EnableProtect System Key

User's Guide

MTA-00020 - Issue 10 - July 2024

1 Contents

Contact Information

Tait Communications

Corporate Head Office

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

Imported into the EU by:
Tait Communications
GmbH
Strozzigasse 10/14
Vienna 1080
Austria

Imported into the UK by:
Tait Europe Limited
Unit A, Buckingway Business Park
Anderson Road
Swavesey
Cambridge, CB24 4UQ
United Kingdom

For the address and telephone number of regional offices, refer to our website: www.taitcommunications.com

Copyright and Trademarks

By using a Tait product you are agreeing to be bound by the terms of the Tait Software Licence Agreement.Please read the Tait Software Licence Agreement carefully before using this Tait product. If you do not agree to the terms of the Tait Software Licence Agreement, do not use the Tait Product. The full agreement is available at www.taitcommunications.com/our-resources/legal#Tait_Software_Licence_Agreement

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, for a complete list please check www.taitcommunications.com/our-resources/legal#Intellectual_Property

The AMBE+2™ voice coding Technology embodied in this product is protected by intellectual property rights including patent rights, copyrights and trade secrets of Digital Voice Systems, Inc. This voice coding Technology is licensed solely for use within this Communications Equipment. The user of this Technology is explicitly prohibited from attempting to decompile, reverse engineer, or disassemble the Object Code, or in any other way convert the Object Code into a human-readable form.

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 and UK WEEE Regulation 2013 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.taitcommunications.com/our-resources/compliance#WEEE. Please be environmentally responsible and dispose through the original supplier, or contact Tait International Limited.

Tait will comply with environmental requirements in other markets as they are introduced.

Preface

Scope of Manual

This manual contains information on how to configure and use system keys, i.e. system key files and Tait EnableProtect Advanced System Key (TASK) 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 manual applies to TASK prime keys and pass keys version 6.0. This version provides the ability to configure a TASK for up to 16 individual WACNs (Wide Area Communications Network) and System IDs on a single pass and prime key. To find the prime and pass key version number, see Key Version under "Pass Key Configuration Utility Reference" on page 20.

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

- TM9100, TP9100, TM9400, TP9400, TM9300, TP9300, TP9600, and TP9800 Programming Application (all versions).
- Pass Key Configuration Utility.
- Tait EnableFleet.

Warning 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 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 setup 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 instructions about the proper use of the product. This manual uses the following types of alert:

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

This alert is used when there is a hazardous situation which, if not avoided, could result in minor or moderate injury.

Notice This alert is used to highlight significant information that may be required to ensure procedures are performed correctly. Incorrectly performed procedures could result in equipment damage or malfunction.

This alert is used to highlight significant information that may be required to ensure that you perform procedures correctly, or to 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, TM9300, TM9400, TM9500, TM9700, TM9800, and TM9900 Programming Application Online Help
- TP9100, TP9300, TP9400, TP9500, TP9600, TP9700, TP9800, and TP9900 Programming Application Online Help
- Tait EnableFleet Client, Tait EnableFleet Web
- Pass Key Configuration Utility Help
- Tait Firmware Upgrade Tool Help
- Tait EnableProtect Advanced System Key - Overview (TN-2131)

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. Look for new or updated technical notes on the Tait Partner Portal.

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
10	June 2024	Added information on Version 6.0, providing the ability to configure a TASK for up to 16 individual WACN (Wide Area Communications Network) and System ID on a single pass and prime key. Moved some content to the Pass Key Configuration Utility. Updated the User's Guide name. General tidy-up.
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

1 About System Keys

System keys 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

A system key file (SKF) is an encrypted file that contains the system ID and WACN of a trunking system. The file, once saved to the system key file directory on a computer, enables a user to program radios or save configuration files with the trunking system (system ID and WACN) contained in the system key file.

If you do not have a relevant system key, you will not be able to configure radios for use on a P25 trunking network.

Tait EnableProtect Advanced System Key

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

1.1 About the Tait EnableProtect Advanced System Key

The TASK offers two types of protection: P25 trunking protection and read/write protection.

It is now possible to add multiple WACN and System ID entries on the same TASK pass key. For information on user implications, see "User tasks with different system key protection" on the next page .

P25 trunking protection is related to protecting a P25 trunking system. You can add your P25 trunking profile only if you have either a system key file or TASK configured for your P25 trunking network. For more information, see "About P25 Trunking Protection" on page 15.

> **Notice** P25 trunking protection is available for TM9100, TP9100, TM9400, TP9400, TP9600, TP9800, and TP9900 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,Tait strongly recommends removing existing system key files from all PCs for security reasons.

Read/write protection is also known as configuration security. For more information, see "Read/Write Protection" on page 18.

> **Notice** Read/write protection is available for TM9100, TP9100, TM9300, TP9300, TM9400, TP9400, TM9500, TP9500, TM9600, TP9600, TM9700, TP9700, TM9800, TP9800, TM9900, and TP9900 series radios.

