KENWOOD

Armada Security Policies and System Keys Guide

The Armada programming software handles all Viking radios. Armada provides two features for restricting radio configuration:

- Security Policies
- System Keys

This document describes these features and how to use them. The following section gives a list of definitions and abbreviations used throughout the rest of this document. Then a high-level overview of these features is given as well as a table of supported versions. The remaining sections go into the details of Security Policies, Radio Security Devices (RSDs), and System Keys.

This manual contains the following sections:

Phone: 972-819-0700, 1-800-328-3911
EF Johnson Technologies, Inc., a JVCKENWOOD Company
www.efjohnson.com
Part Number 002-ARMADAKEYS-100 Rev 00
September 2023

1 Definitions and Abbreviations

Table 1 summarizes definitions and abbreviations used in this document.

Table 1 Definitions and Abbreviations

Item	Description
Security Policy	A collection of settings defining codeplug access permissions.
Authorization	The process performed by the user to indicate that they are allowed to edit and assign a security policy.
RSD	Radio Security Device: A secure USB Dongle.
Parent RSD	An RSD capable of modifying Security Policies with matching organization name. Formerly “Master RSD”.
Child RSD	An RSD created by Armada with a Parent RSD. It is not capable of modifying security policies. Formerly “Slave RSD”.
Master RSD	See Parent RSD; this terminology is still used in software.
Slave RSD	See Child RSD; this terminology is still used in software.
Organization Name	An optional identifier unique to an organization; may be used with a Parent RSD to gain authorization to a policy.
System Key	An authorization token needed to edit P25 and V16 trunking systems.
Soft System Key	A system key in the form of a file on a computer.
ESK	Enhanced System Key: System key stored on an RSD.
Hard System Key	See ESK.
Parent ESK	An ESK capable of editing any system parameter. Formerly “Master ESK”.
Child ESK	An ESK created by Armada with a Parent ESK. It may have restricted system editing abilities. Formerly “Slave ESK”.
Master ESK	See Parent ESK; this terminology is still used in software.
Slave ESK	See Child ESK; this terminology is still used in software.
Profile	The codeplug of a radio or template.
Unit ID	Unique identifier of a radio on a trunking system.
TG	Talkgroup of a trunking system.
AG	Announcement Group of a trunking system.

2 Overview

Security Policies and System Keys are used to restrict and prevent editing and/or viewing of certain radio parameters. Security policies are for protecting all configuration on your radios. System Keys are for protecting the configuration of your V16 or P25 system on everyone's radios.

Security Policies are a special radio configuration that goes onto the radio. Authorization is required to apply a policy to a radio and edit a policy. This is the primary way to protect a radio's configuration from being changed or even viewed by someone who is not authorized. Radios linked to a template will share that template's security policy. Security Policies may be locked by either a password or the Organization Name of an RSD.

System Keys exist outside of radios and are only used to configure V16 and P25 systems on radios and link to templates. To edit a V16/P25 system or its channels, a valid system key must be present (depending on a system's strictness rules). There are several types of system keys: soft and hard (called Enhanced System Keys or ESKs) with ESKs coming in Parent and Child variants. Child System Keys may be programmed with specific restrictions on which system parameters they may edit. A valid System Key for each V16/P25 system is required to link a template to a radio and assign a Unit ID.

Radio Security Devices (RSDs) play a role in both Security Policies and ESKs. RSDs are physical USB dongles, as shown in Figure 1. They too come in Parent and Child variants. Parent RSDs may be ordered with your organization name, which is used to create a Child RSD by assigning its organization name to a blank RSD. RSDs may also hold ESKs. Parent ESKs are fixed and cannot be changed but are used to create Child ESKs on other RSDs. An RSD can hold many ESKs. Typically, a Parent RSD will have Parent ESKs, but this need not be the case as Child ESKs from a different system can be added to an RSD with a Parent ESK. RSDs have an internal clock that can be used to enforce expiration dates.

Figure 1 Radio Security Device (RSD), the USB Dongle (Hardware May Vary)

This section contains information on the following topics:

2.1 Security Policy Release History

Table 2 outlines the feature release history of security policies.

Table 2 Security Policy Feature Updates by Armada Version

Feature Type	Feature	✓ = Available in Armada Version:		
		1.4.x-1.8.x	1.10.x-1.36.x	1.40.15 and Later
Password Policy	Read/Write Password	✓	✓	✓
RSD Policy	Read/Write Password	✓	✓	✓
	ESK to Read/Write	✓	✓	✓
	Require ESK to Edit Systems	✓	✓	✓
	Require RSD to Edit Radio password	✓	✓	✓
	Allow Uninhibit with RSD	✓	✓	✓
	Access Modes		✓	✓
Parent RSD	Expiration Date	✓	✓	✓
	Organization Name	✓	✓	✓
Child RSD	Expiration Date	✓	✓	✓
	Organization Name	✓	✓	✓
	Apply/Remove Policy			✓

2.2 System Key Release History

Table 3 provides the compatibility table of system key improvements over time.

