key on the PDA to move it.



CAUTION

Clearing passwords removes the passwords for both administrator and operator.

Step result: The passwords have been cleared.

- 4 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.1.4.4 Selecting the Password Masking Mode

There are two masking modes available for the KVL passwords: all characters masked, or the last character non masked.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **Masking mode**.

Step result: A screen with the list of available options appears.

- 2 Select the masking mode of your choice.

Step result: The masking mode is selected and you return to the previous screen.

- 3 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.2 KVL 4000 System-Dependent Parameters

Set the parameters in this section depending on the particular system (ASN, ASTRO® 25, or Radio Authentication) in which the KVL is operating.

2.2.1 KVL 4000 – Switching Between the Modes of Operation

The KVL provides three modes of operation: ASN (Advanced SECURENET®), ASTRO® 25, and Radio Authentication. The KVL is shipped from the factory to power on in the ASTRO® 25 mode. Then, the KVL powers on in the mode it was operating in when it was last powered off.

Prerequisites:

This procedure is applicable if your KVL is configured to operate in more than one mode of operation.

When and where to use:

Use these steps to switch between the modes of operation.



IMPORTANT

In the Radio Authentication mode, the KVL operates in FIPS Level 2 only. Before changing the mode of operation to Radio Authentication, ensure FIPS Level 2 is set for the mode the KVL is currently operating in.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **System**.

Step result: A list of available modes appears (ASN, ASTRO® 25, and Radio Authentication), with the currently used mode highlighted.



NOTE

To return to the previous screen without changing the mode, tap **Cancel**.

-
- 2 Tap the desired mode of operation.

Step result: The mode is changed.

-
- 3 Tap **Done** to return to the KVL main screen.
-

2.2.2 Setting the Baud Rate for RS-232 Communication

When using the KVL DB9 Port (RS-232) to communicate with external equipment (such as a KMF, or a modem), select the proper baud rate.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **General** → **Baud Rate**.

Step result: A list of available values appears, with the currently set value highlighted. You can choose from the following values:

- 9600
- 19200
- 57600
- 115200



NOTE

To return to the previous screen without changing the current value, tap **Cancel**.

- 2 Tap the desired value.
 - 3 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.2.3 Changing the FIPS Mode

The KVL can operate in a mode that is compliant with the U.S. Federal Information Processing Standard (FIPS) guidelines. To be FIPS-compliant, set passwords on your KVL.

Prerequisites:

Only an Administrator can change the FIPS mode.

When and where to use:

Use these steps to change the FIPS mode.



CAUTION

Changing the FIPS mode erases all keys, Store and Forward messages, target devices to update, and sets the System Key to its default value.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **FIPS mode**.

Step result: The list of available values appears, with the currently selected value highlighted.



NOTE

The available values are:

- **Level 3 (High Security)**
- **Level 2 (Standard)**



IMPORTANT

Use **Level 3** for high security. If FIPS Level 3 is active, the Sharing setting is disabled and cannot be turned on.



IMPORTANT

In the Radio Authentication mode, the KVL operates in FIPS Level 2 only. Before changing the mode of operation to Radio Authentication, ensure FIPS Level 2 is set for the mode the KVL is currently operating in.

-
- 2 Select the desired value.

Step result: A **Warning** screen appears, informing that changing the FIPS mode will remove all keys.

-
- 3 Select **Yes, change FIPS mode** if you are sure that you want to continue.

Step result: The FIPS mode is changed.

-
- 4 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

2.2.4 Managing the System Key (DVI-XL Only)

The KVL requires a 128-digit System Key to communicate in DVI-XL systems. Each KVL is shipped from the factory with a default System Key.



IMPORTANT

Changing the System Key causes all keys defined with the DVI-XL algorithm (including the UKEK for ASTRO® 25) to be erased (includes DVI-XL keys in both ASN and ASTRO® 25 memory).

2.2.4.1 Entering the User-Defined System Key

Prerequisites:

Only an Administrator can enter the System Key.

When and where to use:

Instead of using the default System Key, you can enter your own System Key.



CAUTION

Changing the System Key deletes all associated keys.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Security** → **System Key**.
- 2 Select the **Enter Key** tab.
- 3 Perform one of the following actions:
 - Select **Auto** to generate the key automatically.
 - Enter the key manually using the Hex keypad.



NOTE

At any time, you can tap the key entry bar to go to the key review screen.

- 4 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.
- 5 Tap **Yes, change system key** to confirm the change.

Step result: The System Key is changed.
- 6 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.4.2 Changing the User-Defined System Key

When and where to use:

Use these steps to change the System Key you have previously entered.



CAUTION

Changing the System Key deletes all associated keys.

Procedure Steps

1 On the KVL main screen, select **Settings** → **Security** → **System Key**.

2 Tap the **New >** key.

Step result: A Key Data Info Field and a Hex Entry Keypad appear.

3 Perform one of the following actions:

- Select **Auto** to generate the key automatically.
- Enter the key manually using the Hex keypad.



NOTE

At any time, you can tap the key entry bar to go to the key review screen.

4 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.

5 Tap **Yes, change system key** to confirm the change.

Step result: The System Key is changed.

6 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.4.3 Setting Up the KVL to Use the Default System Key

Procedure Steps

1 On the KVL main screen, select **Settings** → **Security** → **System Key**.

2 Tap the **Use default** tab.

Step result: A message appears, informing that the default system key will be used.

3 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.

4 Tap **Yes, change system key** to confirm the change.

Step result: The default System Key is restored.

5 Tap **Done** on the consecutive screens to return to the KVL main screen.

3 KVL 4000 – Managing Encryption Keys

3.1 Entering Encryption Keys

This section covers the following topics:

- [3.1.1 Entering Encryption Keys Manually, page 3-1](#)
- [3.1.2 Auto-Generating Encryption Keys, page 3-3](#)

3.1.1 Entering Encryption Keys Manually

Prerequisites:

Only an Administrator can enter keys.

When and where to use:

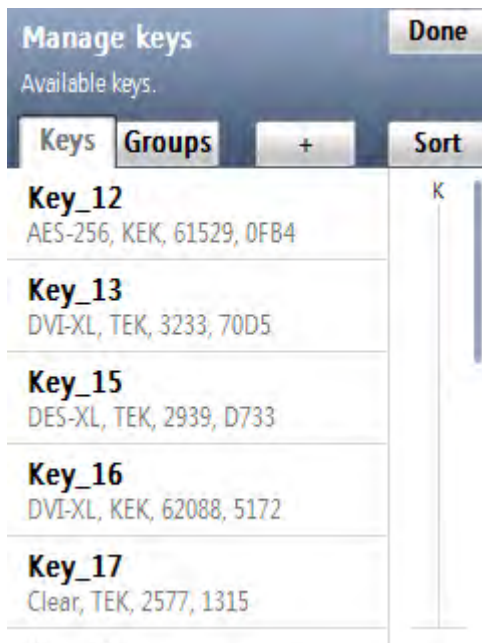
Use these steps to manually enter a Traffic Encryption Key (TEK) or a Key Encryption Key (KEK) into the KVL internal key database.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears.

Figure 3-1 Manage Keys Screen – Entering a Key (Example)



2 Select the + button to define a new key.

3 Select **Enter manually** to enter keys one by one.

4 Enter the name of the key using the PDA keypad.



The name can consist of up to 8 characters, including spaces.

5 Select **Algorithm** and choose one of the algorithms from the list.

6 Select **Key Type** and choose one of the key types from the list.

7 Select **CKR ID** and type the Common Key Reference number.



Valid CKRs for TEKs are 1 through 4095. Valid CKRs for KEKs are 61440 through 65535.

8 Tap **Done** when ready.

9 Select **Key ID** and type the hexadecimal number to set the key location.



The possible range is 0000–FFFF. The KVL does not accept keys of the same algorithm type with duplicate Key IDs (each key of a particular algorithm type must have a unique KID).

10 Tap **Done** when ready.

11 Tap **Enter Key >**.

- 12 Tap **Auto** to generate the key automatically, or enter the key using the keypad.

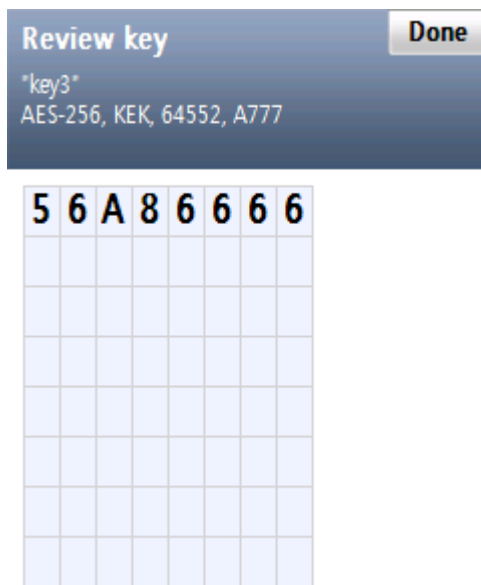


At any time, you can review the digits you have entered by tapping anywhere on the Key Data Info field. This brings up a Review key screen.



For DES keys only: As you enter each digit of the encryption key, the KVL checks it for validity. If you enter an invalid number, it flashes red. In this case, tap **< Del** and correct the number. Every two numbers entered for the key represent a byte of data that must have odd-parity for DES keys. For non-DES keys: Encryption key validity is checked only after you entered the entire key and tapped **Done**.

Figure 3-2 Review Key Screen (Example)



8 of 64 digits entered & validated.

- 13 Once you have entered the key, tap **Done** to confirm, or **Next Key** to confirm and enter a new key with the same parameters.
- 14 Tap **Done** to return to the KVL main screen.

3.1.2 Auto-Generating Encryption Keys

Prerequisites:

Only an Administrator can enter keys.

When and where to use:

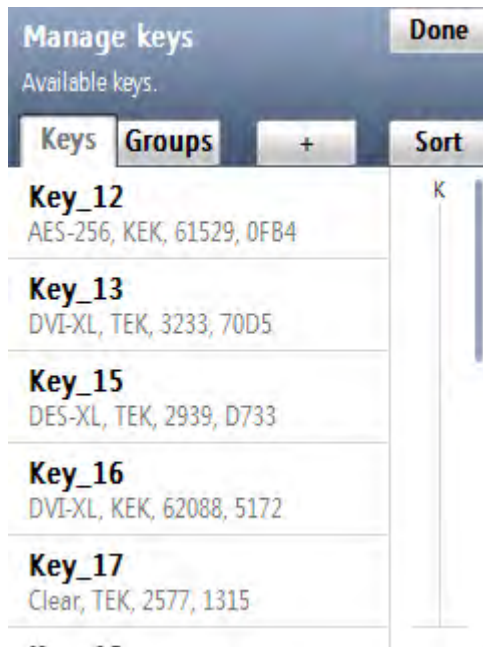
Use these steps to quickly generate multiple encryption keys.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears.

Figure 3-3 Manage Keys Screen – Entering a Key (Example)



- 2 Select the + button to define a new key.
- 3 Select **Auto generate** to generate multiple keys quickly.
- 4 Enter the number of keys to auto generate and tap **Next Step >**.

**NOTE**

You can generate a maximum of 100 keys at a time.

- 5 Type the naming pattern for the new keys using the PDA keypad.
- 6 Select **Algorithm** and choose one of the algorithms from the list.
- 7 Select **Key Type** and choose one of the key types from the list.

-
- 8 Select **Initial CKR ID** and type the CKR for the first key. Consequent keys will increment from that ID.

**NOTE**

Valid CKRs for TEKs are 1 through 4095. Valid CKRs for KEKs are 61440 through 65535.

- 9 Tap **Done** when ready.
-

- 10 Select **Initial Key ID** and type the Key ID for the first key. Consequent keys will increment from that ID.

**NOTE**

The KVL does not accept keys of the same algorithm type with duplicate Key IDs (each key of a particular algorithm type must have a unique KID).

- 11 Tap **Done** when ready.
-

- 12 Tap **Generate** >.

Step result: A progress animation appears, indicating that the keys are being generated. When the process is completed, you return to the **Manage keys** screen.

- 13 Tap **Done** to return to the KVL main screen.
-

3.2 Using Key Groups

The KVL provides a convenient feature called key groups. This feature allows you to associate several keys stored in the KVL memory with a specified group name. You can then load the entire group of keys to the target device in a single operation. This is especially useful when loading the same group of keys to several target devices, such as a fleet of radios.

The KVL supports the existence of up to 20 groups at a time, with each group consisting of 16 keys (TEKs, KEKs, or a combination of both). If there are fewer than 20 groups, a group can consist of more than 16 keys, limited by the KVL memory capacity.

3.2.1 Creating a Group

Prerequisites:

Only an Administrator can create a group.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears with a list of available keys.

Figure 3-4 Manage Keys Screen – Creating a Group (Example)



- 2 Select the **Groups** tab.
- 3 Tap the + button to define a new group.
- 4 Type the group name using the PDA keypad, and tap **Next Step >**.



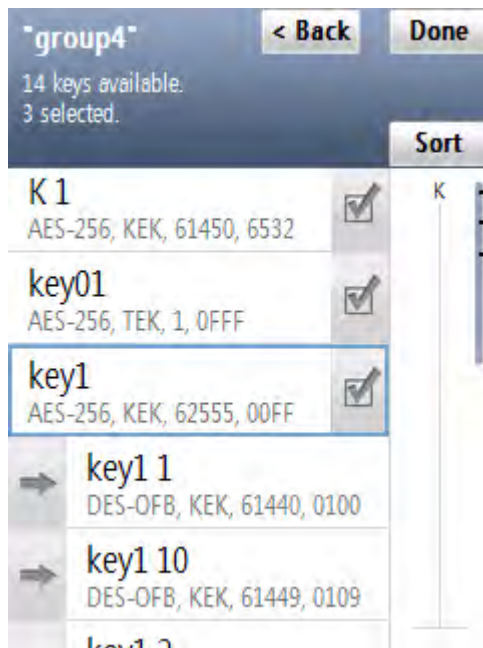
NOTE

Group names may contain 18 characters, including spaces.

- 5 Add all the desired keys to the created group. To add a key, drag the slider to the right. To exclude a key, drag the slider to the left. When finished, tap **Done**.

Step result: The group is saved and displayed in the groups list.

Figure 3-5 Adding Keys to a Group – Example



- 6 Tap **Done**.
- 7 Tap the + button to create another group, or tap **Done** to return to the KVL main screen.

3.2.2 Modifying Groups

When the KVL contains one or more key groups, you can perform the following tasks on them:

- view keys in a group
- add keys to a group
- delete keys from a group
- delete a group
- rename a group

3.2.2.1 Viewing Keys in a Group

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears with a list of available keys.

- 2 Select the **Groups** tab.



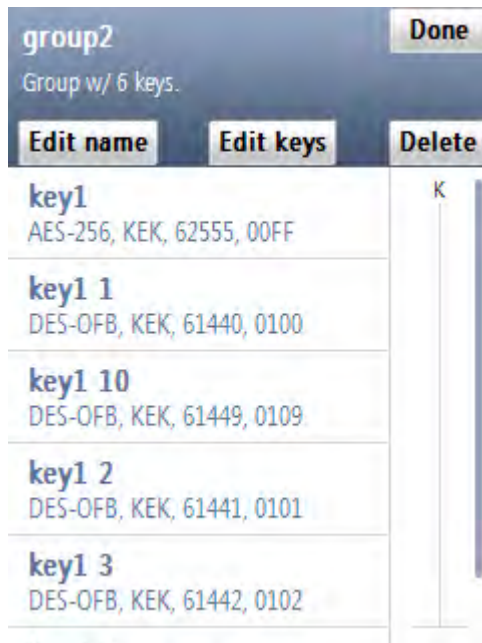
NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Select the group you want to see the keys for.

Step result: The group with all keys associated with it appears.

Figure 3-6 Viewing Keys in a Group (Example)



- 4 When finished, tap **Done** on the consecutive screens to return to the KVL main screen.

3.2.2.2 Adding Keys to a Group

Prerequisites:

Only an Administrator can add keys to a group.

When and where to use:

Use these steps to add keys to a group.



A group may consist of up to 512 keys.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears.

- 2 Select the **Groups** tab.



You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

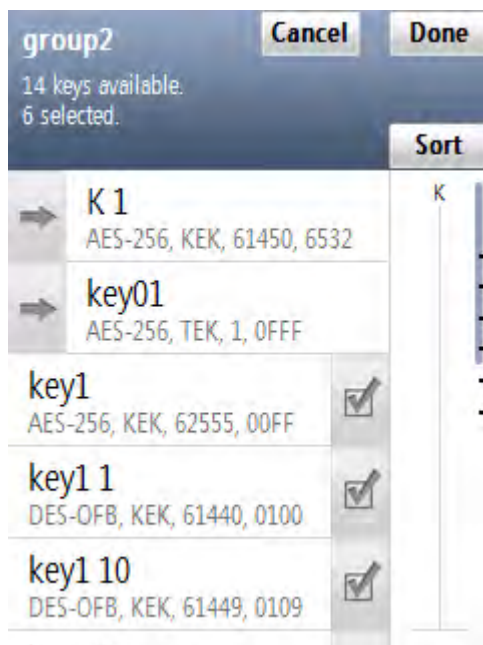
- 3 Select the group you want to add keys to.

