Tait EnableProtect Advanced System Key

User's Guide

MTA-00020-09 · Issue 9 · September 2018

www.taitradio.com

Contact Information

Tait Communications
Corporate Head Office

Tait International Limited
P.O. Box 1645
Christchurch
New Zealand

For the address and telephone number of regional offices, refer to our website: 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, NZ530819, NZ534475, NZ547713, NZ577009, NZ579051, NZ579364, NZ586889, NZ610563, NZ615954, NZ700387, NZ708662, NZ710766, NZ711325 , NZ726313, NZ593887, AU2015215962, AU339127, AU339391, AU2016259281, AU2016902579, EU000915475-0001, EU000915475-0002, GB2532863, US14/834609 Div. no 1, US15/346518 Div.no 2, US15/350332, US15/387026 Div., US20150085799, US20160044572, US20160057051, US640974, US640977, US698339, US702666, US7758996, US8902804, US9107231, US9504034, US9559967.

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

Preface **6**

1 About System Keys **9**

1.1 About the Tait EnableProtect Advanced System Key 10

1.1.1 USB Dongle Expiry 12

1.1.2 USB Dongle Passwords 12

1.2 About System Key Files 14

1.3 Ordering System Keys 14

1.3.1 Completing the Advanced System Key Request Form 15

1.4 Recording and Identifying System Keys 17

1.5 Installing the Software and USB Dongle Drivers 18

1.6 Repairing and Servicing Protected Radios 20

2 Trunking Protection **21**

2.1 About P25 Trunking Protection 21

2.2 About Anti-cloning 22

2.3 Setting Up P25 Trunking Protection 23

3 Read/Write Protection **24**

3.1 About Read/Write Protection 24

3.2 Setting Up Read/Write Protection 25

3.3 Enabling Read/Write Protection on Radios 26

4 Pass Key Configuration Utility **28**

4.1 Configuring a Pass Key 28

4.2 Pass Key Configuration Utility Reference 29

5 Programming Application Information **33**

5.1 Using a System Key to Program a Radio or Save to File 33

5.2 Reporting 35

6 Frequently Asked Questions **37**

6.1 General Information 37

6.2 Security 38

6.3 Ordering System Keys 40

6.4 About the Hardware 41

6.5 Using the System Keys and Software 41

7 Troubleshooting 43
7.1 Firewall Settings 45
7.2 Reinstalling the USB Dongle Drivers 46
7.3 About Flat Dongle Batteries 46
7.4 Resetting a Corrupt Pass Key 46

Glossary 48

Tait Software License Agreement 50

List of Figures and Tables

Figure 1.1 Advanced System Key dongles. 9
Table 1.1 User tasks with different system key protection 10
Table 1.2 System key order codes. 15
Figure 1.2 DMR Advanced System Key information in the XPA 16
Figure 1.3 P25 Advanced System Key information in the XPA 16
Table 1.3 System key file location 19
Figure 1.4 Connected Trunking Keys dialog 19
Figure 1.5 Device Configuration dialog. 20
Figure 4.6 Pass Key Configuration Utility. 30
Table 4.4 Pass Key Configuration Utility options 30
Figure 5.7 Log entries form 35
Figure 5.8 Printed system key logs. 35
Table 5.5 Information on Log Entries form 36

Preface

Scope of Manual

This guide contains information on how to configure and use system keys, such as system key files and Tait EnableProtect Advanced System Key prime keys and pass keys. It is intended primarily for system administrators and system key end users (see "Typographical conventions" below), and does not include processes internal to Tait such as system key creation and provisioning.

This guide applies to Tait EnableProtect Advanced System Key prime keys and pass keys v5. To find the prime and pass key version number, see Key Version under "Pass Key Configuration Utility Reference" on page 29).

This guide also applies to various related software applications, including:

- TM9100, TP9100, TM9400, TP9400, TM9300 and TP9300 Programming Application (all versions).
- Pass Key Configuration Utility.
- Tait EnableFleet.

Tait International Limited accepts no responsibility for any security breach that may arise from the use of this manual. No example quoted here should be understood to be a recommendation on security policy. Your organization is solely responsible for all decisions related to security.

Typographical conventions

Some information in this guide is intended for specific users only. This information is identified with a symbol and **Information for**, with up to two user types as follows:

Information for System administrators and/or system key end users.

- **System administrators** are responsible for managing system keys according to organization policy. Typical tasks include ordering system keys, configuring pass keys, and distributing pass keys or system key files to end users. System administrators typically work for owners of large (for example, state-wide) trunking systems.

- **System key end users** are authorized by system administrators to use pass keys or hardware system keys or system key files to set up or program protected settings. End users are typically radio shops or dealers, who supply radios or programming files to customers preprogrammed with trunked settings. End users may also be radio installers who are responsible for the initial set up of radio hardware and software. Often there is a contractual agreement in place between the system owner and radio shop, dealer or installer.

Information without a user referenced is generic information that applies to all users (including users without system keys).

Alerts

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 manual uses the following types of alert:

This alert is used to warn about the risk of data loss or corruption.

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.

Associated documentation

The following associated documentation is available for this product:

- TM9100, TP9100, TM9400, TP9400, TM9300 and TP9300 Programming Application Online Help
- Pass Key Configuration Utility Help
- Tait Firmware Upgrade Tool Help
- Tait EnableProtect Advanced System Key - Overview (TN-2131)

The characters xx represent the issue number of the documentation.

Technical notes are published from time to time to describe applications for Tait products, to provide technical details not included in manuals, and to offer solutions for any problems that arise.

Technical notes and product manuals are published on the Tait Technical Support website (www.taitworld.com/technical), and may also be published on the relevant product CD. Help files can be accessed via the Help menu or by pressing the F1 key from the respective application.

Publication record

Issue	Publication Date	Description
9	September 2018	Tait Limited changed to Tait International Limited. EnableProtect changed to Tait EnableProtect.
8	March 2018	Major changes to ordering processes and forms for pass and prime keys, minor changes to WACN and Sytem ID, and general edit.
7	October 2014	Documentation updated to include read/write protection for DMR
6	May 2014	Minor updates for later model Sentinel dongles
5	November 2013	Added information on: ■ New labels for keys ■ Role option for the Pass Key Configuration Utility ■ Resetting a forgotten pass key password ■ Filling out the authorization form ■ Reinstalling the USB dongle drivers ■ Flat dongle batteries ■ Resetting a corrupt pass key
4	February 2012	■ Added information on ‘Memory Used’ progress bar and increased range settings ■ Clarified ‘Max Programs’ option only applies to trunking protection
3	November 2011	■ Changed expired key flag ■ Changed system key order codes ■ Added firewall information
2	June 2011	Added information on: ■ system key files ■ hardware system keys ■ passwords ■ ‘maximum number of programs’ feature (for pass keys)
1	December 2010	First release

1 About System Keys

System keys (either USB dongles or system key files) offer various levels of programming protection and control. Radio equipment owners, who are typically responsible for large systems (for example, state-wide), often require programming protection to safeguard against unauthorized radio programming and use. There are two types of system keys: system key files and Tait EnableProtect Advanced System Key dongles.

System Key Files

System key files offer simple trunking protection only, and are still supported in recent versions of programming applications. You can use existing system key files to program trunked settings, and you can still order new system key files from Tait. However, if system key files have been replaced by Tait EnableProtect Advanced System Key pass keys, you should remove existing system key files from all PCs for security reasons.

Tait EnableProtect Advanced System Key

The Advanced System Key offers various levels of programming protection and control using specially-configured USB dongles (Figure 1.1). It provides additional features and a more secure method of protecting P25 trunking data than system key files.

Figure 1.1 Advanced System Key dongles

1.1 About the Tait EnableProtect Advanced System Key

The Advanced System Key offers two types of protection: P25 trunking protection and read/write protection. For more information on user implications, see Table 1.1 below.

- **P25 trunking protection** is related to protecting a P25 trunking system. Trunking protection guards against a radio being programmed with P25 trunked settings that would enable it to operate illegally on a trunked network. Trunking protection is typically required for large (for example, state-wide) systems. For more information, see "About P25 Trunking Protection" on page 21.

  Notice P25 trunking protection is available for TM9100, TP9100, TM9400 and TP9400 series radios only.

  The previous method of P25 trunking protection using system key files is still supported in the programming application. You can use existing system key files to program trunked settings, and you can still order new system key files from Tait. However, if system key files have been replaced by pass keys, you should remove existing system key files from all PCs for security reasons.

- **Read/write protection** (also known as configuration security) is intended to protect the radio asset. It guards against someone repurposing a radio (for example, if stolen), and against someone misusing a radio in an organization (for example, reprogramming a radio with additional channel frequencies). In combination with the radio inhibit feature, read/write protection is a powerful tool and a deterrent against radio theft. For more information, see "About Read/Write Protection" on page 24.

  Notice Read/write protection is available for TM9100, TP9100, TM9400, TP9400, TM9300 and TP9300 series radios.

The Tait EnableProtect Advanced System Key uses prime keys and pass keys, which are USB dongles. Prime keys and pass keys together enable and provide the full range of Advanced System Key features.

Table 1.1 User tasks with different system key protection

User	User tasks with P25 trunking protection only	User tasks with read/write protection
System administrator	Orders keys. If using prime/pass keys, uses prime key to configure pass keys. Distributes keys.	Orders keys, uses prime key to configure pass keys, then distributes keys.

