tait
communications

Tait EnableProtect Key Fill Device
User’s Guide

MNE-00010-05· Issue 5 · April 2021

www.taitradio.com

Copyright and trademarks

Disclaimer

There are no warranties extended or granted by this document. Tait International Limited accepts no responsibility for damage arising from use of the information contained in the document or of the equipment and software it describes. It is the responsibility of the user to ensure that use of such information, equipment and software complies with the laws, rules and regulations of the applicable jurisdictions.

Enquiries and comments

If you have any enquiries regarding this document, or any comments, suggestions and notifications of errors, please contact your regional Tait office.

Updates of manual and equipment

In the interests of improving the performance, reliability or servicing of the equipment, Tait International Limited reserves the right to update the equipment or this document or both without prior notice.

Intellectual property rights

This product may be protected by one or more patents or designs of Tait International Limited together with their international equivalents, pending patent or design applications, and registered trade marks: NZ409837, NZ409838, NZ415277, NZ415278, NZ508806, NZ530819, NZ534475, NZ547713, NZ577009, NZ579051, NZ579364, NZ586889, NZ610563, NZ615954, NZ700387, NZ708662, NZ710766, NZ711325 , NZ726313, NZ733434, NZ593887, AU2015215962, AU339127, AU339391, AU2016259281, AU2016902579, AU2017204526, EU000915475-0001, EU000915475-0002, GB1518031.8, GB1710543.8, GB2532863, US14/834609 Div. no 1, US15/346518 Div.no 2, US15/350332, US15/387026 Div., US29/614639, US62/713910, US62/729478, US62/730107, US62/767041, US62/781642, US62/778238, US9794940 Div. no 1, US20150085799, US20160044572, US20160057051, US20170142646, US20170055267 Div. no 2, US20180006844, US640974, US640977, US698339, US702666, US7758996, US8902804, US9107231, US9504034, US9559967.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Environmental responsibilities

Tait International Limited is an environmentally responsible company which supports waste minimization, material recovery and restrictions in the use of hazardous materials.

The European Union's Waste Electrical and Electronic Equipment (WEEE) Directive requires that this product be disposed of separately from the general waste stream when its service life is over. For more information about how to dispose of your unwanted Tait product, visit the Tait WEEE website at www.taitradio.com/weee. Please be environmentally responsible and dispose through the original supplier, or contact Tait International Limited.

Tait International Limited also complies with the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Directive in the European Union.

In China, we comply with the Measures for Administration of the Pollution Control of Electronic Information Products. We will comply with environmental requirements in other markets as they are introduced.

Contents

1 About this guide

This user’s guide provides information on encryption, and how to use the Tait EnableProtect Key Fill Device (KFD) to load keys into target devices. The features described in this guide apply to KFDs with application version 4.2 (see “Obtaining the application version number” on page 78).

The pictures, sample data and other information in this guide are based on a typical customer setup. This may differ for your unit depending on the extent of Android® personalization and requirements for your organization.

Safety warnings used in this guide

Please follow exactly any instruction that appears in the text as an ‘alert’. An alert provides necessary safety information as well as instruction in the proper use of the product. This user’s guide uses the following types of alert:

⚠ **This alert is used to warn about the risk of data loss or corruption (for example, a risk of lost, invalid or compromised encryption keys).**

ⓘ This alert is used to highlight significant information that may be required to ensure procedures are performed correctly, or draw your attention to ways of doing things that can improve your efficiency or effectiveness.

Related documentation

The following documentation is also available for your Tait radio, which you can access from the Tait Technical Support website (http://support.taitradio.com):

Title	Contains
TM9100 User's Guide (MMA-00007-xx) TM9400 User's Guide (MMB-00003-xx)	Information on using encryption with Tait P25 mobile radios.
TP9100 User's Guide (MPA-00001-xx) TP9400 User's Guide (MPD-00003-xx)	Information on using encryption with Tait P25 portable radios.
TB9100/P25 CG/P25 TAG Installation and Operation Manual (MBA-00002-xx)	Information on using encryption with Tait P25 console gateways and trunked analog gateways.
Tait EnableProtect Key Management Facility Key Management Manual (MBA-00048-xx)	Information on using the KFD with the Tait EnableProtect Key Management Facility.

2 Getting started

This section contains an overview of encryption, and describes the basic operation of the Tait EnableProtect Key Fill Device (KFD).

This section covers:

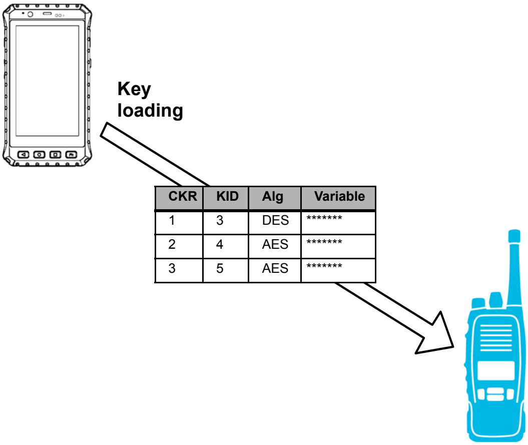
- About encryption
- Configuring encryption on the target device
- About KFD feature licenses
- Basic operation

About encryption

Encryption enables secure voice and data communications across a radio system, so third parties cannot listen in. Encryption requires the use of encryption keys which must be loaded into all radios that will communicate on the system.

The Tait EnableProtect Key Fill Device (KFD) can be used for this task. First you enter the encryption keys required, and then you connect the KFD to each target device in turn, loading one or more keys.

If your system has gateways (such as P25 Console Gateways), they must also be supplied with encryption keys, as they are an encryption and decryption point.



CKR	KID	Alg	Variable
1	3	DES	*******
2	4	AES	*******
3	5	AES	*******

Entering keys using the KFD

The KFD supports two types of encryption key, traffic encryption keys (TEKs), and key encryption keys (KEKs).

TEKs are used for the encryption of user voice and data messages on the system. KEKs are used by the radio and key management facility (KMF) to encrypt and protect keys during over-the-air (OTAR) transactions.

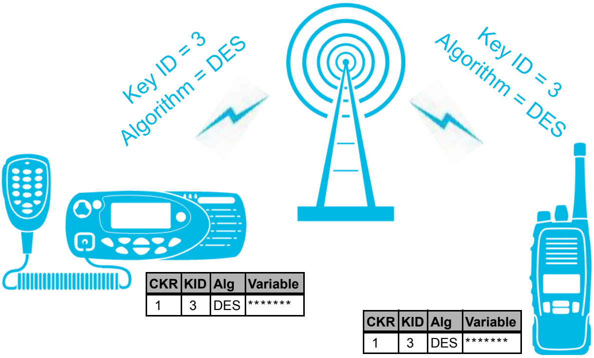
When you enter a key into the KFD, you must specify a Common Key Reference (CKR). This is the reference number for a set of secure key data.

The key data consists of the following information:

- Key ID, used to identify the key over the air to the device decrypting the call.
- Algorithm ID, which specifies which encryption algorithm is to be used (DES or AES).
- Key variable, a multi-digit number that the crypto-module uses when encrypting and decrypting. Once the key variable is created, it can never be viewed again. The KFD subsequently shows the key variable as a series of asterisks.

Making an encrypted call

When a radio makes an encrypted call, it includes in the call the Key ID and the Algorithm ID that it used. If the receiving radio has the same key, it can decrypt the call. The algorithm ID tells it the encryption algorithm to use, and this, along with the key ID, tells it what key to use.



CKR	KID	Alg	Variable
1	3	DES	*******

CKR	KID	Alg	Variable
1	3	DES	*******

Keysets and key changeover

Tait mobiles, portables and gateways have two traffic encryption key (TEK) keysets. At any one time, one keyset is the active keyset, and the other is the inactive keyset. The active and inactive keysets can be swapped using a menu option on the radio, using a KFD (see “Swapping keysets” on page 46), or a Tait EnableProtect Key Management Facility (KMF).

Tait mobiles, portables and gateways use the active keyset to encrypt and decrypt calls. The inactive keyset is never used to encrypt calls. However, if a radio receives a call and the Key ID is in the inactive keyset, the call will be decrypted[1].

The inactive keyset can be used to manage encryption key changeover, as shown in the following example:

1. Near the changeover time, one or more new keys are loaded into the inactive keyset (for each radio as convenient).
2. At changeover time, the inactive keyset is swapped with the active keyset (all radios).
3. Once a fleet of radios has been successfully updated and communications have been confirmed on the new keys, then the old (now inactive) keys can be zeroized or overwritten ready for the next changeover.

At key changeover time, the dispatcher must be able to hear calls encrypted with new keys, and old keys, to support radios that have not yet changed over to the new keys.

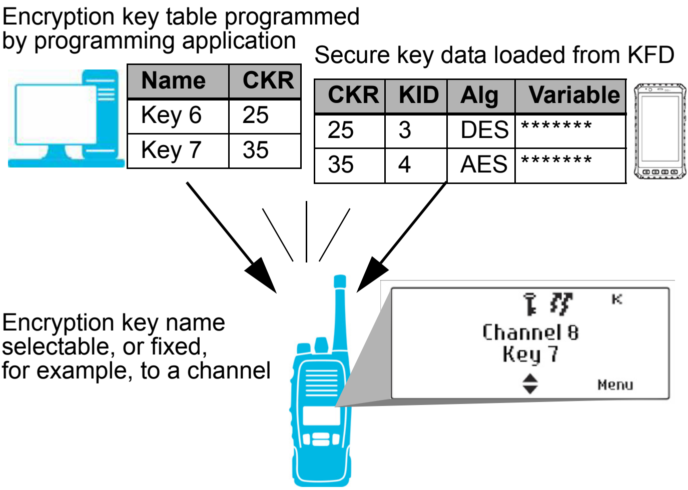
[1] Only if proper key detect is not used. Proper key detect means a call is only decrypted if the received encryption key matches the currently selected transmit encryption key.

Configuring encryption on the target device

In addition to loading secure key data into target devices from the KFD, you need to configure the way each device uses these keys. This is done using the programming software for the device (such as the TM9100, TP9100, TM9400 and TP9400 Programming Application or TB9100 Customer Service Software).

You must program the following for each device:

- the software license for DES (base) encryption, and if necessary, AES encryption.
- a key table that maps each CKR number to a name. The name is how the secure key data is referenced in the software, and on the radio.
- P25 console gateways and trunked analog gateways: encryption enabled per calling profile.
- mobile and portable radios: encryption enabled per channel profile.


Encryption key table programmed by programming application
Secure key data loaded from KFD
Encryption key name selectable, or fixed, for example, to a channel
K
Channel 8
Key 7
Menu

Name	CKR
Key 6	25
Key 7	35

CKR	KID	Alg	Variable
25	3	DES	*******
35	4	AES	*******

About KFD feature licenses

The KFD utilizes feature licenses to unlock specific features within the Key Fill Device application. KFDs can be licensed with **Standard Key Fill**, **Fast Key Fill**, or both. Licenses will be displayed on the Key Fill Device password screen upon starting the application. The following table shows the available actions for different feature license combinations.

	Feature Licenses		
Features	Standard Key Fill	Fast Key Fill	Standard Key Fill & Fast Key Fill
Create Keys	✔	✖	✔
Edit Keys	✔	✖	✔
Import Keystores	✔	✖	✔
Export Keystores	✔	✖	✔
Modify Keys on Target Devices	✔	✖	✔
Create Scripts	✖	✖	✔
Edit Scripts	✖	✖	✔
Export Scripts	✖	✖	✔
Import Scripts	✖	✔	✔
Run Scripts on Target Devices	✖	✔	✔

Use Standard Key Fill to create and maintain your encryption keys at a central location, where the KFD can be kept under lock and key for security purposes. Standard Key Fill is also used to manually manage provisioning keys as part of a KMF solution.

Use Fast Key Fill on KFDs in the field, where encryption keys can be downloaded and rapidly deployed on radios and other devices.