Step result: The group with all keys associated with it appears.

- 4 Tap **Edit keys**.

Step result: A list of all available keys appears.

Figure 3-7 Group with Available Keys (Example)



- 5 Add all the desired keys to the group. To add a key, drag the slider to the right. To exclude a key, drag the slider to the left. When finished, tap **Done**.

Step result: The list of all the keys in the group appears.

- 6 Tap **Done**.

Step result: The new configuration is saved.

- 7 Tap **Done** again to return to the KVL main screen.
-

3.2.2.3 Deleting Keys from a Group

Prerequisites:

Only an Administrator can delete keys from a group.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears with a list of available keys.

- 2 Select the **Groups** tab.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

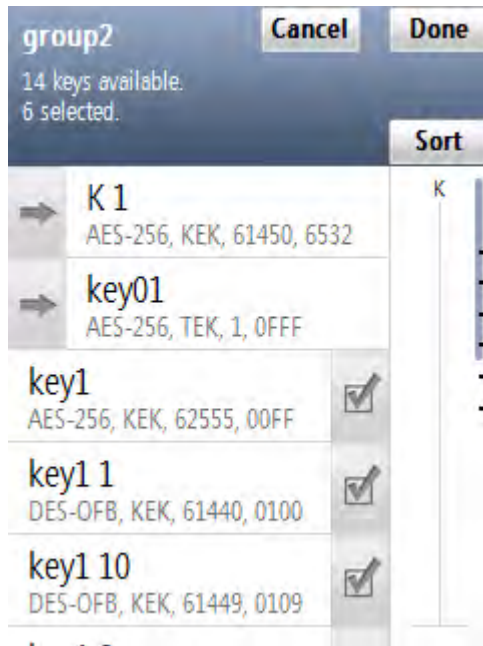
- 3 Select the group you want to delete keys from.

Step result: The group with all keys associated with it appears.

- 4 Tap **Edit keys**.

Step result: A list of all available keys appears.

Figure 3-8 Deleting Keys from a Group (Example)



- 5 Delete all the desired keys from the group. To delete a key, drag the slider associated with the selected key to the left. When finished, tap **Done**.
- 6 Tap **Done**.
Step result: The new configuration is saved and the groups list appears.
- 7 Tap **Done** to return to the KVL main screen.

3.2.2.4 Deleting a Group

Prerequisites:

Only an Administrator can delete a group.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears with a list of available keys.

- 2 Select the **Groups** tab.

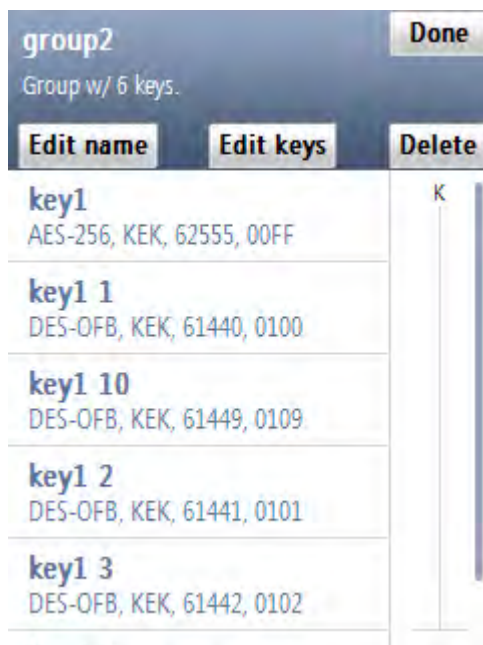
**NOTE**

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Select the group you want to delete.

Step result: The group with all keys associated with it appears.

Figure 3-9 Deleting a Group (Example)



- 4 Tap **Delete**.

Step result: The group has been deleted.

**NOTE**

If you want to restore the deleted group, tap **Restore** before leaving the confirmation screen.

- 5 Tap **Done** to confirm.
-

- 6 Tap **Done** to return to the KVL main screen.
-

3.2.2.5 Renaming a Group

Prerequisites:

Only an Administrator can rename a group.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears.

- 2 Select the **Groups** tab.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

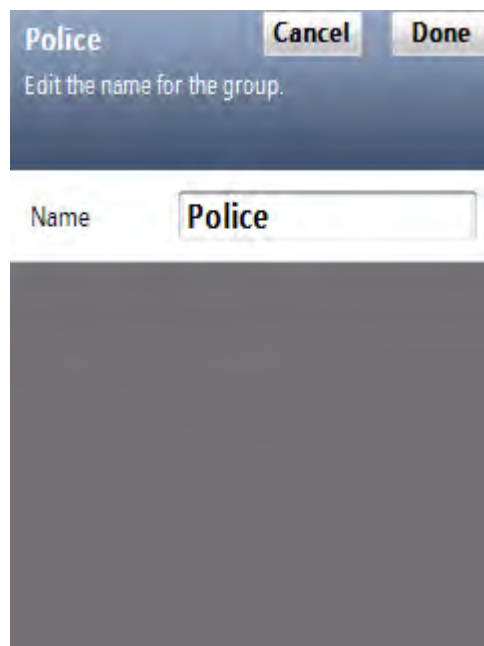
- 3 Select the group you want to rename.

Step result: The group with all keys associated with it appears.

- 4 Tap **Edit name**.

Step result: The name field appears.

Figure 3-10 Group Name Field (Example)



- 5 Delete the current name and type a new one using the PDA keypad.
-

- 6 Tap **Done** to confirm.
 - 7 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

3.3 Modifying Encryption Keys

You can modify an Encryption Key (TEK or KEK) stored in a specific CKR location in the KVL memory.

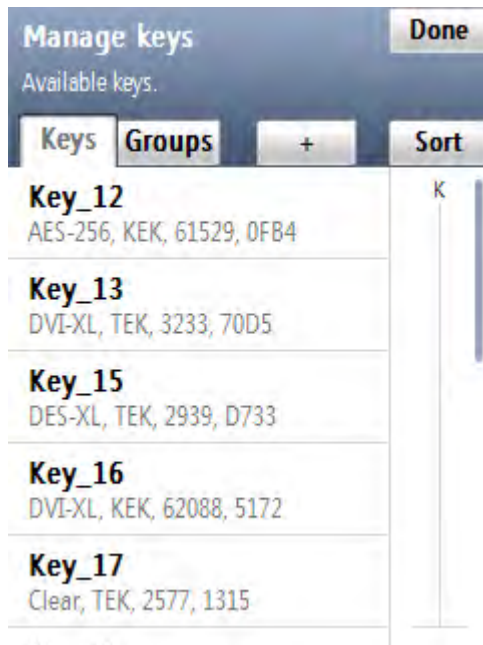
Prerequisites:

Only an Administrator can modify keys.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.
Step result: The **Manage keys** screen appears.

Figure 3-11 Manage Keys Screen – Modifying a Key (Example)



- From the list of available keys, select the key you want to modify.

**NOTE**

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

Step result: A screen with details for the selected key appears.

Figure 3-12 Key Details Screen (Example)

The screenshot shows a mobile application interface for key details. At the top, the key name 'key1' is displayed next to 'Cancel' and 'Done' buttons. Below this, the text 'Details for this key:' is shown. There are two buttons: 'Convert to ASN' and 'Delete'. The main content consists of several rows, each with a label and a value: 'Name' with 'key1', 'Algorithm' with 'AES-256', 'Key Type' with 'KEK', 'CKR ID' with '62555', and 'Key ID' with '00FF'. The 'Key ID' field has a right-pointing arrow.

**NOTE**

The **Algorithm**, **Key Type**, and **CKR ID** entries are read-only.

- Modify the **Name** of the key using the PDA keypad.
- Select and modify **Key ID** using the Hex keypad.

**NOTE**

The KVL does not accept keys of the same algorithm type with duplicate Key IDs (each key of a particular algorithm type must have a unique KID).

- Tap **Done** when ready.

Step result: You return to the screen with the key details.

- 6 Scroll down the screen and select **Key**.

Step result: The **Enter** key screen appears with the Hex keypad.

- 7 Tap **Auto** to generate the key automatically, or enter the key using the Hex keypad.



NOTE

For DES keys only: As you enter each digit of the encryption key, the KVL checks it for validity. If you enter an invalid number, it flashes red and a **bad bonk** sound is played. In this case, tap **< Del** and correct the number. Every two numbers entered for the key represent a byte of data that must have odd-parity for DES keys. For non-DES keys: Encryption key validity is checked only after you entered the entire key and tapped **Done**.

- 8 Once you have entered the key, tap **Done** to confirm.

Step result: The key has been modified and you return to the list of keys.

- 9 Tap **Done** to return to the KVL main screen.
-

3.4 Deleting Encryption Keys

You can erase an Encryption Key (TEK or KEK) stored in a specific CKR location in the KVL memory. Deleting permanently erases the Encryption Key currently stored in the location. The location is then considered to be undefined and may be used to hold another Encryption Key.

Prerequisites:

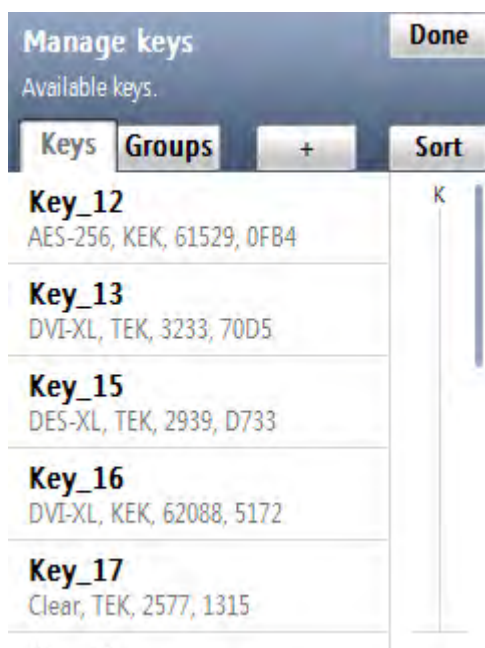
Only an Administrator can delete keys.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.

Step result: The **Manage keys** screen appears with the list of available keys.

Figure 3-13 Manage Keys Screen – Deleting a Key (Example)



- 2 From the list of available keys, select the key you want to delete.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Tap **Delete**.

Step result: The key has been deleted.



NOTE

If you want to restore the deleted key, tap **Undo** before leaving the confirmation screen.

- 4 Tap **Accept** to confirm.

- 5 Tap **Done** to return to the KVL main screen.

4 KVL 4000 – Loading Encryption Keys into Target Devices

You can load encryption keys into one of the following devices:

- Secure ASTRO® 25 Single Key Target Radio
- Secure ASTRO® 25 Multiple Key Target Radio
- Another KVL unit (see [Chapter 6 KVL 4000 – Sharing Keys Between KVLs](#))
- Radio Network Controller (RNC)
- Digital Interface Unit (DIU)
- Motorola Gold Elite Gateway (MGEG)
- MCC 7500 Console
- PDEG Encryption Unit
- CAI Data Encryption Module (CDEM)
- Key Management Facility (KMF) (see [Chapter 7 Using KVL 4000 in OTAR Systems](#))
- KMF CryptR
- CRYPTR micro (used with MCC 7100 IP Dispatch Console and AME 1500/2000)

4.1 Loading a Selected Key

Prerequisites:

There are encryption keys in the KVL database.

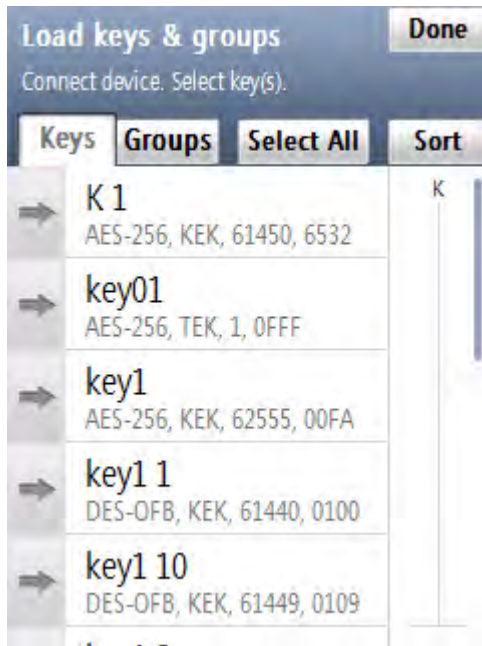
When and where to use:

Use these steps to load a selected key into a target device.

Procedure Steps

- 1 On the KVL main screen, Select **Load keys & groups** → **Load keys & groups**.
Step result: The list of available keys appears.

Figure 4-1 Load Keys & Groups Screen – Example



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

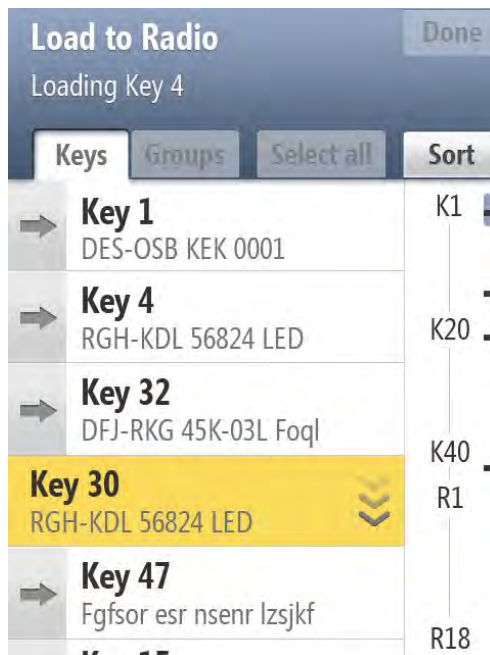
- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

- 3 Select the key you want to load by dragging the slider to the right.


NOTE

KVL displays an animation indicating a busy loading state. During this time, you can scroll to find the next key.

Figure 4-2 Loading a Key (Example)



Step result: The key has been loaded to the target device.

- 4 Select another key to load, or tap **Done**.


NOTE

If you want to load the same key to another target device, disconnect the current target device and connect another one. The loading process starts automatically.

- 5 Tap **Done** to return to the KVL main screen.

4.2 Loading a Key Group

Prerequisites:

There are key groups in the KVL database.

When and where to use:

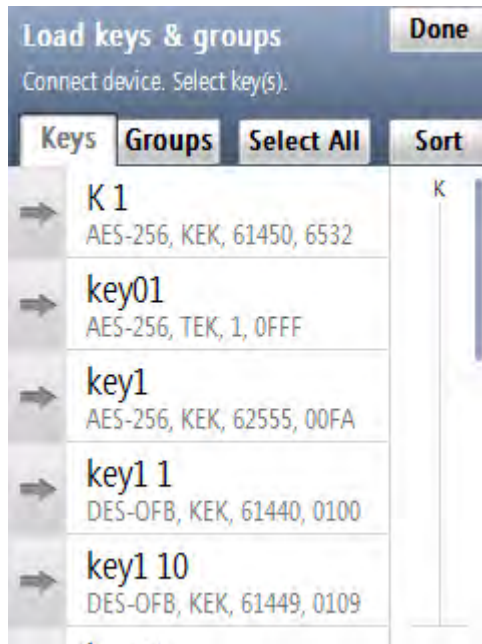
Use these steps to load a key group into a target device.

Procedure Steps

- 1 On the KVL main screen, select **Load keys & groups** → **Load keys & groups**.

Step result: The list of keys appears.

Figure 4-3 Load Keys & Groups Screen – Loading a Group (Example)



- 2 Select the **Groups** tab.



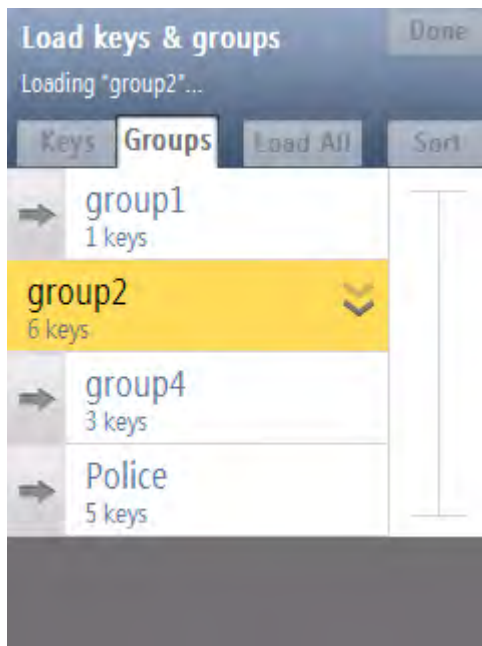
You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)
-

- 4 Select the group you want to load by dragging the slider to the right.