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

1.1.1 User tasks with different system key protection

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.
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.

Table 1.2 Prime key and pass key comparison

	Prime Key	Pass Key
Description	Pre-configured by Tait. Using a matching prime key, system administrators can configure or reconfigure pass keys in conjunction with the Pass Key Configuration Utility (PCU). A 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.	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.

	Prime Key	Pass Key
Features	All preconfigured by Tait: • WACN/System ID • key name • password • optional expiry date	• WACN/System ID – preconfigured by Tait • key name • optional password • expiry date • maximum number of programs • read/write protection • range limits for Unit and Talkgroup ID
Users	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.	Users program radios according to the pass key's configuration. For example, a pass key may enable a user to program a P25 trunking system (identified by WACN and System ID, they are read-only and preconfigured by Tait), trunked radio Unit IDs within a range, and trunked Talkgroup IDs within a range. System key end users and users without a system key read and program radios that have read/write protection enabled.
Appearance	Red USB dongle 	Black USB dongle 

1.1.2 USB Dongle Expiry

Due to the internal battery, USB dongles have a specified shelf life of four years. To ensure the dongles are always operational when required, they need to be replaced within that four-year period.

Both prime keys and pass keys have a real-time clock and support a programmable expiry date to force replacement.

For more information, refer to PCU > Help > USB Dongle Expiry.

1.1.3 USB Dongle Passwords

For more information, see Passkey Configuration Utility > Help.

Prime key password

The prime key password is set by Tait. This password cannot be changed.

Pass key passwords

Pass key passwords are optional.

To set, reset, or remove a password, access the Passkey Configuration Utility:

- To set a password for a new pass key, go to Help > Configuring a Pass Key.
- To reset or remove a password, go to Help > USB Dongle Passwords.

To avoid issues with forgotten passwords, record all new or recently changed passwords in a safe location such as a system key register. See "Recording and Identifying System Keys" on the facing page.

1.2 About System Key Files

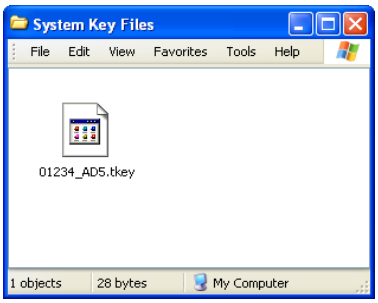
System key files are still supported by the programming application and are preconfigured by Tait to provide access to a trunking system only.

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 13) 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 Upgrading to Version 6.0

For TASK to support multiple WACN and System IDs, the prime and pass keys must be provisioned for, or upgraded to, Version 6. This can only be undertaken by Tait.

To provision or upgrade your key(s), send the following to Tait:

- your existing pass and prime keys,
- completed order form V4 or later, available via Tait Map Tick the Version 6 selection box. See "Ordering System Keys" on page 33.

TASK does not support multiple Group IDs.

1.4 Recording and Identifying System Keys

Information for system administrators

When you receive a dongle or system key file, record the key type and name, date received, and intended use. For USB dongles, also record the serial number, expiry date, and password (if relevant). This is useful 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 30). Tait recommends using a system key register such as an encrypted and password-protected spreadsheet, database, or application.

You may also want to contractually require 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, or for a regular report to be sent to you .

Tait USB dongles come with a tag that you can write on 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 the System ID. This is especially relevant when 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, TP9300, TP9600, or TP9800 Programming Application.
2. During installation, you are presented with the option **Restrict programming of terminals to those with Read/Write Protection enabled**. This option prevents unprotected radios being deployed into the field. Consider selecting this checkbox if you use read/write protection (see "Read/Write Protection" on page 18).

   > Selecting this checkbox 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 checkbox blank when installing the programming application.

   Selecting this checkbox selects and grays out the following checkboxes in the **Tools > Options** dialog of the programming application:

   - **Display status when reading, interrogating, and programming radios**
     Displays the protection status of the attached radio (... Enabled or … Not Enabled) in the Reading Radio, Radio Interrogation, or Programming Radio dialog boxes when carrying out those actions.
   - **Only program protected radios**
     Displays a message and stops you from programming a radio if that radio does not

have read/write protection enabled.

3. 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.

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

Table 1.3 System key file location

Operating system	Default directory
Windows 10 Windows 11	`%USERPROFILE%\Documents\Tait Applications\System Key Files`

Checking 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:
   - Prime Key – from the Pass Key Configuration Utility, click **Read Keys**. 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. See Figure 1.1 below.