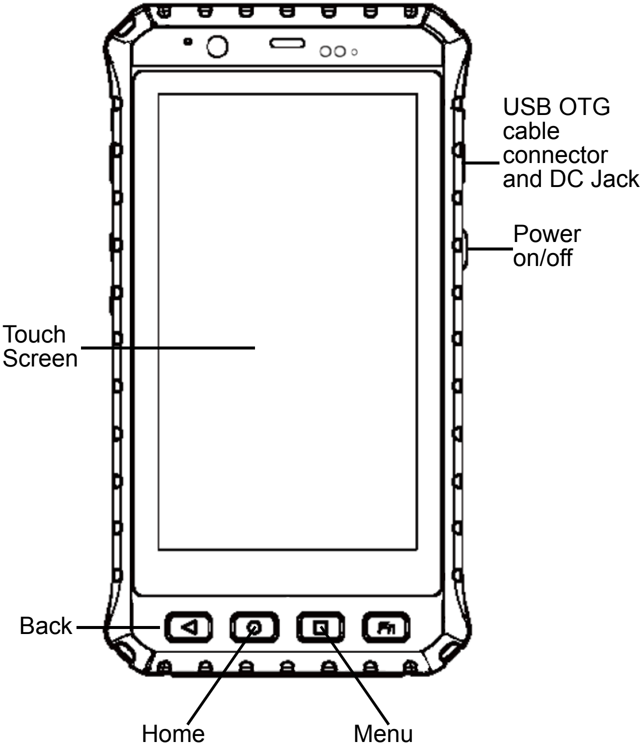
Fast Key Fill deployment requires an executable script created and exported by a KFD with both Standard Key Fill and Fast Key Fill feature licenses.

Basic operation

Before initial use, ensure the KFD is fully charged. For information on this and for more detailed information on how to operate the unit, refer to the complete user guide at: https://bit.ly/2UH5lRi

Operating the handheld unit

The main KFD controls are described below.



Control	Name	Function in KFD software modules
○	Home	Exits the Key Fill Device application and returns to the Home screen.
□	Menu	Functions as an alternative to tapping ⋮
◁	Back	Returns to the previous screen. If the on screen keyboard is open, the keyboard closes.
⏻	Power	To power the device on, press the **Power** button until the screen activates. To power the device off, press and hold the **Power** button until the menu appears, then tap **Power Off**. To turn off the screen without powering off the device, short-press the **Power** button once.

The Tait EnableProtect Key Fill Device (KFD) is built from an application installed on the E500 handheld unit running Android™ 4.1.

A screen lock password or PIN can be set for the KFD. Press □ > System settings > Security > Screen lock, then select and enter either password or PIN.

For security purposes, the Wi-Fi and Bluetooth capabilities of this device should remain switched off at all times.

About the KFD user interface

The Tait EnableProtect Key Fill Device (KFD) application makes full use of the standard user interface features of the Android platform, such as action bars, the navigation drawer and the on-screen keyboard. This section describes the KFD-specific features.

The **top action bar** indicates what is shown on the screen.

When ≡ is shown to the left of the KFD icon 🔑, the **navigation drawer** is available to switch between the main options of the KFD. Swipe from the left edge to open the navigation drawer.

When in a sub-screen (e.g. when adding a new key), the icon to the left of the KFD icon will change to ‹ allowing you to go to the previous screen without applying the changes. You can also press the ◁ button of the KFD. **All changes made to the screen will be lost**.

Tap ✓ Apply in the top right corner to complete editing a screen and save the changes.

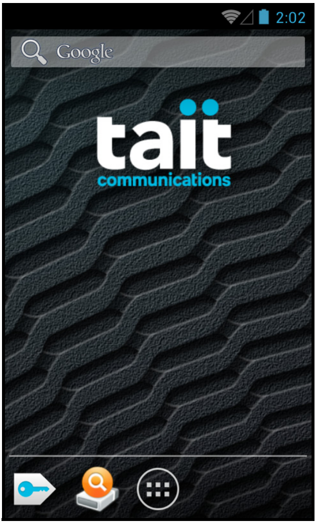
The **bottom action bar** offers actions valid for your screen and selection, such as adding, deleting or editing an item.

Tap ⋮ to display further options valid for your screen and selection. You can also press the ▣ button of the KFD.

Starting the KFD software

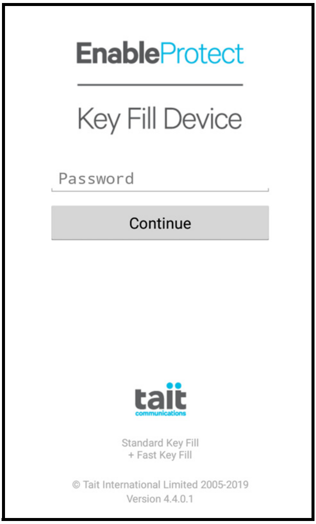
1. Press the **Power** key.
2. Tap the **Key Fill Device** icon.
3. Enter your password.

- ■ If this is the first time you have started the KFD software, follow the prompts to enter and confirm a new password, and tap **Set password**.



- ■ If you have used the software before, enter the existing password and tap **Continue**.

  See “About passwords” on page 22 for more information.


EnableProtect

Key Fill Device

Standard Key Fill
+ Fast Key Fill

© Tait International Limited 2005-2019
Version 4.4.0.1

About passwords

Stored encryption keys are protected by a user-defined password. The correct password must be entered in the following situations:

- When starting the KFD application.
- When resuming operation after the unit is turned off (manually, or due to inactivity).

To change the password:

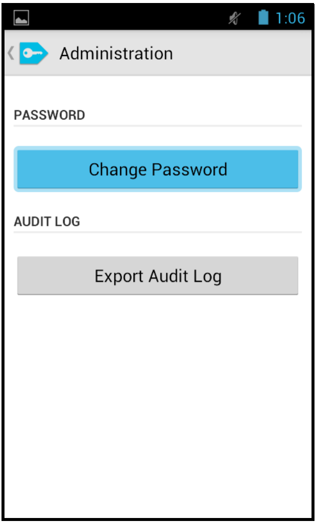
1 Tap ⋮ > **Administration** > **Change Password**.

2 Enter your current password.

3 Enter and confirm a new password.

(See Password tips below).

4 Tap **Set password**.



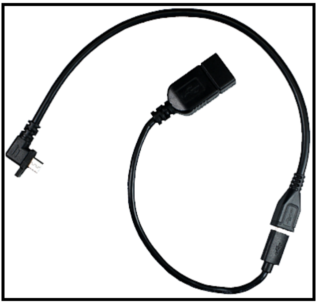
Password tips

A good password includes long alpha-numeric strings with special characters. Use the **Password strength** indicator as a guide. Avoid known words and their reverses, and dates. Avoid reusing passwords from other areas in an organization.

Share the password only with others who must have access to the KFD, and change passwords frequently. If you must store the password, make sure it is stored in an encrypted format, with controlled access.

Connecting the KFD to a target device

1 Connect the KFD to the non-IS target device using a USB OTG cable connector, which is included, and also available as a spare part (219-03803-00), and a standard Tait USB programming cable
(TPK-SV-009).



USB OTG cable connector (included in the box)

Tait USB Programming Cable

These are to be used in conjunction with the following adapters. **Included unless otherwise stated**:

- TM9100 and TM9400 mobile radios:
  TPA-SV-006 programming cable with
  TMAA20-04 adapter (RJ12 to RJ45).
- TP9100 portable radios:
  TPA-SV-006 programming cable and
  TPA-SV-007 adapter (RJ12 to RJ45).
- TP9400 non-IS portable radios:
  TPA-SV-006 programming cable and
  T03-00118-0101 adapter (RJ12 to RJ45).
- Tait gateways: The 219-03805-00 cable with a USB OTG connection to the Winmate E500, and a female DB-9 enabling connection to the TAG. **Not included.**

The target device resets and is out of service for the duration of keyloading mode. Before connecting a device, make sure you have taken the necessary actions to prepare for this (for example, if connecting a P25 console gateway, make sure there are no currently active calls on the channel).

2 Turn the target device on (if not already on).

3 Tap ≡ and then **Device**. Also, check that the target device resets and indicates keyloading mode.

Connection to a target device can also be checked by selecting a key in the Keystore screen. If a connection is present the ⇥ icon will be displayed on the bottom action bar.

To connect your KFD to a computer, use the supplied standard USB OTG cable connector.

Disconnecting a device

When you are finished, exit the application by pressing the **Home** button or disconnecting the cable. This causes the target device to automatically reset and exit keyloading mode.

Ending a session

1. Return to the Home screen if not there already.
2. Hold the **Power** key and tap **Power Off** to turn the unit off. Alternatively, short-press the Power key to turn off the screen.

3 Standard Key Fill

This section describes how to use Standard Key Fill to load keys onto target devices.

This section covers:

- About Standard Key Fill
- Managing keys in the KFD keystore
- Modifying keys on target devices

About Standard Key Fill

Standard Key Fill provides the holding database of imported, manually entered, or randomly generated encryption keys for loading into target devices. Standard Key Fill can also be used in conjunction with Fast Key Fill to create executable scripts for use on other KFDs loaded with Fast Key Fill (see “Creating scripts” on page 51), and to manage provisioning keys for KMF operation (see “Importing KMF keys into Standard Key Fill” on page 72).

You can use Standard Key Fill to do the following tasks:

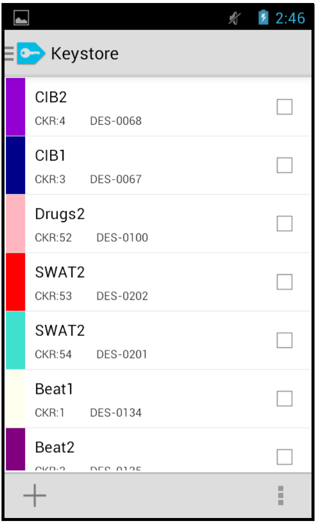
- Maintain a keystore of all necessary encryption keys (old, current and future keys as required), identified by user-defined label and color.
- Add new keys to the keystore using the following methods:
    - import keys created from another KFD, and merge or replace with existing keys.
    - enter the key information manually, using either a randomly-generated or manually-entered key variable.
- View the keys loaded on a radio or other device, and display a label from the keystore if the key ID and algorithm match.

ⓘ This task can only display information about loaded keys, not the key variables themselves.

- Create scripts that can be used by KFDs running Fast Key Fill.

ⓘ Scripts can only be created if the KFD has both Standard Key Fill and Fast Key Fill feature licenses.

- Import keys from a KMF instructions file.
- Change KMF-related parameters on the connected device.
- Load, reload, or update one or more keys on a radio or other device.
- Zeroize one or more keys on a radio or other device.
- Work with keys directly in either the active or inactive keyset, and swap keysets.



2:46

Keystore

CIB2 □
CKR:4 DES-0068

CIB1 □
CKR:3 DES-0067

Drugs2 □
CKR:52 DES-0100

SWAT2 □
CKR:53 DES-0202

SWAT2 □
CKR:54 DES-0201

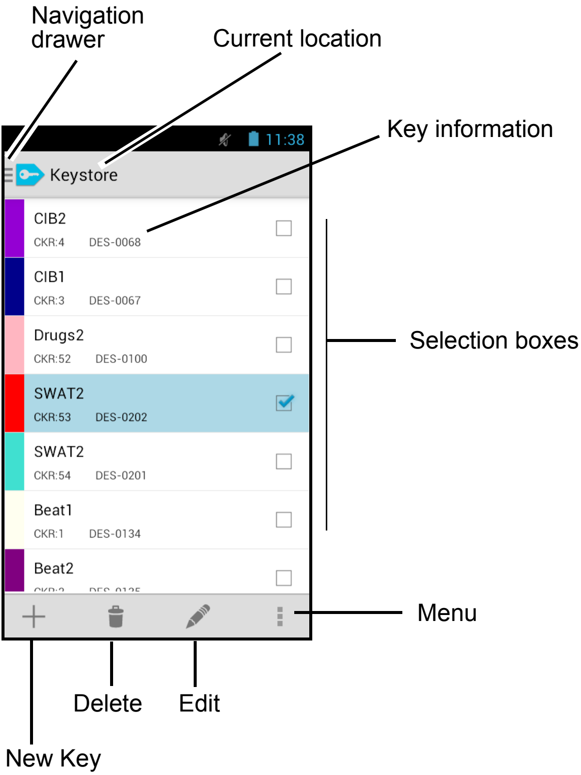
Beat1 □
CKR:1 DES-0134

Beat2 □
CKR:2 DES-0135

Standard Key Fill overview

The KFD defaults to the Drawer. Tap **Keystore** to enter the Standard Key Fill screen.