Step result: An animation appears next to the group to indicate it is being loaded. When the process is successful, a **completed** tone is played.

Figure 4-4 Loading a Group (Example)



NOTE

Because key groups may contain undefined keys (CKRs with no KID or key data), the number of keys loaded may differ from the number of keys in the key group. Only the defined keys in a key group are loaded into the target device.

- 5 Select another group to load, or tap **Done**.



NOTE

If you want to load the same group to another target device, disconnect the current target device and connect another one. The loading process starts automatically.

- 6 Tap **Done** to return to the KVL main screen.

4.3 Loading All Keys

Prerequisites:

In order to load all keys from the KVL into the target device, the KVL and the target device must be equipped with the same algorithms.

When and where to use:

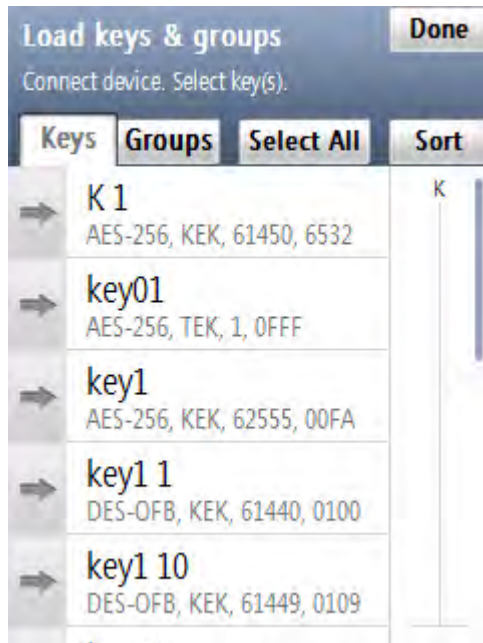
Use these steps to load all keys into a target device.

Procedure Steps

- 1 On the KVL main screen, select **Load keys & groups** → **Load keys & groups**.

Step result: The list of keys appears.

Figure 4-5 Load Keys & Groups Screen – Loading All Keys (Example)



- 2 Tap **Select all**.

Step result: All the keys on the list are selected.



NOTE

If the target device is already connected, the button says **Load all** instead. Tap it to start the loading process.

- 3 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played to indicate the start of the loading process and a progress animation appears, indicating the current key and the total number of keys being loaded. Smart bar indicates the current key being loaded through blinking indication. When the loading process is completed, a **completed** tone is played and a confirmation screen appears.



The following are the possible statuses indicated on the list of keys:

- Check mark – the key has been loaded.
- Animation – the key is currently being loaded.
- Selection – the key is waiting to be loaded.

Figure 4-6 Loading a Key – Statuses (Example)



- 4 Disconnect the target device.
- 5 Connect another target device to load all keys to (the loading process starts automatically), or tap **Done** on the consecutive screens to return to the KVL main screen.

4.4 Loading All Key Groups

Prerequisites:

There are key groups in the KVL database.

When and where to use:

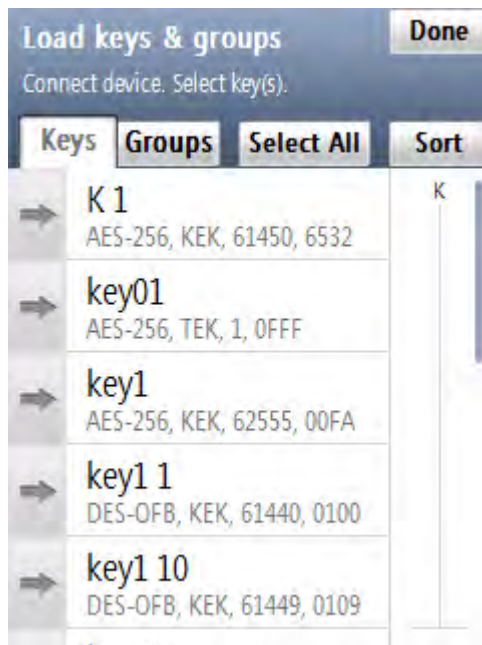
Use these steps to load all key groups into a target device.

Procedure Steps

- 1 On the KVL main screen, select **Load keys & groups** → **Load keys & groups**.

Step result: The list of keys appears.

Figure 4-7 Load Keys & Groups Screen – Loading All Groups (Example)



- 2 Select the **Groups** tab.

- 3 Tap **Select all**.

Step result: All the groups on the list are selected.



If the target device is already connected, the button says **Load all** instead. Tap it to start the loading process.



Because key groups may contain undefined keys (CKRs with no KID or key data), the number of keys loaded may differ from the number of keys in the key group. Only defined keys in a key group are loaded into a target device.

- 4 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played to indicate the start of the loading process and a progress animation appears, indicating the current group and the total number of groups being loaded. Smart bar indicates the current group being loaded through blinking indication. When the loading process is completed, a **completed** tone is played and a confirmation screen appears.

**NOTE**

The following are the possible states indicated on the list of key groups:

- Check mark – the key group has been loaded.
- Animation – the key group is currently being loaded.
- Selection – the key group is waiting to be loaded.

-
- 5 Disconnect the target device.

-
- 6 Connect another target device to load all key groups to (the loading process starts automatically), or tap **Done** on the consecutive screens to return to the KVL main screen.
-

5 KVL 4000 – Managing Keys in Target Devices

5.1 Removing Keys from Target Devices

KVL allows you to erase encryption keys stored in a secure target device, such as a radio. This feature permanently erases the encryption key from the CKR memory location in the target device.

This section covers the following topics:

- [5.1.1 Removing a Key from a Target Device, page 5-1](#)
- [5.1.2 Removing a Key Group from a Target Device, page 5-3](#)
- [5.1.3 Removing All Keys from a Target Device, page 5-6](#)
- [5.1.4 Removing All Key Groups from a Target Device, page 5-8](#)
- [5.1.5 Removing All Keys and All Key Groups from a Target Device, page 5-10](#)

5.1.1 Removing a Key from a Target Device

Prerequisites:

There are encryption keys in the target device.

Procedure Steps

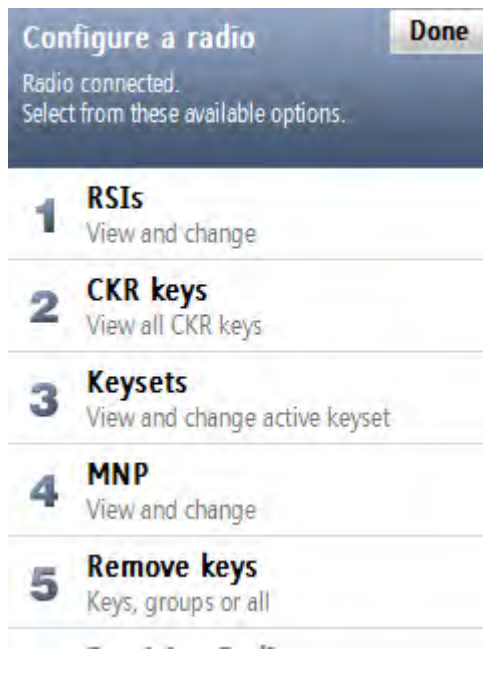
- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect the target device.

- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played and a list of available options appears.

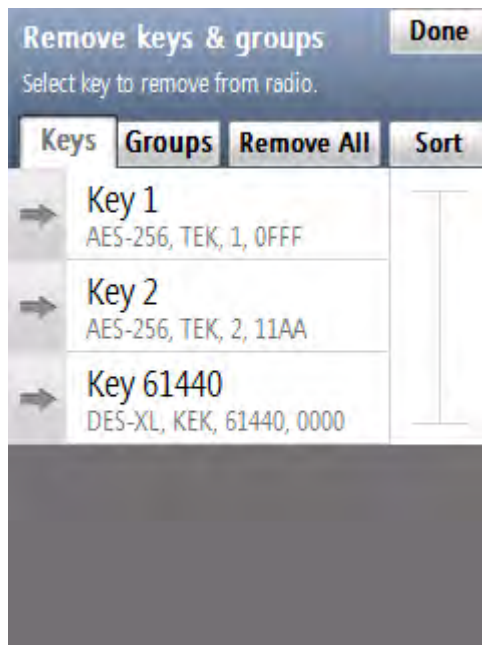
Figure 5-1 Configure a Radio Screen



- 3 Select **Remove keys** → **Remove keys & groups**.

Step result: The list of keys appears.

Figure 5-2 Remove Keys & Groups Screen (Example)



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 4 Select the key you want to remove by dragging the slider of the key from left to right.
Step result: An animation appears while the key is being removed. When the key has been removed, a **completed** sound is played.
- 5 Remove another key, or tap **Done** on the consecutive screens to return to the KVL main screen.

5.1.2 Removing a Key Group from a Target Device

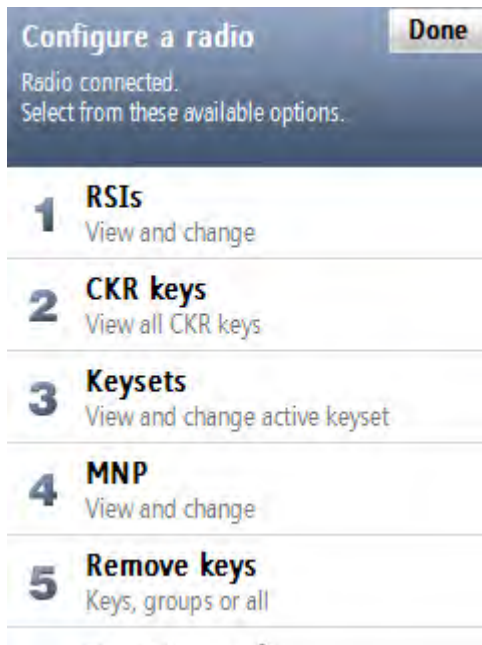
Prerequisites:

There are key groups in the target device.

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.
Step result: You are prompted to connect the target device.
- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)
Step result: A tone is played and a list of available options appears.

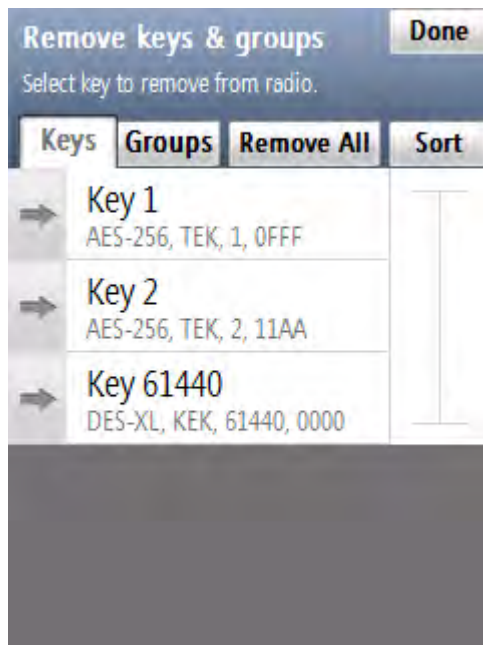
Figure 5-3 Configure a Radio Screen – Removing a Group



- 3 Select **Remove keys** → **Remove keys & groups**.

Step result: The list of keys appears.

Figure 5-4 Remove Keys & Groups Screen – Removing a Group (Example)



- 4 Select the **Groups** tab.

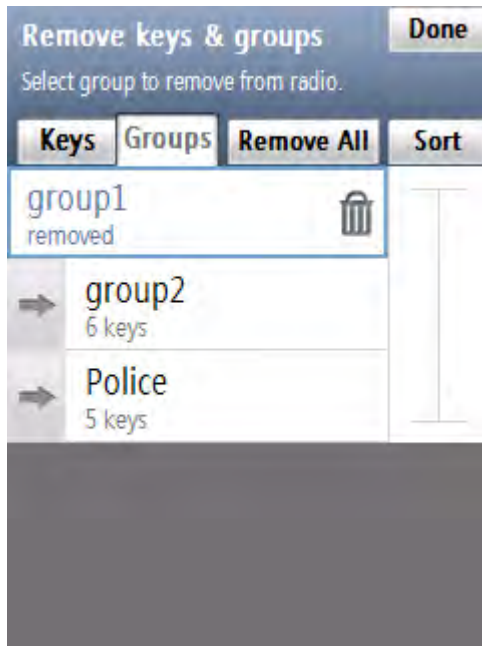


NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 5 Select the group you want to remove by dragging the slider from left to right.
Step result: An animation appears and a group is removed from the target device.

Figure 5-5 Group Removed (Example)



- 6 Remove another group, or disconnect the target device and tap **Done** on the consecutive screens to return to the KVL main screen.
-

5.1.3 Removing All Keys from a Target Device

Prerequisites:

There are keys in the target device.

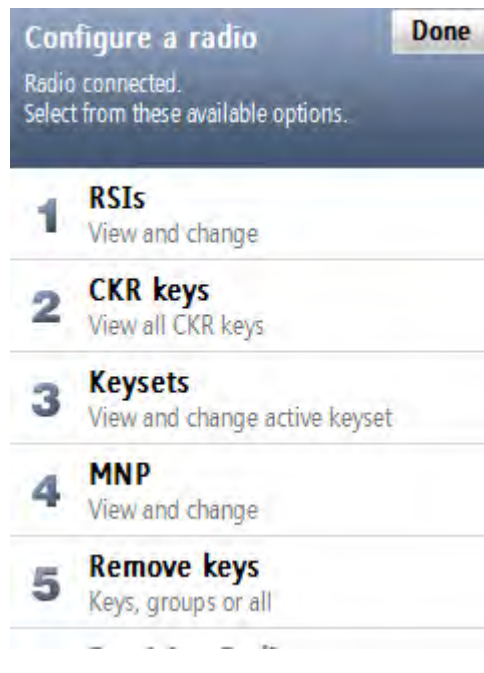
Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.
Step result: You are prompted to connect the target device.
-

- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played and a list of available options appears.

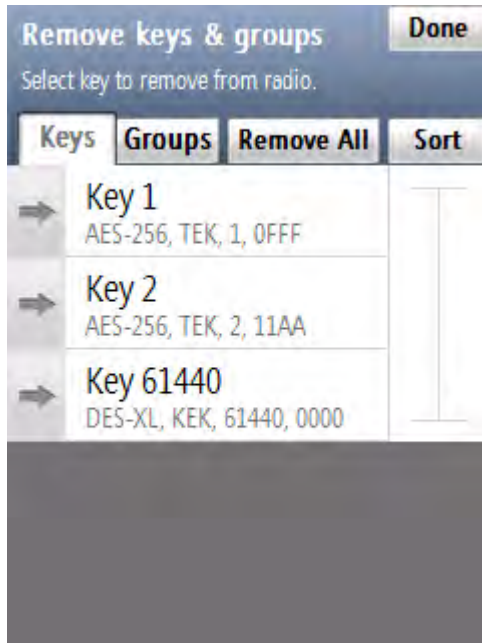
Figure 5-6 Configure a Radio Screen – Removing All Keys



- 3 Select **Remove keys** → **Remove keys & groups**.

Step result: The list of keys appears.

Figure 5-7 Remove Keys & Groups Screen – Removing All Keys (Example)



-
- 4 Select the **Remove All** button.

Step result: A warning screen appears.

-
- 5 Select **Yes, remove keys**.

Step result: A progress animation appears, indicating that the keys are being removed. When the operation has completed successfully, a **completed** tone is played.

-
- 6 Disconnect the target device and connect another target device to remove keys from, or tap **Done** on the consecutive screens to return to the KVL main screen.
-

5.1.4 Removing All Key Groups from a Target Device

Prerequisites:

There are key groups in the target device.

Procedure Steps

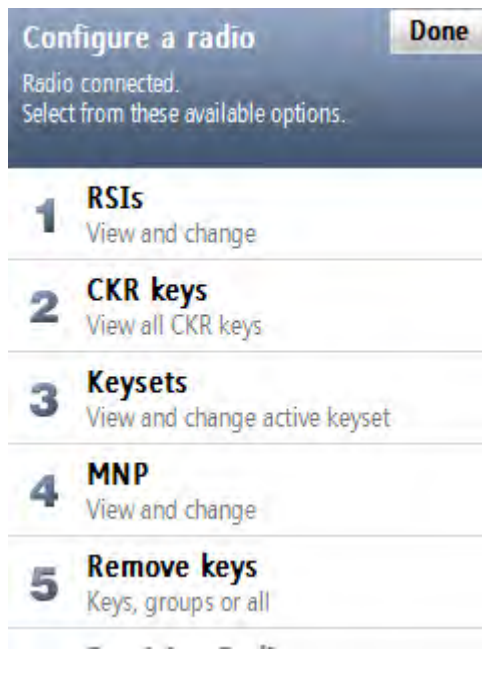
- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect the target device.

- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played and a list of available options appears.

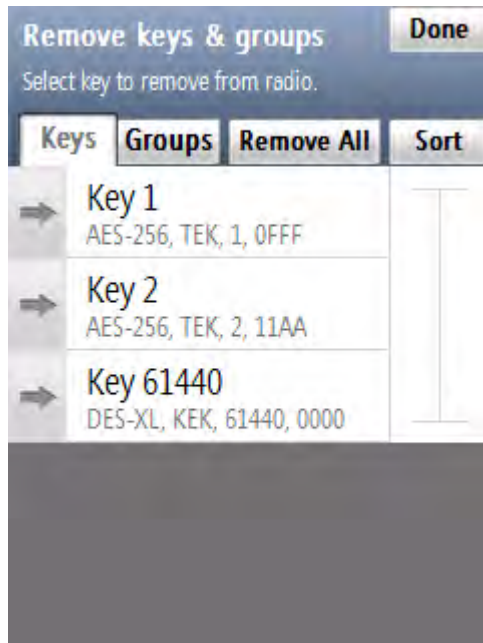
Figure 5-8 Configure a Radio Screen – Removing All Groups



- 3 Select **Remove keys** → **Remove keys & groups**.

Step result: The list of keys appears.

Figure 5-9 Remove Keys & Groups Screen – Removing All Groups (Example)



- 4 Select the **Groups** tab.

- 5 Select the **Remove All** button.

Step result: A warning screen appears.

- 6 Select **Yes, remove groups**.

Step result: A progress animation appears, indicating that the groups are being removed. When the operation has completed successfully, a **completed** tone is played.

- 7 Disconnect the target device and connect another target device to remove groups from, or tap **Done** on the consecutive screens to return to the KVL main screen.

5.1.5 Removing All Keys and All Key Groups from a Target Device

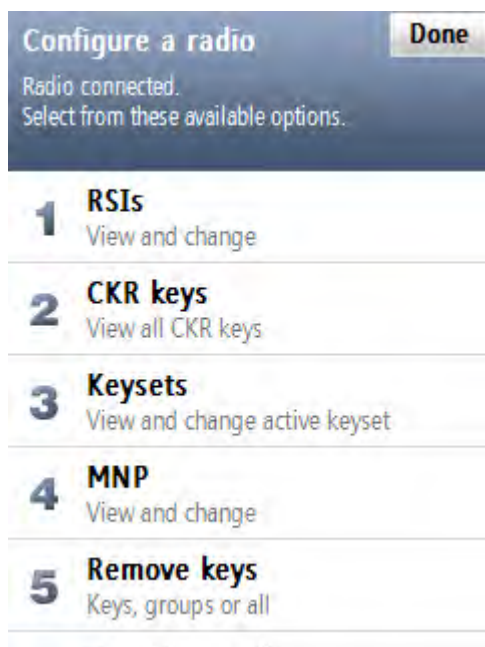
Prerequisites:

There are keys and key groups in the target device.

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.
Step result: You are prompted to connect the target device.
- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.](#))
Step result: A tone is played and a list of available options appears.

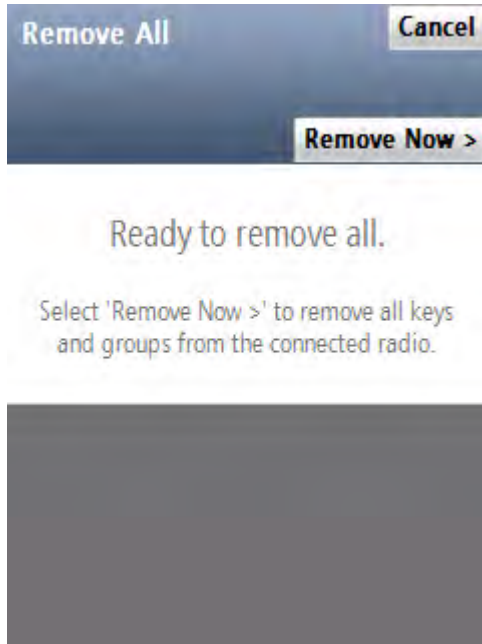
Figure 5-10 Configure a Radio Screen – Removing All Keys and Groups



- 3 Select **Remove keys** → **Remove all**.

Step result: A confirmation screen appears.

Figure 5-11 Remove All Screen



-
- 4 Tap **Remove Now >**.

Step result: All keys and key groups are removed.

-
- 5 Disconnect the target device and connect another target device to remove keys and key groups from, or tap **Done** on the consecutive screens to return to the KVL main screen.
-

5.2 Viewing Keys in Target Devices

Prerequisites:

There are encryption keys in the target device.

Procedure Steps

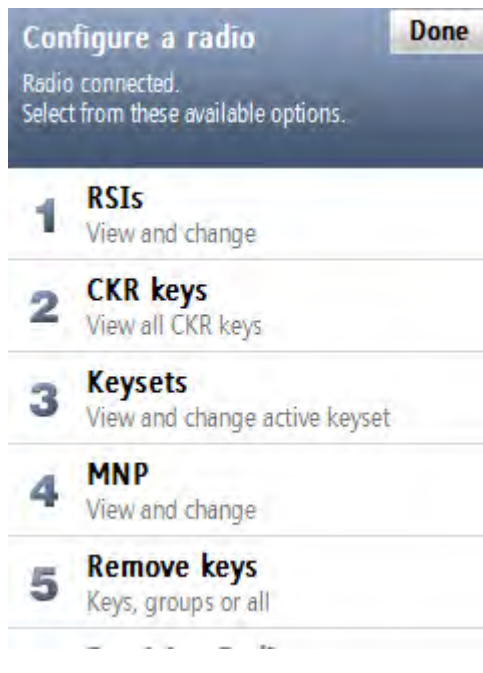
-
- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect the target device.

- 2 Connect the target device to the KVL using an appropriate key load cable. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A tone is played and a list of available options appears.

Figure 5-12 Configure a Radio Screen – Viewing Keys



- 3 Select **CKR keys**.

Step result: The list of all available CKR keys appears.



The list is read-only.



Three sort methods are allowed:

- By the CKR ID (default)
- By the Key ID
- By the Key type

Switch between sort methods by tapping the **Sort** button. It cycles through the sort methods from 1 to 3, then back to 1.

- 4 When you have finished viewing the keys, tap **Done** on the consecutive screens to return to the KVL main screen.

6 KVL 4000 – Sharing Keys Between KVLs

In addition to loading keys into target devices, the KVL can also load (share) its keys to another KVL of the same or different model.

The following sharing functions are supported:

- Sharing a single key - The source KVL can share a selected key with another KVL.
- Sharing a key group - The source KVL can share its key groups (and the keys associated with these key groups) with another KVL.
- Sharing all keys and all key groups - The source KVL can share all of its keys (including Traffic keys, Shadow keys, macros, and indexes) with another KVL.

The following rules apply to sharing:

- Sharing must be turned ON in both the source and target KVL. See [2.1.3 Turning Sharing On/Off, page 2-3](#).
- The target KVL must be on its main screen.
- Sharing cannot be performed between a KVL in ASN mode and a KVL in ASTRO® 25 mode. (To change the mode of operation, see [2.2.1 KVL 4000 – Switching Between the Modes of Operation, page 2-11](#).)
- Only key data and key groups are shared. KVL configuration settings, the UKEK for each algorithm, and log records for the target KVL remain unchanged.
- In order to share single keys or key groups that contain DVI-XL keys, the System Keys of both KVLs must match.

6.1 Sharing a Single Key

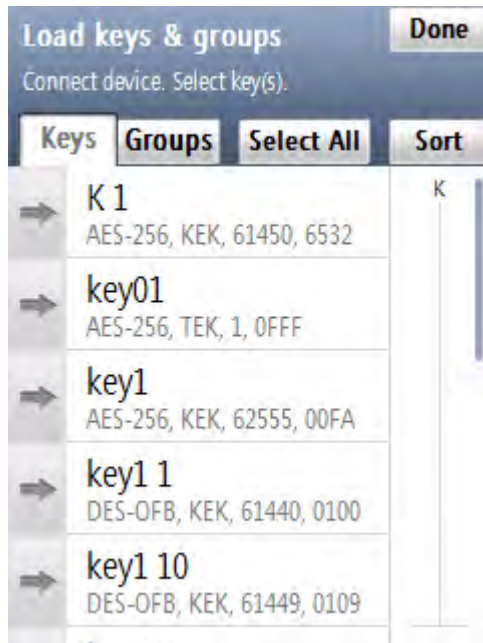
Prerequisites:

In order to share a selected key, the target KVL must support the algorithm of the key being shared. If you want to share a DVI-XL key, the System Keys in both KVLs must match for the sharing to be successful.

Procedure Steps

- 1 On the KVL main screen, select **Load keys & groups** → **Load keys & groups**.
Step result: The list of available keys appears.

Figure 6-1 Load Keys & Groups Screen – Sharing a Key (Example)



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 2 Connect the target KVL using the KVL to KVL cable. (See [1.4.4.2 Connecting Two KVL Units, page 1-16.](#))



NOTE

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

- 3 Select the key you want to share by dragging the slider from left to right.



NOTE

The KVL displays an animation indicating a busy sharing state. During this time, you can scroll to find the next key.

Step result: The key has been shared with the target KVL.

- 4 Select another key to share, or disconnect the KVLs and tap **Done** on the consecutive screens to return to the KVL main screen.

6.2 Sharing a Key Group and Associated Keys

Prerequisites:

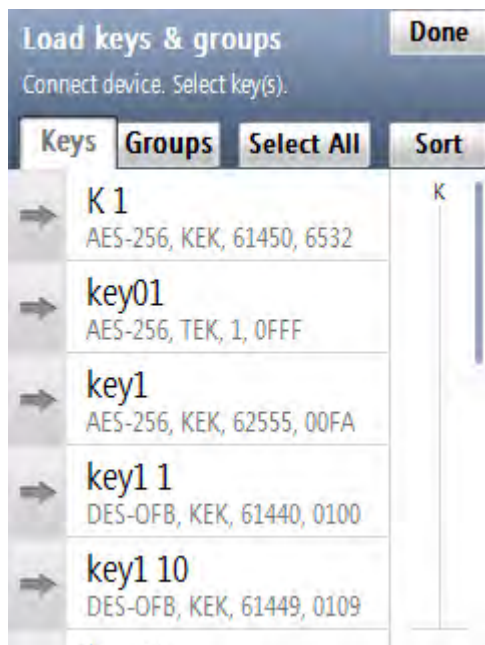
If you share a key group that contains at least one DVI-XL key, the System Keys in both KVLs must match for the sharing to be successful.

Procedure Steps

- 1 On the KVL main screen, select **Load keys & groups** → **Load keys & groups**.

Step result: The list of available keys appears.

Figure 6-2 Load Keys & Groups Screen – Sharing a Group (Example)



- 2 Select the **Groups** tab.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Connect the target KVL using the KVL to KVL cable. (See [1.4.4.2 Connecting Two KVL Units, page 1-16.](#))

**NOTE**

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

- 4 Select the group you want to share by dragging the slider from left to right.

Step result: A progress animation appears, indicating that the group is being shared. When the operation has completed successfully, you are returned to the list of groups.

**NOTE**

Because groups may contain undefined keys (CKRs with no KID or key data), the number of keys shared may differ from the number of keys in the group. Only the defined keys in a group are shared with the target KVL.

- 5 Select another group to share, or disconnect the KVLs and tap **Done** on the consecutive screens to return to the KVL main screen.
-

6.3 Sharing All Keys and All Groups

Prerequisites:

In order to share all keys, the target KVL must support the same algorithms as the source KVL (assuming that there is at least one key defined for each algorithm).

- **Example 1:** The source KVL is equipped with DES-XL, DES-OFB, and DVP-XL, and there is at least one key defined for each algorithm. The target KVL must also be equipped with DES-XL, DES-OFB, and DVP-XL.
- **Example 2:** The source KVL is equipped with AES-256, DES-OFB, and DVP-XL, but there are keys defined only for AES-256. The target KVL must also be equipped with at least AES-256.

Procedure Steps

- 1 Select **Load keys & groups** on the KVL main screen.
- 2 Connect the target KVL using the KVL to KVL cable. (See [1.4.4.2 Connecting Two KVL Units, page 1-16.](#))

**NOTE**

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

- 3 Select **Load all to Another KVL**.
Step result: The confirmation screen appears.

- 4 Tap **Load Now >**.

Step result: A progress animation appears, indicating that the keys and groups are being shared. When the operation has completed successfully, a confirmation screen appears and a **completed** tone is played.

**NOTE**

Because key groups may contain undefined keys (CKRs with no KID or key data), the number of keys shared may differ from the number of keys in the key group. Only the defined keys in a key group are shared with the target KVL.

- 5 Disconnect the KVLs and connect another KVL to load keys and key groups to, or tap **Done** on the consecutive screens to return to the KVL main screen.
-

7 Using KVL 4000 in OTAR Systems



NOTE

This chapter is applicable if your KVL is configured to support KMF operation.

The Motorola Over-the-Air Rekeying (OTAR) system is a secure communications system in which encryption keys can be sent to subscriber units via radio transmission in addition to directly connecting a KVL to a radio to load keys. OTAR provides flexibility and convenience in managing and administering encryption keys.

One of the infrastructure components in an OTAR system is the Key Management Facility (KMF). The KMF is a Windows NT-based computer that is responsible for:

- Storing and managing the encryption keys for an OTAR system
- Initiating key transmissions to radios



NOTE

Before using the KVL to perform tasks in an OTAR system, program several parameters, as described in [7.1 Setting Up the KVL for KMF Operations, page 7-1](#).

The KVL can interface with the KMF to provide the following functions:

- **Transfer the encryption keys required by the OTAR system from the KVL to the KMF** – You load the required keys into the KVL, connect the KVL to the KMF via a standard key load cable, and transfer the keys (one at a time) to the KMF for storage and management (see [4.1 Loading a Selected Key, page 4-1](#)). The KMF then transfers encryption keys to target devices via OTAR.
- **Download encryption keys from the KMF into the KVL** – Two methods are available for transferring encryption keys when OTAR cannot be performed, such as for radios that do not support OTAR, radios that are out of range, or radios that have not yet been initialized. The download from the KMF to the KVL may be performed either by direct cable connection or through a modem connection. The two methods of downloading keys are:
 - Individual keys are downloaded to the KVL key database which are then loaded directly into target devices (see [Chapter 4 KVL 4000 – Loading Encryption Keys into Target Devices](#)). This method requires that you know the CKRs of the keys in the KVL key database.
 - With the use of the Store and Forward ASTRO® 25 feature, Key Management Messages (KMMs) – usually containing encryption keys – are downloaded to the KVL that is in turn used to update target devices. This operation does not require that you know the CKRs of the keys in the KVL database. This simplifies the key loading procedure. (See [7.2.4 Updating a Target Device, page 7-15](#).)

7.1 Setting Up the KVL for KMF Operations

Before using your KVL to work with a KMF, program several KMF-related parameters.

Prerequisites:

Your KVL supports KMF operation.

Process Steps

- 1 Enter a Unique Key Encryption Key (UKEK) required per algorithm in the KVL for OTAR systems. See [7.1.1 Entering the UKEK, page 7-2](#).

**NOTE**

The UKEK consists of a KID and Key Data.

- 2 Enter a 7-digit KMF Radio Set Identifier (KMF RSI) number. See [7.1.6 Entering the KMF RSI, page 7-8](#).
- 3 Enter a 5-digit Message Number Period (MNP). See [7.1.7 Entering the MNP for OTAR, page 7-9](#).

**NOTE**

The MNP provides additional rekeying security for OTAR systems.

- 4 Enter a 7-digit KVL Radio Set Identifier (KVL RSI) number. See [7.1.8 Entering the KVL RSI for OTAR, page 7-10](#).
 - 5 Select the Main or Backup KMF. See [7.1.2 Selecting Main or Backup KMF, page 7-3](#).
 - 6 If required, enter the Main and Backup KMF dial-up phone numbers for modem connections. See [7.1.3 Entering Main and Backup KMF Phone Numbers, page 7-4](#).
 - 7 If required, enter the Main and Backup KMF port for the Network connection. See [7.1.4 Entering Main and Backup KMF Ports, page 7-6](#).
 - 8 If required, enter the Main and Backup KMF IP address for the Network connection. See [7.1.5 Entering Main and Backup KMF IP Addresses, page 7-7](#).
-

7.1.1 Entering the UKEK

For an OTAR operation, program a Unique Key Encryption Key (UKEK) into the KVL for each algorithm being used. Each UKEK is a multi-character key typically assigned by the Crypto/Security Officer for the system, and is used to communicate with other secure equipment such as a KMF. The exact number of characters is determined by the algorithm.

Prerequisites:

Only an Administrator can enter the UKEK for KMF operation.

When and where to use:

Use these steps to enter the UKEK.