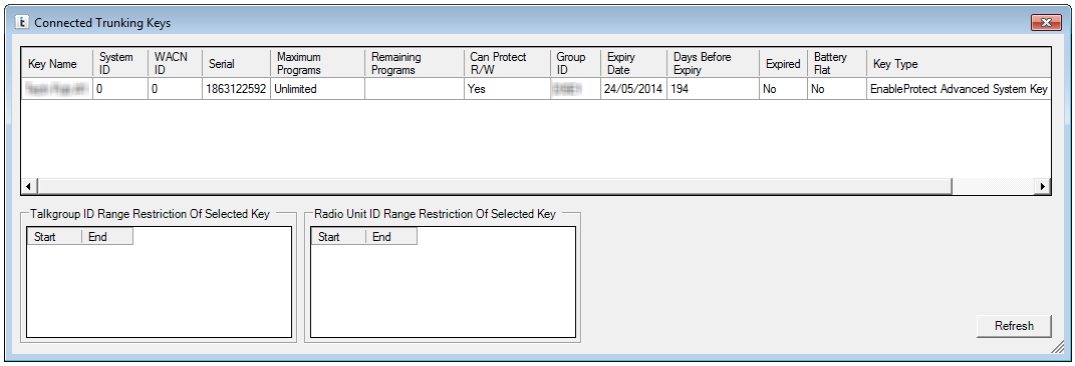


Figure 1.1 Connected Trunking Keys dialog box

   - 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. See Figure 1.2 on the facing page.

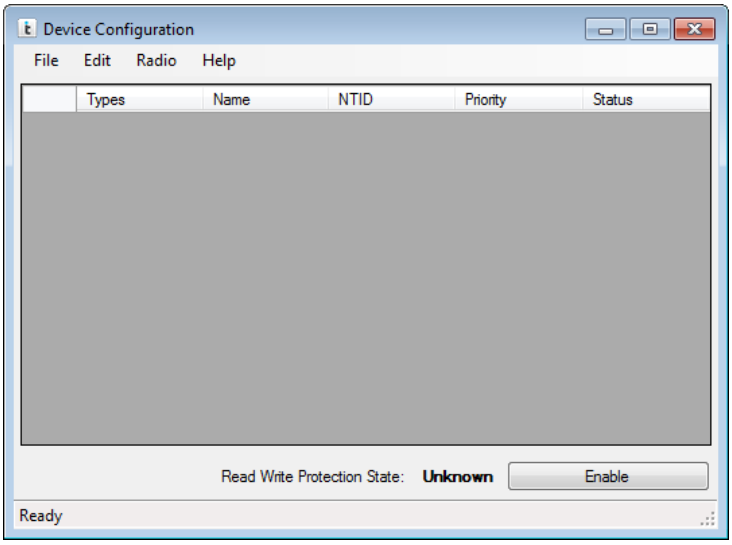


Figure 1.2 Device Configuration dialog box

1.6 Repairing and Servicing Protected Radios

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

If read/write protection is enabled:

1. Either:
    - 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.
    - provide an unlocked radio programmed with a default programming file.
2. Send to your regional Tait Office for repair.

    This enables those centers to perform tasks such as calibrating radios and upgrading firmware.

If you use P25 trunking protection but no read/write protection, repair or service centers do not require a system key. If required, the center can reprogram a radio under repair as follows:

1. Read the radio and save the radio's programming file. If the radio cannot be read, the center must request a file from the customer.
2. Repair the radio.
3. Reprogram 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 pre-enabled in the programming application.

Features of P25 trunking protection include:

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

Programming

- To program P25 trunking-related settings, you must use a Tait EnableProtect pass key, a system key file, or an already set-up programming file. See "Using a TASK to Program a Radio or Save to File" on page 28
- To program trunked radios without a system key, see "Programming Trunked Radios without a System Key" on page 29

Configuring

- To configure P25 trunking-related settings, you must use a Tait EnableProtect pass key or a system key file, or an already set-up programming file for P25 trunking.
- You can only configure radios for use on a P25 trunking network if you have a relevant system key or a preconfigured programming file.

If there is more than one system key, the programming application will check which system key file and TASK are available. The **Home System ID** field (P25 Trunking form) will provide details of the available WACN and System IDs. You can select the one you wish to use.

2.2 About Anti-cloning

Anti-cloning prevents someone obtaining a radio's trunking data. Unless there is a good reason not to, always enable anti-cloning.

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** checkbox.

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 following are grayed out and disabled, along with all other P25 trunked settings:
        - the P25 Radio ID field (Channel Profiles > Basic Settings form)
        - all talkgroups on the Talkgroup Lists form
        - the radio Serial Number (Specifications form).
    - 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, the following fields are editable:
    - all P25 trunked settings and related ID fields
    - the Serial Number field, so you can set up configuration files for users who want to program radios but do not have a system key.

> Changing the serial number is used to check anti-cloning and is only reflected in the saved configuration file. The serial number is never programmed to the radio.

For more detail on saving P25 radio configurations and anti-cloning, refer to the Help in the latest P25 Terminals Programming Application.

2.3 Setting Up P25 Trunking Protection

Information for system administrators

1. Ensure your organization 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?".
2. Order the required system key(s) from Tait. See "Ordering System Keys" on page 33.