Table 1.1 User tasks with different system key protection

User	User tasks with P25 trunking protection only	User tasks with read/write protection
System key end user (for example, radio shop or dealer)	Uses a pass key or system key file to program radios or set up programming files with P25 trunked settings.	Uses a pass key to enable read/ write protection in radios, and to program radios with settings.
Users without a system key (for example, end customers or subscribers)	Can read, interrogate and program radios, but cannot change P25 trunked settings. Can use preconfigured files to program trunked settings into radios, and can also change non-trunking settings (such as conventional profiles and personality options).	Cannot read, interrogate or program radios.

Prime Key


early model shown

Description: A prime key is a red USB dongle, and is provided pre-configured by Tait. The only function of the prime key is to enable system administrators to configure or reconfigure pass keys in conjunction with the Pass Key Configuration Utility. The prime key cannot function as a pass key—that is, it cannot be used to program trunked network settings, or to lock/unlock radio configurations.

Features: WACN/System ID, key name, password, optional expiry date (all preconfigured by Tait).

Usage: Prime keys are used by system administrators to configure pass keys. They should not be used by end users, who are usually the recipients of pass keys that a prime key configures.

Pass Key


early model shown

Description: A pass key is a black USB dongle, which authorizes users to program radios according to the pass key's configuration (by the system administrator using a matching prime key). For example, a pass key may enable a user to program a P25 trunking system (identified by WACN ID and System ID, which are read-only and preconfigured by Tait), trunked radio Unit IDs within a range, and trunked Talkgroup IDs within a range. A pass key can also permit users to read and program radios that have read/write protection enabled.

Features: WACN/System ID (preconfigured by Tait), key name, optional password, maximum number of programs, expiry date, read/write protection, unit and Talkgroup ID range limits.

Usage: Pass keys are ideal for medium-to-large (for example, state-wide) systems where high numbers of radios are programmed and multiple system keys need to be distributed. Pass keys provide the best flexibility and level of control for network owners.

1.1.1 USB Dongle Expiry

USB dongles have a specified life of 4 years, and therefore should be replaced within that 4 year period to ensure the dongles are always operational when required. Both prime keys and pass keys have a real-time clock, and support a programmable expiry date to force replacement of keys. In addition, there is a limit on the number of times pass keys can be used to program P25 trunked radios.

The pass key's expiry date and maximum number of program uses is set using the Pass Key Configuration Utility. Programming application users can view this using the Trunking Keys dialog (via the **Tools** > **Trunking Keys** menu). Depending on a setting in **Tools** > **Options**, programming application users receive a warning if the expiry date is 14 days or less away, or if the maximum number of program uses remaining is 10 or less.

When a pass key expires, the **Expired** field shows **Yes** in the Connected Trunking Keys dialog, and you can no longer use the key to change P25 trunked settings or program read/write protected radios.

You can reconfigure the expiry date and maximum number of program uses using the Pass Key Configuration Utility and a matching prime key, but the new expiry date must be before the **Max Expiry Date** (which is either 4 years from the first use of the pass key, or the prime key expiry date if the prime key has an expiry date).

The expiry date for prime keys is optional, and is preconfigured by Tait. The person ordering keys can state an expiry date of less than 4 years from the date of order. A prime key expiry date can be used as a way of ensuring that keys are replaced before the guaranteed battery life (4 years) expires, or that keys are deactivated at the end of a project.

When a prime key expires, you can no longer use it and you must order a new key from Tait. A prime key with no expiry date continues to work until its internal battery runs flat, which may occur at any time after 4 years without warning.

1.1.2 USB Dongle Passwords

USB dongles come with a password (mandatory for prime keys, optional for pass keys) that you must enter before using the key. Passwords are a form of two-factor authentication that increase the protection provided by system keys (the user must know the password and must have the dongle).

The password for prime keys is automatically generated by Tait. Tait sends this password to the email address you supply after it dispatches the keys, and the password cannot be changed. If you forget a prime key password and don't have the original password email available, Tait can resend the password after you complete and send the "Tait EnableProtect Advanced

System Key Prime Key Password Request Form". Contact Tait for a copy of this form.

Pass keys support an optional password that is set using the Pass Key Configuration Utility. You must enter the password when the programming application first accesses a pass key (for example, after clicking **Tools** > **Trunking Keys**, when setting a Channel Profile to P25 Trunking, or when attempting to program a radio). The password is cached, so that a user only needs to enter a pass key password once per session.

If you forget a pass key password, you can reset it using a matching prime key and the Pass Key Configuration Utility. See "Resetting a Forgotten Pass Key Password" below.

After 5 incorrect attempts at entering a pass key password, the pass key is locked for 5 minutes. The number of failed attempts and the lock time are not configurable.

To avoid issues with forgotten passwords, you should record all new or recently-changed passwords in a safe location (such as a system key register). For more information see "Recording and Identifying System Keys" on page 17.

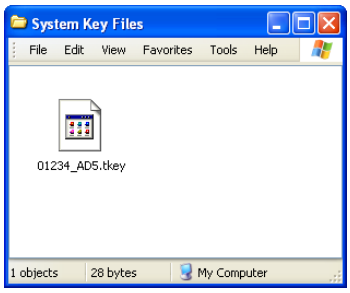
Resetting a Forgotten Pass Key Password

1. Start the Pass Key Configuration Utility and insert the pass key and prime key into spare USB ports on your PC.
   - Insert the pass key with the forgotten password.
   - Insert the matching prime key (formatted with the same Group ID).
2. Click the **Read Keys** button.
3. Enter the password for the attached prime key, and then click **OK**.
4. Enter a new pass key **Password** by selecting and typing over all ••••••••••• characters, or remove the password by clearing all characters so that the field is blank.
5. Click the **Write Pass Key** button.

If successful, the status bar indicates **Pass Key successfully written**.

1.2 About System Key Files

System key files are still supported by the programming application, and are preconfigured by Tait to provide access to a trunking system only.



Description: A system key file is an encrypted file generated by Tait that contains the WACN and System ID of a P25 trunking system. Tait only sends the file to approved recipients (typically system administrators), who can then copy and redistribute the file. End users should save the file to a system key file directory (seeTable 1.3 on page 19) on their PC, and then either generate programming files or program radios with the P25 trunking system (WACN and System ID) contained in the file. No hardware dongle is required.

Features: WACN/System ID

Usage: System key files are more flexible, but less secure than USB dongles. You can email copies of files at short notice to rapidly deploy them onto a system. However, due to this flexibility and lack of password protection and expiry date, you should carefully consider whether to use them. They are best suited to test systems, demonstrations or training.

1.3 Ordering System Keys

Information for System administrators.

Tait only supplies Tait EnableProtect Advanced System Keys and/or System Key Files to approved recipients. Every sales order for system keys must be accompanied by a system key request form. A form is required even for subsequent sales orders from the same customer. You must sign the form, and include details such as name and contact address, and—if P25 trunking protection is required—WACN and System ID. Tait thoroughly checks, verifies and archives each system key request form, and adds the details to a secure database. Once Tait has verified an order, we send you the system key hardware and/or software related to your order.

- Pass keys: you will receive the number of keys you ordered along with a programming CD.
- Prime keys: you will receive the number of prime keys you ordered, an email containing the prime key password (see “USB Dongle Passwords” on page 12), a programming CD, and a system key CD with the Pass Key Configuration Utility (see “Pass Key Configuration Utility” on page 28), a copy of the system key request form, and this user’s guide.

- System key file: you will receive an email or CD with the system key file.

To obtain a copy of the system key request form, contact Tait Communications. For order codes, see Table 1.2.

Table 1.2 System key order codes

Key type	Order code
System key file	TMAA23-10
ASK starter kit	TMAA23-03
Prime key	TMAA23-04
Pass key	TMAA23-05

1.3.1 Completing the Advanced System Key Request Form

You must complete a Tait System Key/EnableProtect Advanced System Key Request form (document ID 6357). A form is required for all new keys, additional keys, replacement keys (for lost or faulty keys), and key upgrades.

Ensure that you complete the form correctly for the order to proceed. Tait rejects incorrectly completed forms, which delays the delivery time.

Order Details

1. **Are you ordering a demo key?**

If you are ordering a key for use on a demo system (for example, a short-term customer demo, trade show, etc.), select **Yes**. Demo keys expire after 90 days, after which you can no longer use them (unless you return them to Tait).

If your order is **not** for a key for use on a demo system, select **No**, and Tait will treat it as a standard order/purchase.

2. **Are you ordering a replacement key or adding a key to an existing set of keys?**

If you are ordering a key to replace an existing one, or ordering an additional key for a system that already uses Advanced System Keys, select **Yes**. This is critical to ensure that Tait programs the new key to be compatible with any existing keys or radios on your system.

3. If you answered **Yes** to question 2, enter the 4-character ASK Group ID (if known).

When ordering replacement or additional keys, the Group ID isn't essential, but it will help us ensure that we put the correct key data file on the keys you order to be compatible with your existing keys.

You can read the Group ID (and WACN and System ID for P25 trunked systems) from an existing key using the Terminal Programming Application (XPA). Plug a pass key for the same system in to your computer, and in the programming application select **Tools** > **Trunking Keys**. The key information should be displayed as per Figures 1.2 and 1.3 below.