Table 3 System Key Feature Updates by Armada Version

Feature Type	Feature	✓ = Available in Armada Version:					
		1.4.x-1.8.x	1.10.x-1.26.x	1.28.x-1.34.x	1.36.14-1.36.20	1.36.21-1.40.13	1.40.15 and Later
Soft System Key		✓	✓	✓	✓	✓	✓
Parent Key Expiration Date		✓	✓	✓	✓	✓	✓
Child ESK	Expiration Date	✓	✓	✓	✓	✓	✓
	Change ESK-Only						✓[1]
	Change Strict Rules						✓
	Unit ID, TG ID, AG ID Range Restrictions	✓	✓	✓	✓	✓	✓
	System Lockout[2]	No Editing	No Viewing or Editing	No Viewing or Editing	Cannot Edit Critical Parameters	Strict Mode Dependent	Strict Mode Dependent
	Channel Lockout[3]						
System Specific	ESK-Only			✓[1]	✓[1]	✓[1]	✓[1]
	Strictness Rules[4]	Always Strict	Always Strict	Always Strict	Always Lenient	Strict or Lenient	Strict, Lenient, or Zone/ Channel

Shaded features indicate unique operation when enabled in Armada Versions 1.36.14 through 1.36.20.

1. This feature is only available for P25 Systems.
2. If enabled, this feature restricts editing and/or viewing system data as described.
3. If enabled, this feature restricts editing and/or viewing channel data as described.
4. For Armada 1.36.20 and earlier, this feature operates as Always Strict or Always Lenient as described. For Armada 1.36.21 and later, this feature has programmable options as described.

3 Security Policies

Security Policies go with radios and restrict who can do what with that radio. Security Policies control your radios. This section first covers how to create security policies, what types exist, and what can be restricted. This is followed by how they are applied and updated to radios.

This section contains information on the following topics:

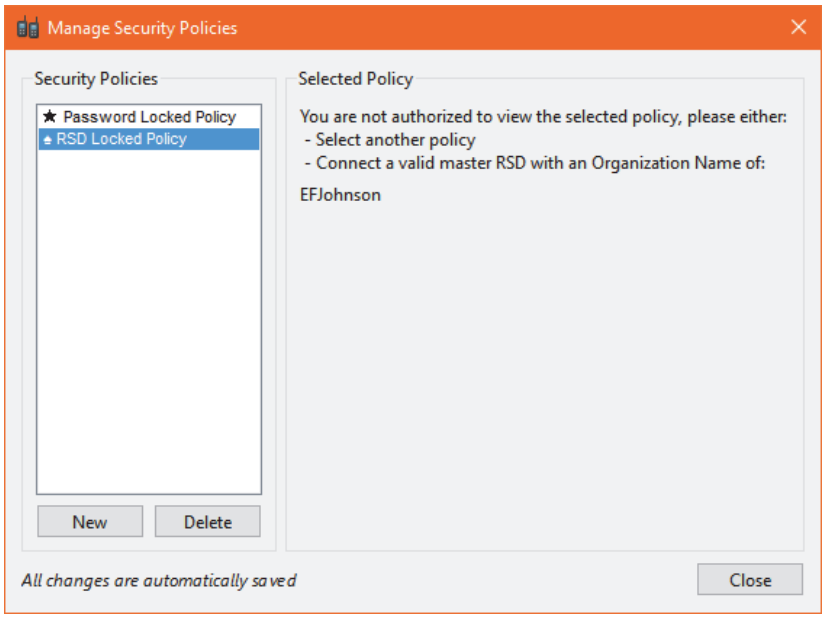
3.1 Creating and Configuring Security Policies

Security Policies come in two variants: Password protected and RSD protected.

To create or configure a Security Policy in Armada, proceed as follows:

1 Go to **Tools > Manage Security Policies.** The Security Policy Dialog appears (Figure 2).

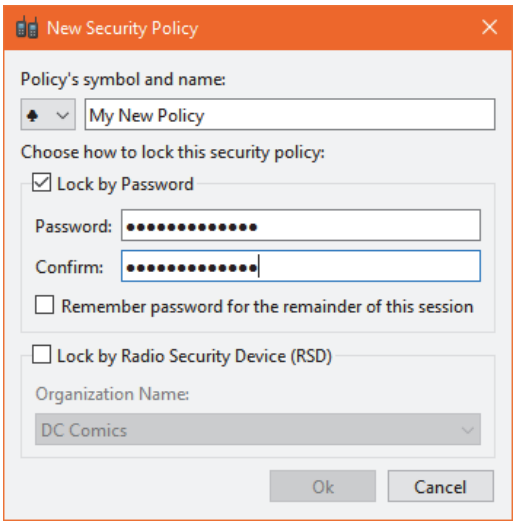
Figure 2 Manage Security Policy Dialog in Armada with Two Policies



2 Clicking **New** will prompt you to choose how you want to lock your policy, as shown in Figure 3. You can specify the policy name and symbol and lock the password or organization name. All of this can be edited later, though you cannot convert a password locked policy to an RSD locked policy or vice versa. To choose **Lock by Radio Security Device (RSD)**, a Parent RSD with an organization name must be plugged in.

Note *If the Security Policy password is forgotten, there is no way to recover it; all radios must be sent back to EFJohnson to be wiped to factory default.*

Figure 3 New Security Policy Prompt in Armada



3 Once you've added a policy, select it, and then authorize access to edit it. This is done by typing in the policy's password or having the corresponding Parent RSD plugged in. The Security Policy settings are shown in Figure 4 and each setting is described in Table 4. See Section 3.3 for information on viewing the Radio's Security Policy. All changes are saved immediately and if any radios have this policy, they'll be scheduled for update automatically. See Section 3.2 below for more information.