Below is an overview of the Standard Key Fill screen:



11:38

Keystore

CIB2 ☐
CKR:4 DES-0068

CIB1 ☐
CKR:3 DES-0067

Drugs2 ☐
CKR:52 DES-0100

SWAT2 ☑
CKR:53 DES-0202

SWAT2 ☐
CKR:54 DES-0201

Beat1 ☐
CKR:1 DES-0134

Beat2 ☐
CKR:2 DES-0135

Changing preferences

From the main screen, Tap ⋮ > **Settings** to access a sub-menu with the following options:

- **Key Creation**: when creating a new encryption key, the software populates the **Key ID** field with the next available ID within this range. The range can be from 1 to FFFF. Make sure that the generated next available key ID is within this range and do not attempt to create key IDs outside of your allocated key ID range.
  Different KFDs may be allocated different key ID ranges. This can help avoid conflicts if multiple users and KFDs are creating keys.

- **Default Algorithm**: changes the algorithm (AES or DES) that appears by default each time you create a new key.

- **Keysets**: sets IDs for the two TEK (traffic encryption key) keysets, and the KEK (key encryption key) keyset. Do not change these from the defaults.

If these settings are altered, the KFD will not work with Tait radios, or any other equipment which uses only keyset 1 and 2 for TEK and 255 for KEK.

- **Key Fill Device**: changes the RSI (radio set identifier) assigned to the KFD unit. You can enter the RSI in either decimal or hexadecimal format. The RSI is used during OTAR transactions.

- **KMF Import**: See “Initializing the KFD” on page 70 for an explanation of this option.

Viewing the audit log

The KFD logs significant user activities within the software, including target device transactions. The audit log file includes a time stamp and summary of each activity.

Target devices are identified in the audit log by radio set identifier (RSI). If you are using the audit log to trace, for example, which Tait mobiles and portables have been re-keyed, you must program a unique RSI for each radio using the radio's programming application.

To view the audit log:

1. Tap ⋮ > **Administration** > **Export Audit Log**.
2. Tap the **Name** field and select the audit log you wish to export.
3. Select the location you wish to export the audit log to.
4. Tap **Export Audit Log**.
5. Connect the KFD to a computer.
6. Using Windows Explorer, navigate to **Portable Devices** > **E500** > **Internal Storage**.
7. Open your exported *.log file to view.

Managing keys in the KFD keystore

⚠ Make sure that you follow your organization’s security policy when handling keys. If encryption information falls into unauthorized hands, the security of voice communications could be compromised.

Before encryption keys are entered, your organization should have developed a policy and procedures for encryption key management. This will answer questions such as “How many keys will be needed?”, “How will re-keying occur?”, “How and when will users change from one key to another?” and “What actions do we need to take when a radio containing encryption keys is lost?”

Before you can update the encryption keys on a radio or other device, you must define the keys in the **Keystore**. There are three methods for this task:

- By importing a keystore file, with the option to either merge with existing keys in the keystore, or replace the existing keys.
- By importing a keystore from an exported KMF instructions file. Imported KMF keystores will always replace your current keystore.
- Create new keys manually. Key variables may be randomly generated, or manually entered.

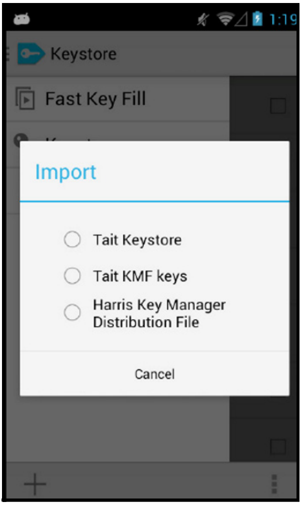
Importing a keystore

You may be able to import keys from a keystore provided, for example, by central headquarters or by another agency.

1 Copy the keystore file to the **Internal Storage** folder on the KFD.

2 Tap ⋮ > **Import** and select the relevant keystore type on the pop-up menu.

3 Select the location of the keystore and tap on the filename below.

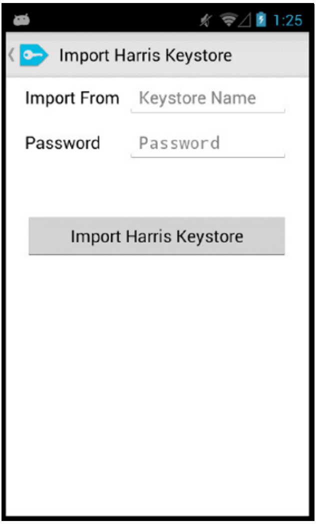


4 Select **Replace**, or **Merge**, from the drop-down menu.

- **Replace**: deletes all keys currently in the keystore (even if those keys have different key IDs), and copies across all keys from the keystore file.

- **Merge**: attempts to add the imported keys to the keystore.

5 Enter the password for the file. This is the password that was defined at the time of export, by the person who exported the keystore.



Import Harris Keystore

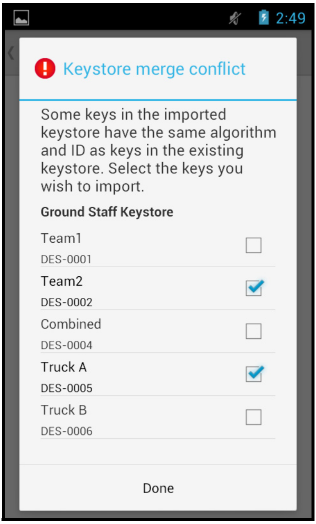
Import From Keystore Name

Password Password

Importing a Harris Key Manager Distribution File will always attempt to **Merge** the imported keys with the current keystore.

6 If a conflict is found (for example, you select Merge and a key ID and algorithm already exists in the keystore), a conflict screen appears.

Select one or more check boxes if you wish to import the new keys, and tap **Done**.



Keystore merge conflict

Some keys in the imported keystore have the same algorithm and ID as keys in the existing keystore. Select the keys you wish to import.

Ground Staff Keystore

Team1 ☐
DES-0001

Team2 ☑
DES-0002

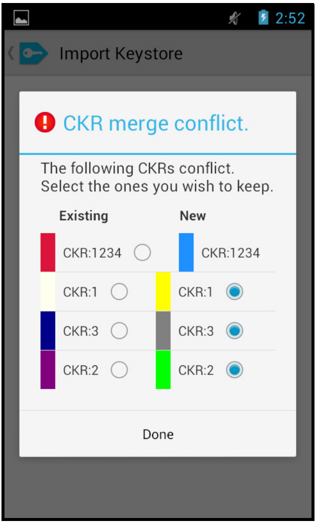
Combined ☐
DES-0004

Truck A ☑
DES-0005

Truck B ☐
DES-0006

7 If a CKR merge conflict is found, another conflict screen will appear.

Select one or more check boxes if you wish to keep the existing CKRs, and tap **Done**.



CKR merge conflict.

The following CKRs conflict.
Select the ones you wish to keep.

Existing		New	
🟥 CKR:1234	○	🟦 CKR:1234	
⬜ CKR:1	○	🟨 CKR:1	●
🟦 CKR:3	○	▨ CKR:3	●
🟪 CKR:2	○	🟩 CKR:2	●

Done

It is common practice to retain old keys (at least the keys immediately prior to changeover) in the keystore. If you are getting this message, you may need to request that new keys are generated with different Key IDs. This can be automated using the **Key Creation** preference (see “Changing preferences” on page 30).

Setting up CKRs

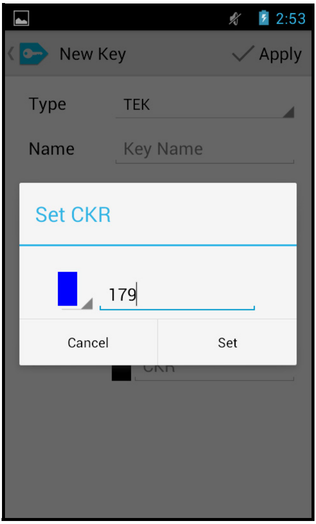
To create new keys, you must have one or more CKR (common key reference) numbers defined that match those used on the radios and other devices using the system.

⚠ **The KFD allows you to load keys to a target device using any CKR. However, you will not be able to use those keys until the CKR has been added to that target device. For more information, see "Configuring encryption on the target device" on page 15.**

1 Tap + to enter the **New Key** sub-screen.

2 Tap on the **CKR** field.

3 Select a color.



New Key

Type TEK

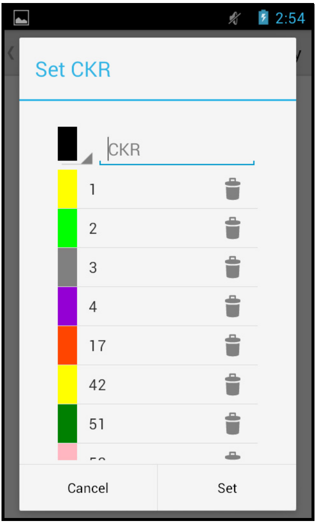
Name Key Name

Set CKR

179

4 Enter a CKR using the numeric keypad provided, and tap **Set**.

- A traffic encryption key (TEK) typically uses a CKR in the range of 1 to 4095.
- A key encryption key (KEK) typically uses a CKR in the range of 61440 to 65535.



You can assign a color to a CKR for quick reference. Tap the black rectangle next to the CKR field to open the color menu, then scroll up/down and tap the desired color to assign it.

5 Repeat steps 2 to 4 to create as many CKRs as required.

- To assign a key with an existing CKR, tap on the CKR you want to assign and tap **Set**.

Creating a new key

You can quickly update a key by editing an existing key. However, this method is not recommended as you lose secure key information for the existing key. Instead, keep the existing key and create a new key with the same CKR.

When creating a new key, there are two ways of creating the key variable:

- Let the KFD generate a random key variable, or
- enter the key variable manually.

1 From the **Keystore** screen, tap + **.**

2 **Type**: Select which type of key you wish to create, TEK or KEK.

3 Tap the **Key Name** field and enter a name.

4 Set the **Algorithm** to DES or AES.

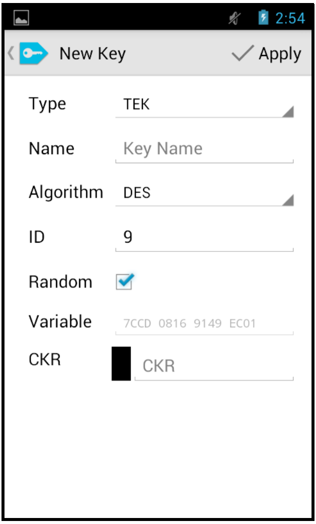
Tip: You can set the default algorithm using ⋮ > **Settings** > **Default Algorithm**.

5 Change the **Key ID** to a value inside your key ID range set in ⋮ > **Settings**.

6 Select **Random** if you wish to generate the key variable using a cryptographically-strong number generator.

- **Variable**: If Random is unchecked, a key variable must be entered manually. This variable is subject to the chosen encryption algorithm as follows.

  DES: enter an 8-octet number (an octet is two hexadecimal numbers). Each octet must have odd parity (an odd number of 1s in the binary number).



Type TEK

Name Key Name

Algorithm DES

ID 9

Random ☑

Variable 7CCD 0816 9149 EC01

CKR CKR

  AES: enter up to 32 octets with no parity restrictions.

7 Tap the **CKR** field, select a common key reference (CKR), and tap **Set**.

8 Tap ✓ Apply .

Editing keys

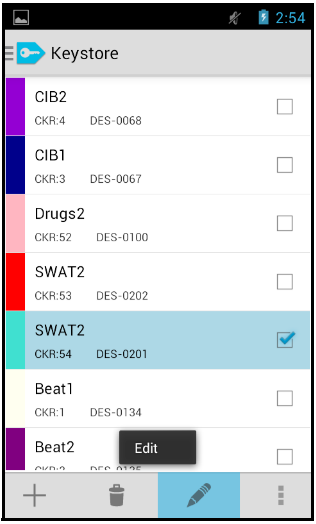
To edit a key:

1 Tap to select the key you wish to edit.

2 Tap ✎ to enter the **Edit Key** sub-screen.

3 Tap ✓ Apply to save any changes.

Do not edit the key variable. Instead, delete and create a new key.



CIB2	CKR:4	DES-0068	☐
CIB1	CKR:3	DES-0067	☐
Drugs2	CKR:52	DES-0100	☐
SWAT2	CKR:53	DES-0202	☐
SWAT2	CKR:54	DES-0201	☑
Beat1	CKR:1	DES-0134	☐
Beat2			☐

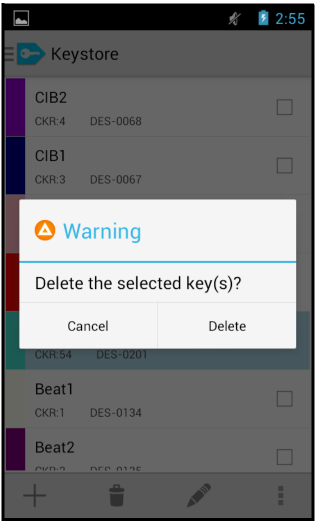
Deleting keys

You may want to delete old keys from the keystore:

- before exporting keys, so they are not deployed to other KFDs, or;
- after a period of time, once they are no longer used by any radios on the system.