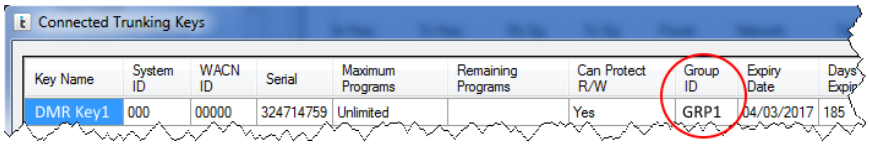


Figure 1.2 DMR Advanced System Key information in the XPA

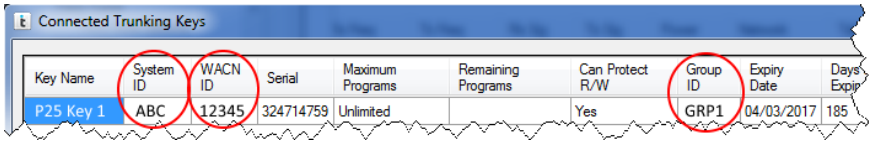


Figure 1.3 P25 Advanced System Key information in the XPA

Quantities

- ASK Starter Kit: 1 Prime + 3 Pass Keys (TMAA23-03)

Enter the number of ASK Starter Kits (if any) that you want to order.

- Prime Keys (TMAA23-04)
  - New Keys: Enter the number of Prime Keys (if any) that you want to order.
  - Reprogram Existing Keys: You can reprogram keys in certain circumstances to facilitate system upgrades (for example, migrating from a non-trunked network to a trunked one), but only with prior agreement from Tait. Once agreed, enter the number of Prime Keys that you are returning to Tait for reprogramming.
- Pass Keys (TMAA23-05)
  - New Keys: Enter the number of Pass Keys (if any) that you want to order.
  - Reprogram Existing Keys: You can reprogram keys in certain circumstances to facilitate system upgrades (for example, migrating from a non-trunked network to a trunked one), but only with prior agreement from Tait. Once agreed, enter the number of Pass Keys that you are returning to Tait for reprogramming.
- Orders that include a Prime Key

Tait can program a Prime Key with a name (maximum of 22 characters) to help identify it. If you want to specify a name for a Prime Key, you can do so here. Otherwise, leave this section blank and we will program the key with a generic name (for example, ‘Prime Key 1’).

- Prime Key Expiry Date

Tait can program a Prime Key with an expiry date (set to any date within 4 years of the order date). When a Prime Key reaches its expiry date, it will deactivate and needs to be replaced.

Expiry dates are a useful means of forcing a key to be replaced before it exceeds the guaranteed battery life (4 years), and of ensuring that keys are deactivated at the end of your project.

If you don't want a key to be programmed with an expiry date, leave this section blank. A Prime Key with no programmed expiry date continues to function until its internal battery runs flat, which may occur at any time without warning after its guaranteed 4-year life.

System Details

- WACN ID

If you are ordering a system key for a P25 trunked network, enter the WACN in hex (5 characters).

- System ID

If you are ordering a system key for a P25 trunked network, enter the System ID in hex (3 characters).

Key Authorizer (System Owner) Details

This section should be completed and signed by a representative/employee of the owner of the radio system who can authorize the request for an Advanced System Key to enable radios to be programmed to work on the radio system.

Key Delivery Address

In this section, enter the details of the person to deliver the key to.

You must activate Pass Keys using a matching Prime Key before you can use them. If you are ordering an additional Pass Key for your system, ensure that it is delivered to the Prime Key holder to be activated and distributed to the end user.

1.4 Recording and Identifying System Keys

Information for System administrators

When you receive a dongle or system key file, you should record the key type and name, date received and intended use. For USB dongles, you should also record the serial number, expiry date and password (if relevant). This is useful for recording keys for audit purposes, identifying when dongles are about to expire, and identifying keys in the programming application's Log Entries form (see "Reporting" on page 35). We recommend using a system key register such as an encrypted, password-protected spreadsheet, database or application.

You may also require (in a contractual agreement) a radio shop or dealer to maintain adequate records. For example, you may require a record to be kept of all radios programmed with a particular key, and a report to be sent back to you on a regular basis.

Tait supplies USB dongles with a plastic label that you can write on with a marker and attach to the dongle (using a split ring). It is good practice to label your dongles with a description (such as the Group ID or key name), and System ID. This is especially relevant if you are dealing with more than one Group ID for different P25 trunking networks or customers.

1.5 Installing the Software and USB Dongle Drivers

Information for System administrators and system key end users

1. Install the relevant programming application, such as the TM9100, TP9100, TM9400, TP9400, TM9300 or TP9300 Programming Application.

If you receive a **Sentinel HASP Run-time installation** error (or similar) during installation, you may need to uninstall the existing USB dongle drivers first. See "Reinstalling the USB Dongle Drivers" on page 46.

2. During installation, you are presented with an option: **Restrict programming of terminals to those with Read/Write Protection enabled**. This option prevents unprotected radios being deployed into the field. You may want to select this check box if you use read/write protection (see "About Read/Write Protection" on page 24).

Selecting this check box means that the programming application can only program read/write protected radios. Only select this option at installation time if it is your organization's policy to do so, and you are aware of the consequences. If you are unsure, leave this check box cleared when installing the programming application.

Selecting this check box selects and grays out the following check boxes in the **Tools** > **Options** dialog of the programming application:

- **Display status when reading, interrogating, and programming radios** check box: Displays the protection status of the attached radio (... Enabled or … Not Enabled) in the Reading Radio, Radio Interrogation, or Programming Radio dialogs when carrying out those actions.
- **Only program protected radios** check box: Displays a message and stops you from programming a radio if that radio doesn't

have read/write protection enabled.

During installation, the drivers for the USB driver dongles are also installed.

A quick way of checking that the USB dongle drivers installed correctly is to insert a dongle and check the status of its LED. If the LED is on, the drivers are working.

3. Add or remove any system key files (as required) from your System Key Files directory. See Table 1.3.

Table 1.3 System key file location

Operating system	Default directory
Windows XP	`%USERPROFILE%\My Documents\Tait Applications\System Key Files`
Windows Vista/ Windows 7	`%USERPROFILE%\Documents\Tait Applications\System Key Files`

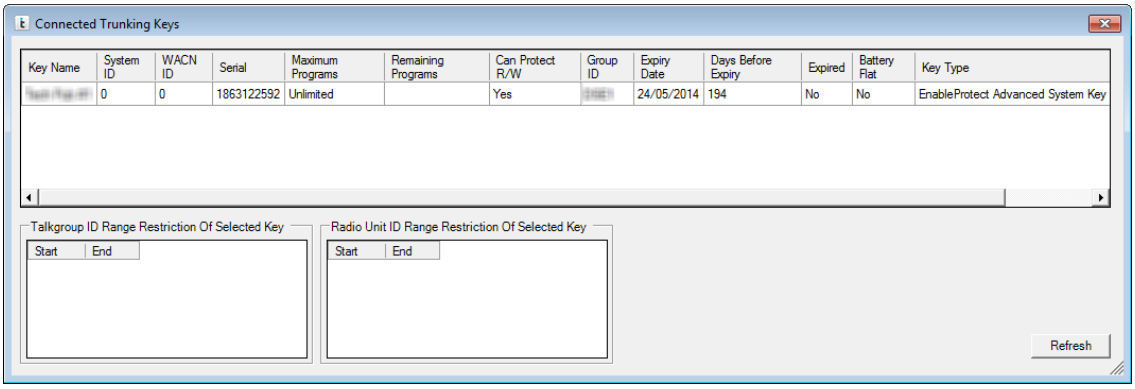
To Check that the Software Recognizes Your System Key(s)

1. Attach a dongle to a USB port on your PC.
2. Check that the relevant software recognizes the system key:

If you receive a message similar to “Could not read attached Trunking Key(s)...”, or if your firewall shows one or more messages during this time, see “Firewall Settings” on page 45.

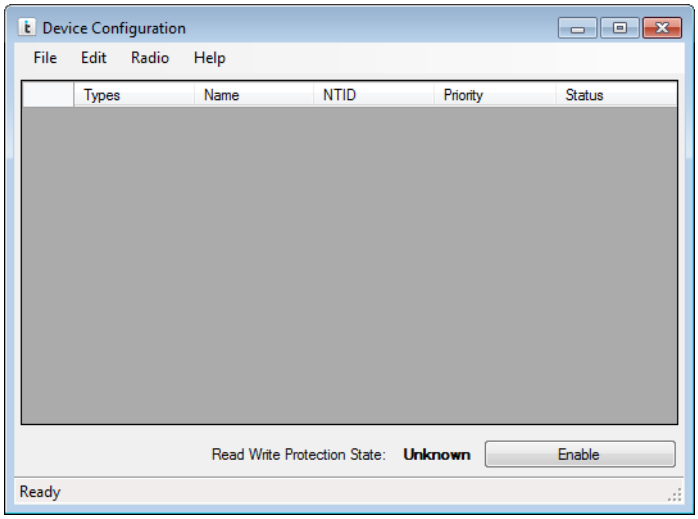
- Prime Key: from the Pass Key Configuration Utility, click the **Read Keys** button. Check that a message appears “Please attach exactly one Pass Key matching the attached Prime Key.”
- Pass Key or System Key File: from the Programming Application, click **Tools** > **Trunking Keys**. Check that the system keys are showing in the Connected Trunking Keys dialog (Figure 1.4).