**IMPORTANT**

You enter the UKEK only once, after which it is permanently stored in the KVL memory. The UKEK is destroyed if the FIPS mode is enabled.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **UKEKs**.

Step result: A list of available algorithms appears.

- 2 Select the algorithm you want to enter the UKEK for.

Step result: A screen with the Hex keypad appears.

- 3 Enter the UKEK using the Hex keypad.

Step result: As you enter the digits, they appear in the info field and the green background indicates the progress. If you enter an incorrect digit, a **bad bonk** tone is played. When you have entered a valid string of digits, a check mark appears next to it.

**NOTE**

To delete a digit you have entered, tap the **< Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.

- 4 Tap **Done**.

Step result: The UKEK for the selected algorithm has been entered.

- 5 Repeat [step 2](#) through [step 4](#) for each algorithm you want to enter a UKEK for. Then, tap **Done** on the consecutive screens to return to the KVL main screen.

7.1.2 Selecting Main or Backup KMF

The KVL supports dial-up phone numbers for a Main and a Backup KMF. You can determine which KMF is communicated with when making a connection.

Prerequisites:

Only an Administrator can select Main or Backup KMF.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **Active KMF**.

Step result: A list of available options (Main or Backup KMF) appears, with the currently selected KMF highlighted.

- 2 Select the desired KMF.

Step result: The KMF you have selected is now active.

- 3 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.3 Entering Main and Backup KMF Phone Numbers

The KVL supports dial-up phone numbers for the Main and Backup KMF.

Prerequisites:

Only an Administrator can enter KMF phone numbers.

When and where to use:

Use these steps to enter the Main and Backup KMF phone numbers.



NOTE

You might have to experiment with your particular calling card service to determine the number of pauses needed and in which locations in the phone number string they must be placed. For example, a typical dialing sequence might be:

- Dial Access Number
- Pause 4 seconds (2 commas)
- Dial the desired phone number
- Pause 2 seconds (1 comma)
- Dial Credit Card Number (or PIN number)

Procedure Steps

-
- 1 On the KVL main screen, select **Settings** → **KMF** → **Phone #s**.

Step result: The phone keypad appears.

Figure 7-1 Phone #s Screen



NOTE

The screen appears with the tab for the currently selected KMF open.

-
- 2 Select the tab for the KMF you want to enter the phone number for.
-

- 3 Enter the phone number using the phone keypad.



NOTE

If you need to enter an * or # characters, use the PDA keypad.



NOTE

- As you tap the digits, they appear in the phone info field.
- To enter a pause, tap the **Pause** button. (A pause appears as comma-space, two pauses as comma-comma, and so on.)
- For the United States, the US parsing rules are used to split the string in 3-3-4 chunks.
- To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits.
- To abort the operation, tap **Cancel**.

-
- 4 When you have entered a valid phone number, tap **Done**.

Step result: The phone number is changed.

- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.4 Entering Main and Backup KMF Ports

For the KVL to connect with the KMF through the Network, you need to configure the KMF port on the KVL.

Prerequisites:

Only an Administrator can enter Main and Backup KMF ports.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **KMF port**.

Step result: A decimal keypad appears.

- 2 Enter the port number for the Main KMF.



NOTE

The available range is 49156 through 65535.



IMPORTANT

If you change the default value, ensure it matches the port number configured on the KMF.

- 3 Select the **Backup** tab and enter the port number for the Backup KMF.
-

- 4 Tap **Done**.

Step result: The KMF ports are set.

- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.5 Entering Main and Backup KMF IP Addresses

For the KVL to connect with the KMF through the Network, you need to configure the KMF IP address on the KVL.

Prerequisites:

Only an Administrator can enter Main and Backup KMF IP addresses.

Obtain the IP address from your radio network administrator.



NOTE

The IP address have to be IPv4.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **IP address**.
Step result: A decimal keypad appears.

 - 2 Enter the IP address of the Main KMF.

 - 3 Select the **Backup** tab and enter the IP address of the Backup KMF.

 - 4 Tap **Done**.
Step result: The IP addresses are set.

 - 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.6 Entering the KMF RSI

The KMF requires a Radio Set Identifier (RSI) in order to operate in the OTAR system. The KVL only accepts keys and KMMs from the KMF with this RSI.

Prerequisites:

Only an Administrator can enter the KMF RSI.

When and where to use:

Use these steps to enter the KMF RSI.



CAUTION

Changing the KMF RSI removes received jobs.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **KMF RSI**.

Step result: The decimal keypad appears.

- 2 Enter the RSI using the decimal keypad.



NOTE

- The available values range from 1 through 9999999. The default value is 9999999.
 - As you enter the digits, they appear in the info field. If you have entered a 7-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.
-

- 3 When you have entered the RSI, tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.7 Entering the MNP for OTAR

The Message Number Period (MNP) is a feature used in an ASTRO® 25 system that provides additional security in the over-the-air rekeying of subscriber units. The MNP number serves as an offset value used in synchronizing OTAR rekeying transmissions.

Prerequisites:

Only an Administrator can enter the MNP.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KMF** → **MNP**.

Step result: A decimal keypad appears.

- 2 Enter the MNP using the decimal keypad.



NOTE

- The available values range from 0 through 65535. The default value is 1000.
 - As you enter the digits, they appear in the info field. If you have entered a 5-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.
-

- 3 When you have entered the MNP, tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.1.8 Entering the KVL RSI for OTAR

The KVL requires a Radio Set Identifier (RSI) in order to operate in the OTAR system.

Prerequisites:

Only an Administrator can enter the KVL RSI.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KVL RSI**.

Step result: A decimal keypad appears.

- 2 Enter the RSI using the decimal keypad.



NOTE

- The available values range from 1 through 9999999. The default value is 9999998.
- As you enter the digits, they appear in the info field. If you have entered a 7-digit value, the keypad becomes disabled.
- To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.



IMPORTANT

The KVL RSI must match the individual RSI assigned to this KVL in the KMF.

- 3 When you have entered the RSI, tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.2 Using the Store and Forward Feature

The Store and Forward feature (supported only in the ASTRO® 25 mode of operation) offers a simple and secure method of transferring keys and other messages from the KMF to target devices through the KVL.



NOTE

The UKEK must be present in the KVL and target devices in order to support the Store and Forward operation.

7.2.1 Downloading Keys from KMF to KVL Using Direct Connection

You can download encryption keys stored in the KMF to the KVL using a direct cable connection.

Prerequisites:

The KVL must have a UKEK assigned for the algorithm type of the keys being downloaded, and the UKEK must match the UKEK defined for this KVL in the KMF.

Procedure Steps

- 1 Connect the KVL to the KMF using the Null Modem Cable. (See [1.4.4.3.1 Connecting the KVL to the KMF – Direct Connection, page 1-16.](#))

 - 2 On the KVL main screen, select **Store & Forward** → **Connect to KMF** → **Direct**.
Step result: The following takes place:
 1. The connection between KVL and KMF is established.
 2. KVL sends status reports of radios to KMF.
 3. KVL receives keys and jobs for radios from KMF.

 - 3 When all the information has been sent, tap **Done** to return to the KVL main screen.
-

7.2.2 Downloading Keys from KMF to KVL Using Modem Connection

You can use a modem connection to download keys from a KMF to a KVL.

The following modem procedures are available:

- [7.2.2.1 Downloading Keys from KMF to KVL Using USB Modem Connection, page 7-12](#)
- [7.2.2.2 Downloading Keys from KMF to KVL Using Serial Modem Connection, page 7-13](#)

7.2.2.1 Downloading Keys from KMF to KVL Using USB Modem Connection

Prerequisites:

Ensure that:

- The KVL has a UKEK assigned for the algorithm type of the keys being downloaded, and the UKEK matches the UKEK defined for this KVL in the KMF.
- You have the power supply and USB modem.

Procedure Steps

- 1 Connect the KVL to the USB modem. (See [1.4.4.3.2 Connecting the KVL to the USB Modem for the KMF Communication](#), page 1-17.)



NOTE

For the USB communication to work, the power supply must be connected to the KVL at all times.

- 2 On the KVL main screen, select **Store & Forward** → **Connect to KMF** → **Through modem (USB)**.

Step result: The following takes place:

1. The connection between KVL and KMF is established.
 2. KVL sends status reports of radios to KMF.
 3. KVL receives keys and jobs for radios from KMF.
-

- 3 When all the information has been sent, tap **Done** to return to the KVL main screen.
-

7.2.2.2 Downloading Keys from KMF to KVL Using Serial Modem Connection

Prerequisites:

The KVL must have a UKEK assigned for the algorithm type of the keys being downloaded, and the UKEK must match the UKEK defined for this KVL in the KMF.

Procedure Steps

- 1 Connect KVL to the serial modem. (See [1.4.4.3.3 Connecting the KVL to the Serial Modem for the KMF Communication, page 1-18.](#))

 - 2 On the KVL main screen, select **Store & Forward** → **Connect to KMF** → **Through modem (Serial)**.
Step result: The following takes place:
 1. The connection between KVL and KMF is established.
 2. KVL sends status reports of radios to KMF.
 3. KVL receives keys and jobs for radios from KMF.

 - 3 When all the information has been sent, tap **Done** to return to the KVL main screen.
-

7.2.3 Downloading Keys from KMF to KVL Using Network Connection

You can download encryption keys stored in the KMF to the KVL using a Network connection.

Prerequisites:

Ensure that:

- The KVL has a UKEK assigned for the algorithm type of the keys being downloaded, and the UKEK matches the UKEK defined for this KVL in the KMF.
- You have entered the KMF port and IP address in the KVL.
- You have performed [1.4.8 Configuring VPN Settings, page 1-26](#), if you want to establish the KVL to KMF Ethernet connection using the VPN client provided by Motorola.
- You have the USB to Ethernet Adapter, MINI-B to Type-A USB Cable, and Ethernet cable.

Procedure Steps

- 1 Connect the KVL to the Network. See [1.4.4.3.4 Connecting the KVL to the Network for the KMF Communication, page 1-19](#).

- 2 If you want to establish the KVL to KMF Ethernet connection using the VPN client provided by Motorola, see [1.4.9 Establishing the VPN Connection, page 1-43](#).

- 3 Launch the KVL application.

- 4 On the KVL main screen, select **Store & Forward** → **Connect to KMF** → **Through network**.
Step result: The connection between the KVL and KMF is established. The KVL sends status reports of radios to the KMF and then receives keys and jobs for radios from the KMF.

- 5 When all the information has been sent, tap **Done** to return to the KVL main screen.

- 6 If you established the KVL to KMF Ethernet connection using the VPN client provided by Motorola, terminate the VPN connection. See [1.4.10 Terminating the VPN Connection, page 1-46](#).

7.2.4 Updating a Target Device

Prerequisites:

Keys are downloaded from the KMF to the KVL.

Procedure Steps

- 1 On the KVL main screen, select **Store & Forward** → **Forward to radio**.

Step result: A list of available target devices appears.



NOTE

You can use the **Sort** button to sort the target devices on the list by:

- Name
- Serial number
- ID
- Update status

You can use the smart bar to scroll through the list or quickly jump within the list to a selected area (tapping a letter on the smart bar takes you to the first item on the list starting with this letter). If the list fits completely on the screen, the smart bar is disabled.

-
- 2 If the target device is an APX or XTS radio, set it to an OTAR-enabled personality.

 - 3 Connect the target device to the KVL using an appropriate key load cable (see [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13](#)) and tap the item for this device on the list.



NOTE

If there are no updates for the device, it is indicated on the screen and the **attention** tone is played.

Step result: A progress animation appears, indicating that the device is being updated. When the update is completed, it is indicated on the screen and the **completed** tone is played.

-
- 4 Disconnect the target device.

 - 5 Connect another target device to update, or tap **Done** to return to the KVL main screen.
-

Postrequisites:

After you have performed a successful update on a target device, it cannot be updated again until you have connected the KVL to the KMF to upload the unit response messages.

7.2.5 Viewing the List of Received Jobs

Prerequisites:

The KVL received keys and jobs for radios from the KMF.

Procedure Steps

- 1 On the KVL main screen, select **Store & Forward** → **View received jobs**.

Step result: A list of received jobs appears.



NOTE

You can use the **Sort** button to sort items on the list by:

- Name
- Serial number
- ID
- Update status

You can use the smart bar to scroll through the list or quickly jump within the list to a selected area (tapping a letter on the smart bar takes you to the first item on the list starting with this letter). If the list fits completely on the screen, the smart bar is disabled.

-
- 2 To clear the list of received jobs, continue to [7.2.6 Clearing the List of Received Jobs, page 7-17](#).
-

7.2.6 Clearing the List of Received Jobs

Prerequisites:

- The KVL received keys and jobs for radios from the KMF.
- Only an Administrator can clear the list of received jobs.

When and where to use:

Use these steps to clear the list of received jobs.



IMPORTANT

Clearing the messages also erases all unit responses. Do not clear the messages until you have reconnected with the KMF and uploaded the unit responses.

Procedure Steps

1 Perform [7.2.5 Viewing the List of Received Jobs](#), page 7-16.

2 Tap the **Clear** button.

Step result: A confirmation screen appears.



NOTE

To restore the list, tap the **Undo** button.

3 Tap **Accept**.

Step result: The list of received jobs has been cleared.

4 Tap **Cancel** to return to the KVL main screen.

7.3 Performing a Keypad Changeover on a Target Device

You can use the KVL to perform a keypad changeover (such as switching from Keypad 1 to Keypad 2) on a target device.

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect a target device.



NOTE

If a device is already connected, this prompt is skipped. If a device becomes disconnected, you are returned to the prompt.

-
- 2 Connect the target device. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.](#))

Step result: A **connected** tone is played and a list of available options appears.

-
- 3 Select **Keysets**.

Step result: A list of available keysets appears, with the active keyset highlighted and indicated with a check mark.

-
- 4 Tap the list item for the keyset which you want to set as active.

Step result: If the change takes more than 1 second, a progress animation appears while the keyset is being changed. Otherwise, the keyset is changed instantly, the **completed** tone is played, and the list item for the new keyset receives a check mark.

-
- 5 Disconnect the target device and tap **Done** on the consecutive screens to return to the KVL main screen.
-

7.4 Managing OTAR Configuration Parameters in Target Devices

The following parameters are required by target devices in order to operate within an OTAR system:

- Target's RSI
- KMF RSI
- MNP

In most cases, these parameters are loaded into the target devices automatically by the KVL during the initial Store and Forward update through the KMF. The KVL has the capability of viewing these parameters, as well as loading new parameters into target devices (if necessary).

7.4.1 Viewing the Target's MNP

You can connect the KVL to a target device (such as a radio, DIU, or RNC) and view the MNP currently stored in the device.

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect a target device.



NOTE

If the device is already connected, this prompt is skipped. If a device becomes disconnected, you are returned to the prompt.

-
- 2 Connect the target device. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.](#))

Step result: A **connected** tone is played and a list of available options appears.

-
- 3 Select **MNP**.

Step result: The **MNP** list item appears with the currently selected value presented.



NOTE

If the value is being actively updated, the list item says **[updating...]** instead of presenting the value.

-
- 4 To change the target device's MNP, continue to [7.4.3 Changing the Target's MNP, page 7-21.](#)
-

7.4.2 Viewing the Target's RSI and KMF RSI

You can connect the KVL to a target device (such as a radio, DIU, or RNC) and view the RSI and KMF RSI currently stored in the device.

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect a target device.



NOTE

If the device is already connected, this prompt is skipped. If a device becomes disconnected, you are returned to the prompt.

-
- 2 Connect the target device. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.](#))

Step result: A **connected** tone is played and a list of available options appears.

-
- 3 Select **RSIs**.

Step result: A list of RSI values appears.



NOTE

- If a value is being actively updated, the list item says **[updating...]** instead of presenting the value.
- The **Group RSI** list item is read-only.

-
- 4 To change the target device's RSI or KMF RSI, continue to [7.4.4 Changing the Target's RSI and KMF RSI, page 7-22.](#)
-

7.4.3 Changing the Target's MNP

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

1 Perform [7.4.1 Viewing the Target's MNP, page 7-19](#).

2 Tap the **MNP** list item.

Step result: A decimal keypad appears.

3 Delete the existing MNP using the < **Del** key, and enter the new MNP using the decimal keypad.



NOTE

- The available values range from 0 through 65535. The default value is 1000.
 - As you enter the digits they appear in the info field. If you have entered a 5-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation and return to the previous screen, tap **Cancel**.
-

4 When you have entered the MNP, tap **Done**.

Step result: The MNP is changed and you return to the previous screen. When the MNP is updated in the target device, the **completed** tone is played.

5 Disconnect the target device, and tap **Done** on the consecutive screens to return to the KVL main screen.

7.4.4 Changing the Target's RSI and KMF RSI

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

1 Perform [7.4.2 Viewing the Target's RSI and KMF RSI, page 7-20](#).

2 Tap the **RSI** or **KMF RSI** list item, depending on which one you want to change.

Step result: A screen with the decimal keypad appears.