To delete keys from the keystore:

1. Navigate to the Keystore screen.
2. Select the check box next to each key you want to delete.
3. Tap 🗑.
4. Tap **Delete** in the pop-up window to confirm your action.



Warning

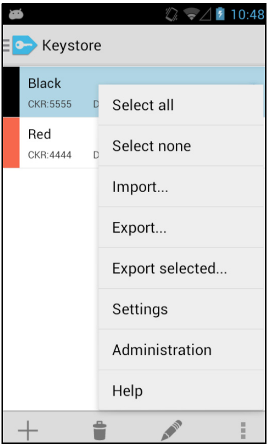
Delete the selected key(s)?

Exporting keys

All keys in the **Keystore** tab can be exported to a file (in an encrypted form with a password). This can be used to back up the keystore, or can be provided to another KFD that can import that data

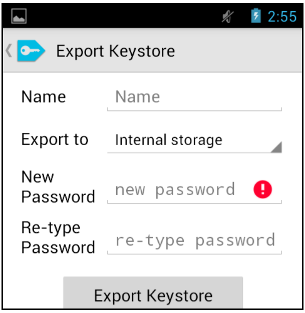
There are **two** menu options when exporting keys:

- **Export:** Exports the entire keystore.
- **Export Selected:** Only exports keys with a check mark beside them (option disabled if no keys selected).



1. From the **Keystore** screen, select the keys to be exported, or to export all, begin at step two.
2. Tap ⋮ > **Export**.
3. Type a name for the file and select the export location from the drop down menu.
4. Create a password and then re-type the password to confirm.

   See “Password tips” on page 22.



5. Tap **Export Keystore**

Files saved to the device’s internal storage can be located in the **Internal Storage** folder once the device is connected to a PC.

Modifying keys on target devices

You can modify keys on target devices in the following ways:

- Load keys
- Swap keysets
- Zeroize keys

Before you start each task, make sure you have connected a device such as a radio. See “Connecting the KFD to a target device” on page 23. Repeat each task as needed for all devices on the system.

Loading keys

1 Connect the KFD to a radio or other device.

2 From the **Keystore** screen, select the keys that you want to load to the target device.

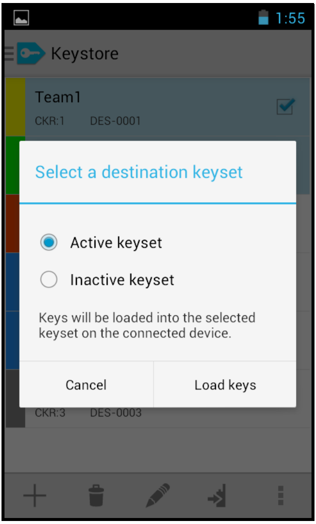
3 Tap ⇥ and select whether you wish to load the keys into the active or inactive keyset.

4 Tap **Load keys**.

If successful, a message appears:

Load into … keyset completed successfully.

5 Tap **OK**.



Select a destination keyset

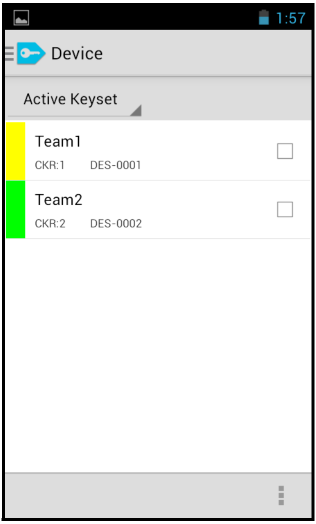
● Active keyset

○ Inactive keyset

Keys will be loaded into the selected keyset on the connected device.

6 Tap ☰ > **Device**.

7 Select **Active Keyset** or **Inactive Keyset** from the drop-down menu and check that the keys appear on the target device.



🟨 Team1 CKR:1 DES-0001 □

🟩 Team2 CKR:2 DES-0002 □

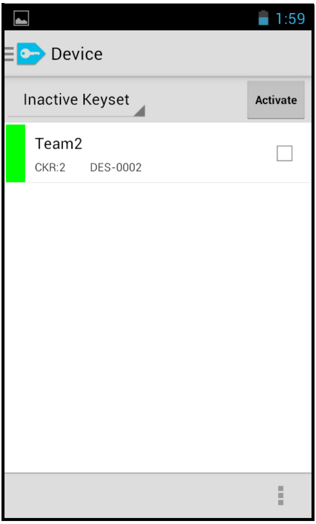
Swapping keysets

Swapping keysets may be required during a changeover to new encryption keys. For more information, see “Keysets and key changeover” on page 13.

Tip: View the keyset IDs from either the **Active Keyset** or **Inactive Keyset** to check the current keyset used. This can be checked before and after the following steps to confirm that the keysets have been successfully swapped.

1 Connect the KFD to a radio or other device.

2 From the **Device** screen select **Inactive Keyset** from the drop-down menu. Make sure the new keys have been loaded into the inactive keyset. See “Loading keys” on page 44 for information on loading keys to the inactive keyset.



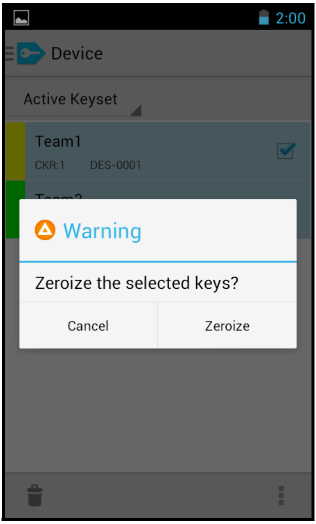
Team2 □
CKR:2 DES-0002

3 Tap **Activate**.

Zeroizing keys

Zeroizing a key overwrites the key material with zeroes, meaning the key can no longer be used to decrypt or encrypt communications. Keys are typically zeroized if they are no longer required (for example, keys in the inactive keyset after key changeover).

1. Connect the KFD to a radio or other device.
2. From the **Device** screen, select the **Active keyset** or the **Inactive keyset** using the drop-down menu.
3. Select the checkboxes of the keys you wish to zeroize.
4. Tap the 🗑 button to zeroize the selected keys.



Zeroize the selected keys?

If you want to quickly zeroize all keys from all keysets, tap the ⋮ button and select **Zeroize all keys**. Tap **Zeroize** on the pop-up menu to complete this action.

4 Fast Key Fill

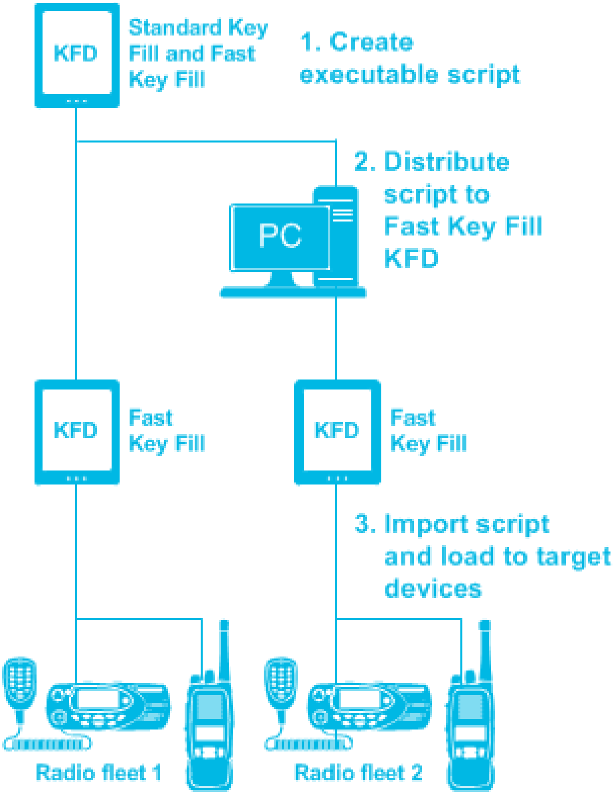
This section describes how to create editable and executable scripts using both Standard Key Fill and Fast Key Fill, and how to use these scripts to deploy keys using KFDs.

This section covers:

- About the Fast Key Fill process
- Creating scripts
- Deploying keys

About the Fast Key Fill process

In typical use, one centrally located, secure KFD is used by an administrator to create and maintain the required encryption keys and scripts, utilizing both the Standard Key Fill and Fast Key Fill features. These keys and scripts are then exported as an executable script to memory cards for distribution to KFDs with only the Fast Key Fill license. Users in the field need have no knowledge of creating and maintaining the encryption keys. Their only task is to run the executable scripts and load the keys on the radios and target devices as required.

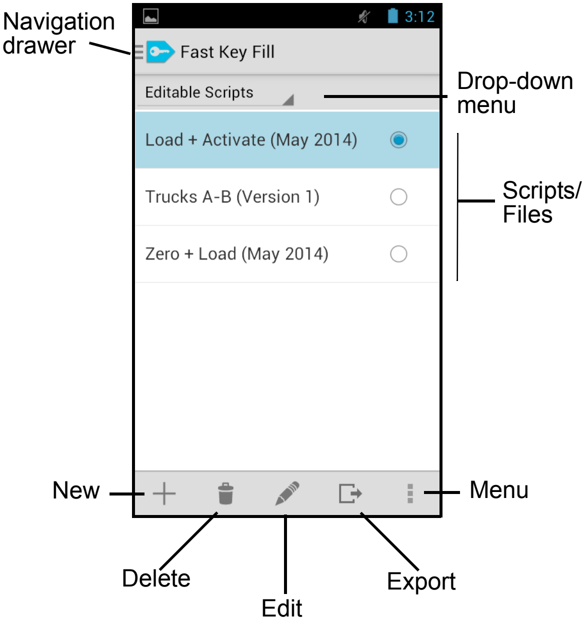

KFD
Standard Key Fill and Fast Key Fill
1. Create executable script
2. Distribute script to Fast Key Fill KFD
PC
KFD
Fast Key Fill
KFD
Fast Key Fill
3. Import script and load to target devices
Radio fleet 1
Radio fleet 2

Executable scripts consist of an editable script that, together with the encryption keys to be downloaded, contains the commands for loading, activating and zeroizing the keys on a radio or target device. Executable scripts cannot be edited, and keystore information and actions are unable to be viewed.

Fast Key Fill overview

The following screen appears when you navigate to the **Fast Key Fill** > **Editable Scripts** screen:

This sub-screen appears only for KFDs that have both Standard Key Fill and Fast Key Fill feature licenses.



Fast Key Fill

Editable Scripts

Load + Activate (May 2014) ●

Trucks A-B (Version 1) ○

Zero + Load (May 2014) ○

Creating scripts

Use Standard Key Fill and Fast Key Fill to create executable scripts.

1 Using Standard Key Fill, create the keys that will be loaded by the executable script. See “Standard Key Fill overview” on page 29.

2 Using Fast Key Fill create an editable script that defines how to use those keys. See “Creating an editable script” below.

3 Export the script for use in other KFDs running Fast Key Fill. See “Exporting a script” on page 58.

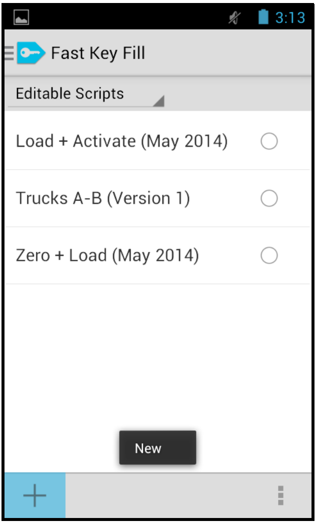
ⓘ Once a script is exported, it becomes an executable script. Executable scripts cannot be edited. If changes are required, you will need to alter the initial editable script and export it again.

ⓘ Editable scripts can be imported. See “Importing executable scripts” on page 60.