Figure 1.4 Connected Trunking Keys dialog



- Pass Key with read/write protection enabled: in the programming application, click **Tools** > **Download** > **Device Configuration** > **Advanced**. Check that a “Read Write Protection State” label is showing, along with text such as Unknown (Figure 1.5).

Figure 1.5 Device Configuration dialog



1.6 Repairing and Servicing Protected Radios

If you use system keys to protect programming and/or programming data, you should consider how servicing and repair tasks will be carried out.

If read/write protection is enabled on radios, you must supply the intended repair or service center with at least one pass key per system or organization that they are likely to receive radios from. This enables those centers to perform tasks such as calibrating radios, upgrading firmware, and backing up programming data to disk in case that data needs to be reprogrammed.

If you use P25 trunking protection but no read/write protection, repair or service centers don’t require a system key. The center (if required) can reprogram a radio under repair as follows:

1. Read the radio and save the radio’s programming file. If the radio can’t be read, the center must request a file from the customer.
2. Repair the radio.
3. Re-program the radio with the file from step 1.

2 Trunking Protection

2.1 About P25 Trunking Protection

Trunking protection protects against unauthorized use of a P25 trunking network. It is already enabled in the programming application, and you must use an Tait EnableProtect pass key, a system key file, or an already set-up programming file to enable you to program P25 trunking-related settings. If you do not have a relevant system key or a preconfigured programming file, you can't configure radios for use on a P25 trunking network.

Features of P25 trunking protection include:

- Preprogrammed WACN and System ID authorized by Tait that cannot be changed
- Access to add or change P25 trunking channel profiles
- Protection against cloning radios
- Restricted talkgroup entry using Talkgroup ID ranges (Tait EnableProtect Advanced System Keys only)
- Restricted radio Unit ID entry using Unit ID ranges (Tait EnableProtect Advanced System Keys only)
- Configurable pass key expiry date (Tait EnableProtect Advanced System Keys only).

ⓘ A user can still program trunked radios without a system key. However, they must first open a programming file or read a radio with a channel profile already set to P25 trunking and trunking-related settings already configured (those settings are grayed out and read-only). If the channel profile was created using a pass key (or if anti-cloning is enabled), fields that must be preconfigured include the P25 radio ID and talkgroups. In addition, if anti-cloning is enabled, a user can't program a radio with a non-matching serial number (see "About Anti-cloning" on page 22).

If there is more than one system key, the **Home System ID** field (P25 Trunking form) becomes a selectable list. To associate a system key with a channel profile, you must select the relevant home system ID from the list.

2.2 About Anti-cloning

Anti-cloning prevents someone obtaining a radio's data (by either opening a configuration file or reading a radio), programming that data into a different radio, and using that radio on the original radio's P25 trunking network. You can enable or disable anti-cloning in a radio's programming database, and set it per channel profile on the P25 Trunking form using the **Anti Cloning** check box. Unless there is a good reason not to, you should always enable anti-cloning.

If a radio has anti-cloning enabled, and someone reads that radio or opens the radio's configuration file, the availability of certain fields and behavior of the programming application depend on whether or not the PC has a matching system key.

- Without a matching system key: the **P25 Radio ID** field (**Channel Profiles** > **Basic Settings** form), **Talkgroup Lists** form, and the radio **Serial Number** (**Specifications** form) are grayed out and disabled (along with all other P25 trunked settings).
  In addition, the programming application checks the serial number of the attached radio at programming time and only programs the radio if the programming application serial number matches the radio.
- With a matching system key: all P25 trunked settings and related ID fields are editable. The **Serial Number** field is also editable, so you can set up configuration files for users who want to program radios but do not have a system key. When you save configuration files, make sure you also change the **Serial Number** (**Specifications** form) to match the radio that the file is intended for. Alternatively, use the programming application's FleetPro feature (via **Tools** > **Fleet Configuration**) to generate multiple files, which will change the serial number automatically.

ⓘ Changing the serial number is only reflected in the saved configuration file (and subsequently used for anti-cloning checks). The serial number is never programmed to the radio.

2.3 Setting Up P25 Trunking Protection

Information for System administrators

Before distributing system keys, your organization should ensure that it has system key management policies and procedures in place. These should answer questions such as "How many keys are needed?", "How will pass keys be reconfigured when they expire?", "How will system keys be stored?" and "What actions must we take if a system key or radio is lost or stolen?"

1. Order the required system key(s) from Tait. See "Ordering System Keys" on page 14.
2. When you receive the key(s), enter the relevant details into your system key register (such as a spreadsheet or database).
   See "Recording and Identifying System Keys" on page 17.
3. If configuring and distributing pass keys:
   a. Use the Pass Key Configuration Utility to configure the pass keys. See "Configuring a Pass Key" on page 28.
   b. For each pass key you configure, update your system key register with information such as the key name, the group the key is for, the key expiry date, and password (if set).
   c. (Optional) Write the group and/or system information onto the white plastic label provided, and attach it to the pass key using the split ring.
4. Distribute system keys to users who are authorized to program or manage radios on your network (such as radio shops or dealers), along with:
   - information about how to install the software and drivers (see "Installing the Software and USB Dongle Drivers" on page 18)
   - information about how to use the programming application, including password information (if relevant) (see "Using a System Key to Program a Radio or Save to File" on page 33)
   - information about system key policies
   - a programming application template for your P25 trunking system
5. Store any USB dongles that you don't distribute to users (such as prime keys) in a secure location, according to your organization's policy.

3 Read/Write Protection

3.1 About Read/Write Protection

Read/write protection prevents unauthorized users from accessing or modifying all configuration data stored in radios (including analog and conventional channel profiles, and radio personality settings). The authorization challenge for this protection is handled by radio firmware, and must be first enabled in radios. Read/write protection is useful if you want to provide protection for non-trunked P25 radios (for example, P25 conventional or DMR radios), or if you want a greater level of protection than P25 trunking protection alone.

System key files cannot be used to enable read/write protection or program read/write protected radios. Only a correctly-configured pass key (via a prime key) provides this functionality.

Read/write protection on radios is enabled using a pass key's Group ID. The Group ID is also used during the authentication challenge when accessing configuration data. Therefore all pass keys used for read/write protection in an organization (or a group within an organization) must share the same Group ID.

Once read/write protection is enabled for a radio, other users such as technicians in the field must have a valid pass key (with matching Group ID) attached to perform the following tasks:

- Read the radio (Programming and Calibration Applications)
- Interrogate the radio (Programming and Calibration Applications)
- Program the radio (Programming and Calibration Applications)
- Calibrate the radio (Calibration Application)
- Upgrade or downgrade firmware for the radio (**Tools** > **Download**)
- Download system configuration tables (**Tools** > **Download** > **Device Configuration** > **Advanced**)
- Enable software features on the radio (**Tools** > **Optional Features**)

You can only enable read/write protection on radios with boot code 2.06 or higher. Because the boot code isn't included as part of the firmware upgrade procedure, it isn't easy to upgrade radios with an earlier version of boot code to support read/write protection. Contact Tait if you are unsure whether or not your radio firmware has a boot code version that supports read/write protection.

3.2 Setting Up Read/Write Protection

Information for System administrators

1. Order at least one prime key from Tait, along with one or more pass keys. See "Ordering System Keys" on page 14.

2. When you receive the keys, enter the relevant details into your system key register (such as a spreadsheet or database). See "Recording and Identifying System Keys" on page 17.

3. Use the Pass Key Configuration Utility to configure the pass keys. Make sure you select the **Allow Enabling of Read/Write Protection** check box on at least one pass key (this is cleared by default). See "Configuring a Pass Key" on page 28.

4. For each pass key you configure, update your system key register with information such as the key name, and the group the pass key is for.

5. (Optional) Write the group name onto the white plastic label provided.

6. Use a pass key (with **Allow Enabling of Read/Write Protection** configured) and the Device Configuration option (via **Tools** > **Download** in the programming application) to enable read/write protection for all deployed radios. See "Enabling Read/Write Protection on Radios" on page 26.

You may need this step to be completed by another party (such as a radio installer). In this case, send that party one or more pass keys along with all other relevant information (such as how to install the software and how to use the pass key to enable read/write protection on radios).

7. Send pass keys (with the same Group ID as the pass key in step 6) to users who are authorized to read and program radios, along with information on how to:
   - install the software and drivers, including whether or not to select the installation option **Restrict programming of terminals to those with Read/Write Protection enabled** (see "Installing the Software and USB Dongle Drivers" on page 18)
   - use the pass key to program radios, including how to enter a pass key password if relevant (see "Using a System Key to Program a Radio or Save to File" on page 33
   - safely store the pass key

8. Store any USB dongles that yo don't distribute to customers (such as prime keys) in a secure location, according to your organization's policy.

3.3 Enabling Read/Write Protection on Radios

Information for System key end users

Read/write protection must be enabled on radios for the read/write protection feature to work. To enable read/write protection on radios, you must have a pass key with **Allow Enabling of Read/Write Protection** configured. To remove read/write protection from radios, you must have a pass key with **Allow Disabling of Read/Write Protection** configured. For more information, see "Configuring a Pass Key" on page 28.

This procedure applies to portable radios and all mobile radios, including radio systems such as terminal repeaters, and dual-head and dual-body mobile radios. For radio systems, the devices must be assigned unique network addresses (NTIDs) and must be connected together. For more information, click the **Help** menu of the Tait Firmware Upgrade Tool.