3. When you receive the key(s), enter the relevant details into your system key register. See "Recording and Identifying System Keys" on page 12.
4. If configuring and distributing pass keys:
    a. Use the Pass Key Configuration Utility to configure the pass keys.
    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.
5. 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 12
    - information about how to use the programming application, including password information, if relevant. See "Using a TASK to Program a Radio or Save to File" on page 28
    - information about system key policies
    - a programming application template for your P25 trunking system.
6. Store any USB dongles that you do not distribute to users 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
- 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. As the Group ID is also used during the authentication challenge when accessing configuration data, 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 be able to:

- 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 is not included as part of the firmware upgrade procedure, it is not easy to upgrade radios with an earlier version of boot code to support read/write protection. Contact your regional Tait Office 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 33.
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 12.
3. Use the Pass Key Configuration Utility to set up read/write protection.

4 Pass Key Configuration Utility

To configure one or more pass keys, use the Pass Key Configuration Utility in conjunction with a prime key.

The Pass Key Configuration Utility:

- can be downloaded from the Tait Partner Portal
- is not required for system key files.

For more information, click **Start > Tait Applications > Pass Key Configuration Utility > Pass Key Configuration Utility > Help.**

4.1 Configuring a Pass Key

Information for system administrators

New P25 pass keys are preconfigured with a WACN, 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.

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

4.2 Pass Key Configuration Utility Reference

Information for system administrators

When you open the Pass Key Configuration Utility, the window in Figure 4.1 on the next page appears. Fields become editable when you attach a prime key and pass key, click **Read Keys**, and enter the correct password(s).

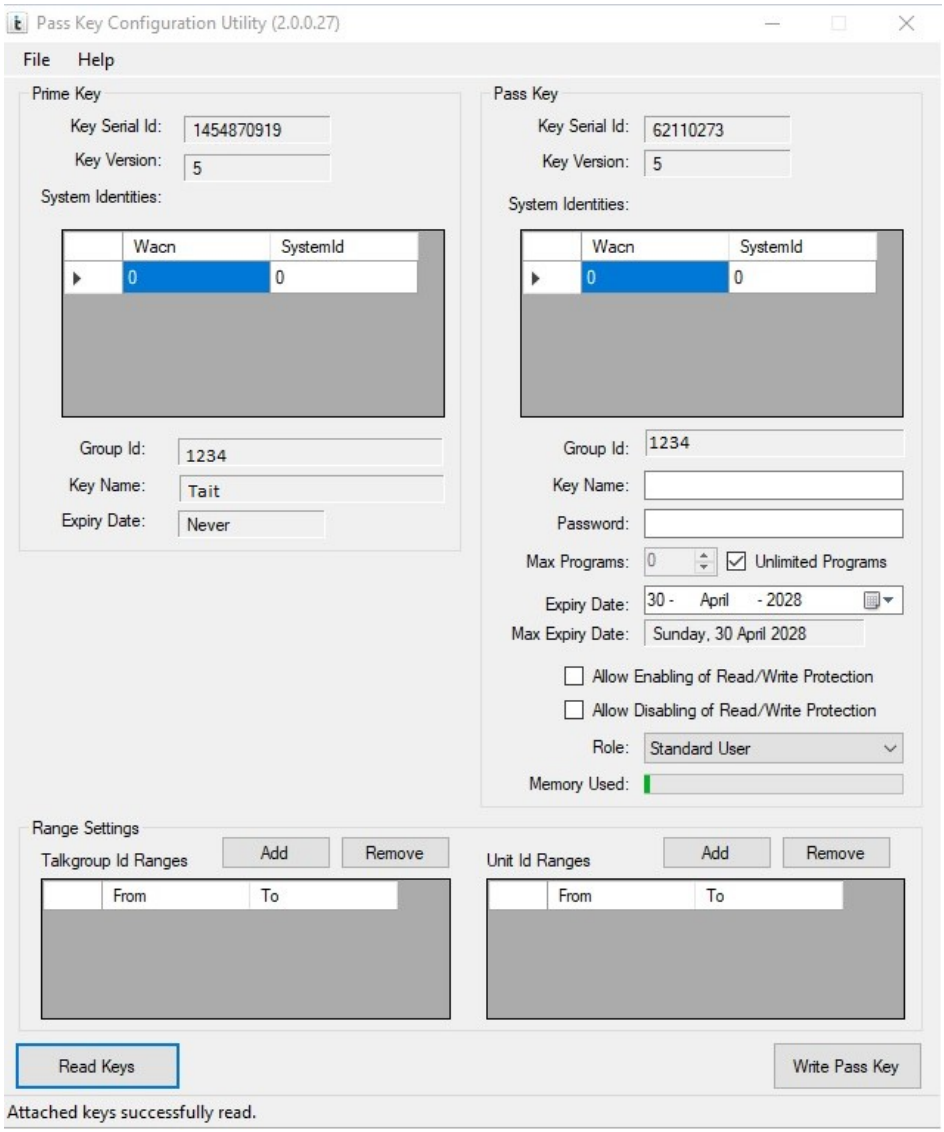


Figure 4.1 Pass Key Configuration Utility

Table 4.1 below describes the different labels and options available in the Pass Key Configuration Utility.