3 Delete the existing value using the < **Del** key, and enter the new value using the decimal keypad.



NOTE

- The available values range from 1 through 9999999. The default value is 9999999.
 - As you enter the digits they appear in the info field. If you have entered a 7-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation and return to the previous screen, tap **Cancel**.
-

4 When you have entered the correct value, tap **Done**.

Step result: The value is changed and you return to the previous screen. When the value is updated in the target device, the **completed** tone is played.

5 Disconnect the target device, and tap **Done** on the consecutive screens to return to the KVL main screen.

8 KVL 4000 Operations Through a Remote Control Head

Sometimes, when servicing a mobile radio's secure parameters, it can be difficult to gain access to the radio's direct key loading port. The radio may be mounted in a vehicles trunk along with other assorted equipment or in another equally inaccessible location.

Motorola's Remote Control Head Key loading feature allows you to remotely perform operations on a radio through a Remote Control Head that can be mounted in a vehicles cabin.

8.1 Performing KVL Operations Through a Remote Control Head

Process Steps

- 1 Set up your KVL for Remote Control Head operations. See [8.2 Setting Up KVL for Remote Control Head Operations, page 8-1](#).
 - 2 Provision a radio for Remote Control Head key loading. See [8.3 Provisioning a Radio for Remote Control Head Key Loading, page 8-5](#).
 - 3 Connect the KVL to the Remote Control Head. See [8.4 Connecting the KVL to the Mobile Radio's Remote Control Head, page 8-6](#).
 - 4 Initiate one of the operations. For details, see the appropriate chapters of this manual:
 - [Chapter 4 KVL 4000 – Loading Encryption Keys into Target Devices](#)
 - [Chapter 5 KVL 4000 – Managing Keys in Target Devices](#)
 - [Chapter 7 Using KVL 4000 in OTAR Systems](#)
-

8.2 Setting Up KVL for Remote Control Head Operations

Before using your KVL to perform operations on a radio through a Remote Control Head, program several security parameters.

Process Steps

- 1 Enter a Signaling Encryption Key (SEK) and a Key Encryption Key (KEK) required per algorithm in the KVL. See [8.2.1 Entering the SEK and KEK, page 8-2](#).



NOTE

- The KEK secures keys exchanged between the KVL and the radio through the Remote Control Head.
- The SEK secures messages exchanged between the KVL and the radio through the Remote Control Head.

-
- 2 Enter a 5-digit Message Number Period. See [8.2.2 Entering the MNP for Remote Control Head Operations, page 8-3](#).



NOTE

The MNP provides additional rekeying security for remote key loading.

-
- 3 Enter a 7-digit KVL Radio Set Identifier (KVL RSI) number. See [8.2.3 Entering the KVL RSI for Remote Control Head Operations, page 8-4](#).
-

8.2.1 Entering the SEK and KEK

In order to perform KVL operations on a radio through a Remote Control Head, define a SEK and KEK for each algorithm used by the KVL.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Control head keys**.

Step result: A list of available algorithms appears.

- 2 Select the desired algorithm.

Step result: A screen with the **SEK** and **KEK** entries appears.



NOTE

Since both parameters are required, the **Done** button is not available until you have entered both the SEK and KEK.

- 3 Select **SEK**.

Step result: A Hex keypad appears.

- 4 Enter the parameter using the Hex keypad and tap **Done**.

Step result: The SEK has been entered.

- 5 Select **KEK** and repeat [step 4](#).

Step result: The KEK has been entered.

- 6 Tap **Done**.
-

- 7 If you want to set up the SEK and KEK for another algorithm, perform [step 2](#) through [step 6](#) for this algorithm. Otherwise, tap **Done** on the consecutive screens to return to the KVL main screen.
-

8.2.2 Entering the MNP for Remote Control Head Operations

The Message Number Period (MNP) is used in an ASTRO® 25 system to provide additional security in the remote rekeying of subscriber units. The MNP number may range from 0 through 65535, and serves as an offset value used in synchronizing remote rekeying transmissions.

When and where to use:

Use these steps to enter the MNP.



NOTE

Entering an MNP value of 0 or 65535 disables Message Number checking and weakens your system's security. Consult with your Security Officer to obtain the recommended value.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Tactical OTAR** → **MNP**.

Step result: A decimal keypad appears.

- 2 Enter the MNP using the decimal keypad.



NOTE

- The available values range from 0 through 65535. The default value is 1000.
 - As you enter the digits they appear in the info field. If you have entered a 5-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.
-

- 3 When you have entered the MNP, tap **Done**.



NOTE

If you have entered an incorrect value, the **Done** button is disabled.

- 4 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

8.2.3 Entering the KVL RSI for Remote Control Head Operations

The KVL requires a Radio Set Identifier (RSI) in order to operate in the Remote Control Head key loading mode.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **KVL RSI**.

Step result: A decimal keypad appears.

- 2 Enter the RSI using the decimal keypad.



NOTE

- The available values range from 1 through 9999999. The default value is 9999998.
 - As you enter the digits they appear in the info field. If you have entered a 7-digit value, the keypad becomes disabled.
 - To delete a digit you have entered, tap the < **Del** key, or hold it to delete all entered digits. To abort the operation, tap **Cancel**.
-

- 3 When you have entered the RSI, tap **Done** on the consecutive screens to return to the KVL main screen.
-

8.3 Provisioning a Radio for Remote Control Head Key Loading

In order to be able to perform operations through a Remote Control Head, provision a radio with keys for the available algorithms.

Prerequisites:

Ensure you have:

- an appropriate key load cable
- an adaptor (if required)

Procedure Steps

- 1 Select **Configure a radio** on the KVL main screen.

Step result: You are prompted to connect a radio.



NOTE

If the device is already connected, this prompt is skipped. If the device becomes disconnected, you are returned to the prompt.

- 2 Connect the radio. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.](#))

Step result: A **connected** tone is played and a list of available options appears.

- 3 Scroll down the screen and select **Provision radio**.

Step result: A list of available algorithms appears.

- 4 Tap **Start** >.

Step result: The provisioning process starts for each of the defined algorithms one by one. The status of the process is indicated on the list item for each algorithm:

- **Waiting...** – waiting to be provisioned
- **Provisioning...** – in process

When all the processes are completed, a screen appears with the statuses for each of the algorithms. The possible statuses are:

- **Provisioning successful** – when the process is completed successfully.
 - **Provisioning failed** – when the process is completed but failed.
 - **Keys not defined** – when there are no keys defined for the particular algorithm.
-

- 5 Disconnect the radio.
-

- 6 If you want to provision another radio, tap **Done** to return to the list of options and repeat [step 2](#) through [step 5](#). Otherwise, tap **Done** on the consecutive screens to return to the KVL main screen.
-

8.4 Connecting the KVL to the Mobile Radio's Remote Control Head

Prerequisites:

Ensure you have:

- Data cable
- DB9 Gender Changer

Procedure Steps

- 1 Take the data cable (HKN6183) and the DB9 Gender Changer (provided with the KVL).
 - 2 Connect the KVL to the mobile radio's Remote Control Head through the DB9 (RS-232) Port and the DB9 Gender Changer.
-

Figure 8-1 KVL Connected to a Mobile Radio's Remote Control Head



9 KVL 4000 – Working with Tactical OTAR Groups

Tactical OTAR is a Motorola feature that allows a KVL to wirelessly manage a key (TEK only) for a small group of radios, with one radio serving as an RF modem. The radio serving as an RF modem must be equipped with the Tactical Rekey/OTAR feature. The radio serving as an RF modem may also be a member of any one of the managed Tactical OTAR groups.

9.1 Equipment Needed For Tactical OTAR

You need the following equipment for Tactical OTAR:

- Data cable (see [Table B-5 Interface Cables](#))
- DB9 Gender Changer
- Radio equipped with the Tactical Rekey/OTAR feature

Figure 9-1 Tactical OTAR Equipment (Example)



9.2 Setting Up Tactical OTAR

Prerequisites:

All radios must be configured with distinct RSIs and IP addresses for proper operation.

Procedure Steps

- 1 Create a Tactical OTAR group (see [9.3 Creating a New Tactical OTAR Group, page 9-2](#)).

Step result: The group is now ready for new members.

- 2 Add members to the Tactical OTAR group (see [9.6 Adding a Member to a Tactical OTAR Group, page 9-5](#)).

Step result: The members are now ready to be updated wirelessly.

- 3 Update the Tactical OTAR group (see [9.9 Updating a Tactical OTAR Group, page 9-8](#)).

Step result: The members can now talk securely.

9.3 Creating a New Tactical OTAR Group

Prerequisites:

Only an Administrator can create a Tactical OTAR group.

When and where to use:

Use these steps to create a Tactical OTAR group.



NOTE

You can create up to 10 Tactical OTAR groups.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available tactical OTAR groups (if any) appears.

- 2 Tap the + button to define the parameters of a new tactical OTAR group.
-

- 3 Enter the name of the group using the PDA keypad.



NOTE

The name can consist of up to 8 characters, including spaces.

-
- 4 Select an algorithm for the group.

**NOTE**

The **Algorithm** list item is read-only if only a single algorithm is defined.

- 5 Select **TEK** to define the Traffic Encryption Key for the group.

Step result: The list of TEKs appears.

- 6 You can either select a key from the list or enter a new key by tapping the + button.

**NOTE**

For details on how to enter encryption keys, see [3.1 Entering Encryption Keys, page 3-1](#). When entering a new key, remember that **Algorithm** and **Key Type** have already been predefined.

- 7 Select **SEK** to define the Signaling Encryption Key for the group.

Step result: The list of SEKs appears.

- 8 You can either select a key from the list or enter a new key by tapping the + button.

**NOTE**

For details on how to enter encryption keys, see [3.1 Entering Encryption Keys, page 3-1](#). When entering a new key, remember that **Algorithm** and **Key Type** have already been predefined.

- 9 Select **KEK** to define the Key Encryption Key for the group.

Step result: The list of KEKs appears.

- 10 You can either select a key from the list or enter a new key by tapping the + button.

**NOTE**

For details on how to enter encryption keys, see [3.1 Entering Encryption Keys, page 3-1](#). When entering a new key, remember that **Algorithm** and **Key Type** have already been predefined.

- 11 If you want to add a member to the group, perform [9.6 Adding a Member to a Tactical OTAR Group, page 9-5](#).
-

- 12 Tap **Done** when ready.

Step result: A new tactical OTAR group has been created.

- 13 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.4 Deleting an Existing Tactical OTAR Group

Prerequisites:

Only an Administrator can delete a Tactical OTAR group.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available tactical OTAR groups (if any) appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

-
- 2 Select the group you want to delete.

Step result: Details for the group appear.

-
- 3 Tap **Delete**.

Step result: A confirmation screen appears.

-
- 4 Tap **Accept** to confirm.



NOTE

To restore the group, tap **Undo**.

Step result: The group has been deleted.

-
- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.5 Viewing the Members of a Tactical OTAR Group

Prerequisites:

A Tactical OTAR group is created.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available Tactical OTAR groups (if any) appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

-
- 2 Select the group you want to view members for.

Step result: The details for the group appear.

-
- 3 Select **Members**.

Step result: A list of available members appears.

-
- 4 When finished, tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.6 Adding a Member to a Tactical OTAR Group

Before a radio can be a part of a Tactical OTAR group, it must first be added to that Tactical OTAR group.

Prerequisites:

A Tactical OTAR group is created.

When and where to use:

Use these steps to add a member to a Tactical OTAR group.



NOTE

You can add up to 50 members to one Tactical OTAR group.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available Tactical OTAR groups (if any) appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

-
- 2 Select the group you want to add a member to.

Step result: The details for the group appear.

-
- 3 Select **Members**.

Step result: A list of available members appears.

-
- 4 Tap the + button.

Step result: You are prompted to connect a radio.

-
- 5 Connect the radio. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: The target radio has been added as a member, and a **completed** tone is played.

-
- 6 Disconnect the radio and connect a new radio if you want to add another target unit as a member, or tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.7 Removing a Member from a Tactical OTAR Group

Prerequisites:

A Tactical OTAR group is created.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available Tactical OTAR groups (if any) appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

-
- 2 Select the group you want to remove a member from.

Step result: The details for the group appear.

-
- 3 Select **Members**.

Step result: A list of available members appears.

-
- 4 Drag the slider from right to left to remove a member from the group.

Step result: The member has been removed.

-
- 5 Remove another member, or tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.8 Editing the TEK of a Tactical OTAR Group

Prerequisites:

Only an Administrator can edit the TEK of a Tactical OTAR group.

Procedure Steps

- 1 On the KVL main screen, select **Tactical OTAR** → **Manage OTAR groups**.

Step result: The list of available Tactical OTAR groups (if any) appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 2 Select the group you want to edit the TEK for.

Step result: The details for the group appear.

- 3 Select **TEK**.

Step result: The list of TEKs appears.

- 4 You can either select a key from the list or enter a new key by tapping the + button.



NOTE

For details on how to enter encryption keys, see [3.1 Entering Encryption Keys, page 3-1](#). When entering a new key, remember that **Algorithm** and **Key Type** have already been predefined.

Step result: The TEK has been modified.



NOTE

Upon the next update request for the Tactical OTAR group using the updated CKR as a TEK, the new key information is sent to all the members of the group.

- 5 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

9.9 Updating a Tactical OTAR Group

Prerequisites:

A Tactical OTAR group is created.

Procedure Steps

- 1 Power on all the member radios of the Tactical OTAR group.
-

- 2 On the KVL main screen, select **Tactical OTAR** → **Update an OTAR group**.

Step result: The list of available Tactical OTAR groups appears.



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 3 Select the group you want to update.

Step result: The list of group members appears.



NOTE

An icon indicates whether a member is updated (check mark), or requires an update (exclamation mark).

- 4 Tap **Quick update** if you want only the members that require and update to be updated or select **Full update** if you want all members to be updated.

Step result: You are prompted to connect the radio.

- 5 Connect the radio. (See [1.4.4.1 Connecting the KVL to a Radio or Another Target Device](#), page 1-13.)

Step result: A progress animation appears, indicating that the group is being updated. When the process is complete, a screen with all Success and Failed members appears.



NOTE

The following status messages are possible during and after the update process:

- No update needed – displayed in case of a quick update.
 - Updating... – displayed for the current member being updated.
 - Update successful – displayed for a successful update.
 - Waiting to be updated – displayed for other members to be updated.
 - Not responding or Can't decrypt messages – Reasons for failed update displayed in case of update failure.
-

- 6 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

10 Managing Log Records

The KVL maintains a running record of the most recent 100 successful key load operations.

The format of each log record entry on the list is as follows:

- First line: Date/Time
- Second line: Role/Action Performed
- Third line: Entity Name/CKR ID/PID/Target ID

Log records can be:

- Viewed and scrolled on the KVL screen.
- Exported to a PC for printing or saving to a file.
- Cleared (erased) from the KVL memory.

10.1 Organization of Log Records

The log records are stored chronologically in a 100-location continuous buffer, with the most recent log record displayed first each time you access the log records.

Each new log record created is appended to the beginning of the buffer, with each existing log record moving down one position.

When the buffer is full (100 entries maximum), the next new log record is appended to the beginning, the existing log records move down one position, and the oldest log record is overwritten.

10.2 Accessing Log Records

Prerequisites:

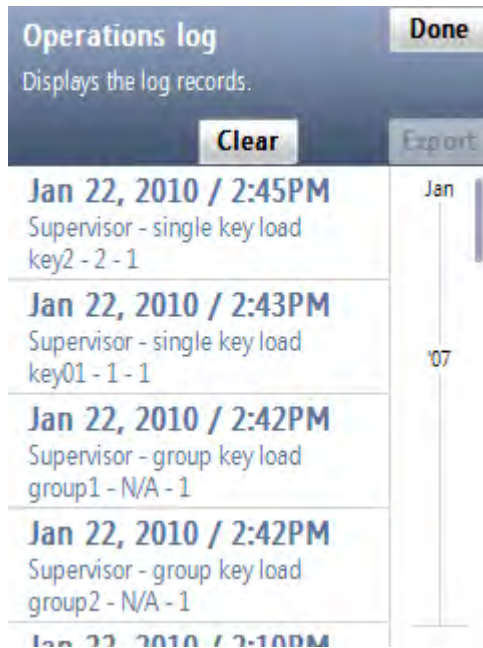
There are log records in the KVL memory.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Operations log**.

Step result: The list of log records appears.

Figure 10-1 Operations Log (Example)



NOTE

You can scroll through the list or quickly jump to a selected area using the smart bar on the right side of the screen.

- 2 When you have finished viewing log records, tap **Done** on the consecutive screens to return to the KVL main screen.
-

10.3 Clearing Log Records

Prerequisites:

Only an Administrator can clear log records.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **Operations log**.

Step result: The list of log records appears.