Creating an editable script

1 From the **Fast Key Fill** screen, select **Editable Scripts** from the the drop-down menu.

2 Tap + .

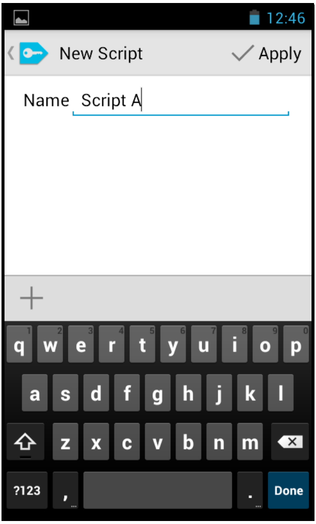


Load + Activate (May 2014) ○

Trucks A-B (Version 1) ○

Zero + Load (May 2014) ○

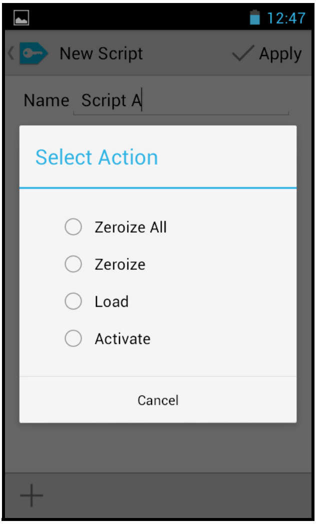
3 Enter a name for the script.



Name Script A

4 Tap + and select one of the four options to begin defining your script.

See the following table for information on these four options.



New Script

Apply

Name Script A

Select Action

○ Zeroize All

○ Zeroize

○ Load

○ Activate

Cancel

Option	Description	To use...
Zeroize All	Zeroizes all active and inactive encryption keys on the target device.	Tap + > **Zeroize All**.
Zeroize	Allows you to specify the encryption key(s) to be zeroized.	Tap + > **Zeroize**. Select the encryption key(s) that you wish to zeroize on the target devices and tap **OK**.
Load	Allows you to select the encryption keys to be included in the keystore package.	Tap + > **Load**. Select the keyset required from the drop-down menu that appears: ■ Keyset 1: is for the active TEKs on the KFD ■ Keyset 2: is for the inactive TEKs on the KFD ■ Keyset 255: is for the KEKs on the KFD When you have selected the required keyset, select the keys that you wish to load and tap **Select keys**.
Activate	Allows you to select which keyset is to be activated on the target device.	Tap + **> Activate**. Select the keyset that will be activated using the drop-down menu. (Note that keyset 255 for KEKs is not displayed.) Tap **Set keyset** to return to the New Script screen.

5 When the script is complete, tap ✓ Apply .

Script example

This example shows how to create an editable script that zeroizes all keys, loads two keys from Keyset 1, then activates Keyset 1.

1 From the **Fast Key Fill** screen, select **Editable Scripts** from the the drop-down menu.

2 Tap + .

3 Enter a name for the script.

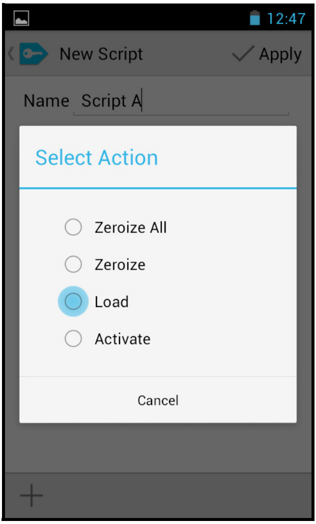
4 Tap + > **Zeroize All**.

5 Tap + > **Load**, and select Keyset 1.

6 Select the keys that you wish to load.

7 Tap **Select keys**.

8 Tap + > **Activate**.



Name Script A

○ Zeroize All

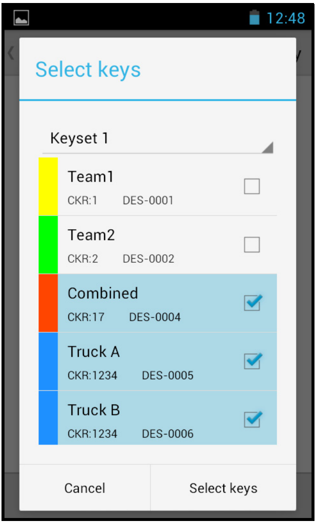
○ Zeroize

● Load

○ Activate

9 Select Keyset 1.

10 Tap **Set keyset**.



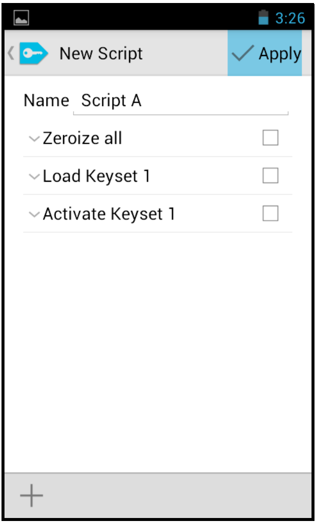
Select keys

Keyset 1

🟨	Team1	CKR:1 DES-0001	☐
🟩	Team2	CKR:2 DES-0002	☐
🟥	Combined	CKR:17 DES-0004	☑
🟦	Truck A	CKR:1234 DES-0005	☑
🟦	Truck B	CKR:1234 DES-0006	☑

11 Review the script details, and tap ✓ Apply .

You can now export the script for use in the Fast Key Fill application. See “Exporting a script” on page 58.



Name Script A

Zeroize all ☐

Load Keyset 1 ☐

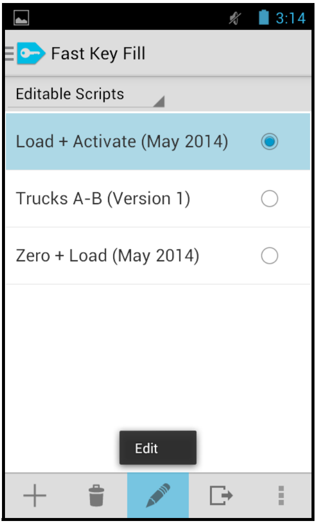
Activate Keyset 1 ☐

Deleting a script

1. From the **Fast Key Fill** screen, select **Editable Scripts** from the the drop-down menu.
2. Select the script you wish to delete and tap 🗑.
3. Tap **Delete** to confirm.

Editing a script

1. From the **Fast Key Fill** screen, select **Editable Scripts** from the drop-down menu.
2. Select the script you wish to edit and tap ✏.
3. Tap ✓ Apply when you have completed your edits.



Load + Activate (May 2014) ●

Trucks A-B (Version 1) ○

Zero + Load (May 2014) ○

Exporting a script

1 Insert a memory card in the KFD (remove the cover on the left-hand side of the KFD to access the card slot).

2 From the **Fast Key Fill** screen, select **Editable Scripts** from the the drop-down menu.

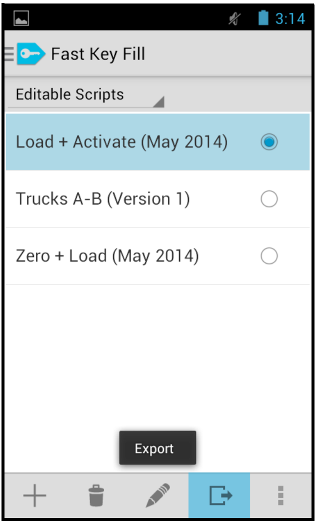
3 Select the script you wish to export and tap ⇨.

4 Select **External memory card** from the **Export to** field.

5 Follow the prompts to enter then re-enter a password.

See “Password tips” on page 22.

6 Tap **Done**.



Editable Scripts

Load + Activate (May 2014) ●

Trucks A-B (Version 1) ○

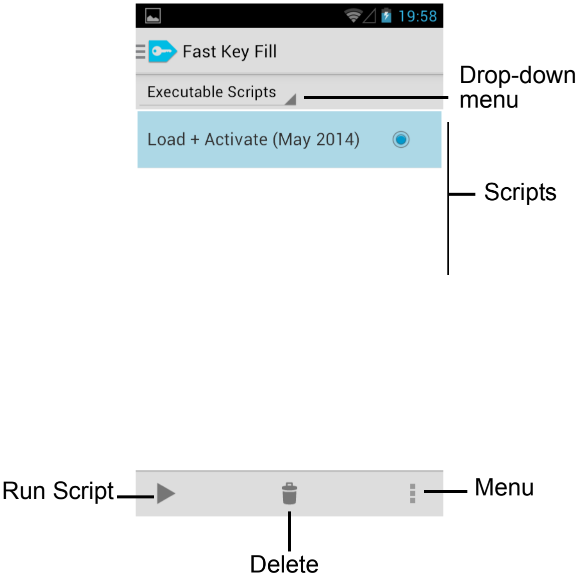
Zero + Load (May 2014) ○

ⓘ Once a script has been exported, it becomes an executable script and can longer be edited, nor can any actions or key information contained in the script be viewed.

Deploying keys

If the Fast Key Fill feature license has been purchased, the KFD can be used to automate the process of loading keys into target devices. This is accomplished using an executable script, defined by a KFD with both Standard Key Fill and Fast Key Fill licenses. Harris UKEK files can also be loaded into target devices, using Fast Key Fill. The Fast Key Fill interface is designed so users can easily load encryption keys without knowledge of encryption key details and the exact tasks required.

KFDs with only the Fast Key Fill feature license will default to the **Executable Scripts** screen.



Importing executable scripts

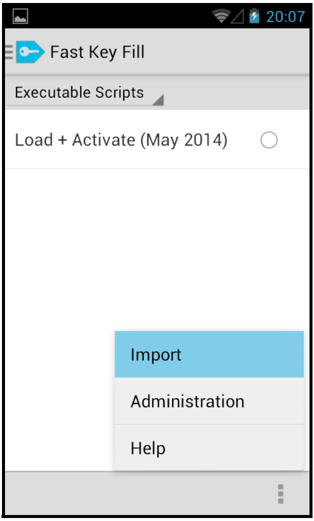
1. Select either Editable Scripts, or Executable Scripts from the drop-down menu.

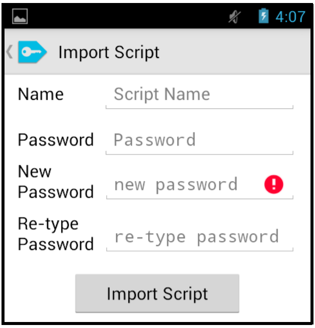
2. Insert the memory card containing the script for importing (remove the cover on the left hand side of the KFD to access the card slot).

3. Tap ⋮ > **Import**.

4. Select the script location from the drop-down menu and check the boxes beside the scripts you want to import. Multiple scripts can be imported if they all share the same password.

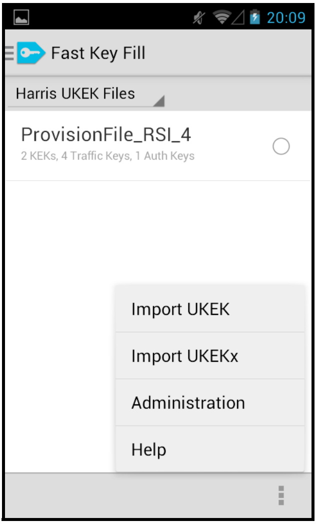
5. Enter a new password for the script and tap **Import Script**.





Not entering a new password will remove the existing password.

Importing Harris UKEK Files



ProvisionFile_RSI_4
2 KEKs, 4 Traffic Keys, 1 Auth Keys

1. Insert the memory card containing the Harris UKEK file for importing (remove the cover on the left hand side of the KFD to access the card slot).
2. Select Harris UKEK files from the drop-down menu.
3. Tap ⋮
4. Select the import file type:
   - Import UKEK: imports a standard Harris *.UKEK file
   - Import UKEKx: imports an encrypted Harris *.UKEKx file
5. Tap the **Import From** field. Select the file location from the drop-down menu and tap the file you want to import.
6. Create and confirm a password for the file. If you are importing a *.UKEKx file, you will also need to enter the existing password.
7. Click **Import File**.

Deploying a Harris UKEK File

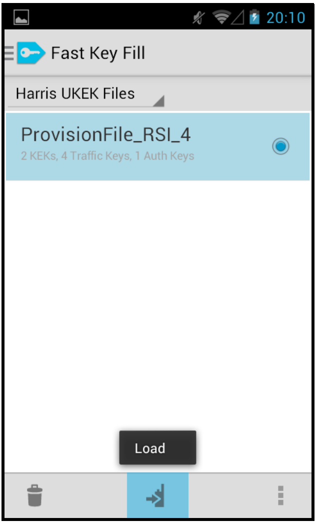
1 Select the Harris UKEK file and tap ⇥ .