Table 4.1 Pass Key Configuration Utility options

Field	Option	Description
Prime key and Pass key	Key Serial Id	Prime key and pass key hardware serial number.
	Key Version	Prime key and pass key version
	System Id	Used to program P25 trunked radios. Preconfigured from Tait based on the information provided in the Tait System Key & EnableProtect Advanced System Key Request Form", and read only.
	WACN	Used to program P25 trunked radios. Preconfigured from Tait based on the information in the Tait System Key & EnableProtect Advanced System Key Request Form, and read only.
	Group Id	Used to enable read/write protection on radios, and also used during the authentication challenge that allows read/write protected radios to be read or programmed. Preconfigured from Tait based on the information in the Tait System Key & EnableProtect Advanced System Key Request Form, and read only. The Group ID field must match for the prime key and pass key, to be able to configure the pass key.
	Key Name	Prime key name is set by Tait based on the information in the Tait System Key & EnableProtect Advanced System Key Request Form and is read only. Pass key name can be modified, typically to specify the dealer, customer, or group within your organization that uses the pass key.
Prime key	Expiry Date	The prime key expiry date is set by Tait based on the information in the Tait System Key & EnableProtect Advanced System Key Request Form, and is read only. To have a previously set expiry date changed—up to the Max Expiry Date—request the latest Tait System Key & EnableProtect Advanced System Key Request Form from your regional Tait Office, fill it in and return it to Tait, together with the prime key dongle.

Field	Option	Description
Pass key	Password	To add, change, or remove a pass key password. If you do not want to set a password, leave this field blank. If you set a password, there will be a password challenge whenever you first access the pass key in a programming session. Ideally, choose a password that includes long alphanumeric strings with special characters. Avoid dates, known words and their reverses, and do not reuse passwords from other system keys or other areas in the organization. For more information, refer to Passkey Configuration Utility > Help or see "USB Dongle Passwords " on page 10

Field	Option	Description
	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 is not 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 do not want to limit the number of program uses, select **Unlimited Programs**. ⓘ This option does not apply if you only use the pass key to program read/write-protected radios.
	Expiry Date	The expiry date can be changed up to the Max Expiry Date.
	Max Expiry Date	The earliest of these options: • 4 years from when Tait manufactures the key. • the prime key expiry date.
	Allow Enabling of Read/Write Protection	Allows using the pass key to enable read/write protection on radios. For more information, see "Read/Write Protection" on page 18 and refer to Passkey Configuration Utility > Help.
	Allow Disabling of Read/Write Protection	Allows using the pass key to remove read/write protection from radios. For more information, refer to Passkey Configuration Utility > Help.

Field	Option	Description
	Role	Sets a role for users of the Programming Application. • Standard user – provides the previous standard functionality of a pass key. It allows the user to read and program a locked radio using Tait EnableFleet Client or the Tait Programming Application. • Installer – allows reading and programming a locked radio using Tait EnableFleet Client. Note that when the pass key is set to 'Installer' and the user uses the Tait Programming application to read or program the radio, the following error message appears – The connected security key does not allow this operation. • 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.
	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 cannot write new data to the pass key.

Field	Option	Description
Range Settings	Talkgroup Id Ranges	To add a range: 1. Click **Add**. 2. Click a cell under **To** and enter a number. 3. Click the adjacent cell under **From** and enter a lower number. Note that: • ranges must not overlap, and ranges combine if they run into each other. • you can enter a number from 0 to 65,535 in each field. • you can enter an unlimited number of ranges. However, if the number of ranges is greater than 100, you may not be able to write data to the pass key. This depends on the Memory Used progress bar.
	Unit Id Ranges	To add a range: 1. Click **Add**. 2. Click a cell under **To** and enter a number. 3. Click the adjacent cell under **From** and enter a lower number. Note that: • ranges must not overlap, and ranges combine if they run into each other. • you can enter a number from 1 to 16,777,214 in each field. • you can enter an unlimited number of ranges. However, if the number of ranges is greater than 100, you may not be able to write data to the pass key. This depends on the Memory Used progress bar.
	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.

Field	Option	Description
	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, Range Settings.
	Status Bar	Shows “Attached keys successfully read” or “Pass Key successfully written”.

5 Programming Application Information

Information for system key end users

You need to use a system key with the programming application when:

- programming P25 trunked settings or creating programming files for radios that operate on a P25 trunking network.
- programming radios with read/write protection enabled.
- reading a radio or opening a programming file, the following are grayed out (disabled), and you want to change those settings:
    - P25 trunked settings
    - P25 Radio ID and talkgroup lists.
- 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...”.
- 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 do not have a valid key:

- 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.
- and you are the system owner or radio owner, contact your regional Tait Office to arrange keys, or to have read/write protection removed from your radio or radios.