Before using the USB dongle, you must install the correct software and drivers. For more information, see "Installing the Software and USB Dongle Drivers" on page 18.

1. Connect the radio to your PC and a reliable power source, and turn the radio on. If the power source is a battery that is not fully charged, place the radio and battery in a charger and turn the charger on. For dual head radios, connect the primary control head to your PC.

You must ensure that power and cable connections are securely fastened throughout this process, and that power is uninterrupted.

2. Attach a valid pass key (black USB dongle, with **Allow Enabling of Read/Write Protection** configured) to a USB port on your PC. Contact the radio owner or Tait if you don't currently have a valid USB dongle.
3. Open the Firmware Upgrade Tool by clicking **Tools** > **Download** from the programming application, or via the **Start** menu.
4. Click **Device Configuration** > **Lock Terminal**.

   If this option is not available, see "The Lock Terminal and Unlock Terminal options are grayed out" on page 45.
5. Enter the password for the pass key (if applicable), and click **OK**.
6. If successful, the status bar indicates "Terminal Locked Successfully".

As an additional check that read/write protection is successfully enabled, remove the pass key, exit the **Device Configuration** dialog,

and attempt to read or program the radio. You should receive the message: **Unable to access security key**.

Removing Read/ Write Protection From a Radio

1. Connect the radio to your PC and a reliable power source, and turn the radio on. If the power source is a battery that is not fully charged, place the radio and battery in a charger and turn the charger on.

You must ensure that power and cable connections are securely fastened throughout this process, and power is uninterrupted.

2. Attach a valid pass key (black USB dongle, with **Allow Disabling of Read/Write Protection** configured) to a USB port on your PC. Contact Tait or the radio owner if you do not currently have a valid USB dongle.

3. Open the Firmware Upgrade Tool by clicking **Tools** > **Download** from the programming application or via the Start menu.

4. Click **Device Configuration** > **Unlock Terminal**.

   If this option is not available see "The Lock Terminal and Unlock Terminal options are grayed out" on page 45.

5. Enter the password for the pass key (if the pass key has a password) and click **OK**.

6. If successful, the status bar will indicate "Terminal Unlocked Successfully".

4 Pass Key Configuration Utility

The Pass Key Configuration Utility is provided on a CD when you order one or more prime keys. You can use the utility, in conjunction with a prime key, to configure one or more pass keys. This utility is not required for system key files.

4.1 Configuring a Pass Key

Information for System administrators

New pass keys are preconfigured with a WACN and System ID, and Group ID. Before sending those pass keys to other users, you must configure those keys to add a maximum number of program uses and an expiry date. You may also want to add a key name and password, restrict entry of talkgroup and radio unit identities, and enable the key to enable and disable read/write protection on radios.

This information assumes you have correctly installed the Pass Key Configuration Utility from the system key CD you received along with the prime and pass keys.

For a description of what each option does, see "Pass Key Configuration Utility Reference" on page 29.

1. Click **Start** > **Tait Applications** > **Pass Key Configuration Utility** > **Pass Key Configuration Utility**.
2. Insert a prime key and a pass key into spare USB ports on your PC. Ensure that the pass key is formatted with the same Group ID as the prime key.

The Pass Key Configuration Utility requires one prime key and one pass key. If your PC has additional USB dongles, you must remove them before you click the **Read Keys** button.

When inserting the dongles, wait a few seconds for the PC to recognize them.

3. Click the **Read Keys** button.
4. Enter the password for the attached prime key and click **OK**.
5. If required, enter a pass key **Key Name**.

6. If required, enter a pass key **Password**.

   A good password includes long alpha-numeric strings with special characters. Avoid dates, known words and their reverses, and avoid reusing passwords from other system keys or other areas in your organization.

ⓘ Ensure that the Caps Lock isn't on when you enter the password, and that you enter all characters correctly.

   To remove a password, delete all ●●●●●●●●●● characters and leave this field blank.

7. Enter a maximum number of program uses for the pass key (**Max Programs**). If you don't want to set a limit on the number of times you can program radios using the pass key, select the **Unlimited Programs** check box.

8. Select a pass key **Expiry Date**.

ⓘ A shorter expiry date (for example, less than a year) and a low number of maximum program uses provides useful protection when pass keys are lost or stolen. But you must also regularly reconfigure pass keys and redistribute them to users.

9. If required, select the **Allow Enabling of Read/Write Protection** and **Allow Disabling of Read/Write Protection** check boxes (these are cleared by default). For more information, see "About Read/Write Protection" on page 24.

10. If required, click the **Add** button to enter **Talkgroup ID Ranges**.

11. If required, click the **Add** button to enter **Unit ID Ranges**.

12. Click the **Write Pass Key** button.

If successful, the status bar indicates **Pass Key successfully written**.

4.2 Pass Key Configuration Utility Reference

Information for System administrators

The window in Figure 4.6 appears when you open the Pass Key Configuration Utility. Fields become editable when you attach a prime key and pass key. Click the **Read Keys** button, and enter the correct password(s).

Figure 4.6 Pass Key Configuration Utility

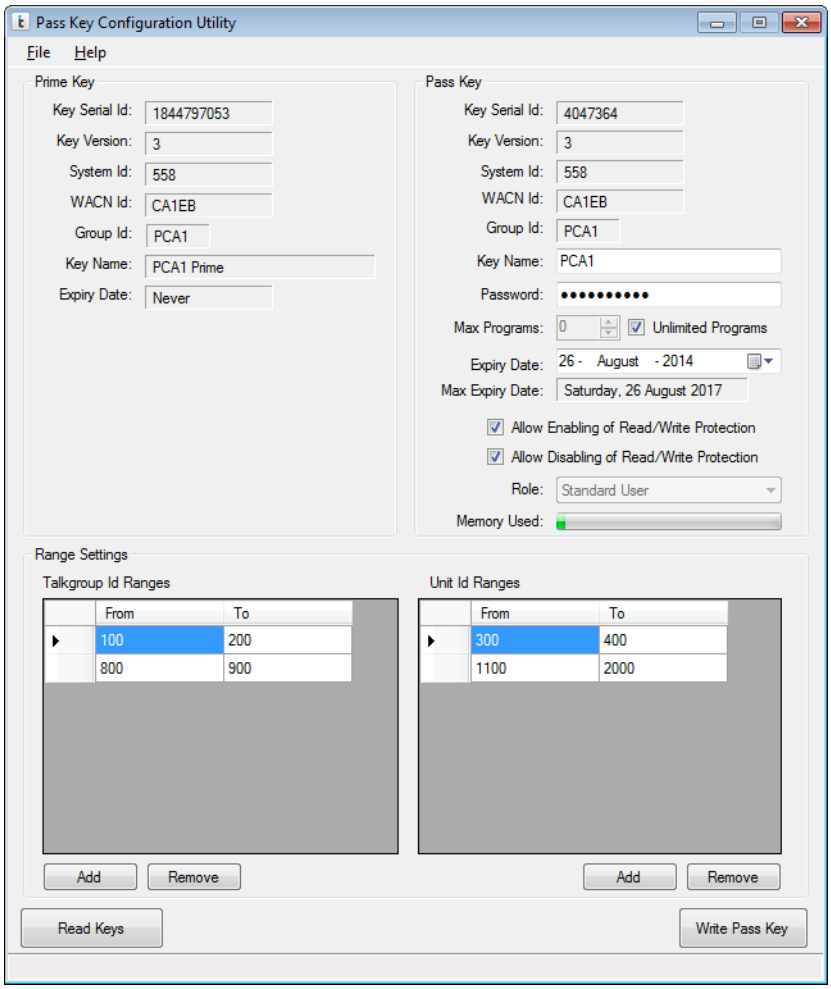


Table 4.4 describes the different labels and options available in the Pass Key Configuration Utility.

Table 4.4 Pass Key Configuration Utility options

Option	Description
Key Serial ID	The serial number and version of the prime key and pass key.
Key Version	
System ID	The system ID, WACN ID and Group ID are preconfigured from Tait, and read-only. The Group ID field must match for the prime key and pass key to be able to configure the pass key. The system ID and WACN ID are used to program P25 trunked radios. The Group ID is used to enable read/write protection on radios, and is also used during the authentication challenge that allows read/write protected radios to be read or programmed.
WACN ID	
Group ID	

Table 4.4 Pass Key Configuration Utility options

Option	Description
Key Name	The prime key name is set by Tait and is read only. You can modify the pass key name, typically to specify the dealer, customer or group within your organization that uses the pass key.
Password	Enables you to add, change, or remove a pass key password. If you set a password, you must enter it whenever you first access the pass key in a programming session (for example, when reading keys using the Pass Key Configuration Utility, or when configuring P25 trunked settings in the programming application). The password should contain alpha-numeric and other characters. If you don't want to set a password, leave this field blank. For more information, see "USB Dongle Passwords" on page 12.
Max Programs	Restricts the number of times you can use the pass key to program P25 trunking information to radios. Each time you use the pass key to program a new P25 trunking profile to a radio, or change trunked settings on a radio such as talkgroups or control channels, this number is reduced by one. The number isn't reduced if the P25 trunking profile already exists on the radio and you change a non-trunking setting, or when you subsequently program using the same key. Once the number reaches zero, you can no longer use the pass key and must reconfigure it. Enter a number between 1 and 10,000. If you don't want to limit the number of program uses, select **Unlimited Programs**. **Note**: This option doesn't apply if you only use the pass key to program read/write protected radios.
Expiry Date	The prime key expiry date is set by Tait and is read only. It can be changed up to the Max Expiry Date.
Max Expiry Date	The Max Expiry Date is either 4 years from the first time you use the pass key, or the prime key expiry date, whichever is soonest. The pass key expiry date can't be longer than this date.
Role	Sets a role for users of the TM9480 and TP9480 Programming Application. Select Standard User, 9480 Installer, or 9480 Technician. ■ Standard User: has standard rights to all non-TM9480 and TP9480 applications. ■ 9480 Installer: has restricted rights to the TM9480 and TP9480 Programming Application, but can't change fields. ■ 9480 Technician: has full rights to the TM9480 and TP9480 Programming Application, and can change fields. This option only appears in certain versions of the software, and can only be edited if the Key Version of the attached pass key is 5 or higher.

