June 2021
Release 4.15

Scout Encryption *Capability Guide*

Introduction

Encryption in Scout includes the process of transforming clear audio to encoded audio to send to the field and the reverse, transforming encrypted audio to clear audio to present to the dispatcher. When two subscriber units engage in an encrypted conversation and the dispatcher is monitoring the group's conversation, Scout decrypts the audio for the dispatcher to understand.

Encryption is the process of encoding audio so that only radios or consoles with the matching key and encryption algorithm can decode and present the audio to the user. Encryption prevents unauthorized listeners from eavesdropping on a conversation. Even if an eavesdropper is listening to a Scout-supported frequency, the listener does not hear intelligible information from an encrypted signal without using the matching key.

Scout offers software-based encryption for P25, Icom IDAS Multi-Site Trunking, Kenwood NEXEDGE, and MOTOTRBO™ Capacity Max, Connect Plus, IP Site Connect, and Multi-Site Capacity Plus systems. Within Scout, VPGate is the component that stores all encryption keys, encrypts the audio before transmission, and when the matching key is provided, decrypts incoming encrypted audio.

Scout's encryption technology conforms to the following standards:

- DES (Data Encryption Standard) – Published in 1977, this standard was influential in the advancement of modern cryptography. Scout supports DES for P25 and Kenwood NEXEDGE.
- AES (Advanced Encryption Standard) – Established by the U.S. National Institute of Standards and Technology in 2001. This standard supersedes DES. Scout supports AES for P25, Icom IDAS Multi-Site Trunking, Kenwood NEXEDGE, and MOTOTRBO™ Capacity Max and IP Site Connect radios.
- Enhanced Privacy – Exclusive to Motorola's MOTOTRBO™ radio systems. Scout supports Enhanced Privacy for Capacity Max, Connect Plus, IP Site Connect, and Multi-Site Capacity Plus systems.

Licensing

Scout does not require a separate license to implement encryption. Only the normal VPGate Base License and Supplemental License are needed. A separate KMF Software License is required only if the optional Key Management Facility (KMF) is to be used.

VPGate Base License – All instances of VPGate in all systems require a VPGate Base License as described in each radio system configuration or capability guide. While the VPGate Base License does not hold encryption keys or activate them, each license is associated with a single instance of VPGate. If licenses

must be swapped or moved, Avtec recommends exporting the encryption keysets and then importing them into the VPGate computer once the license is replaced and a new password is established. Otherwise, the keysets must be reloaded.

To ensure endpoint encryption capability remains operational, do not upgrade licensing or move licenses between VPGate computers without first exporting the encryption keysets. As an anti-tampering control, an electronic link exists between keys stored in Avtec's Encryption Key Manager software on the VPGate computer and the VPGate computer's licensing. Changing licensing removes the link to the encryption keyset data and causes the endpoints to lose their encryption capabilities. In this case, consoles might not transmit encrypted audio or receive encrypted audio from the radio system. However, if the original license is returned to the VPGate computer, the encryption capability returns.

> **NOTE**
> At the console level, the endpoint transmit encryption state does not persist across VPGate failovers. If an endpoint is placed into encrypted mode at a console and a VPGate failover occurs, the endpoint enters the Gone state and becomes unavailable for operation.
>
> When the endpoint returns from the Gone state, it returns in clear mode and transmits audio to the field in clear mode. The dispatcher must return the endpoint to encrypted mode, using the Clear/Encrypt Mode function pad, to transmit encrypted audio to the field.
>
> VPGate failovers have no effect on the ability to receive encrypted audio from the field if the encryption keysets are available and properly configured in the backup VPGate computer.

VPGate Supplemental License – All radio systems require a VPGate Supplemental License as described in each radio system's configuration or capability guide.

KMF Software License – Specify model number SFW-VPG-KMF or SFW-VPG-KMF-SK (software key) only if the Key Management Facility (KMF) is to be used.

Avtec's Encryption Key Manager

With digital encrypted audio, radios and consoles use keys to encrypt and decrypt the audio entering and exiting the Scout console system, which includes all Scout consoles, VPGates, and in trunked systems, the trunking controller. A key, which is a unique series of digits, controls the encryption between the Scout console system and the radio. To communicate, the keys in Scout and the keys in the radio must match.