2 Enter the Password and tap **Connect**.

3 Attach the KFD to the device the file is to be loaded on.

4 Once the device is attached tap Load File.

5 When the file has been loaded a message will appear.



ProvisionFile_RSI_4
2 KEKs, 4 Traffic Keys, 1 Auth Keys

6 Repeat steps 3 to 4 for as many devices as required.

7 Press ↩ to take you back to the main Fast Key Fill screen.

ⓘ Upon completion, the KFD will display the number of keys successfully deployed.

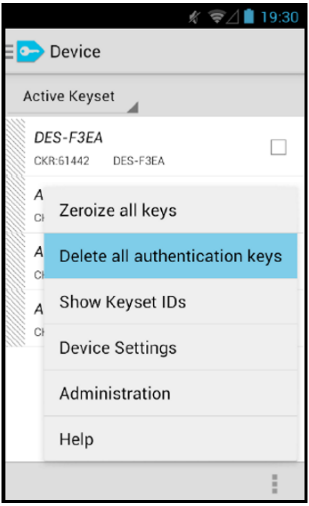
Deleting authentication keys

Authentication keys are used to connect devices to protected networks. These are loaded onto devices using Harris *.UKEK or *.UKEKx files. To delete all authentication keys from a device:

1 Attach the KFD to the device.

2 Tap ⋮ > **Delete all authentication keys**.

3 Tap **Delete**.

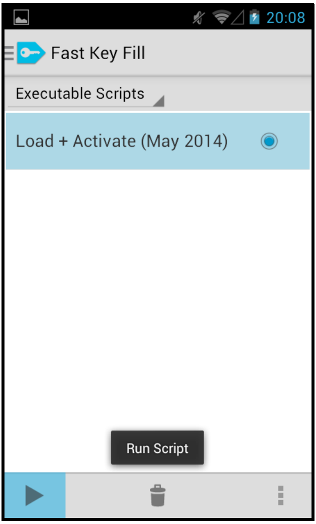


This process will not delete any other type of encryption key. A message will display how many authentication keys were deleted.

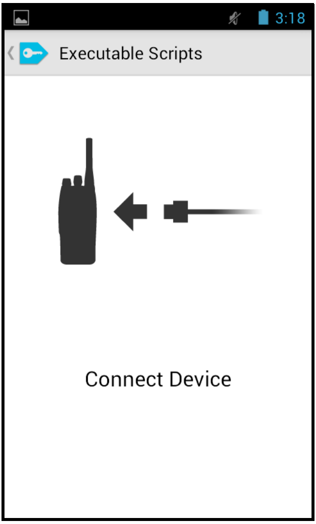
Running executable scripts

1 Select the executable script and tap ▶.

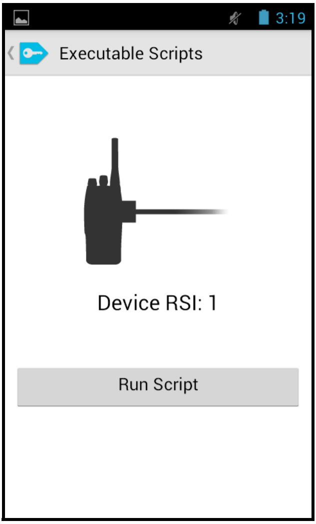
2 Enter the password for the script and tap **Connect**.



3 Attach the KFD to the device the script is to be run on.



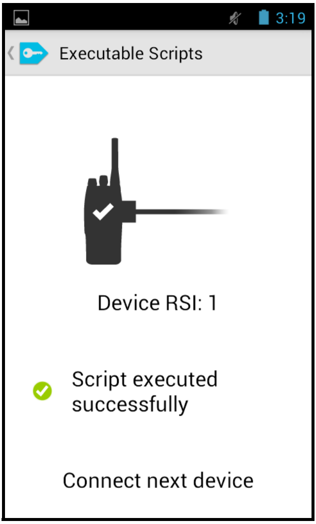
4 Once the device is attached, tap **Run Script** to load the keystore.



Device RSI: 1

If you receive the **Script failed to complete** message, see “Troubleshooting” on page 76 and the problem and solution on page 82.

5 **Script executed successfully** will appear when the new keys and script commands have been loaded.



Device RSI: 1

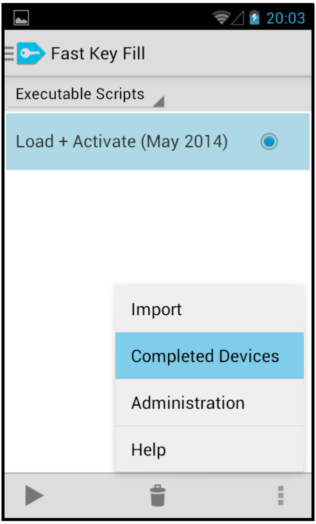
✓ Script executed successfully

Connect next device

6 Repeat steps 3 to 4 for as many devices as required to update encryption keys across a fleet.

7 Press ↩ to take you back to the main Fast Key Fill screen.

8 To display a list of all the radios that have had a specific script applied: select a script, then tap ⋮ > **Completed Devices**.



Deleting an executable script

1 From the **Fast Key Fill** > **Executable Scripts** screen, select the executable script to delete.

2 Tap 🗑.

3 The following message will be displayed: **Delete the selected script?**

4 Select **Delete** to delete the selected script(s).

5 Using the KFD with a KMF

This section describes how to use the KFD with a KMF (Key Management Facility).

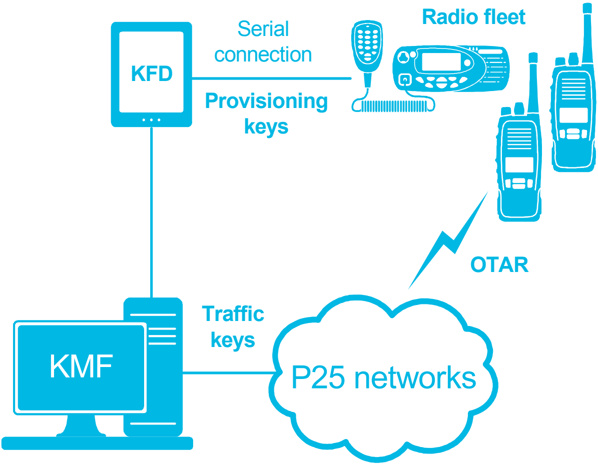
This section covers:

- About using the KFD with a KMF
- Initializing the KFD
- Importing KMF keys into Standard Key Fill
- Changing KMF parameters on the connected radio

About using the KFD with a KMF

A KMF (Key Management Facility) provides a complete solution to securely manage and distribute encryption keys for a radio fleet. The primary function of the KMF is to manage over-the-air rekeying (OTAR) of radios.

The KFD is an integral part of a KMF solution. One of the most important roles of the KFD is to load provisioning keys to the fleet of radios.
A provisioning key is the initial unique key encryption key (UKEK) that enables the KMF to communicate via OTAR with a radio. Once a provisioning key has been loaded, the KMF can then load more secure individual UKEKs to radios, and load the initial set of traffic encryption keys (TEKs). The following diagram explains the different roles of the KFD and the P25 network in distributing encryption keys.



The KFD can also be used (alongside a KMF) to load keys into devices that do not support OTAR (such as the P25 console gateway) or lie outside OTAR coverage, or to re-load keys after radio repair or maintenance, or if a radio has had encryption keys zeroized.

Initializing the KFD

Before importing files from the Tait EnableProtect Key Management Facility (KMF), the KFD must be declared to the KMF and the KFD then initialized. This creates a secure communications channel that enables the KFD to receive keys and files exported from the KMF.

ⓘ This information applies to the Tait EnableProtect Key Management Facility only.

Declaring the KFD to the KMF

Before the KFD can be initialized, it must be declared to the KMF. This task is carried out by the KMF user who has the role of Security Officer. You may need to provide details of the KFD, including the serial number (see “Obtaining the KFD serial number” on page 78), preferred KFD name and password, asset number and user name.

The Security Officer will declare the KFD to the KMF and add it to a KFD Group. They will then provide you with an initialization file (*.kmfinit) along with a password.

Importing the initialization file

To perform this task, you must have an initialization file (*.kmfinit) and password generated specifically for the KFD from the KMF. If you do not have that file, contact your KMF Security Officer who will either declare the KFD to the KMF (see “Declaring the KFD to the KMF” above), or generate a new initialization file if already declared.

To transfer the initialization file to the KFD, use a memory card, or transfer the file from another computer.

1 To copy the initialization file from another computer:

   a Connect the computer to the KFD using the USB OTG cable connector.

   b Using Windows Explorer, navigate to ‘E500’.

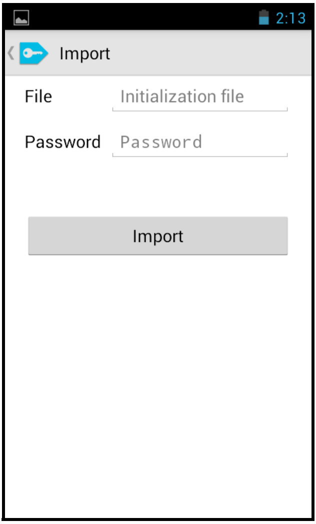
   c Create a folder for initialization files and copy the initialization file into the folder.

2 To transfer the initialization file from a memory card, insert the memory card containing the file (remove the cover on the left-hand side of the KFD to access the card slot).

3 From the **Keystore** screen tap ⋮ > **Settings** > **KMF Import**.

4 Tap the **File** field to select the location and tap the *.kmfinit file.

5 Enter the password for the file and tap **Import**. This is the password that was defined at the time of export, by the person who exported the initialization file.



Importing KMF keys into Standard Key Fill

ⓘ This information applies to the Tait EnableProtect Key Management Facility only.

You can import keys from a KMF *.instructions file into Standard Key Fill. This enables you to use those keys for standard key fill tasks, such as loading keys to target devices manually.

To transfer a *.instructions file to the KFD, use a memory card, or transfer the file from another computer.

1 To copy the *.instructions file from another computer:

- **a** Connect the computer to the KFD using the USB OTG cable connector.
- **b** Using Windows Explorer, navigate to **Portable Devices** > **E500** > **Internal Storage**.
- **c** Copy *.instructions files from the computer and paste the files into the **Internal Storage** folder.

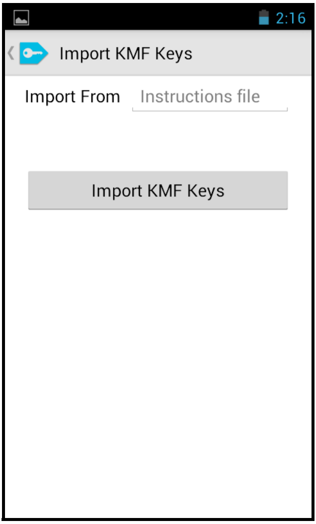
2 To import the *.instructions file from a memory card, insert the memory card containing the *.instructions file (remove the cover on the left-hand side of the KFD to access the card slot).

3 From the **Keystore** screen, tap ⋮ > **Import** > **Tait KMF Keys**.

4 Tap on the **Import From** field to navigate to the *.instructions file that contains the keys you want to import.

5 Tap **Import KMF Keys**.

6 Keys will now appear in the Keystore tab, and can be used for Standard Key Fill tasks such as loading keys (see page 44).



If keys conflict, then the imported keys will automatically replace existing keys in the keystore.

Changing KMF parameters on the connected radio

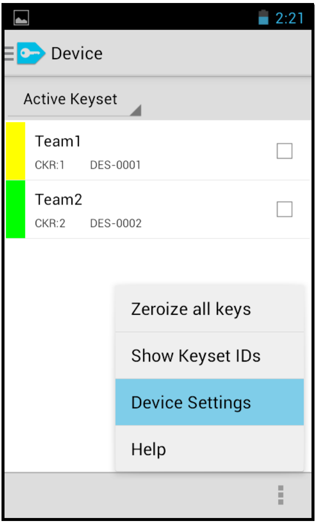
Standard Key Fill enables you to change certain KMF-related parameters on the connected radio. These parameters are normally left at their defaults, and must only be changed if there are specific requirements.

1 Start Standard Key Fill.

2 Connect the KFD to a radio or other device.

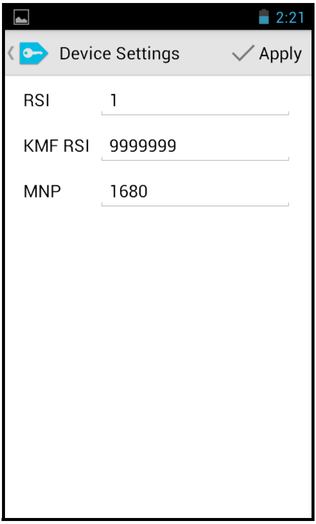
3 Tap ⋮ > **Device Settings**.

