# EnableProtect | Key Management Facility
SPECIFICATIONS

# Manage encryption across your radio fleet

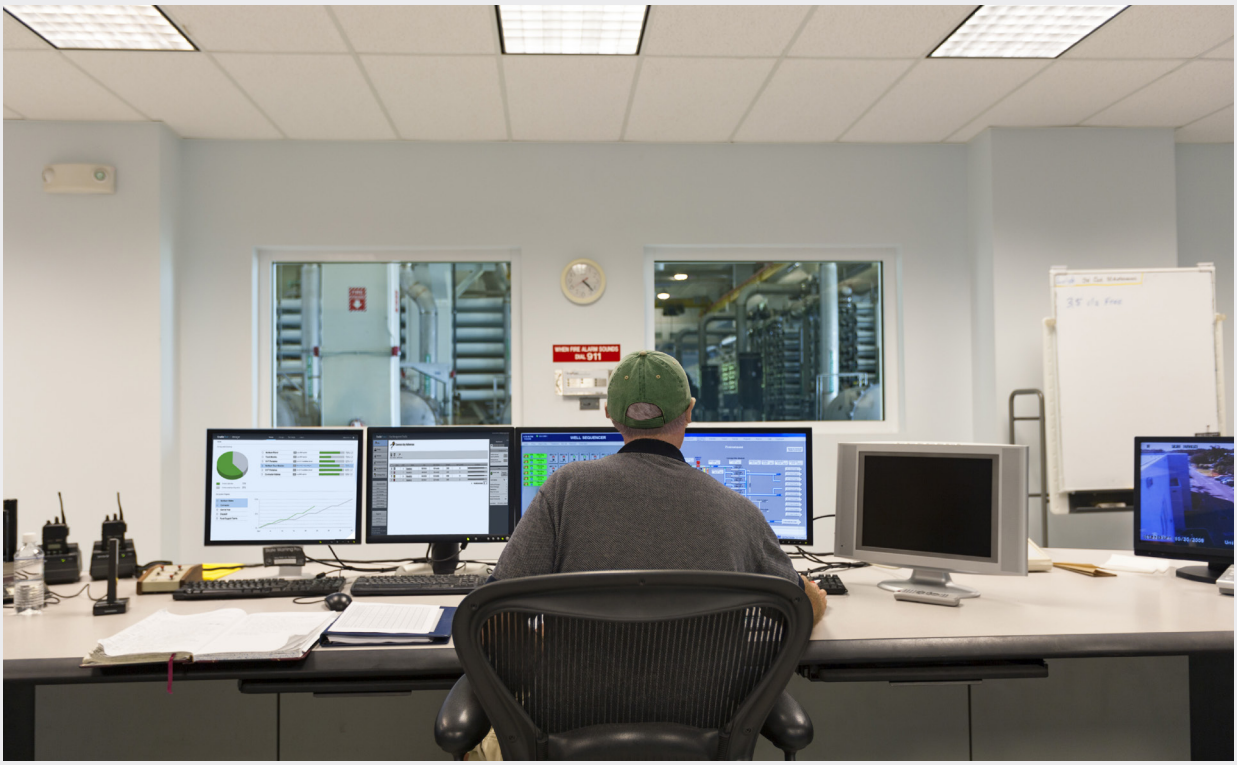
**Manage encryption across your fleet confidently and efficiently with the flexible and powerful EnableProtect Key Management Facility.**


## KEY FEATURES AND BENEFITS

- Centralized key management
- Standards compliant Over The Air Rekeying (OTAR)
- Dashboard provides clear fleet status information
- Secure intuitive web-based user interface for set and forget operation
- Remotely inhibit/permit radios

# EnableProtect | Key Management Facility

SPECIFICATIONS



### Centralized key management

The user-friendly EnableProtect Key Management Facility (KMF) brings the management of your P25 encryption into one central location, making it easier to manage and update the encryption keys used across your organization. A complete set of diagnostics across all devices allows crypto officers to troubleshoot and resolve problems remotely, saving technician time if issues occur.