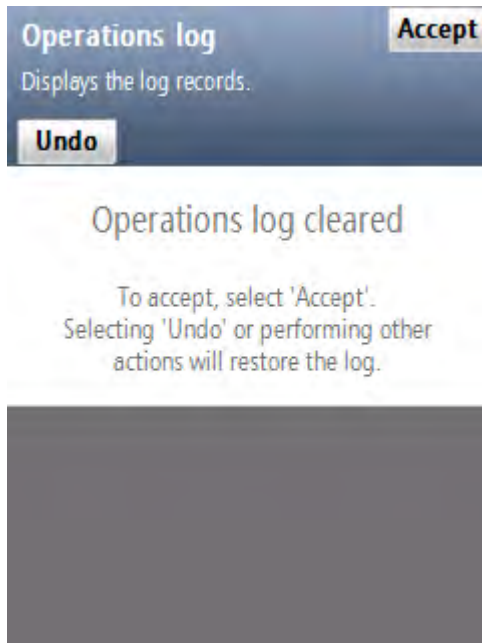
Figure 10-2 Operations Log – Clear (Example)



- 2 Select the **Clear** button.

Step result: A confirmation screen appears.

Figure 10-3 Clearing Logs – Confirmation Screen



NOTE

To restore the log, tap **Undo**.

-
- 3 Tap **Accept** to confirm.



IMPORTANT

Only the logs for the current mode of operation (ASN, ASTRO® 25, or Radio Authentication) are cleared.

Step result: The log records have been cleared.

-
- 4 Tap **Done** to return to the KVL main screen.
-

10.4 Exporting Log Records to a PC

You can connect the KVL to a COM port on a PC (typically a laptop) and export log records to the PC. You can then print log records from the PC or save them on the PC as a file.

Prerequisites:

A communications program, such as Microsoft HyperTerminal, must be running on the PC in order to export log records.

Procedure Steps

- 1 Connect an appropriate cable between the KVL DB9 Port (RS-232) and a COM port on the PC. Depending on the cable type, you may need to use a gender changer.

**NOTE**

Ensure that the baud rate set up in the KVL matches the baud rate in the communications program.

- 2 Launch a communications program on the PC (such as Microsoft HyperTerminal or equivalent). Set up the program as follows:

- No parity
 - 8 bits
 - 1 stop bit
 - Translate line feeds <LF> to Carriage Return and Line Feed <CR><LF>
 - 80 character width
-

- 3 On the KVL main screen, select **Settings** → **Operations log** → **Print** → **Print Now**.

Step result: A progress animation appears, indicating that the log records are being exported to the PC. When the log records have been exported successfully, you return to the list of log records.

- 4 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

11 Keys

KVL 4000 – Converting Encryption



NOTE

This chapter is applicable only if your KVL is configured to work in both ASN and ASTRO® 25 modes of operation.

If your KVL is configured to work in both ASN and ASTRO® 25 modes of operation, you can convert encryption keys between these two modes. Converting keys allows you to copy an ASN Traffic or Shadow key from its ASN memory location (stored to a PID and containing a LID) and load it into an empty ASTRO® 25 TEK or KEK memory location (stored to a CKR and containing a KID), and the other way around.

11.1 When to Convert Keys

Converting keys is used most commonly for copying keys between ASN and ASTRO® 25 in the KVL memory.

There may be occasions when you have an existing key in an ASN memory location and wish to duplicate it for use on an ASTRO® 25 target. By converting the key from the ASN memory to ASTRO® 25 memory within the KVL, you save the effort of recreating the key in the ASTRO® 25 memory and reentering the encryption key data. You may also convert keys from the ASTRO® 25 memory and load them into the ASN memory.

11.2 Key Converting Restrictions and Guidelines

Observe the following restrictions and guidelines when converting keys:

- Only keys with AES-256, DES-OFB, DES-XL, DVP-XL, and DVI-XL algorithms can be converted.
- TEKs of the same algorithm type stored in ASTRO® 25 memory cannot have duplicate KIDs (including 0000).
- Traffic Keys (ASN) can be converted only to Traffic Encryption Keys (TEK) locations in ASTRO® 25 memory (and the other way around); Shadow Keys (ASN) can be converted only to Key Encryption Keys (KEK) locations in ASTRO® 25 memory (and the other way around).
- Keys can be converted only to an empty memory location; overwriting is not allowed.
- Keys must be converted one at a time.

11.3 Converting a Key from ASN to ASTRO 25

Prerequisites:

Only an Administrator can convert keys.

Procedure Steps

- 1 On the KVL main screen, select **Manage** → **Keys**.

Step result: The **Manage keys** screen appears, with a list of available Traffic keys.

Figure 11-1 Manage Keys Screen – Converting ASN Key (Example)



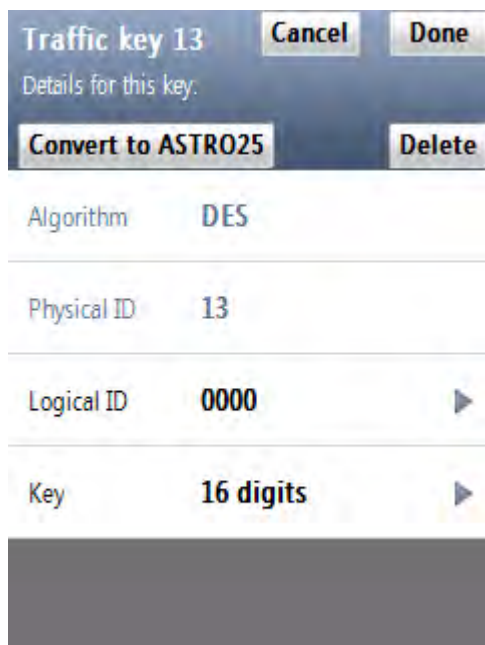
NOTE

To see the list of available Shadow keys, select the **Shadow** tab. You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 2 Select the desired key.

Step result: A screen with details for the selected key appears.

Figure 11-2 Converting to ASTRO 25 (Example)



- 3 Select **Convert to ASTRO25**.

Step result: If you have made changes to the key, you are prompted to confirm conversion. Otherwise, you are prompted to provide details for the ASTRO® 25 key.

- 4 From the list of available algorithms, select the algorithm for the key.

Step result: A screen with the decimal keypad appears, prompting you to enter the CKR ID for the key.

- 5 Enter the CKR ID using the decimal keypad.



NOTE

If you are converting a Traffic key, the valid CKR range is 1-4095. If you are converting a Shadow key, the valid CKR range is 61440-65535.

- 6 Tap **Convert >**.

Step result: A screen appears, informing that the conversion has completed successfully.

- 7 Tap **OK**.

- 8 Tap **Done**.

- 9 If you want to convert another key, perform [step 2](#) through [step 8](#) for this key. Otherwise, tap **Done** to return to the KVL main screen.
-

11.4 Converting a Key from ASTRO 25 to ASN

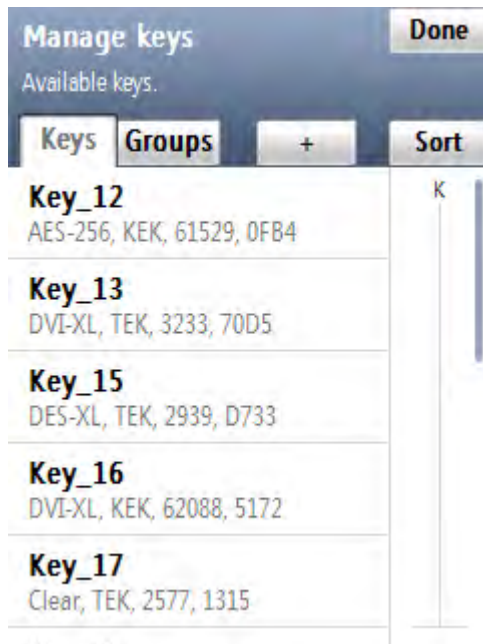
Prerequisites:

Only an Administrator can convert keys.

Procedure Steps

- 1 Select **Manage keys** on the KVL main screen.
Step result: A list of available keys appears.

Figure 11-3 Manage Keys Screen – Converting ASTRO 25 Key (Example)



NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

- 2 Select the desired key.

Step result: A screen with details for the selected key appears.

Figure 11-4 Converting to ASN (Example)



- 3 Select **Convert to ASN**.

Step result: If you have made changes to the key, you are prompted to confirm conversion. Otherwise, a screen with the decimal keypad appears, prompting you to enter the Physical ID for the key.

- 4 Enter the PID for the key using the decimal keypad.



NOTE

The valid PID range is 0–511.

- 5 Tap **Convert >**.

Step result: A screen appears, informing that the conversion has completed successfully.

- 6 Tap **OK**.

- 7 If you want to convert another key, perform [step 2](#) through [step 6](#) for this key. Otherwise, tap **Done** to return to the KVL main screen.

12 KVL 4000 – Troubleshooting

12.1 KVL Error Messages

Error messages displayed by the KVL can be divided into two types:

- **User Entry Errors** - Displayed in response to an illegal or disallowed action (such as entering an invalid value, entering a duplicate KID, and so on). See [12.1.1 KVL User Entry Errors, page 12-1](#).
- **Operational Errors** - Displayed during normal operation in response to a user-initiated action, such as attempting to load a key to a target device. See [12.1.2 KVL Operational Errors, page 12-2](#).

12.1.1 KVL User Entry Errors

This section lists all possible user entry errors along with their probable causes and remedies.

Table 12-1 KVL User Entry Errors

Error/Status Message	Probable Cause	Remedy
Algorithm mismatch	(Displayed for a single algorithm mismatch.) 1. During key loading, the KVL does not have the same algorithm as the target device. 2. During sharing, the KVLs do not have the same algorithm.	1. Use the KVL that has the same algorithm as the target device. 2. Purchase an appropriate algorithm and add it to the KVL or target device.
[X] algorithm mismatches.	(Displayed for more than one algorithm mismatch.) 1. During key loading, the KVL does not have the same algorithms as the target device. 2. During sharing, the KVLs do not have the same algorithms.	1. Use the KVL that has the same algorithms as the target device. 2. Purchase appropriate algorithms and add them to the KVL or target device.
Error Key could not be converted. Enter another CKR value.	Displayed when you have entered a duplicate CKR value while attempting to convert an ASN PID key to an ASTRO® 25 CKR Key.	Enter another CKR value.

Table 12-1 KVL User Entry Errors (cont'd.)

Error/Status Message	Probable Cause	Remedy
Error Key could not be converted. Enter another PID value.	Displayed when you have entered a duplicate PID value while attempting to convert an ASTRO® 25 CKR Key to an ASN PID key.	Enter another PID value.
Error The key entered is weak. Enter a strong key.	Displayed when you have entered key that has been determined to be cryptographically weak and unworthy for use in the system.	Try entering another key.
Oops Red key transfers are not allowed in FIPS Level 3 mode.	Displayed when an unencrypted (red) key transfer is initiated while in FIPS Level 3 mode, where only encrypted (black) key loading is allowed.	Use a target device that supports encrypted (black) key loading only, or change FIPS to Level 2.
Error Duplicate Key ID found.	A key with this KID already exists in the KVL database.	Enter another KID value.
Error Duplicate Name found.	The name you have entered for the key already exists.	Enter another name.
Error Duplicate CKR ID found.	A key with this CKR already exists in the KVL database.	Enter another CKR value.

12.1.2 KVL Operational Errors

This section lists all operational errors along with their probable causes and remedies.

For most of the operational errors, the cause is a faulty cable connection between the KVL and the target device. Ensure that the connection is good and try the operation again. If it still fails, contact Support (see [12.9 Contacting Motorola, page 12-14](#)).

Table 12-2 KVL Operational Errors

Error/Status Message	Probable Cause	Remedy
Out of memory	The KVL internal database is full and cannot store any more data.	Delete any items stored in the KVL to make room for new data. This includes items such as unused keys, logs, and Store & Forward jobs.
No updates for this radio.	No jobs have been received for the connected target device.	Connect to KMF to obtain jobs for the target device.

**NOTE**

The KMF operator may have to associate this target device with the KVL in use to have the KVL Store &

Table 12-2 KVL Operational Errors (cont'd.)


Error/Status Message	Probable Cause	Remedy
		Forward jobs for this target device.
Radio has already been updated.	The KVL has already delivered the jobs it had to this target device. No additional updates can be made.	Connect to the KMF before attempting another upload to this target device.
Error Serial connection could not be established. Retry?	The direct link or modem link between the KVL and the KMF could not be established. Serial cable may be detached.	Check the connection and select Yes, try connecting again .
Error USB connection could not be established. Retry?	A connection between the KVL and the USB modem could not be established. USB modem may be detached or Security Adapter external power adapter may not be attached.	Check the connection and select Yes, try connecting again .
		 NOTE External power adapter must be used for USB modems.
Error Load All could not be performed. {Out of memory}	The target device or KVL cannot hold any more keys.	Remove any keys or Store & Forward messages in the target device or KVL to make room for the keys that the KVL is trying to send.
Error Load All could not be performed. {Algorithm mismatch}	Displayed for a single algorithm mismatch during a share operation when the source KVL is trying to send a key to the destination KVL that has an algorithm that the destination KVL does not support.	Do not attempt to share keys with an algorithm that is not supported by the destination KVL.
Error Load All could not be performed. {[X] algorithm mismatches.}	Displayed for more than one algorithm mismatch during a share operation when the source KVL is trying to send a key to the destination KVL that has algorithms that the destination KVL does not support.	Do not attempt to share keys with algorithms that are not supported by the destination KVL.
Error Database has been corrupted.	The KVL has suffered an event that left its database corrupted and the resulting data cannot be trusted.	Perform a System Reset or exit the application.
Can't decrypt messages.	A Tactical OTAR member has not been provisioned correctly. Either the Tactical TEK, SEK or KEK is missing from the radio.	Add the member again to the Tactical OTAR group.
Error Security adapter not connected. Check connection.	The Security Adapter got disconnected.	Reattach the Security Adapter and select Retry connection .

Table 12-2 KVL Operational Errors (cont'd.)

Error/Status Message	Probable Cause	Remedy
Oops Could not update radio. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Oops Could not get the radio's MNP. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Oops Could not get the radio's keysets. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Oops Could not get the radio's KMF RSI. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Oops Could not get the radio's RSI. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Oops Could not change the radio's active keysets. Check connection.	The target device may be disconnected.	Check connection and retry the operation.
Check radio's algorithm (Displayed as a key subtitle)	An algorithm issue occurred.	Check the connection to the target device and make sure that the target device supports the algorithm of the key being loaded.
Not supported by radio (Displayed as a key subtitle)	An algorithm is not supported.	Check the connection to the target device and make sure that the target device supports the algorithm of the key being loaded.
The KVL 3000/3000 Plus is emitting continuous success tones when connected to the KVL 4000 for sharing.	The KVL 4000 is trying to determine if the KVL 3000/3000 Plus is connected or disconnected.	Turn off the sound for the KVL 3000/3000 Plus.

12.2 Performing a System Reset

Resetting causes the KVL to erase the UKEKs, all stored keys, key groups, log records, and passwords, and reset the configuration settings to the factory defaults. For KVLs equipped for triple mode operation (ASN, ASTRO® 25, and Radio Authentication), resetting erases UKEKs, ASN keys, ASTRO® 25 keys, all stored radio – key pairs, macros, key groups, log records, and passwords.

Procedure Steps

- 1 On the KVL main screen, select **Settings** → **System reset**. Alternatively, if user authentication is set on your KVL, press the Windows key on the PDA and hold it for 5 seconds to go to the System Reset screen.



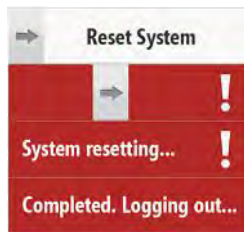
CAUTION

Use this option with caution as a system reset resets the KVL to its original state. All settings are reset and all data is deleted.

- 2 Drag the Reset System slider from left to right. Alternatively, highlight the slider and use the navigation key on the PDA to move it.

Step result: The system is being reset. When the action is completed, you are logged out of the KVL application and the Welcome screen appears.

Figure 12-1 KVL System Reset Slider – Subsequent States



12.3 Unlocking the Operator Account

Prerequisites:

Only an Administrator can unlock the Operator account.

Procedure Steps

- 1 Select **Settings** → **Security** → **Unlock operator account** → **Yes, unlock now**.

Step result: The Operator account is unlocked.


- 2 Tap **Done** on the consecutive screens to return to the KVL main screen.
-

12.4 Setting the PDA USB Mode

When and where to use:

Sometimes, the PDA may not automatically detect whether it should work in a Host mode (when connected to the Security Adapter), or in a Client mode (when connected to a PC). In such a case, use these steps to set the PDA USB mode manually.

Procedure Steps


- 1 On the Today screen, select .

- 2 Select **Settings** → **System** → **USBConfig**.