5.1 Using a TASK to Program a Radio or Save to File

Information for system key end users

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

1. Install the software and drivers. See "Installing the Software and USB Dongle Drivers" on page 12.
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, refer to Passkey Configuration Utility > Help.

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 13 for the default system key file location.
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** checkbox.
   c. Ensure that the **P25 Radio ID** and **Serial Number** match the radio that the programming file is intended for, and that all talkgroups 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 do not 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 16.
7. If you are programming a radio: attach the radio to your PC, turn the radio on, and click **Radio > Program**.

5.2 Programming Trunked Radios without a System Key

To program trunked radios without a system key, either:

- open a programming file
- 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, the P25 radio ID and talkgroups must be preconfigured.

If anti-cloning is enabled:

- the P25 radio ID and talkgroups must be preconfigured.
- a user has to use a matching serial number to program a radio. See "About Anti-cloning" on page 16.

5.3 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—see Figure 5.1 below—or printed—see Figure 5.2 below.

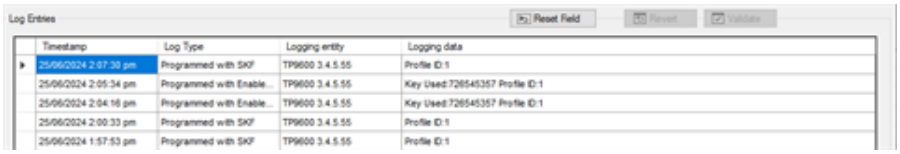


Figure 5.1 Log Entries form

TP9600 - 25/06/2024 2:09:16 pm

Specifications

Radio Unit Information
Serial Number: [redacted]
Radio Type: Standard
Band: K5
Customer Information:
Enhanced Terminal: False
Radio Name:
Band Range: 757-870 MHz
Radio Configuration Information
Radio Language: English (United States)
Standards Compliance: FCC-TIA
Configure as 110W Radio: False
Inhibit Settings
Allow Programming Mode When Inhibited: False
Allow Uninhibit via Programming: False

Log Entries

Timestamp	Log Type	Logging entity	Logging data
25/06/2024 2:07:30 pm	Programmed with SKF	TP9600 3.4.5.55	Profile ID:1
25/06/2024 2:05:34 pm	Programmed with EnableProtect Advanced System Key	TP9600 3.4.5.55	Key Used: [redacted] Profile ID:1
25/06/2024 2:04:16 pm	Programmed with EnableProtect Advanced System Key	TP9600 3.4.5.55	Key Used: [redacted] Profile ID:1
25/06/2024 2:00:33 pm	Programmed with SKF	TP9600 3.4.5.55	Profile ID:1
25/06/2024 1:57:53 pm	Programmed with SKF	TP9600 3.4.5.55	Profile ID:1

Figure 5.2 Printed system key logs

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 12.

Reporting on a radio's programming history

1. Connect a radio to your PC, turn the radio on, and click **Radio > Read**.
2. In the P25 programming application, go to Global/Conventional/P25.
3. Click on the **Log Entries** form to view log information. See Table 5.1 below for a description of the fields.

Table 5.1 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. If there was no system key and the programming application allowed the radio to be programmed, this is either **Programmed with EnableProtect Advanced System Key**, **Programmed with SKF** (system key file), or **Programmed without trunking key**.
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 programmed 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.

1. Print or save the information if required:
    a. Click **File > Print**.
    b. Select the **Log Entries** form checkbox (if not selected already), and the **Specifications form** checkbox, so you know the serial number of the radio that the log entries apply to.
    c. Do one of the following:
        - Click **Save as XML** or **Save as CSV** – Enter a filename, select a location for the file, and click **Save**.
        - 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:

6.1 General Information

Is Tait EnableProtect Advanced System Key (TASK) right for my organization?

The TASK is the most secure method of protecting P25 trunked network data. If network protection is important to you and you want your network to be as secure as possible, using USB dongles is the best solution.

Are there any alternatives to Tait EnableProtect 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**.

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.

6.2 Security

How secure is Tait EnableProtect Advanced System Key?

The Thales 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 do not have a system key?

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

Can someone with a Tait EnableProtect Advanced System Key for their 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 configuration matches the configuration originally used to lock the radio.

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 checkbox on the P25 trunking form is selected, users who do not have a matching system key cannot change the P25 Radio ID or talkgroups, and cannot 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 before programming?

Yes, but only if the pass key configuration is the same as the configuration originally used to lock the radio. To avoid someone bypassing security, 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

Who can order system keys?

Tait only supplies Tait EnableProtect Advanced System Keys and System Key Files to approved recipients.

- You can only order new keys for your own network or radios.
- You cannot order keys for someone else's system without prior approval; the request needs to come from the original owner.

How do I order initial Tait EnableProtect Advanced System Keys?