Figure 4 Managing an RSD Locked Policy

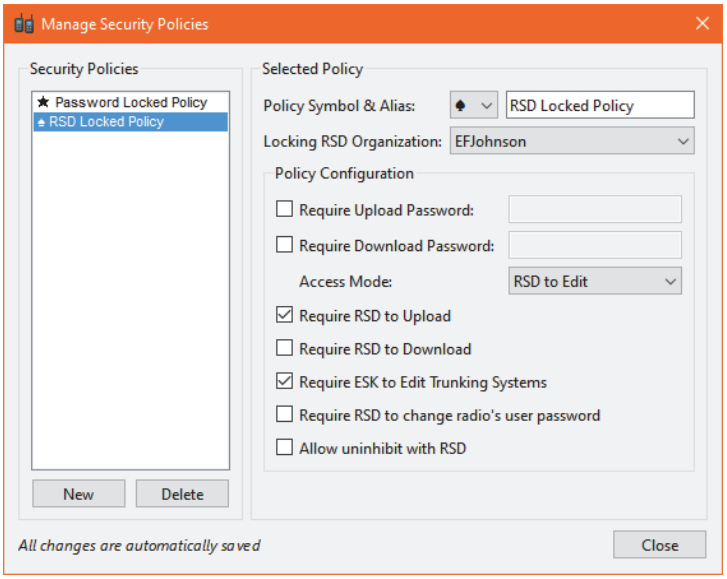


Table 4 Description of each Security Policy Parameter

Parameter	Policy Type	Description	Armada Release
Symbol	RSD, Password	Used for quick reference in the Armada fleet pane.	1.4.x and Later
Alias	RSD, Password	The name of the policy; limited to 32 characters.	1.4.x and Later
Password	Password	Password of the policy, never shown; click to enter a new password and confirm it to change; limited to 32 characters.	1.4.x and Later
Organization	RSD	The organization name that authorizes this policy; must have two Parent RSDs to change this.	1.4.x and Later
Upload Password	RSD, Password	If checked, this password must be entered to upload or import a profile with this policy; limited to 32 characters.	1.4.x and Later
Download Password	RSD, Password	If checked, this password must be entered when writing to radio with this policy; limited to 32 characters. See Section 3.4 for more information on this restriction.	1.4.x and Later

Table 4 Description of each Security Policy Parameter (Continued)

Parameter	Policy Type	Description	Armada Release
Access Mode	RSD	Can be set to one of four Access Modes: • **Unrestricted** - Anyone can view and edit. • **RSD to Edit** - Anyone can view. Parent or Child RSD can edit. • **RSD to View** - Parent or Child RSD can view. Parent RSD can edit. • **Parent RSD** - Parent RSD can view and edit. A radio's properties may be viewed without meeting the view requirement. Security Policies with a non-unrestricted access mode are not allowed to be written to radios at Armada1.8.x and earlier.	1.10.x and Later
RSD to Upload	RSD	An RSD is required to upload or import a profile with this policy.	1.4.x and Later
RSD to Download	RSD	An RSD is required to write to a radio with this policy.	1.4.x and Later
ESK to Edit Systems	RSD	When set, soft system keys are ignored when editing any trunking system on profiles with this policy.	1.4.x and Later
RSD to change user password	RSD	When set, an RSD must be present to change the user password of a profile with this policy.	1.4.x and Later
Allow Uninhibit with RSD	RSD	Radios may not be uninhibited by Armada unless they have a security policy with this set and an RSD present.	1.4.x and Later

Note *You are prohibited from deleting a Security Policy from Armada if any radio or template in your fleet has that policy assigned or pending.*

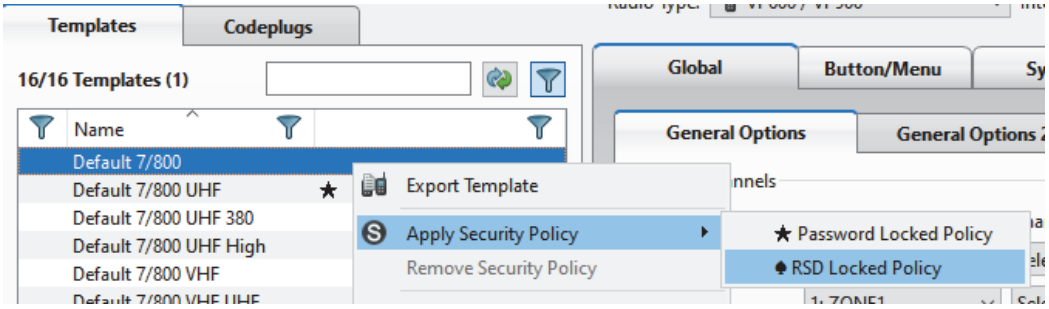
3.2 Assigning and Synchronizing Policies

To apply a Security Policy to a radio or template, simply right click the profile, select **Apply Security Policy**, then choose your policy from the sub-menu (see Figure 5). You must authorize this operation by doing one of the following:

- Entering the password
- Having the Parent RSD present
- Having the Child RSD programmed with **Apply/Remove Security Policies** present

If the profile had another security policy, you'll have to authorize both policies to make this change. See Section 4 below for information on how to manage your RSDs, including how to create Child RSDs.