- 3 Perform one of the following actions:
 - If there are two options available (**USB Host** and **USB Client**), then select **USB Host** if you need to connect the PDA to the Security Adapter, or select **USB Client** if you need to connect the PDA to a PC.
 - If there are three options available (**USB Host**, **USB Client**, and **USB OTG**), then select **USB OTG** to allow the KVL to auto detect whether it is connected to the Security Adapter or a PC.

12.5 KVL 4000 Disaster Recovery

Table 12-3 KVL 4000 Disaster Recovery

Event	Remedy
Hardware failure	Replace the device and reenter all the lost data. Refer to this manual to configure your KVL with all the necessary parameters.
	<div style="text-align: center;">  SUGGESTION </div> <p>Keep non-sensitive data in a secure location so that you can restore it quickly when needed.</p>
KVL application failure	Reinstall the KVL application. See “Running the KVL Software Installation Wizard” in the <i>KVL 4000 FLASHPort Upgrade User Guide</i> .

12.6 Troubleshooting KVL Application and/or VPN Software Failure

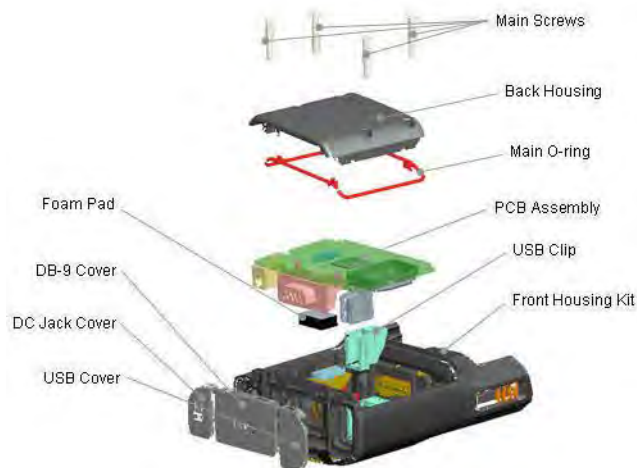
If you are experiencing problems with the KVL and/or NCP applications, follow “Running the KVL Software Installation Wizard” in the *KVL 4000 FLASHPort Upgrade User Guide* to reinstall the applications.

12.7 Disassembling the Security Adapter

When and where to use:

Use these steps to disassemble the Security Adapter.

Figure 12-2 Security Adapter – Exploded View



CAUTION

Make sure to exit the KVL application on the PDA before disconnecting the Security Adapter. Otherwise, you may lose any unsaved work or cause data corruption.

Procedure Steps

- 1 Remove the self-tapping screws and then remove the back housing.

Figure 12-3 Removing Back Housing



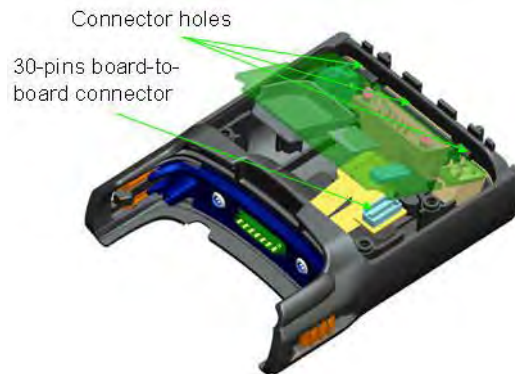
- 2 Remove the dust covers from the tongue features on the front housing.

Figure 12-4 Removing Dust Covers



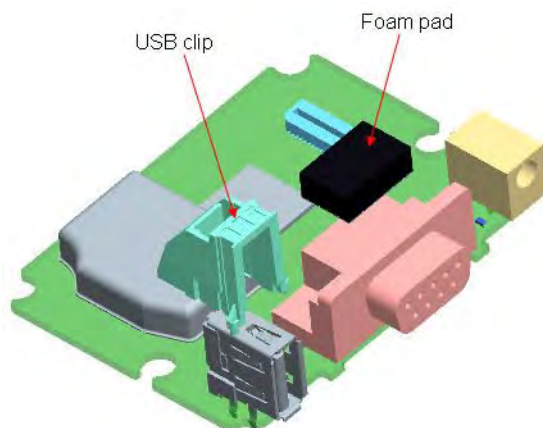
- 3 Remove the connectors from the front housing connector holes, disconnect the 30-pins board-to-board connector from the flex to the PCB, and remove the PCB assembly from the front housing.

Figure 12-5 Removing PCB Assembly



- 4 Remove the USB clip from the USB connector and the foam pad from the DB-9 connector on the PCB assembly.

Figure 12-6 Removing USB Clip and Foam Pad

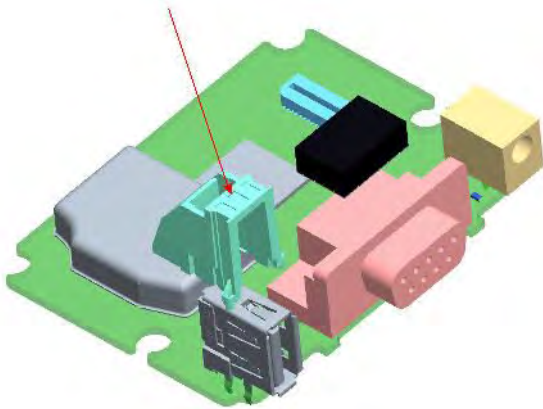


12.8 Assembling the Security Adapter

Procedure Steps

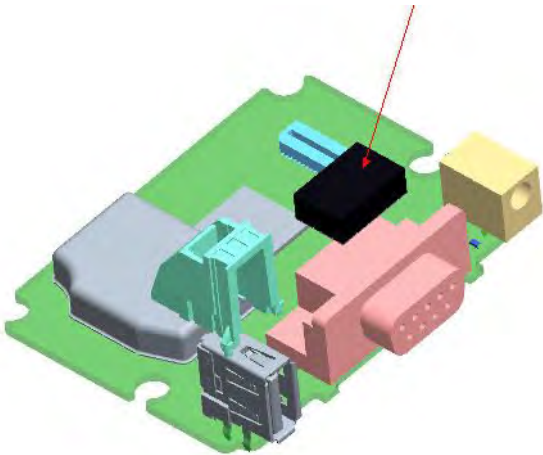
- 1 Attach the USB clip to the USB connector on the PCB.

Figure 12-7 Assembling USB Clip



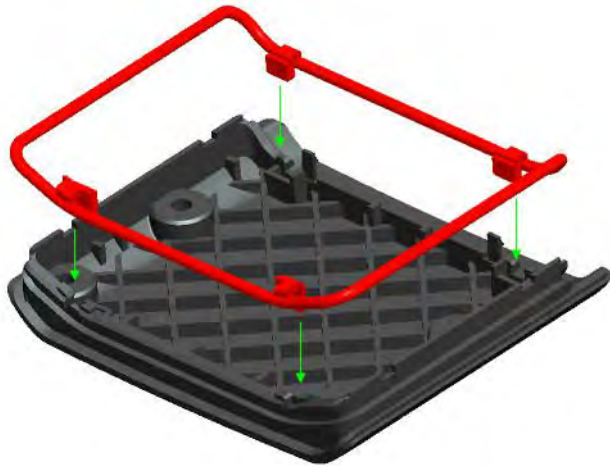
- 2 Attach the foam pad on top of the DB-9 connector. Ensure that the foam pad is aligned to the middle of the DB-9 face.

Figure 12-8 Assembling Foam Pad



- 3 Dress the O-ring to the O-ring groove at the back housing. Ensure that the O-ring tabs are slotted to the back housing features. Orient the O-ring so that its tabs' size matches the back housing features' size.

Figure 12-9 Assembling O-Ring



- 4 Connect the 30-pins board-to-board connector from the flex to the PCB.

Figure 12-10 Assembling Front Housing – PCB



- 5 Slot the connectors through the front housing connector holes.

Figure 12-11 Assembling Front Housing – Connectors



-
- 6 Place the PCB assembly to the front housing. Ensure the PCB sits properly on screw bosses.

Figure 12-12 Assembling Front Housing – PCB Placed



- 7 Slot in the dust cover retention holes through the tongue features on the front housing.

Figure 12-13 Assembling Dust Covers



- 8 Press down the back housing to the front housing vertically. Before closing the back housing, verify that the USB clip is assembled correctly.

Figure 12-14 Assembling Back Housing to Front Housing



- 9 Tighten the back housing with the self-tapping screws (tightening torque: 7 lbf.in).

Figure 12-15 Tightening Back Housing



-
- 10 Press the dust covers until they are flush with the front housing.

Figure 12-16 Pressing Dust Covers



Result:
The assembly is complete.

12.9 Contacting Motorola

This section contains information about calling Motorola for help.

12.9.1 Motorola System Support Center and Radio Support Center

After collecting the required information and writing a detailed problem report, contact one of the following support centers to help with the problem:

- Motorola System Support Center (SSC):
 - North America: 800-221-7144
 - International: 302-444-9800



NOTE

The Motorola System Support Center (SSC) provides technical support, return material authorization (RMA) numbers, and confirmations for troubleshooting results. Call the System Support Center for information about returning faulty equipment or ordering replacement parts.

- Motorola Radio Support Center:
 - Phone: 800-247-2346
 - Fax: 800-318-0281



NOTE

The Motorola Radio Support Center repairs mobile and portable radios, and related RF equipment.

12.9.2 North America Parts Organization

The North America Parts Organization is your source for manuals, replacement parts, and assemblies.

Table 12-4 North America Parts Organization Telephone Numbers

Purpose	Telephone Number
For ordering	<ul style="list-style-type: none"> • 800-422-4210 (US and Canada orders) • 302-444-9842 (International orders)
For Fax Orders	800-6226210 (US and Canada orders)
For help identifying an item or part number	800-422-4210; select choice 3 from the menu

Appendix A: KVL 4000 - Performance Specifications

Table A-1 Physical Characteristics

Item	Description
KVL (PDA + Security Adapter)	Height: 216 mm (8.5 in)
	Width: 84 mm (3.3 in)
	Depth: 39 mm (1.5 in)
	Weight: 473 g

Table A-2 Encryption

Supported Encryption Protocols	12 kbps Advanced SECURENET® 9.6 kbps Secure ASTRO® (VSELP Vocoder) 9.6 kbps Secure APCO Project 25 (IMBE Vocoder)
Encryption Keys	1,024 Total Traffic and Shadow Keys (ASN) Traffic Encryption Keys (TEK) and Key Encryption Keys (KEK) (ASTRO® 25)
Standards	FIPS 46-3 FIPS 140-2 FIPS 197

Table A-3 Supported Algorithms

Algorithm	ASN	ASTRO 25	KMF (ASTRO 25 Only)	Radio Authentication
DES	✓	✗	✗	✗
DES-XL	✗	✓	✓	✗
DES-OFB	✗	✓	✓	✗
DVI-XL	✓	✓	✓	✗
DVP-XL	✓	✓	✓	✗
AES-128	✗	✗	✗	✓
AES-256	✓	✓	✓	✗
ADP	✗	✓	✗	✗



NOTE

In the ASN mode, the KVL GUI does not distinguish between DES, DES-XL, and DES-OFB, but you can load keys for all DES types by selecting the DES option.



NOTE

ADP does not support the following features related to OTAR:

- Store & Forward
- KEK Key loading
- Tactical OTAR
- Remote Control Head Key loading

Table A-4 Electromagnetic Compatibility

EN 55022 Class A
EN 55024
FCC Part 15 Class A

Table A-5 Regulatory Compliance and Approvals

Safety	EN 60950-1
	UL 60950-1
	cUL 60950-1

Appendix B: KVL 4000 – Orderable Parts

Table B-1 KVL 4000 Model

Item	Count	Part Number
MC55 Kit (see Table B-2 MC55 Kit)	1	NNTN7864
Security Adapter Super Tanapa (see Table B-3 Security Adapter Super Tanapa)	1	NTN2564
KVL 4000 Documentation CD	1	CLN8627
KVL 4000 Quick Start Guide	1	6871015P34
DB9 Gender Changer	1	2871926H02
Packing Kit	1	HBN5096

Table B-2 MC55 Kit

Item	Count	Part Number
MC55 PDA	1	MC55A0-P30SWQQA79R
Power Supply	1	PWRS-14000-249S
Battery (2400 mAH)	1	BTRY-MC55EAB00
MC55 Quick Start Guide	1	72-127603-02
MC55 Regulatory Guide	1	72-108860-02

Table B-3 Security Adapter Super Tanapa

Item	Count	Part Number
Front Housing Assembly (see Table B-4 Front Housing Assembly – Orderable Parts)	1	01009328004
PCB Assembly Kit	1	NNTN7650
Back Housing	1	15009431001
Main O-ring	1	32009316001
Self tapping screw Dia. 3 x 18 mm	4	03009288001
USB Cover	1	32012053001
DB-9 Cover	1	32012052001
DC Jack Cover	1	32012051001
Foam Pad	1	75009419001
USB Clip	1	42009269001

Table B-4 Front Housing Assembly – Orderable Parts

Item	Count	Part Number
MX Dust Cover	1	32012050001

Table B-5 Interface Cables

Item	Part Number	Used with	Adaptor Required	
Key Load Cable	TKN8531	XTL 5000/2500	TRN7414 (W Control Head) HKN6182 (M/O Control Head)	
		XTS 5000/3000/2500	NTN8613	
		ASTRO Spectra	TRN7414	
		APX 7500/6500	HKN6182	
		APX 7000/6000/4000	NNTN7869	
		RNC, DIU, MGEG, MCC 7500 Console, KMF, PDEG, CDEM, KMF CryptR	n/a	
		CKN6886	XTS 4000	n/a
		TDN9390	XTS 5000/3000/2500	n/a
		WPLN6904	APX 7000/6000/4000	n/a
		TKN1039	CRYPTR micro	n/a
OTAR / Radio Authentication Cable	HKN6183	APX 7500/6500, XTL 5000/2500, ASTRO Spectra	n/a	
		NKN1027	XTS 4000	n/a
		RKN4106	XTS 5000/3000/2500	n/a
		WPLN6905	APX 7000/6000/4000	n/a
KVL To KVL Cable	TKN8209	KVL 3000/3000 Plus/4000	n/a	
USB Programming Cable	25-108022-02R	PDA to PC	n/a	
MINI-B to Type-A USB Cable	25-68596-01R	USB to Ethernet Adapter	n/a	
Other	CKN6324	Serial Modem	n/a	
	TKN8210	Service Monitor	n/a	

Table B-6 Optional Accessories

Item	Part Number
AC Line Cord US	50-16000-182R
AC Line Cord cEE7/16 Plug	50-16000-255R
AC Line Cord BS 1363 Plug	50-16000-670R
AC Line Cord GB 2099-1-1996 Plug	50-16000-664R
AC Line Cord AS3112 Plug	50-16000-666R
AC Line Cord Brazil	50-16000-726R

Table B-6 Optional Accessories (cont'd.)

Item	Part Number
MultiMobile™ USB Modem V.92/56K	DSMT9234MUCDCXR
CradlePoint Technology USB to Ethernet Adapter	PS6U1UPE
3600mAH Battery	BTRY-MC55EAB02

Appendix C: Radio Frequency Interference Requirements

C.1 Radio Frequency Interference Requirements – USA

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

C.2 Radio Frequency Interference Requirements – Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme la norme NMB-003 du Canada.

C.3 Radio Frequency Interference Requirements – European Union – EMC Directive 2004/108/EC

This is an EMC Class A product.

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce magnetic emissions to prevent interference to the reception of radio and television broadcast.

Appendix D: Acronyms

Table D-1 Acronyms

Item	Description
ADP	Advanced Digital Privacy
AES	Advanced Encryption Standard
AME	Assured Mobile Environment
ASN	Advanced SECURENET
CKR	Common Key Reference
CSK	Common Shadow Key
DES	Data Encryption Standard (Cipher)
DES-OFB	Data Encryption Standard-Output Feedback
DES-XL	Data Encryption Standard-Counter Addressing
DIU	Digital Interface Unit
DVI-XL	Digital Voice International-Range Extension
DVP	Digital Voice Protection
DVP-XL	Digital Voice Protection-Range Extension
FIPS	Federal Information Processing Standard
I/O	Input/Output
KID	Key ID
KEK	Key Encryption Key
KMF	Key Management Facility
KMM	Key Management Message
SEK	Signaling Encryption Key
KVL	Key Variable Loader
LED	Light Emitting Diode
LID	Logical ID
MDC	Motorola Data Communications
MGEG	Motorola Gold Elite Gateway
MNP	Message Number Period
OTAR	Over-the-Air Rekeying
PID	Physical ID
RNC	Radio Network Controller
RSI	Radio Set Identifier
TEK	Traffic Encryption Key
UKEK	Unique Key Encryption Key

Table D-1 Acronyms (cont'd.)

Item	Description
USK	Unique Shadow Key
VPN	Virtual Private Network
WACN	Wide Area Communications Network