The KMF is an ideal encryption management tool for networks that are geographically dispersed and/or have a large number of terminals.

### Standards compliant Over The Air Rekeying (OTAR)

The EnableProtect Key Management Facility uses industry standard cryptographic systems for OTAR. As part of a Tait conventional or trunked OTAR infrastructure solution, the efficient and easy-to-use KMF utilizes DES/AES security, which provides increased confidence in the system, and greatly reduces both RF traffic and user requests to rekey.

For terminals that cannot be reached over the air, or for tactical teams, the EnableProtect Key Fill Device can be used to distribute keys using a physical connection to the radio.

### Dashboard provides clear fleet status information

Users are able to view information the way they need to on the Key Management Facility's custom dashboard. The dashboard allows you to set up, sort and see the keys, groups, and radios you want to, as well as track Key Update Tasks, Common Key References, groups and devices that you are interested in. Other manufacturers' P25 radios can also be conveniently managed via the dashboard.

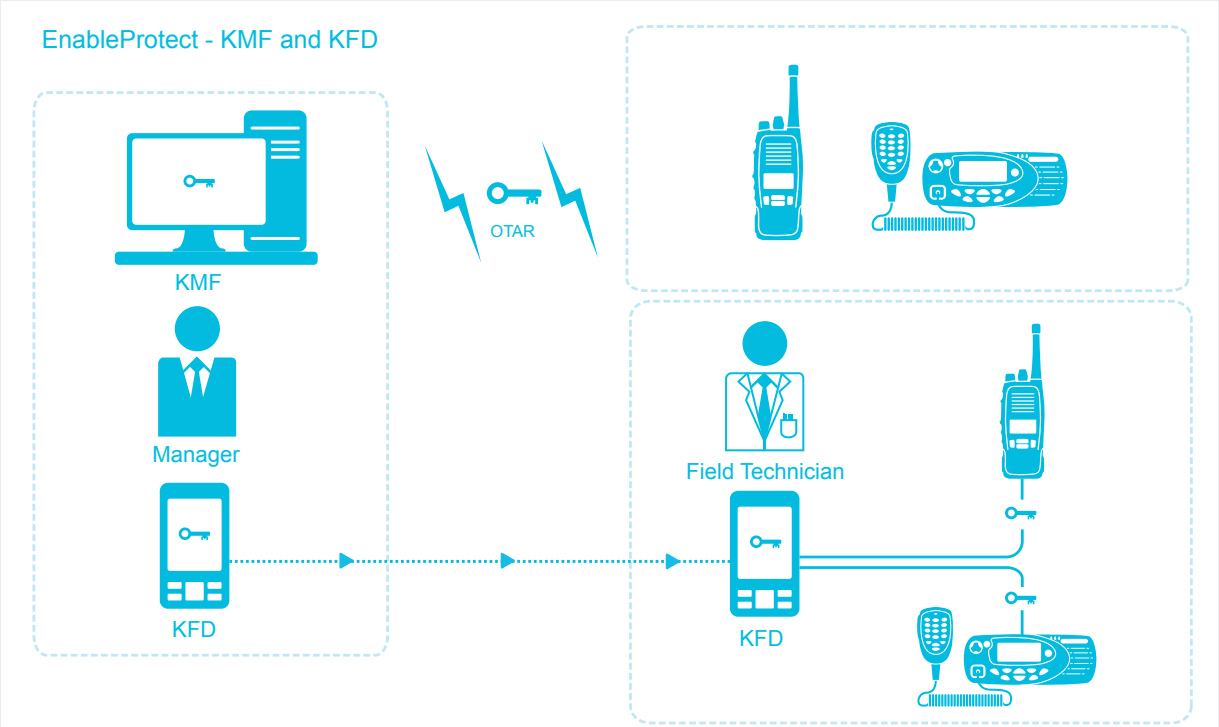
### Intuitive, web-based user interface for set and forget operation

The web-based user interface has been designed to make it easy for crypto officers to update different teams' keys when it best suits their workloads and schedules, as well as update groups of radios over the air at the press of a button.