A screen appears showing various KMF-related parameters that are currently set on the radio.



The RSI settings are used to identify the radio and the KMF for OTAR transactions.

The MNP (message number period) sets the maximum difference between message numbers that can occur before a message is declared invalid.



RSI 1

KMF RSI 9999999

MNP 1680

4 Tap a box and use the numeric keypad on the touch screen to change a value.

ⓘ Before closing this screen, wait a few seconds for the application to process the updated settings.

6 Troubleshooting

This section contains reference information if you encounter a problem with the KFD or with loading encryption keys.

For further troubleshooting, refer to the E500 User Guide at:

https://www.winmate.com.tw/TabletPC/TabletPCSpec.asp?Prod=13_0236

You can also contact Technical Support.

This section covers:

- Copying software licenses to the KFD
- Version and serial numbers
- Problems and solutions

Copying software licenses to the KFD

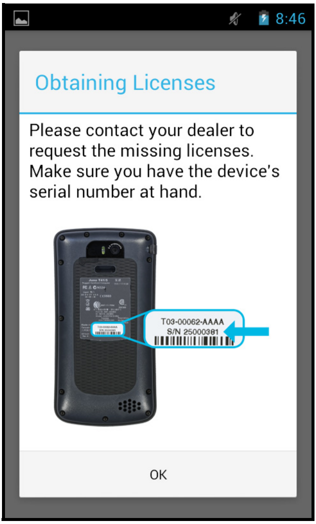
If you are upgrading the KFD by enabling additional features, you must install the relevant feature license(s).

1 Contact your regional Tait office to obtain the necessary licenses. You must provide the KFD serial number (see “Obtaining the KFD serial number” on page 78).

2 Connect the KFD to your PC and copy the license file(s) to the KFD’s **Internal Storage\TaitLicensing** folder.

Internal Storage is the folder that first appears when using Windows to explore the device.

3 To check that the software licenses are valid, turn on the KFD and check that the software features (such as Fast Key Fill) start as expected.



Obtaining Licenses

Please contact your dealer to request the missing licenses. Make sure you have the device's serial number at hand.

Version and serial numbers

When contacting Technical Support, you may need to supply version and serial numbers.

Obtaining the application version number

To obtain the application version number for a KFD module, you must ensure that the on-screen keyboard at the initial password screen is hidden.

1. Tap the **Key Fill Device** icon on the home screen to run the KFD application.
2. The application version number appears at the bottom of the password screen under the Tait logo.

Obtaining the KFD serial number

The KFD (Tait) serial number appears on a sticker located on the rear of the device.

If, for any reason, this sticker is lost or destroyed, the Winmate serial number, located on the bottom of the device (next to the power connector) can be used. In such cases, Tait Technical Support must be informed that the Winmate serial number is being provided.

The Winmate serial number can also be found on the device software. From the Home screen press ☰ and select **System settings** > **About Phone** > **Status** > **Serial number**.

Problems and solutions

Problem	Solution(s)
Cannot connect to target device (for example, no indication of keyloading mode).	Turn the target device off, wait five seconds, then turn the device on again.
	The programming cable between the KFD serial port and target device may not be connected properly. Make sure all cables are working and are connected.
	GPS mode may need to be disabled on some portable handsets where the KFD utilizes the same port to communicate with the device (port 20).
	If none of the above steps resolve the problem, hold the **Power** button and tap **Reboot** to restart the Android operating system. Once the device has rebooted, attempt to connect the KFD to the target device.
Cannot use inactive keyset.	Older versions of Tait P25 console gateways, P25 trunked analog gateways, mobiles and portables do not support two keysets. Either load keys directly to the active keyset, or upgrade the device firmware.

Problem	Solution(s)
Cannot load keys.	The target device may not be properly configured for encryption. Check the programming file for the device, and make sure encryption has been configured correctly. See “Configuring encryption on the target device” on page 15.
	There is a limit to the number of keys target devices can store. Reduce the number of keys selected of type KEK and/or TEK, and attempt to load again.
A message appears similar to: **Key ID is already in use for that algorithm**	The combination of Key ID and algorithm must be unique in the keystore. Use a different Key ID.
When importing keys from a KMF *.instructions file you receive the message: **Your KMF import settings don’t allow you to read this file.**	Check with your security officer that the KMF file has been exported for use with your KFD.

Problem	Solution(s)
Forgotten password.	There is no mechanism available to reset the password and access the current keystore. If you forget the password, your only option is to delete the existing (now defunct) keystore, and start again with a new keystore and password. To do this: ⚠ **The following steps will delete all keys in the KFD, and should only be carried out in accordance with your organization's security policy.** 1. From the Home screen tap ☰ and select **System settings**. 2. Tap **Apps** > **Key Fill Device** > **Clear data**. 3. Tap **OK** on the pop-up menu.
A message appears when attempting to access a software feature: **Not all required licenses are available ...**	Tap the link below this message for information on how to obtain and install the licenses that are reported as missing. For more information, see "Copying software licenses to the KFD" on page 77.

Problem	Solution(s)
You receive a message: **No storage card present.**	It is recommended that you use a storage card for exporting keystores and executable scripts. For information on using and inserting a memory cartographer to the E500 User Guide at https://www.winmate.com.tw/TabletPC/TabletPCSpec.asp?Prod=13_0236
After tapping **Run Script** to load an executable script, you receive a message: **This script is invalid.**	The executable script may be corrupt, or is invalid for the connected device. Either load keys manually using Standard Key Fill, or try again with a new executable script.
You have restored the unit to a factory default state.	The E500 handheld user's guide has information on restoring the device to a factory default state. ⚠ **All KFD software, licenses and keystore information is lost if you perform this function.** If the unit has been restored to a factory default state, you will need to contact a Tait technical support agent.

7 Glossary

A

active keyset

The active keyset is used by the radio to encrypt calls. The active keyset includes KEK keyset keys.

AES

Advanced Encryption Standard. AES256 is a very secure 256-bit encryption algorithm, now released as FIPS 197.

algorithm

The encryption method used. Supported algorithms are AES and DES.

APCO

The Association of Public Safety Communications Officials.
The APCO Project 25 standards committee (http://www.apcointl.org/) defined a digital radio standard. The standard is often referred to as ‘APCO’ or ‘P25’.

C

channel

In a conventional system, a channel is a pair of frequencies used to transmit and receive radio signals.

In a P25 trunking system, a channel is a group of radio users, which is further divided into one or more talkgroups.

CKR Common Key Reference. The reference “slot” or container that is common to the KFD or OTAR protocols, and radios or other devices operating on the system. When a key is sent to a target device, it is sent to a specific CKR, which is then mapped to a name.

D

DES Data Encryption Standard. US encryption standard for non-classified text, published as FIPS standard 46-3. The KFD uses a DES with a 64-bit algorithm (56 bits + 8 parity check bits).

I

inactive keyset The keyset on portable and mobile radios that holds unused keys (for example, new keys until a key changeover occurs).

K

KEK Key Encryption Key. An encryption key used specifically for the encryption of other keys. A KEK is used whenever secure OTAR messages are transmitted.

keystore The encryption keys stored on the actual KFD unit, and shown on the Keystore screen. The keystore can be any combination of previously used keys, current keys, or future keys, depending on requirements.

key variable A multi-digit number that the crypto-module uses when encrypting and decrypting. The key variable is also known as key material.

keyset A group of encryption keys on the radio. Tait mobile and portable radios support an active keyset, an inactive keyset, and a KEK keyset. The KEK keyset shows in the Active Keyset view.

KFD Key Fill Device. The generic term used for a computing device that uses a direct connection to deploy encryption keys (compare with OTAR).

KID Key ID. The unique number used to identify which key is used when a message is encrypted. The key ID is used at the receiving device to help it select the appropriate decryption key.

KMF Key Management Facility. The generic term used for computing devices that deploy encryption keys to radios over-the-air (OTAR).

O

OTAR Over the Air Rekeying. General name for the protocol used for re-keying radios over a wireless radio link.

N

navigation drawer The navigation drawer is a panel that transitions in from the left edge of the screen and displays the application’s main navigation options (Keystore, Fast Key Fill, Device).

P

P25 Project 25. The Association of Public Safety Communications Officials (APCO) established Project 25 (P25). This project was led by United States Federal, state, and local government representatives to develop standards for interoperable digital radios and systems to meet the needs of public safety users.
See http://www.project25.org for further information.

R

RSI Radio Set Identifier. Used to identify a radio, KFD or KMF for OTAR transactions.

S

script Scripts allow users to easily load keys without knowledge of encryption key details and tasks required. An administrator uses the KFD with Standard Key Fill and Fast Key Fill feature licenses to create and distribute a password-protected Fast Key Fill file. The file contains tasks defined in a script, as well as the encryption keys to load. Once the file is deployed to other KFDs, a Fast Key Fill user loads the file, connects a device, and taps ▶ to run the actions defined in the script.

T

talkgroup A talkgroup is a collection of radio users with whom you want to have private conversations.

TEK Traffic Encryption Key. Used by radios and other devices for the encryption of user voice and data messages.

traffic channel The traffic channel is the channel on a trunking system to which the parties participating in a call are directed for the duration of the call. When the call ends, the traffic channel is returned to the pool of channels for use in a new call.

Z

zeroize To zeroize one or more encryption keys is to render them useless by overwriting the key material with zeroes.

Index

Tait Software License Agreement

This Software License Agreement ("Agreement") is between you (“Licensee”) and Tait International Limited (“Tait").

By using any of the Software items embedded and pre-loaded in the related Tait Designated Product, included on CD, downloaded from the Tait website, or provided in any other form, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, do not install or use any of the Software. If you install or use any of the Software, that will be deemed to be acceptance of the terms of this Agreement.

For good and valuable consideration, the parties agree as follows:

SECTION 1 DEFINITIONS

“Confidential Information” means all or any information supplied to or received by Licensee from Tait, whether before or after installation or use and whether directly or indirectly pertaining to the Software and Documentation supplied by Tait, including without limitation all information relating to the Designated Products, hardware, software; copyright, design registrations, trademarks; operations, processes, and related business affairs of Tait; and including any other goods or property supplied by Tait to Licensee pursuant to the terms of this Agreement.

“Designated Products” means products provided by Tait to Licensee with which or for which the Software and Documentation is licensed for use.

“Documentation” means product and software documentation that specifies technical and performance features and capabilities; user, operation, and training manuals for the Software; and all physical or electronic media upon which such information is provided.

“Executable Code” means Software in a form that can be run in a computer and typically refers to machine language, which is comprised of native instructions the computer carries out in hardware. Executable code may also refer to programs written in interpreted languages that require additional software to actually execute.

“Intellectual Property Rights” and **“Intellectual Property”** mean the following or their substantial equivalents or counterparts, recognized by or through action before any governmental authority in any jurisdiction throughout the world and including, but not limited to all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation; including any adaptations, corrections, de-compilations, disassemblies, emulations, enhancements fixes, modifications, translations and updates to or derivative works from, the Software or Documentation, whether made by Tait or another party, or any improvements that result from Tait processes or, provision of information services.

“Licensee” means any individual or entity that has accepted the terms of this License.

“Open Source Software” means software with freely obtainable source code and license for modification, or permission for free distribution.

“Open Source Software License” means the terms or conditions under which the Open Source Software is licensed.

“Person” means any individual, partnership, corporation, association, joint stock company, trust, joint venture, limited liability company, governmental authority, sole proprietorship, or other form of legal entity recognized by a governmental authority.

“Security Vulnerability” means any flaw or weakness in system security procedures, design, implementation, or internal controls that if exercised (accidentally triggered or intentionally exploited) could result in a security breach such that data is compromised, manipulated, or stolen, or a system is damaged.

“Software” (i) means proprietary software in executable code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, new versions and new releases of the software provided by Tait; (iii) means any upgrades, enhancements or other functions or features to the Software provided by Tait; and (iv) may contain one or more items of software owned by a third-party supplier. The term "Software" includes the applicable “Software Key” and does not include any third-party software provided under separate license or not licensable under the terms of this Agreement.

“Source Code” means software expressed in human readable language necessary for understanding, maintaining, modifying, correcting, and enhancing any software referred to in this Agreement and includes all states of that software prior to its compilation into an executable programme.