Table 4.4 Pass Key Configuration Utility options

Option	Description
Allow Enabling of Read/ Write Protection	Enables the pass key to enable read/write protection on radios. For more information, see "About Read/ Write Protection" on page 24 and "Enabling Read/ Write Protection on Radios" on page 26.
Allow Disabling of Read/ Write Protection	Enables the pass key to remove read/write protection from radios. For more information, see "Removing Read/Write Protection From a Radio" on page 27.
Memory Used	Shows a progress bar that indicates the total amount of memory currently used on a pass key. This bar is updated after a pass key is read. If the memory is full, you can't write new data to the pass key.
Range Settings (Talkgroup ID Range and Unit ID Range)	Restricts which Talkgroup IDs and Unit IDs the user can enter when configuring P25 trunking systems with the pass key. You can enter an unlimited number of ranges. However, a large number (greater than 100) may prevent you writing data to the pass key (depending on the **Memory Used** progress bar). To add a range: 1. Click the **Add** button. 2. Click a cell under **To** and enter a number. 3. Click the adjacent cell under **From** and enter a higher number. Ranges must not overlap, and ranges combine if they run into each other. ■ Talkgroup ID Range: Enter from 0 to 65,535 in each field. ■ Unit ID Range: Enter from 1 to 16,777,214 in each field.
Read Keys	Reads details from the prime key and pass key attached to your PC. If you have any more or any less than one of each, you receive an error message.
Write Pass Key	Re-configures the attached pass key with the options you have changed (such as Key Name, Expiry Date, Allow Enabling of Read/Write Protection, and Range Settings.
Status Bar	Shows "Attached keys successfully read" or "Pass Key successfully written".

5 Programming Application Information

Information for System key end und users

You need to use a system key with the programming application in the following situations:

- You need to program P25 trunked settings, or create programming files for radios that operate on a P25 trunking network.
- You need to program radios with read/write protection enabled.
- When reading a radio or opening a programming file, P25 trunked settings are grayed out (disabled) and you want to change those settings.
- When reading a radio or opening a programming file, the P25 Radio ID and talkgroup lists are grayed out (disabled) and you want to change those settings.
- When changing settings or saving a programming file, and you receive a message about trunking keys such as: “A valid trunking key must be connected...” or “A valid trunking key is not connected...”.
- When attempting to read or program a radio, you receive a message such as: “Unable to access configuration security key”, “... Response - firmware code component not authorized”, and/or “The radio rejected the request for authorization”.

If you don’t have a valid key, then you must request one from the administrator of the P25 trunking system that you are setting up, or the owner of the protected radios that you are programming. If you are the system owner or radio owner, then contact Tait to arrange keys, or to have read/write protection removed from your radio or radios.

5.1 Using a System Key to Program a Radio or Save to File

Information for System key end users

1. Install the software and drivers. See “Installing the Software and USB Dongle Drivers” on page 18.
2. If you have a pass key (black USB dongle), attach it to an available USB port on your PC.

Click **Tools** > **Trunking Keys** to check that the programming application recognizes the system key, and to check which values you can change.

If you receive a message similar to “Could not read attached Trunking Key(s)...”, or if your firewall shows one or more messages during this time, see “Firewall Settings” on page 45.

3. If a system key file is your only means of programming a P25 trunking system, make sure that you copy it to your System Key Files directory. See Table 1.3 on page 19 for the default system key file location.

You may be prompted during one of the following steps to enter a pass key password. If you don’t know the password, contact your system key administrator.

4. If you are setting up a P25 trunking system:
   a. Add a P25 trunking channel profile, and enter all relevant information for the system that the radio operates on.

The **Home System ID** and **WACN ID** fields are populated with the WACN and System ID from the system key.

   b. Select the **Anti-Cloning** check box.
   c. Ensure that the **P25 Radio ID** and **Serial Number** match the radio that the programming file is intended for, and that all talk-groups are set up correctly.

5. Change other settings as required.

The **P25 Radio ID** and **Talkgroup ID** fields may restrict what you can enter. If you go outside that range, you receive an error similar to: “Please make sure a valid trunking key is connected and the value for P25 Radio ID is in ranges as defined in the pass key.”

6. If you are saving to file, click **File** > **Save As**, or **File** > **Save As With Password**.

If you are setting up P25 trunking files for other users who don’t have system keys, make sure that each file has the correct settings for the target radio (step 4). For more information, see “About Anti-cloning” on page 22.

7. If you are programming a radio: attach the radio to your PC, turn the radio on, and click **Radio** > **Program**.

5.2 Reporting

The programming application has a Log Entries form that you can use to view system key information for a read radio or a programming file. This is useful if you want to find out the history of a radio that you suspect has unauthorized access to a P25 trunking system. The information can be viewed on screen (Figure 5.7), or printed (Figure 5.8).

Figure 5.7 Log entries form

Log Entries

Timestamp	Log Type	Logging entity	Logging data
13/11/2013 2:51:09 p.m.	Programmed with EnableProtect Advanced System Key	TM9480 2.28.0.61	Key Used:1863122592 Profile ID:2
13/11/2013 2:46:22 p.m.	Programmed with SKF	TM9480 2.28.0.61	Profile ID:3
13/11/2013 2:46:22 p.m.	Programmed with EnableProtect Advanced System Key	TM9480 2.28.0.61	Key Used:1863122592 Profile ID:2
13/11/2013 2:43:18 p.m.	Programmed with EnableProtect Advanced System Key	TM9480 2.28.0.61	Key Used:1863122592 Profile ID:2

Figure 5.8 Printed system key logs

[redacted] - 13/11/2013 2:57:47 p.m.

Specifications

Radio Unit Information
Serial Number: 19985295
Band: B1 (136-174 MHz)
Customer Information:
Enhanced Terminal: False

Log Entries

Timestamp	Log Type	Logging entity	Logging data
13/11/2013 2:51:09 p.m.	Programmed with EnableProtect Advanced System Key	[redacted] 2.28.0.61	Key Used:1863122592 Profile ID:2
13/11/2013 2:46:22 p.m.	Programmed with SKF	[redacted] 2.28.0.61	Profile ID:3
13/11/2013 2:46:22 p.m.	Programmed with EnableProtect Advanced System Key	[redacted] 2.28.0.61	Key Used:1863122592 Profile ID:2
13/11/2013 2:43:18 p.m.	Programmed with EnableProtect Advanced System Key	[redacted] 2.28.0.61	Key Used:1863122592 Profile ID:2
13/11/2013 2:41:46 p.m.	Programmed with EnableProtect Advanced System Key	[redacted] 2.28.0.61	Key Used:1863122592 Profile ID:2

You must maintain separate records if you want more detailed reporting, such as an overview of all keys distributed or a list of all radios programmed to operate on a P25 trunking network. Examples include a system key register maintained by the system administrator and a record of radios programmed maintained by a radio shop or dealer. For more information, see “Recording and Identifying System Keys” on page 17.

To Report on a Radio's Programming History

1. Connect a radio to your PC, turn the radio on, and click **Radio** > **Read**.

2. Click on the **Log Entries** form to view log information. See Table 5.7 for a description of the fields.

Table 5.5 Information on Log Entries form

Field	Description
Timestamp	Displays the time (stored in UTC format and shown in local time) that the radio was programmed.
Log Type	Displays the record type. This is either **Programmed with Tait EnableProtect Advanced System Key**, **Programmed with SKF** (system key file), or **Programmed without trunking key** if there was no system key and the programming application allowed the radio to be programmed.
Logging Entity	Displays the programming application version number used to program the radio. It can display up to 10 different version numbers.
Logging Data	Displays information such as the serial number of the pass key that was attached when the radio was programmed, and the P25 trunking channel profile that was programed using the system key.

Because log entries can be reset (if starting from a new file), or carried across (if cloning a radio or a file), only the most recent entry or entries (the first entries of the same date and time in the list) can be guaranteed to be accurate after reading a radio.

3. Print or save the information if required:
   a. Click **File** > **Print**.
   b. Select the **Log Entries** form check box (if not selected already), and the **Specifications form** check box (so you know the serial number of the radio that the log entries apply to).
   c. Click **Save as XML**, or **Print**.
   - If saving as XML, enter a filename and select a location for the file, and click **Save**.
   - If printing, select the printer to 'print to', configure other print options if necessary, and click **Print**.

6 Frequently Asked Questions

The following answers relate to some of the more common system key-related questions. They cover General Information, Security, Ordering System Keys, About the Hardware, and Using the System Keys and Software.