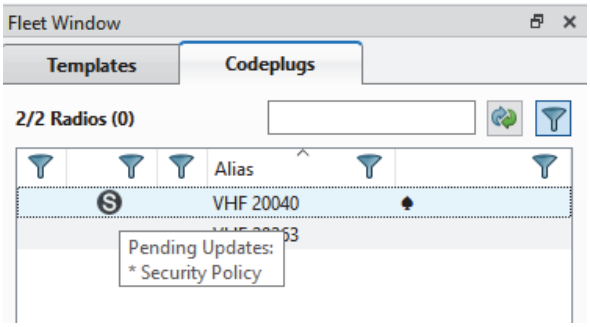
Figure 5 Apply Security Policy in Armada's Fleet Pane's Context Menu



When using the Provisioning Wizard, the selected source profile's security policy is applied to the target radio.

After applying a Security Policy, you'll see its symbol listed next to the profile. If you assigned the policy to a template, all linked radios have this policy as well. When a radio's policy changes for any reason, a write will automatically be scheduled, as shown in Figure 6.

Figure 6 Pending Security Policy Write to Radio "VHF 20040"

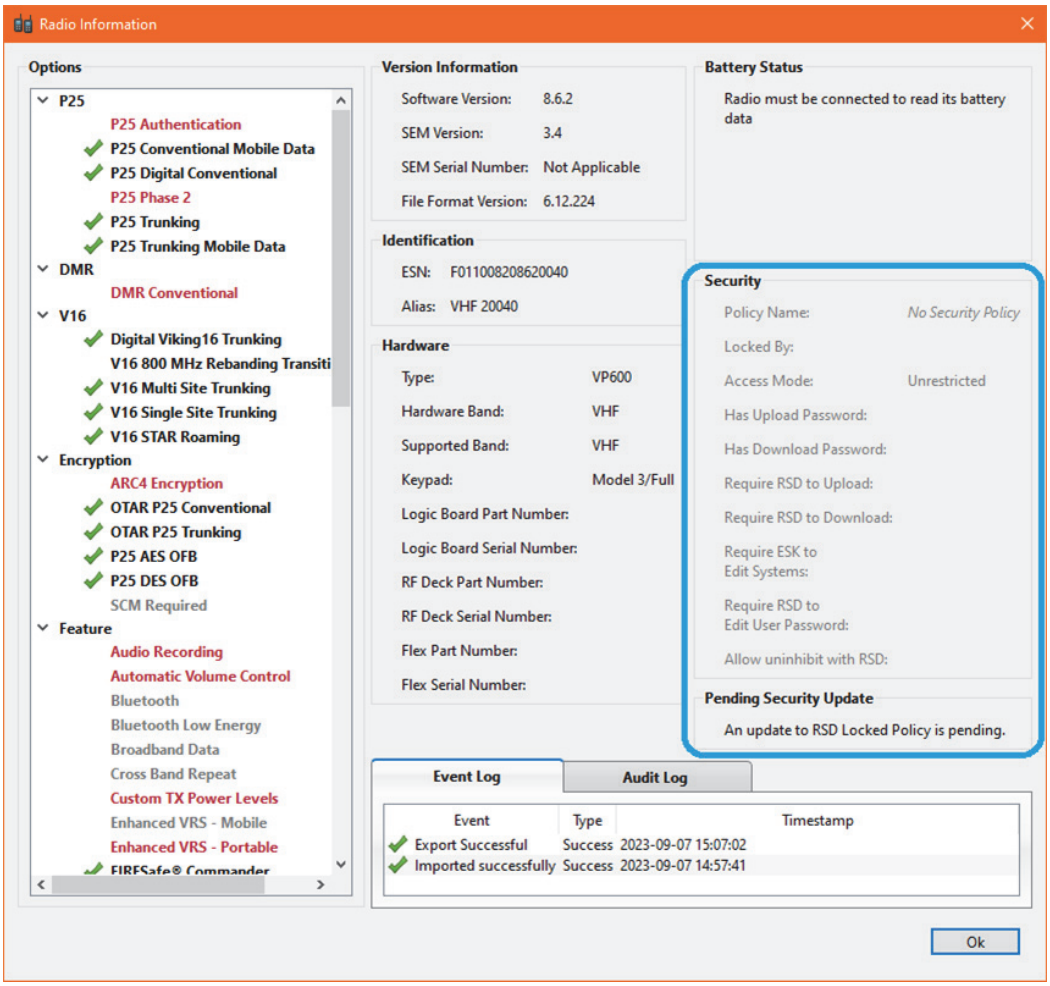


If a newer version of a Security Policy is observed (through import or reading of a radio), Armada will automatically update its copy of the policy and schedule a security policy write for all radio with that policy. This update cannot be canceled.

3.3 Viewing a Radio's Security Policy

To view the Security Policy on a radio, right click the radio in the fleet pane and select **Properties**. The exact policy that is on the radio itself is displayed as well as if a policy write is pending (Figure 7).

Figure 7 No Security Policy on Radio "VHF 20040", but Write Scheduled



3.4 More on Security Policy Restrictions

Table 4 above briefly describes all security policy restrictions. More details are mentioned here.

The upload password/RSD requirement applies to import as well, but the download password/RSD requirement does not apply to export. When writing to radios with download restrictions, you must authorize the write, but the timing of the authorization depends on your version of Armada. Prior to the 1.36.12 release, you could schedule a write without authorization, but would have to authorize the write when the radio connected. Starting with Armada 1.36.12, you must authorize the write when you schedule the write.