Place your order along with a completed and signed Tait System Key & EnableProtect Advanced System Key Request Form. The order can only proceed if the form is completed correctly. Tait rejects incorrectly completed forms, which delays the delivery time.

To obtain a copy of the request form, contact your regional Tait Office.

Tait thoroughly checks, verifies, and archives each system key request form and adds the details to a secure database.

How is the hardware or software delivered to me?

Tait sends the system key hardware and/or software related to your order once the order has been verified.

The TASK prime key password is delivered separately to the authorised person on the request form. This is usually via a secure medium.

What are the system key order codes?

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

How do I complete the Tait System Key & EnableProtect Advanced System Key Request Form?

Order details

Are you ordering a demo key?

Indicate the TASK version required.

If the order is for a key to use on a demo system—for example a short-term customer demo, trade show—select **Yes**. Demo keys expire after 90 days; please return them to Tait after expiry so they can be reset.

If the order is not for a demo key , select **No**. Tait will treat it as a standard purchase.

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

Indicate the TASK version required.

If the order is to replace an existing key or to add a key for a system that already uses TASKs, 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.

If you answered **Yes**, enter the 4-character TASK Group ID (if known).

- When ordering replacement or additional keys, the Group ID is not essential, but it will help Tait ensure that the correct key data file is added to the ordered keys so that they are compatible with existing keys.
- The Group ID—and WACN and System ID for P25 trunked systems—can be read from an existing key by using the Terminal Programming Application (XPA). Plug a pass key for the same system into your computer. In the programming application select **Tools > Trunking Keys**. The key information is displayed below.

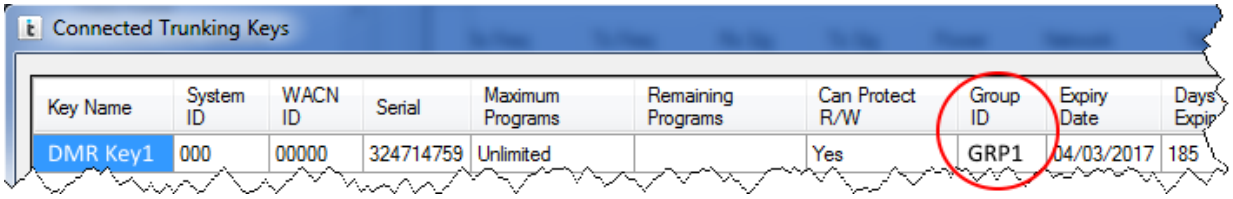


Figure 6.1 DMR TASK information in the XPA

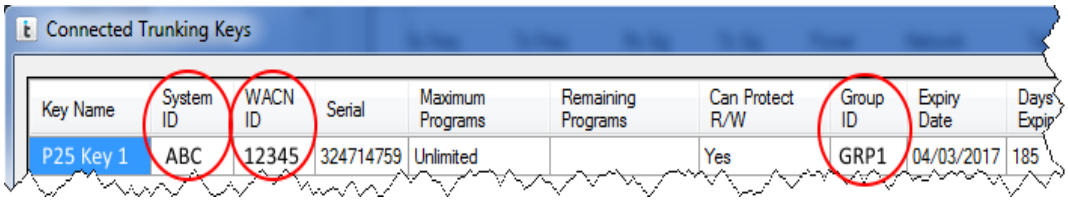


Figure 6.2 P25 TASK information in the XPA

Physical TASK key quantities

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

Enter the number of TASK Starter Kits (if any) that you want to order – most of the time, this is 1.

Prime Key (TMAA23-04)

New keys – Enter the number of prime keys (if any) that you want to order.

Reprogram existing keys – In certain circumstances you can reprogram keys to facilitate system upgrades, e.g. migrating from a non-trunked network to a trunked one. You will need prior agreement from Tait. Once agreed, enter the number of prime keys that you are returning to Tait for reprogramming.

Pass Key (TMAA23-05)

New keys – Enter the number of pass keys (if any) that you want to order.

Reprogram existing keys – In certain circumstances, you can reprogram keys to facilitate system upgrades, e.g. migrating from a non-trunked network to a trunked one. You will need prior agreement from Tait. Once agreed, enter the number of pass keys that you are returning to Tait for reprogramming.

For orders including Prime Keys

Prime key name – Tait can program a prime key with a name to help identify it. If you want to specify a name for a prime key, you can do so here – 22 characters or fewer. Otherwise, leave this section blank and Tait 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 of 4 years, and of ensuring that keys are deactivated at the end of your project.

If you do not 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

If you are ordering a system key for a P25 trunked network, enter a 5-character WACN in hex, for example A12B3. The value cannot be 00000 or FFFFF.

System ID

If you are ordering a system key for a P25 trunked network, enter a 3-character System ID in hex, for example A1B. The value cannot be 000 or FFF.

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 a TASK 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.

How do I order more system keys in the future?