Reminders can be set up to prompt you when keys need changing, and you can schedule and deploy Key Update Tasks to run automatically. The status bars show how current keys and update tasks are, and color coding and visual displays make decision-making clear and simple.

### Remotely inhibit/permit radios

This feature enables crypto officers to remotely inhibit a radio to prevent its use if it is not required for a period of time or has been stolen. The radio can also easily be allowed back on the network with this feature.




### Authorities

With the Key Management Facility, owners can be assigned to keys and groups, whose contact information is stored in the KMF. This helps crypto officers contact those responsible for the keys and groups if a problem arises.

### Diagnostics Tool

The EnableProtect Key Management Facility has comprehensive diagnostics that have been designed specifically to establish the state of devices on the network. You can check to see if a device is on the system, verify the keys it has and update all the keys, as well as perform a number of other diagnostic tests with this tool.

### Sectors

To make devices easier to track, they can be assigned to sectors. A sector can be a region or an agency.

### Key Update Task

With the Key Management Facility, messages are sent only to radios specified by the Key Update Task, so you do not need to address the entire fleet. You can schedule Key Update Tasks to automatically run at any time, improving your security and bandwidth use.

### Problem Devices

This unique feature makes it easy to track devices that can be contacted but cannot be updated. The Problem Device indicator is highlighted if there is any change to the list of Problem Devices.

### Redundancy

The EnableProtect Key Management Facility can be configured with multiple levels of redundancy. This feature gives users real peace of mind because they are protected against hardware and power failures with virtually no downtime.

### Unique Key Encryption Key (UKEK)

Most agencies use a Common Provisioning Key (sometimes called a “shop key”) for the UKEK in all radios. The Key Management Facility can automatically generate a truly unique UKEK for every radio. These can either be exported to a Key Fill Device for use when commissioning new radios in the shop, or the Key Management Facility can replace the Common Provisioning Key with a unique UKEK the first time a radio goes on the network.

# **Enable**Protect | Key Management Facility

SPECIFICATIONS

| GENERAL | |
|---|---|
| Server | Rack mounted server with quad-core Intel processor |
| Redundancy | Dual hot-swappable power supplies, dual RAID hot-swappable hard drives |
| Cryptographic services | FIPS certified tamper-proof hardware security module |

| SOFTWARE OPTIONS | |
|---|---|
| TKAS101 | KMF 1-150 Devices |
| TKAS102 | KMF 151-1,000 Devices |
| TKAS103 | KMF 1,001-4,000 Devices |
| TKAS104 | KMF 4,001-10,000 Devices |
| TKAS106 | KMF key export (to EnableProtect Key Fill Device) |

## TAIT COMMUNICATIONS

Our clients protect communities, power cities, move citizens, harness resources and save lives all over the world. We work with them to create and support the critical communication solutions they depend on to do their jobs.

Digital wireless communication forms the central nervous system of everything we do. Around this resilient, robust core we design, develop, manufacture, test, deploy, support and manage innovative communication environments for organizations that have to put their total trust in the systems and people they work with. We've worked hard to develop genuine insight into our clients' worlds, and have pursued engineering, operational and services excellence for more than 40 years. This understanding, and our belief in championing open-standards technology, means we can give our clients the best possible choice and value to achieve the human outcomes they're driven by.

We're not simply aligned with our clients; we're devoted to their cause.



Tait_SS_EnableProtect-KMF_A4_US_v3

Tait Limited facilities are certified for ISO9001:2008 (Quality Management System), ISO14001:2004 (Environmental Management System) and BS OHSAS 18001:2007 (Occupational Health and Safety Management System) for aspects associated with the design, manufacture and distribution of radio communications and control equipment, systems and services. In addition, all our Regional Head Offices are certified to ISO9001:2008.