Note *When the radio connects, it must be in the same state as it was when the write was scheduled, otherwise the write must be reauthorized.*

4 Radio Security Devices (RSDs)

Radio Security Devices (RSDs) come in Parent and Child variants and can hold ESKs. Parent RSDs are capable of modifying Security Policies with matching organization name, but Child RSDs do not have the same capability. Child RSDs, with their organization name, are useful for security policy management. Parent RSDs may be ordered from EFJohnson and can be used to create Child RSDs.

This section contains information on the following topics:

- Managing Parent RSDs
- Managing Child RSDs
- Maintaining RSDs

4.1 Managing Parent RSDs

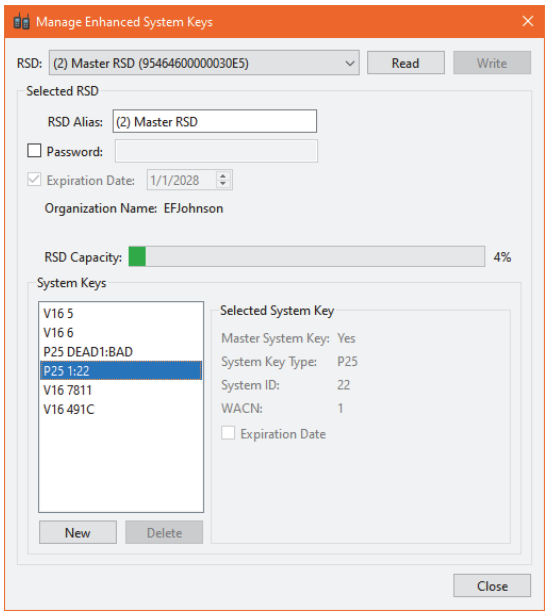
Refer to Section 5.3 for information on Parent ESKs.

To view all ESKS on a Parent RSD, proceed as follows:

1 Connect a Parent RSD with an organization name.

2 In Armada, select **Tools > Manage Enhanced System Keys**. The Manage ESK Dialog appears (Figure 8).

Figure 8 Parent RSD Manage ESK Dialog



4.2 Managing Child RSDs

Refer to Section 5.4 for information on Child ESKs.

To create a Child RSD, proceed as follows:

1 Connect a blank RSD and a Parent RSD with an organization name.

2 In Armada, select **Tools > Manage Enhanced System Keys**. The Manage ESK Dialog appears (Figure 9). This is the dialog where you manage everything to do with RSDs, including the system keys they hold.

3 Select the blank RSD and choose your organization name from the dropdown menu.

4 Click the **Write** button to commit the changes.

Figure 9 RSD portion of the Child RSD Manage ESK Dialog

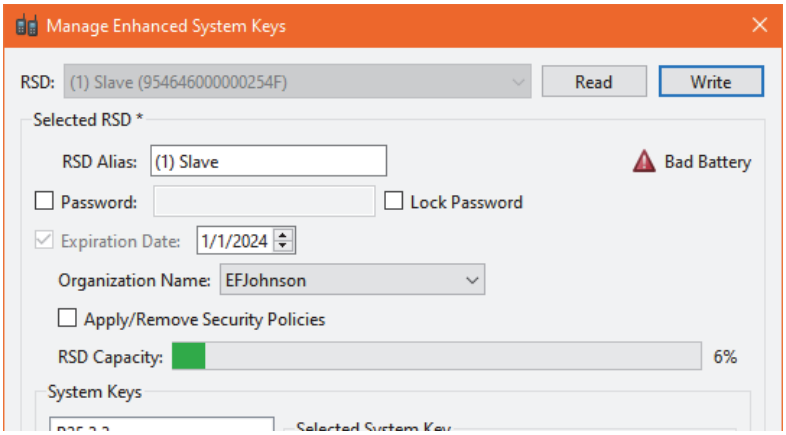


Table 5 describes each RSD parameter and its use. You must click **Write** to commit changes to the device.

Table 5 RSD Parameters

Parameter	Description	Armada Release
Alias	The name of the RSD – limited to 32 characters.	1.4.x and Later
Password	If enabled, this password must be entered each time this RSD is connected. Otherwise, the RSD and all its ESKs are ignored. If you change the password, you'll be prompted to confirm it. Passwords are limited to 32 characters.	1.4.x and Later
Lock Password	Applies only to Child RSDs (with an Organization Name); if set, the Parent RSD must be present to change the password.	1.4.x and Later
Expiration Date	If set on a Parent RSD, it cannot be changed; you will have to contact EFJohnson for another Parent RSD once it expires. On a Child RSD, an expiration date will automatically be set when the Organization Name is assigned, and this date cannot be later than that of the Parent RSD. Otherwise, with the Parent RSD present, a Child RSD may have any expiration date set. Once a Child RSD expires, it and its ESKs are ignored, but if a Parent RSD is present, the date may be extended.	1.4.x and Later
Organization Name	A unique identifier for your organization; unchangeable for Parent RSDs; may be assigned to blank RSDs converting them into Child RSDs.	1.4.x and Later

Table 5 RSD Parameters (Continued)

Parameter	Description	Armada Release
Apply/Remove Security Policies	If checked, a Child RSD may apply or remove Security Policies to radios or templates, locked by the organization name, but the Child RSD cannot modify the policy itself.	1.40.15 and Later
RSD Capacity	This is how much space is available on the RSD; it is only accurate after a fresh read or after clicking "Write". The number of ESKs that can fit on an RSD depends on their restrictions, but an RSD can fit about 50 average sized ESKs. If there is not enough room, an error message will appear when you click write.	1.4.x and Later

4.3 Maintaining RSDs

Each RSD has an internal real-time clock which is used to verify the expiration date. A rechargeable, battery keeps the clock accurate; if the battery ever runs out, a "Bad Battery" message will be displayed in the dialog. At least one RSD with a good battery must be present to give access to any RSD or ESK with an expiration date.