6.1 General Information

What is Tait EnableProtect Advanced System Key? The Advanced System Key provides secure hardware protection against unauthorized use of a P25 trunking network, and/or protection against reading and programming radios.

Is Tait EnableProtect Advanced System Key right for my organization? The Advanced System Key is the most secure method of protecting P25 trunked network data. If network protection is important to you, and you want it to be as secure as possible, then using USB dongles is the best solution.

Are there any alternatives to the Advanced System Key? For P25 trunking protection, you can use system key files to create programming files or program radios directly. For configuration security (as an alternative to or in addition to read/write protection), you can add password protection to programming files using **File** > **Save As With Password**.

What is a prime key? The prime key is a red USB dongle, which Tait supplies preconfigured with a Group ID, WACN and System ID, and expiry date. The prime key enables a system administrator to configure one or more pass keys. It does not enable access to P25 trunking data on its own.

What is a pass key? A pass key is a black USB dongle, which enables a user to configure a radio for use on a particular network, to enable read/write protection on radios, and to read or program a read/write protected radio.

What is a system key file? System key files are software files and the legacy method of programming P25 trunked radios. They are still supported as an alternative to Tait EnableProtect Advanced System Key. After you have saved a system key file to the system key files directory, you can use it to program radios or set up programming files for use on a P25 trunking system.

Can I use system key files at the same time as pass keys? Yes. However, if you have replaced system key files with pass keys, you should remove existing system key files from all PCs for security reasons.

What is a hardware system key? A hardware system key is a purple USB dongle, and is provided from Tait pre-configured with a system ID and WACN. The hardware system key allows a user to configure a trunking system in the same way as the previous simplified system key. A hardware system key is only issued by Tait in special circumstances.

6.2 Security

How secure is Tait EnableProtect Advanced System Key? The Safenet USB dongle is tamper-proof and encrypted. It uses on-chip 128-bit AES encryption and a secure communication channel when data is accessed. Read/write protection is based on authentication challenges between the radio and the programming application, which is encrypted using the Tiny Encryption Algorithm (also 128-bit).

Can a user change a radio if they don't have a system key? If the radio has read/write protection enabled, the user can't read or program the radio without a valid pass key. Without read/write protection, P25 trunked settings are grayed out and can't be changed, but the user can still change non-trunked settings, such as personality settings and conventional profiles.

Can someone with an advanced system key for someone else's system program settings to work on my system? No, prime keys, pass keys and system key files are preconfigured with a WACN and System ID, which determine what you can program radios with.

Can I remove read/write protection once enabled? Yes, you can configure one or more pass keys to 'Allow Disabling of Read/Write Protection', which means read/write protection can be removed from a radio via **Tools** > **Download**, then **Device Configuration** > **Unlock Terminal** from the programming application.

If I use one pass key to enable read/write protection on a radio, can someone else use a different pass key to the read and program that radio? Yes, if the pass key has the same Group ID.

If one or more pass keys are lost or stolen, what can I do?
You can minimize the impact of such an event by:

- Programming a password for each pass key.
- Programming short expiry dates and a low number of 'Max Programs' into each pass key, and reconfiguring the keys regularly.
- Limiting the Unit ID range that a pass key can program. Then, if a pass key is lost, remove those Unit IDs from the network, provide a new pass key and Unit ID range, and reprogram all terminals.

If there is no read/write protection, can someone bypass security by cloning a radio? If the Anti-Cloning check box on the P25 trunking form is selected, users who don't have a matching system key can't change the

P25 Radio ID or talkgroups, and can’t program any radio with a different, non-matching serial number.

Can someone get around the 'Max Programs' feature by creating a file and then unplugging the pass key prior to programming?
Yes. To avoid this, you can implement read/write protection on radios, or regularly audit radios using the Log Entries form. You can mandate all radios to have 'Programmed with Tait EnableProtect Advanced System Key' rather than 'Programmed without trunking key'.

6.3 Ordering System Keys

How do I order initial advanced system keys? Place your sales order, along with a completed and signed Advanced System Key Request form. See "Ordering System Keys" on page 14.

How do I order more system keys in the future? Follow the same process as for the initial system keys. Even though the details are already in a secure database, additional orders must always be accompanied by an Advanced System Key Request form.

Can I order pass keys preconfigured with a password or short expiry date directly from Tait? Pass keys are preconfigured with a WACN and System ID. Other settings (such as a password and customized expiry date) can only be configured in the field using the prime key with your network information.

Can I order more than one prime key, so that multiple users can configure pass keys? Yes, you can have as many prime keys are you want, all with the same Group ID.

Can people order system keys directly from the manufacturer (Safenet)? No, the USB dongles contain an encrypted vendor code that is unique to Safenet and Tait. That code is not shared with any other party.

What stops someone else ordering a pass key for my system? Orders for all system keys must be accompanied by a completed and signed Advanced System Key Request form. Tait checks and verifies these details, and keeps a copy of the form on file.

Can I still order system key files? Yes, use the same Advanced System Key Request form as for prime and pass keys. Once Tait verifies the request, we will send you the relevant system key file.

6.4 About the Hardware

Who makes advanced system keys, and where can I find model numbers, web site info, and technical specs? The supplier of the advanced system keys is Safenet (previously Aladdin). The model is Sentinel HASP HL (Pro, NetTime or Time) for early model keys, and Sentinel HL (NetTime or Time) for later model keys. For information, brochures and technical specifications, see www.safenet-inc.com.

Can someone identify the manufacturer, part number, and system information for a system key? Prime keys and pass keys bear identification text such as the manufacturer and model (for example "HASP HL"). Anyone can use the programming application to view information on pass keys, including WACN and System ID, Group ID and serial number.

Can I have multiple dongles on the same PC, for example, old serial HASP dongles from Tait, an iButton from Motorola, a prime key, and pass keys? Yes, if you have the available ports on your PC.

Can I use a USB hub to attach multiple dongles? Yes, you can use a USB hub to provide additional USB ports for multiple dongles.

Can I mark USB dongles so they can be identified as belonging to my system? Tait provides a white plastic label that you can mark and attach to the dongle using a split ring.

6.5 Using the System Keys and Software

Are there any other tools that can access information on these dongles? There are diagnostics utilities from Safenet that can read certain information on the dongle. However, to use these utilities, you must provide the encrypted vendor code that is unique to Safenet and Tait. Even if someone gets access, the system key information is also encrypted, and cannot be read or modified in any way by other tools.

Is there any way I can identify which radios have been programmed using a particular system key? The programming application has a Log Entries form. To see what system key was used to program a radio, read that radio using the programming application. The first entries of the same date and time list all system keys that were connected at the time of programming. Other information (such as the type of system key and pass key serial number) is under **Log Type** and **Logging data**.

Can you program a radio to operate on multiple systems, each with different system keys? Yes, if you have the relevant system keys plugged into your PC or files saved to your system key files directory when setting up the programming file. You only need the system keys for the systems you are adding or changing.

What happens a USB dongle expires? Can I reuse dongles by resetting their expiry date? Once a prime key has expired, you can no longer use it and you must order a new prime key from Tait. If a pass key was originally configured with a date less than the maximum expiry date, you can reconfigure the pass key with a new expiry date using a prime key and the Pass Key Configuration Utility. The new expiry date must be before than the maximum expiry date. If the maximum expiry date has passed, you can no longer reconfigure the pass key and must order a new key.

Does the maximum number of program uses (if configured for a pass key) reduce if I program the same radio twice? If you program the same radio multiple times (using the same pass key), the number of program uses is only ever reduced by 1.

What happens if I forget a password? If you forget the password for a pass key, you can reset it using a matching prime key and the Pass Key Configuration Utility. See "Resetting a Forgotten Pass Key Password" on page 13.

If you forget the password for a prime key and you don't have the original password email available, Tait can resend the password after you fill out and send the "Tait EnableProtect Advanced System Key Prime Key Password Request Form".

7 Troubleshooting

Problem	Solution(s)
When attempting to read or program a radio, you receive a message or messages: ■ Unable to access security key ■ ... Response: firmware code component not authorized ■ The radio rejected the request for authorization	The radio has read/write protection enabled, and you don't have a valid pass key attached to your PC or the device drivers aren't installed correctly (see "Reinstalling the USB Dongle Drivers" on page 46).
When reading a radio or opening a programming file, fields such as P25 trunked settings, the P25 Radio ID, or talkgroup lists are grayed out (disabled), or When changing settings or saving a programming file, you receive a message about trunking keys such as: "A valid trunking key must be connected..." or "Could not read attached Trunking Key(s)...".	■ You don't have a valid pass key attached to your PC or a system key file saved to the correct directory. See "Using a System Key to Program a Radio or Save to File" on page 33. ■ Attach the USB dongle to a different USB port on your PC, and then try again. ■ Your firewall may be blocking access to prime and pass keys. See "Firewall Settings" on page 45. ■ The USB drivers may not be installed correctly. Reinstall the drivers by reinstalling the application (see "Reinstalling the USB Dongle Drivers" on page 46). ■ Too many incorrect password attempts have locked the pass key (see "You have entered the wrong password too many times" below). ■ The USB dongle battery may be flat (see "About Flat Dongle Batteries" on page 46).
You enter the wrong password too many times, or when using the programming application or Pass Key Configuration Utility, you receive the message: "Too many failed attempts, Key ... locked. Try again later."	You have entered an incorrect password for a USB dongle 5 times. This is recorded in the key itself, and you can't use the key in any application for 5 minutes. After 5 minutes, repeat the steps that resulted in the message, and enter the correct password for the key (if known). If you don't know the password, contact your system key administrator, or contact Tait to discuss your options.
You receive the message in the Pass Key Configuration Utility when writing the pass key: "The data to write exceeds the memory capacity of the connected key by ... per cent."	The pass key memory (as shown in the Memory Used progress bar) is full or nearing full. Click the **Delete** button under **Talkgroup ID Ranges** or **Unit ID Ranges** to free up memory, and then try again.