When configuring the radio endpoint in Scout, the Scout System Administrator defines the keys the endpoint needs and the type of encryption to use through Avtec's Encryption Key Manager software (EKM). Scout provides the EKM as part of the VPGate Advanced Radio software package supplied with the system's VPGate Supplemental License. The EKM provides key data storage and enables administrators to enter keys using one or more of following methods, depending on the radio system in use:

- Manual Entry – Keys entered manually into the EKM.
- Key Fill Device (KFD) – Use of a handheld KFD to create keys and connect to the computer to load the keys to the EKM. The KFD creates keys based on its own algorithm and stores them in the device. The KFD can also load encryption keys into radios one at a time. KFDs are sometimes referred to as key loaders. The EKM is tested and approved for use with the Tait KFD and the Motorola KVL 3000 and KVL 4000 using the Tait TPA-SV-020 adapter.

- Key Management Facility (KMF) – Connecting to a KMF receives keys automatically and maintains synchronization between keys deployed to Scout and to radios. A KMF connects to the EKM over the network and connects with radios using over-the-air-rekeying (OTAR). The EKM is tested and approved for use with Tait's KMF.
-

> **NOTE**
> Use of the KMF interface requires a KMF Software License.

Once Avtec's Encryption Key Manager software holds the keys and keysets needed for encryption, the Scout System Administrator configures the radio's endpoint interface in VPGate to identify which keyset to use for the radio's encrypted communication.

Capabilities-at-a-Glance

The following table lists the encryption types and options Scout supports for each radio technology.

Radio Technology	Encryption Types	Key Creation Options	Model Number
Icom IDAS Multi-Site Trunking	AES	Manual Entry, KFD	SFW-VPG-NXDN-TRNK-XX
Kenwood NEXEDGE®	AES, DES	Manual Entry	SFW-VPG-NXDN-XX and SFW-VPG-NXDN-TRNK-XX
Motorola APX™ 4500	DES	Manual Entry	
Motorola APX™ 6500, 7500, and 8500	AES, DES	Manual Entry	
MOTOTRBO™ Capacity Max	AES, Enhanced Privacy	Manual Entry	SFW-VPG-MTCP-XXX
MOTOTRBO™ Connect Plus	Enhanced Privacy	Manual Entry	SFW-VPG-MTCP-XXX
MOTOTRBO™ IP Site Connect	AES, Enhanced Privacy	Manual Entry	SFW-VPG-TRBO-IPSC-XXX
MOTOTRBO™ Multi-Site Capacity Plus	Enhanced Privacy	Manual Entry	SFW-VPG-MTCP-XXX
P25 CSSI	AES, DES	Manual Entry, KFD, interface with KMF	SFW-VPG-P25-XXX
P25 DFSI	AES, DES	Manual Entry, KFD, interface with KMF	SFW-VPG-DFSI-XXX
P25 Privileged	AES, DES	Manual Entry, KFD, interface with KMF	SFW-VPG-P25-XXX

Related Information and Documentation

For additional information, refer to the following capability guides:

- *IDAS Multi-Site Trunking System*
- *Kenwood NEXEDGE®*
- *Motorola APX™ Mobile via Outpost*
- *Motorola APX™ Control Station via Outpost Plus*
- *MOTOTRBO™ Capacity Max*

- *MOTOTRBO™ Connect Plus*
- *MOTOTRBO™ IP Site Connect*
- *MOTOTRBO™ Multi-Site Capacity Plus*
- *P25 CSSI*
- *P25 Digital Fixed Station Interface*
- *P25 Privileged*
- *Trunking Gateway*

For information regarding configuration for Scout and encrypted radios, refer to the following resources:

- Avtec Encryption Key Manager Online Help
- *IDAS Multi-Site Trunking System Configuration Guide*
- *Kenwood NEXEDGE® Configuration Guide*
- *Motorola APX™ Mobile via Outpost Configuration Guide*
- *Motorola APX™ Control Station via Outpost Plus Configuration Guide*
- *MOTOTRBO™ Capacity Max Configuration Guide*
- *MOTOTRBO™ Connect Plus Configuration Guide*
- *MOTOTRBO™ IP Site Connect Configuration Guide*
- *MOTOTRBO™ Multi-Site Capacity Plus Configuration Guide*
- *P25 CSSI Configuration Guide*
- VPGate Online Help, Configuring Avtec Routing Controller topics
- VPGate Online Help, Trunking Gateway topics