Note *Older purple RSDs did not have a rechargeable battery and have a shelf life of four years from manufacturing date. RSDs should be plugged in to charge for several hours at least once every three years.*

RSDs written by newer Armadas are backwards compatible if and only if they do not use newer features. E.g. you can create a Child RSD with Armada 1.40.15 to use in Armada 1.36.24 as long as you do not check **Apply/Remove Security Policies**.

Each RSD has a unique ID, displayed when choosing the RSD. This is unchangeable and doesn't affect any programming in Armada.

5 System Keys

System Keys are necessary to edit V16 and P25 system and channel data, though a system may be configured to use less strict rules. System Keys are used to restrict editing your system on everyone's radios, not just yours. Each system key is tied to a specific System ID (and WACN). There are three types of System Keys:

- Soft System Keys
- Parent ESKs
- Child ESKs

New systems have no key (no System ID or WACN) and may be edited without restriction. A valid System Key is required to assign or change the System ID (and WACN) of a Trunking System. If a Child ESK is present, all restrictions must be met (e.g. all assigned Talkgroups are in range) to make an assignment. If system lockout is set, a Child ESK cannot be used to assign a System ID/WACN.

A valid System Key is required to apply templates, clone, and paste (whole codeplug or just systems) to radios as this involves assigning a valid Unit ID to each system. However, System Keys are not required to be present when writing to a radio or scheduling a write.

This section covers how specific system parameters interact with system keys. This is followed by an explanation of each key type, including Child key restrictions, and additional system key details.

This section contains information on the following topics:

5.1 System Specific Parameters

There are currently two system specific parameters that affect how a trunking system interacts with System Keys, including what can be done without System Keys present. Figure 10 shows the System Specific parameters. Table 6 briefly describes these parameters with more discussion below.

Figure 10 System Specific System Key Parameters in Armada

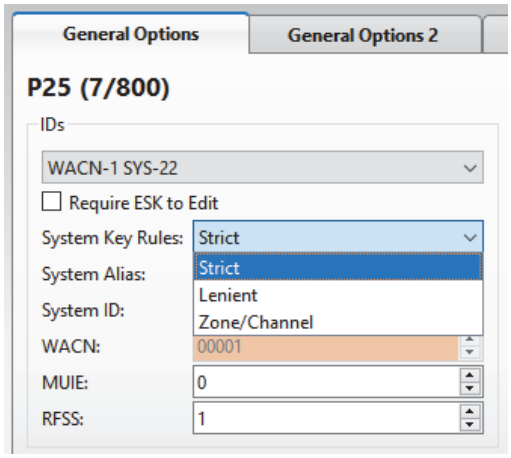


Table 6 System Specific Parameters related to System Keys

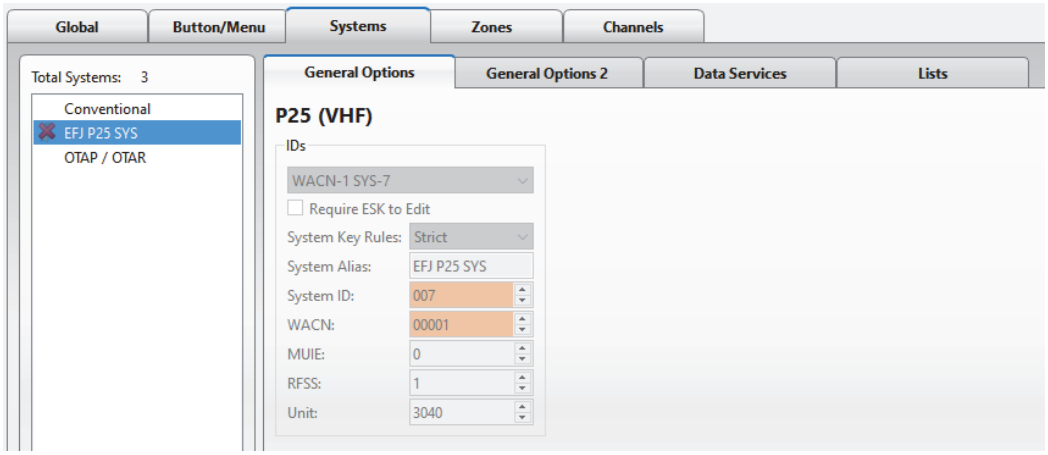
Parameter	System Type	Description	Armada Release
Require ESK to Edit	P25	If checked, Soft System Keys are ignored and an ESK must be present to edit this system. Radios below Firmware Version 8.28.x may not be written to with this setting enabled. When changing a system's key, this value will be unchecked automatically.	1.28.x and Later
Use Strict System Key Rules	V16, P25	Checked by default. If set, will prohibit all editing and viewing of system and corresponding channel data. If not set, all system data is visible and non-critical system parameters may be edited without a system key.	1.36.21-1.40.13
System Key Rules	V16, P25	This parameter replaces the "Use Strict System Key Rules" checkbox that appears in Armada releases 1.36.21 through 1.40.13. There are now three dropdown menu choices for System Key rules: • Strict (default) • Lenient • Zone/Channel These rules are described in detail below.	1.40.15 and Later

If **Require ESK to Edit** is set (it is off by default), Soft System Keys may not be used to edit this system. This parameter is only available for P25 systems. If a radio detects one of its P25 systems has changed from **Require ESKs to Edit** to not requiring it (e.g. after a write), all authentication keys for that system are dropped from the radio. This setting cannot be checked if the system's system key rules are set to **Zone/Channel**. To check this value, you must have a Parent ESK or a Child ESK with **Allow Change of "Require ESK to Edit"** present.