Problem	Solution(s)
You receive a message when trying to use a pass key that suggests the pass key is “corrupted” or similar.	You can reset the key using the Pass Key Configuration Utility. See “Resetting a Corrupt Pass Key” on page 46.
When programming a radio, you receive the message: “Anti-Cloning is enabled for this data. The data can only be programmed to a radio with matching serial number.”	The data (from either reading a radio or opening a programming file) has anti-cloning enabled. If you don’t require P25 trunked settings, recreate the radio’s settings from a new programming file and reprogram the radio. If you require P25 trunked settings: 1. Open a file with a serial number that matches the attached radio. 2. Attach a pass key or save a system key file to your PC. Then, either: ■ Change the **Serial Number** field to match the radio ■ Clear the **Anti Cloning** check box ■ Request a file from the agency that programs radios for the P25 trunking system you want to operate on.
When reading keys in the Pass Key Configuration Utility, you receive the message: “Please attach exactly one Prime Key” or “Please attach exactly one Pass Key matching the attached Prime Key”.	You must attach one prime key, and one pass key with matching Group IDs. If you have more than one pass key or more than one prime key, remove the additional key(s). If you have a non-matching pass key, remove it and insert a pass key that matches the prime key. If you have inserted a prime key but continue to get a message, the device drivers may not be installed correctly (see “Reinstalling the USB Dongle Drivers” on page 46) or the battery may be flat (see “About Flat Dongle Batteries” on page 46).
You receive the message: “The key ... has only ... programs remaining” and/or “The key ... has only ... days before it expires.”	The pass key attached to the PC will soon become unusable. You must contact the system administrator to arrange a suitable time to either reconfigure the pass key (set a new expiry date and/or reset the number of programs), or replace the key with a new one.

Problem	Solution(s)
You receive a message that a prime key or pass key has expired, or a pass key is showing as red in the programming application's **Tools** > **Trunking Keys** dialog.	For pass keys, you must return the key to your system administrator who may be able to reconfigure it, or alternatively will replace your key with a new one. If a prime key expires, you must order a new key from Tait.
The **Lock Terminal** and **Unlock Terminal** options are grayed out (Under the **Tools** > **Download** > **Device Configuration** menu)	Hover over the text and read the message. If it says "There are no valid keys connected" or "... drivers are not installed", ensure that you have attached a correctly-configured pass key (with the **Allow Enabling of Read/Write Protection** and **Allow Disabling of Read/Write Protection** check boxes selected), and that you have installed the correct drivers (see "Installing the Software and USB Dongle Drivers" on page 18). For dual head or dual body mobile radio systems, you must enable read/write protection manually using **Device Configuration** > **Advanced**. For more information, click the **Help** menu in the Tait Firmware Upgrade Tool.

7.1 Firewall Settings

You may receive a message when the software is accessing a prime key or a pass key similar to: "Could not read attached Trunking Key(s)...". If you use a firewall other than Windows® Defender, this message may indicate a firewall problem. To solve this issue, try one or more of the following:

- If your firewall requests access to IP 127.0.0.1 (the computer's network loopback function), or software relating to Tx9100 or Sentinel HASP, click **Allow** or **Accept**.
- Check that your firewall has a rule that permits local loopback—specifically, that remote IP 127.0.0.1 is in your firewall's trusted zone or equivalent.
- Add "C:\Windows\System32\hasplms.exe" to your firewall's safe list or equivalent.
- Allow incoming connections on port 1947 (UDP and TCP) and 1028 (UDP).

If the problem continues, refer to "Troubleshooting" on page 43.

7.2 Reinstalling the USB Dongle Drivers

If you receive a message when installing a programming application, or you cannot use Tait EnableProtect Advanced System Keys as expected, you may need to reinstall the dongle drivers.

A quick way of checking that the USB dongle drivers have installed correctly is to insert a dongle and check the status of its LED. If the LED is on, the drivers are working.

1. Open your **Windows Install/Uninstall** dialog (via **Start** > **Add or Remove Programs** or **Programs and Features**).
2. Uninstall all instances of “Sentinel Runtime” and “Sentinel HASP Runtime”.
3. Reboot your PC.
4. Install the latest version of the programming application to reinstall the drivers (see “Installing the Software and USB Dongle Drivers” on page 18).

If you continue to experience problems, contact Tait Technical Support.

7.3 About Flat Dongle Batteries

If an application cannot read a USB dongle, then the dongle’s internal battery may be flat. A battery may be flat if the dongle is nearing its four year expiry date, and:

- was previously working on the same PC and now is not
- does not work on any other PCs or with any other related applications
- is not corrupt (no message similar to “A corrupt trunking key has been detected...” appears when you access the key).

If a pass key’s battery is flat, the pass key won’t be displayed in the programming application’s **Tools** > T**runking Keys** dialog.

Dongles with a flat battery can’t be repaired, and must be replaced with a new prime or pass key. You should dispose of old dongles in an appropriate manner.

7.4 Resetting a Corrupt Pass Key

If a pass key becomes corrupt and can no longer be used to program radios, you can reset and reconfigure the key using the Pass Key Configuration Utility v1.02 or higher. Corrupt keys display a message in the programming application similar to “A corrupt trunking key has been detected...”.

1. Start the Pass Key Configuration Utility, and attach the corrupt pass key (and the matching prime key) to your PC.

2. Click the **Read Keys** button.

   The software displays the message: “The configurable data on the attached Pass Key could not be read. This key will be reset...”

3. Click **OK** to reset the key.

Resetting a key erases the configurable data (such as the read/write protection check boxes and ID ranges).

Glossary

This glossary contains an alphabetical list of terms and abbreviations related to Tait EnableProtect Advanced System Key.

Tait EnableProtect Advanced System Key

Tait EnableProtect Advanced System Key provides secure hardware protection against unauthorized use of a P25 trunking network, and/or protection against reading and programming radios.

Group ID

The Group ID is a unique alpha-numeric ID that identifies a user who orders USB dongles. The Group ID (along with the WACN and System ID if P25 trunking protection is required) is preconfigured onto each prime key and pass key.

hardware system key

A hardware system key is pre-configured with a system ID and WACN and allows a user to configure a trunking system in the same way as the previous simplified system key.

P25 Radio Unit ID

The P25 Radio Unit ID identifies the radio on a P25 system. The P25 Radio Unit ID is also known as a subscriber unit (SU) identity or SUID. This number is used as the source ID for all transmissions, and is used to register on a P25 trunking system or to individually call the radio.

Pass Key Configuration Utility

The Pass Key Configuration Utility is a software application provided by Tait for adding and modifying various settings on pass keys.

pass key

A pass key enables a user to configure a radio for use on a particular P25 trunking system, to enable read/write protection on radios, and to read or program a read/write protected radio.

PC

A PC (personal computer) is required for running Tait software and using system keys.

prime key

The prime key is a USB dongle that enables a system administrator to configure or reconfigure one or more pass keys. It does not provide access to P25 trunking data on its own.

programming application

The programming application is a Tait software tool for changing configuration data for radios.

programming file

A programming file contains all the settings configured using the programming application.

system

A system refers to a P25 trunking network. Trunking is a radio communications system that dynamically shares a number of channels

among a large number of users. This ensures equal channel loading, and achieve a greater user-per-channel ratio than conventional systems. A system is identified by its WACN and System ID.

System ID The System ID uniquely identifies a P25 system. The WACN and System ID are preconfigured in each system key.

system key The system key is software either in a file or loaded onto a USB dongle that enables P25 trunking parameters (and other settings depending on configuration) to be programmed.

system key file A system key file (SKF) is an encrypted file generated by Tait that contains the WACN and System ID of a P25 trunking system. Once saved to the system key file directory on a PC, the file enables a user to program radios or save programming files with the P25 trunking system (WACN and System ID) contained in the system key file.

system key register A system key register is a record of system keys maintained by the system administrator. It can stored in a secure database, spreadsheet or other custom application, and typically includes details of all received and distributed system keys, such as serial number, intended customer, expiry date, and password.

talkgroup A P25 talkgroup (conventional or trunked) divides users into separate groups for communication purposes. You can make a call to the currently-selected talkgroup (usually shown on the radio display) by pressing the PTT.

USB dongle A hardware device that uses a USB (universal serial bus) interface port on a PC to protect against unauthorized software use. The USB dongles used for Tait EnableProtect Advanced System Key have a microprocessor, an internal battery, and a real time clock.

vendor code The vendor code is an alphanumeric identifier that is programmed into a Safenet dongle (by Safenet) prior to distribution. This code is only shared between Safenet and Tait.

WACN ID The WACN ID uniquely identifies a P25 Wide Area Communications Network. The WACN and System ID are preconfigured in each system key.

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, enhancements, new versions and new releases of the software provided by Tait; and (iii) may contain one or more items of software owned by a third-party supplier. The term "Software" 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.

“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. 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:

http://support.taitradio.com/go/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. 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.