For additional keys, replacement keys, lost or faulty keys, 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 a Tait System Key & EnableProtect Advanced System Key Request Form.

How do I request a key upgrade?

Return the pass and prime keys to Tait, along with the Tait System Key & EnableProtect Advanced System Key Request Form.

Even though the details are already in a secure database, key upgrades must always be accompanied by the 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 as you want, all with the same Group ID.

Can people order system keys directly from the manufacturer?

No. The USB dongles contain an encrypted vendor code that is unique to Thales 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 Tait System Key & EnableProtect 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 Tait System Key & EnableProtect Advanced System Key Request Form as for prime and pass keys. Once Tait verifies the request, they will send you the relevant system key file.

6.4 Hardware

Who makes Tait EnableProtect Advanced System Keys, and where can I find model numbers, web site info, and technical specs?

The supplier of the TASKs is Thales (previously Safenet or 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 more information, refer to www.cpl.thalesgroup.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 Thales that can read certain information on the dongle. To use these utilities, you must provide the encrypted vendor code that is unique to Thales and Tait. Even if someone gets access, the system key information is 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 when 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 "USB Dongle Passwords " on page 10.
- prime key and you do not have the original password email available, Tait can resend the password after you fill out and send theTait System Key & EnableProtect Advanced System Key Request Form.

7 Troubleshooting

Problem	Possible cause	Solution
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 do not have a valid pass key attached to your PC, or the device drivers are not installed correctly.	Refer to PCU > Help > Troubleshooting.
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 do not have either a valid pass key attached to your PC or a system key file saved to the correct directory.	See "Using a TASK to Program a Radio or Save to File" on page 28.
		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.	Refer to PCU > Help > Troubleshooting.
	The USB drivers may not be installed correctly.	Reinstall the drivers by reinstalling the application. Refer to PCU > Help > Troubleshooting.
	Too many incorrect password attempts have locked the pass key .	See “Too many failed attempts, Key ... locked. Try again later.” below.
	The USB dongle battery may be flat.	Refer to PCU > Help > Troubleshooting.

Problem	Possible cause	Solution
“Too many failed attempts, Key ... locked. Try again later.”	You entered the wrong password too many times when using the programming application or Pass Key Configuration Utility.	You have entered an incorrect password for a USB dongle 5 times. This is recorded in the key itself; you cannot 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 do not know the password, contact your system key administrator, or contact Tait to discuss your options.
“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.	Free up memory: 1. Click the **Delete** button under **Talkgroup ID Ranges** or **Unit ID Ranges** 2. Try again.
When trying to use a pass key you receive a message that suggests the pass key is “corrupted” or similar.	The battery is flat, or the pass key is damaged.	Try to read the corrupt pass key. Refer to PCU > Help > Troubleshooting > A corrupt trunking key has been detected...

Problem	Possible cause	Solution
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 do not require P25 trunked settings: 1. Recreate the radio’s settings from a new programming file. 2. Reprogram the radio. If you do 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** checkbox • 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 • one pass key with matching System ID, WACN ID, and Group ID.	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 or the battery may be flat. Refer to PCU > Help > Troubleshooting.

Problem	Possible cause	Solution
“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 expire.	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.
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.	Prime or pass key has expired.	Pass key – Return the key to your system administrator. They may be able to reconfigure it, or alternatively will replace your key with a new one. Prime key – Order a new key from Tait.
The **Lock Terminal** and **Unlock Terminal** options are grayed out. (To be found under the **Tools > Download > Device Configuration** menu.)	The pass key matching the details of the pass key that locked the radio is not detected, i.e. is not connected or present.	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** checkboxes selected), and that you have installed the correct drivers (see "Installing the Software and USB Dongle Drivers" on page 12). 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.
During installation, you receive a **Sentinel HASP Run-time installation** error or similar.		Uninstall the existing USB dongle drivers. Refer to PCU > Help > Troubleshooting.

8 Glossary

C

Configuration security

A different name for read/write protection

G

Group ID

The Group ID is a unique alphanumeric 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. It is primarily used to lock a device, provided Allow Enabling of Read/Write Protection is selected.

N

NTID

Network ID

P

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

A pass key is a black USB dongle that 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.

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.

Prime key

The prime key is a red USB dongle, which Tait supplies preconfigured with a Group ID, WACN, 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.

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.

R

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 to work.

S

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 achieves a greater user-per-channel ratio than conventional systems.

System ID

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

System key

A 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 (SKF)

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, 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.

T

Tait EnableProtect Advanced System Key

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

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 button.

Trunking

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 allows a greater user-per-channel ratio than found in conventional systems. Compare with conventional data from 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 trunking network.

Trunking key file

See System key file (SKF).

Trunking protection

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.

U

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.

V

Vendor code

The vendor code is an alphanumeric identifier that is programmed into a Sentinel HL key—provided by Thales—before distribution. This code is only shared between Thales and Tait.

W

WACN

Wide Area Communications Network

WACN ID

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