There are three "System Key Rules" sets any given V16/P25 system can have: Strict, Lenient and Zone/Channel. The rules operate as follows:

Strict Rules - When strict rules are selected (the default setting), all system parameters are hidden and may not be edited without a valid System Key. This includes channel parameters.

Figure 11 P25 System with Strict Rules Set and No System Key Present



Lenient Rules - Allow all system parameters to be seen and “non-critical” system parameters to be edited without a System Key. Figure 12 through Figure 19 outline the “critical” parameters. Table 7 outlines the location of each “critical” parameter in Armada.

Table 7 “Critical” System Parameters and Locations

Armada Window for “Critical” P25 System Parameters	
Systems >	General Options > IDs
	General Options > System Settings
	General Options 2 > Transmit Timeout
	Lists > Announcement Groups
	Lists > Channel ID
	Lists > Control Channels
	Lists > Roaming Systems
	Lists > System Preferred Sites
	Lists > Talkgroups
Channels >	IDs
	Security
	Other > TX Disabled
	Other > Dynamic Regrouping
Armada Window for “Critical” V16 System Parameters	
Systems >	General Options > IDs
	General Options > Remove Monitor
	General Options > System Settings
	General Options 2 > Transmit Timeout
	Lists > Announcement Groups
	Lists > Control Channels
	Lists > Rebanded Control Channels
	Lists > System Preferred Sites
	Lists > Talkgroups
Channels >	IDs
	Other > TX Disabled
	Other > Dynamic Regrouping