“Software Key” means a code or key that is supplied by Tait to access, enable and use the Software or certain functions or features of the Software.

“Tait” means Tait International Limited and includes its Affiliates.

Section 2 SCOPE

This Agreement contains the terms and conditions of the license Tait is providing to Licensee, and of Licensee’s use of the Software and Documentation. Tait and Licensee enter into this Agreement in connection with Tait delivery of certain proprietary Software and/or products containing embedded or pre-loaded proprietary Software.

SECTION 3 GRANT OF LICENSE

3.1. Subject to the provisions of this Agreement and the payment of applicable license fees, Tait grants to Licensee a personal, limited, non-transferable (except as permitted in Section 7), and non-exclusive license to use the Software in executable code form, and the Documentation, solely in connection with Licensee's use of the Designated Products for the useful life of the Designated Products. This Agreement does not grant any rights to source code.

3.2. The Licensee acknowledges that one or more Software Keys may be required from Tait for the Software or certain functions or features of the Software. The Licensee may only access, enable and use such Software or functions or features of the Software with Software Keys issued by Tait. Tait may provide the Licensee with a Software Key for the Software or certain functions or features of the Software agreed to by the parties as part of this Agreement. The Software Key may control the functions or features of the Software licensed in accordance with this Agreement. The Licensee’s license to the Software Key is limited to a license to use the Software Key only to access, enable and use the Software or certain functions or features of the Software that Tait has agreed to provide to the Licensee and only in accordance with the Documentation.

3.3. If the Software licensed under this Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not in this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the any applicable Open Source Software Licenses, the terms and conditions of the Open Source Software Licenses will take precedence. For information about Open

Source Components contained in Tait products and the related Open Source licenses, see: https://www.taitradio.com/opensource

SECTION 4 LIMITATIONS ON USE

4.1. Licensee may use the Software only for Licensee's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited. Without limiting the general nature of these restrictions, Licensee will not make the Software available for use by third parties on a "time sharing," "application service provider," "service bureau" basis, or for any other similar commercial rental or sharing arrangement.

4.2. Licensee will not, and will not directly or indirectly allow or enable any third party to: (i) reverse engineer, disassemble, extract components, decompile, reprogram, or otherwise reduce the Software or any portion thereof to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party; (iv) grant any sublicense or other rights in the Software or Documentation to any third party; (v) take any action that would cause the Software or Documentation to be placed in the public domain; (vi) remove, or in any way alter or obscure any copyright notice or other notice of Tait or third-party licensor's proprietary rights; (vii) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by, any third party or on any machine except as expressly authorized by this Agreement; or (viii) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software by any means whatsoever other than what is permitted in this Agreement. Licensee may make one copy of the Software to be used solely for archival, back-up, or disaster recovery purposes; provided that Licensee may not operate that copy of the Software at the same time as the original Software is being operated. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

4.3. Unless otherwise authorized by Tait in writing, Licensee will not, and will not enable or allow any third party to: (i) install a copy of the Software on more than one unit of a Designated Product; or (ii) copy or transfer Software installed on one unit of a Designated Product to any other device. Licensee may temporarily transfer Software installed on a Designated

Product to another device if the Designated Product is inoperable or malfunctioning. Temporary transfer of the Software to another device must be discontinued when the original Designated Product is returned to operation and the Software must be removed from the other device.

4.4. Licensee will maintain, during the term of this Agreement and for a period of two years thereafter, accurate records relating to this license grant to verify compliance with this Agreement. Tait, or a third party nominated by Tait, may inspect Licensee’s premises, books and records, upon reasonable prior notice to Licensee, during Licensee’s normal business hours and subject to Licensee's facility and security regulations. Tait is responsible for the payment of all expenses and costs of the inspection, provided that Licensee shall indemnify Tait for all costs (including audit costs and legal costs on a solicitor client basis) if Licensee has breached the terms of this Agreement. Any information obtained by Tait during the course of the inspection will be kept in strict confidence by Tait and used solely for the purpose of verifying Licensee's compliance with the terms of this Agreement.

SECTION 5 OWNERSHIP AND TITLE

Tait, its licensors, and its suppliers retain all of their Intellectual Property Rights in and to the Software and Documentation, in any form. No rights are granted to Licensee under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Agreement. All Intellectual Property developed, originated, or prepared by Tait in connection with providing the Software, Designated Products, Documentation, or related services, remains vested exclusively in Tait, and Licensee will not have any shared development or other Intellectual Property Rights.

SECTION 6 LIMITED WARRANTY; DISCLAIMER OF WARRANTY

6.1. The commencement date and the term of the Software warranty will be a period of one (1) year from Tait shipment of the Software. If Licensee is not in breach of any obligations under this Agreement, Tait warrants that the unmodified Software, when used properly and in accordance with the Documentation and this Agreement, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect has occurred will be determined solely by Tait. Tait does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. Tait makes no representations or warranties with respect to any third-party software included in the Software.

6.2 Tait sole obligation to Licensee, and Licensee's exclusive remedy under this warranty, is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant, demonstrable program or documentation errors or Security Vulnerabilities. If Tait cannot correct the defect within a reasonable time, then at Tait option, Tait will replace the defective Software with functionally equivalent Software, license to Licensee substitute Software which will accomplish the same objective, or terminate the license and refund Licensee's paid license fee. If Tait investigation of the perceived defect reveals that no such defect in fact exists, Tait may recover its costs in respect of such investigation from Licensee.

6.3. Tait disclaims any and all other warranties relating to the Software or Documentation other than the express warranties set forth in this Section 6. Warranties in Section 6 are in lieu of all other warranties whether express or implied, oral or written, and including without limitation any and all implied warranties of condition, title, non-infringement, merchantability, or fitness for a particular purpose or use by Licensee (whether Tait knows, has reason to know, has been advised of, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, Tait disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

Section 7 TRANSFERS

7.1. Licensee will not transfer the Software or Documentation to any third party without specific prior written consent from Tait. Tait may withhold such consent or at its own discretion make the consent conditional upon the transferee paying applicable license fees and agreeing to be bound by this Agreement.

7.2. In the case of a value-added reseller or distributor of Tait Designated Products, the consent referred to in Section 7.1 may be contained in a Tait

Reseller or Tait Distributor Agreement.

7.3. If the Designated Products are Tait vehicle-mounted mobile products or hand-carried portable radio products and Licensee transfers ownership of the Tait mobile or portable radio products to a third party, Licensee may assign its right to use the Software which is embedded in or furnished for use with the radio products and the related Documentation; provided that Licensee transfers all copies of the Software and Documentation to the transferee.

7.4. 7.4.For the avoidance of any doubt, Section 7.3 excludes TaitNet Infrastructure, or the products listed at any time under network products at: http://www.taitradio.com.

7.5. If Licensee, as a contractor or subcontractor (integrator), is purchasing Tait Designated Products and licensing Software not for its own internal use but for end use only by a Customer, the Licensee may transfer such Software, but only if a) Licensee transfers all copies of such Software and the related Documentation to the transferee and b) Licensee has first obtained from its Customer (and, if Licensee is acting as a subcontractor, from the interim transferee(s) and from the ultimate end user sub license) an enforceable sublicense agreement that prohibits any other transfer and that contains restrictions substantially identical to the terms set forth in this Software License Agreement. Except as stated in the foregoing, Licensee and any transferee(s) authorised by this Section may not otherwise transfer or make available any Tait Software to any third party nor permit any party to do so. Licensee will, on request, make available evidence reasonably satisfactory to Tait demonstrating compliance with all the foregoing.

SECTION 8 TERM AND TERMINATION

8.1. Licensee's right to use the Software and Documentation will commence when the Designated Products are supplied by Tait to Licensee and will continue for the life of the Designated Products with which or for which the Software and Documentation are supplied, unless Licensee breaches this Agreement, in which case this Agreement and Licensee's right to use the Software and Documentation may be terminated immediately upon notice by Tait.

8.2. Within thirty (30) days after termination of this Agreement, Licensee must certify in writing to Tait that all copies of the Software have been removed or deleted from the Designated Products and that all copies of the Software and Documentation have been returned to Tait or destroyed by

Licensee and are no longer in use by Licensee.

8.3. Licensee acknowledges that Tait made a considerable investment of resources in the development, marketing, and distribution of the Software and Documentation and that Licensee's breach of this Agreement will result in irreparable harm to Tait for which monetary damages would be inadequate. If Licensee breaches this Agreement, Tait may terminate this Agreement and be entitled to all available remedies at law or in equity including immediate injunctive relief and repossession of all non-embedded Software and associated Documentation. Licensee shall pay all Tait costs (on an indemnity basis) for the enforcement of the terms of this Agreement.

Section 9 Confidentiality

Licensee acknowledges that the Software and Documentation contain proprietary and Confidential Information valuable to Tait and are Tait trade secrets, and Licensee agrees to respect the confidentiality of the information contained in the Software and Documentation.

Section 10 Limitation of Liability

10.1. In no circumstances shall Tait be under any liability to Licensee, or any other person whatsoever, whether in Tort (including negligence), Contract (except as expressly provided in this Agreement), Equity, under any Statute, or otherwise at law for any losses or damages whether general, special, exemplary, punitive, direct, indirect, or consequential arising out of or in connection with any use or inability of using the Software.

10.2. Licensee’s sole remedy against Tait will be limited to breach of contract and Tait sole and total liability for any such claim shall be limited at the option of Tait to the repair or replacement of the Software or the refund of the purchase price of the Software.

Section 11 General

11.1. COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.

11.2. COMPLIANCE WITH LAWS. Licensee acknowledges that the Software may be subject to the laws and regulations of the jurisdiction covering the supply of the Designated Products and will comply with all applicable laws and regulations, including export laws and regulations, of that country.

11.3. ASSIGNMENTS AND SUBCONTRACTING. Tait may assign its rights or subcontract its obligations under this

Agreement, or encumber or sell its rights in any Software, without prior notice to, or consent of, Licensee.

11.4. GOVERNING LAW. This Agreement shall be subject to and construed in accordance with New Zealand law and disputes between the parties concerning the provisions hereof shall be determined by the New Zealand Courts of Law. Provided however Tait may at its election bring proceedings for breach of the terms hereof or for the enforcement of any judgment in relation to a breach of the terms hereof in any jurisdiction Tait considers fit for the purpose of ensuring compliance with the terms hereof or obtaining relief for breach of the terms hereof.

11.5. THIRD-PARTY BENEFICIARIES. This Agreement is entered into solely for the benefit of Tait and Licensee. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this Agreement. Notwithstanding the foregoing, any licensor or supplier of third-party software included in the Software will be a direct and intended third-party beneficiary of this Agreement.

11.6. SURVIVAL. Sections 4, 5, 6.3, 7, 8, 9, 10, and 11 survive the termination of this Agreement.

11.7. ORDER OF PRECEDENCE. In the event of inconsistencies between this Agreement and any other Agreement between the parties, the parties agree that, with respect to the specific subject matter of this Agreement, this Agreement prevails.

11.8 SECURITY. Tait uses reasonable means in the design and writing of its own Software and the acquisition of third-party Software in order to limit Security Vulnerabilities. While no software can be guaranteed to be free from Security Vulnerabilities, if a Security Vulnerability is discovered, Tait will take the steps specified in Section 6 of this Agreement.

11.9 EXPORT. Licensee will not transfer, directly or indirectly, any Designated Product, Documentation or Software furnished hereunder or the direct product of such Documentation or Software to any country for which New Zealand or any other applicable country requires an export license or other governmental approval without first obtaining such license or approval.

11.10 SEVERABILITY. In the event that any part or parts of this Agreement shall be held illegal or null and void by any court or administrative body of competent jurisdiction, such determination shall not affect the remaining terms which shall remain in full force and effect as if such part or parts held to be illegal or void had not been included in this Agreement. Tait may replace the invalid or unenforceable provision with a valid and enforceable provision that achieves the original intent and economic effect of this Agreement.

11.11 CONSUMER GUARANTEES. Licensee acknowledges that the licenses supplied in terms of this agreement are supplied to Licensee in business, and that the guarantees and other provisions of prevailing consumer protection legislation shall not apply.

11.12 WHOLE AGREEMENT. Licensee acknowledges that it has read this Agreement, understands it and agrees to be bound by its terms and conditions. Licensee also agrees that, subject only to the express terms of any other agreement between Tait and Licensee to the contrary, this is the complete and exclusive statement of the Agreement between it and Tait in relation to the Software. This Agreement supersedes any proposal or prior agreement, oral or written, and any other communications between Licensee and Tait relating to the Software and the Designated Products.