Figure 12 Restricted/Critical P25 System Parameters

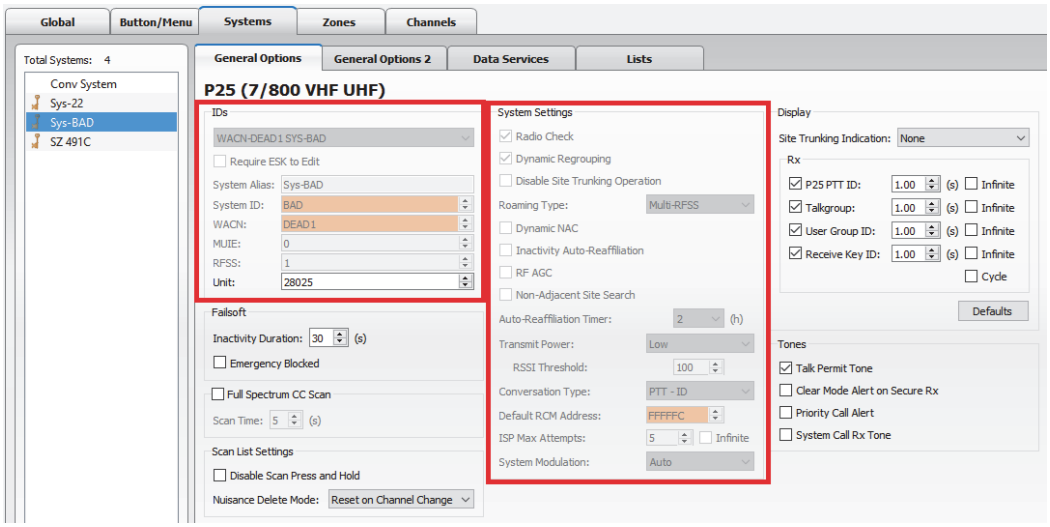


Figure 13 Additional Restricted/Critical P25 System Parameters

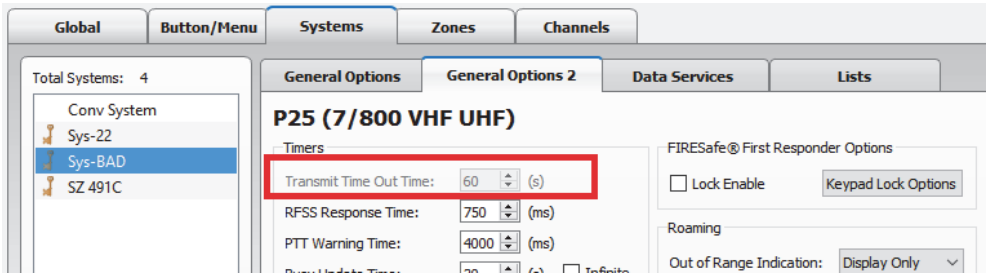


Figure 14 Restricted/Critical P25 System List Parameters

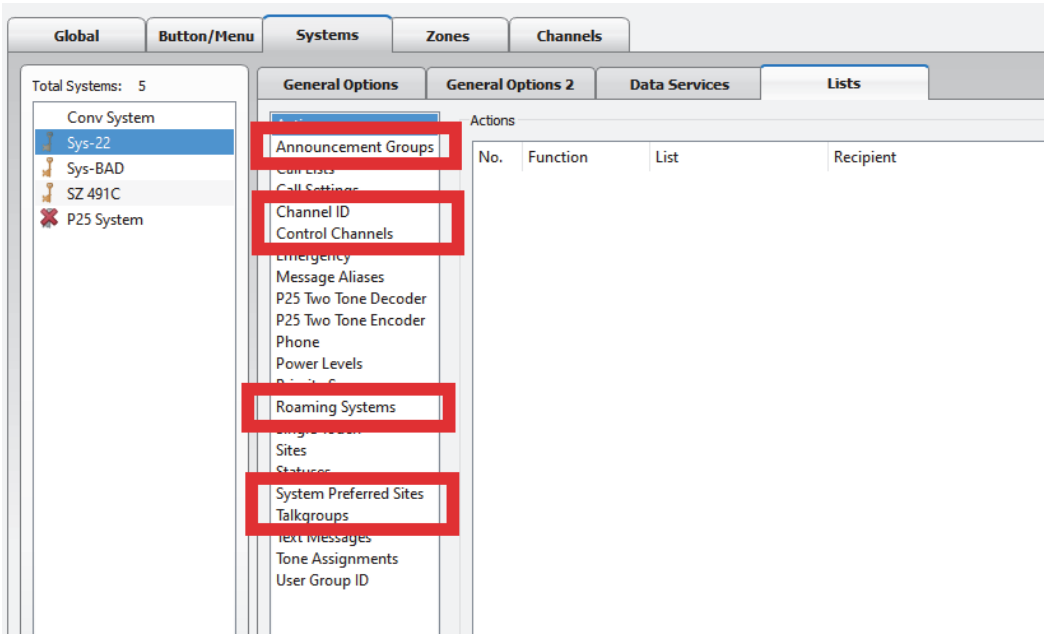


Figure 15 Restricted/Critical P25 Channel Parameters

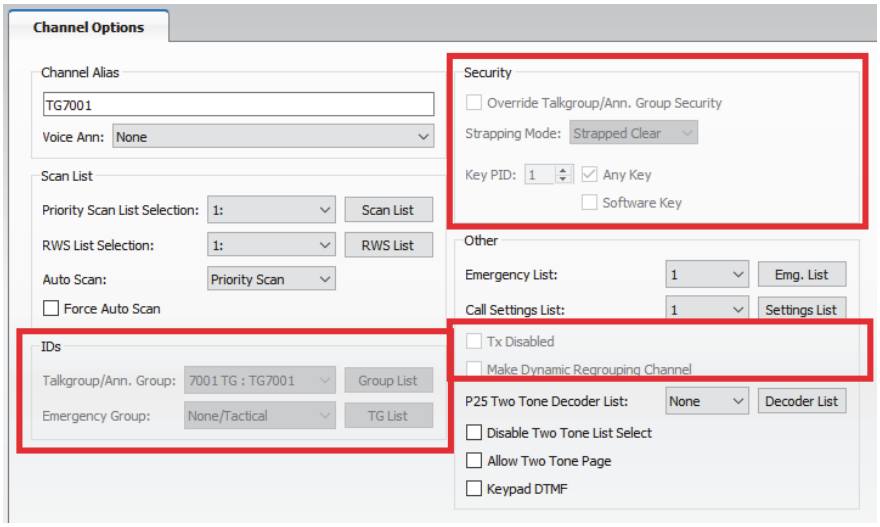


Figure 16 Restricted/Critical V16 System Parameters

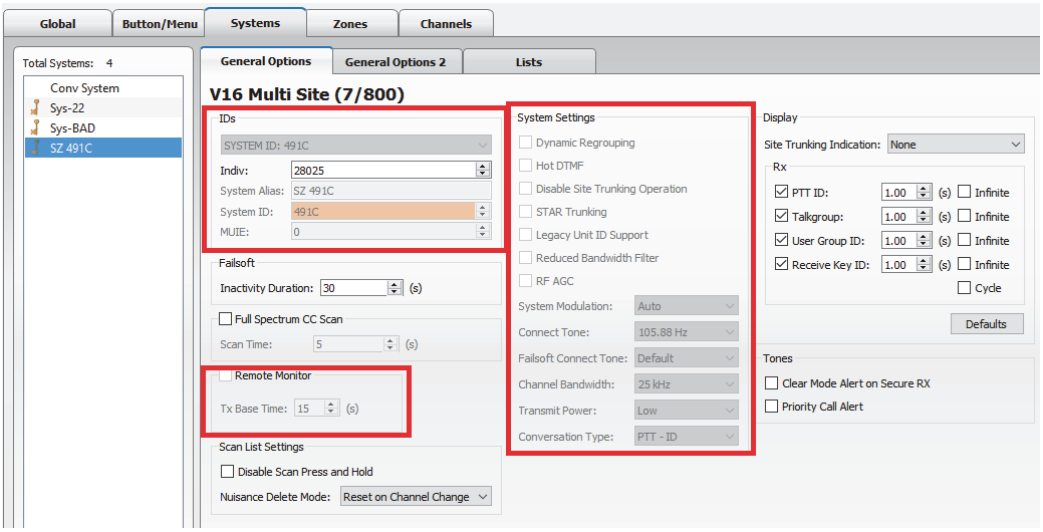


Figure 17 Additional Restricted/Critical V16 System Parameters

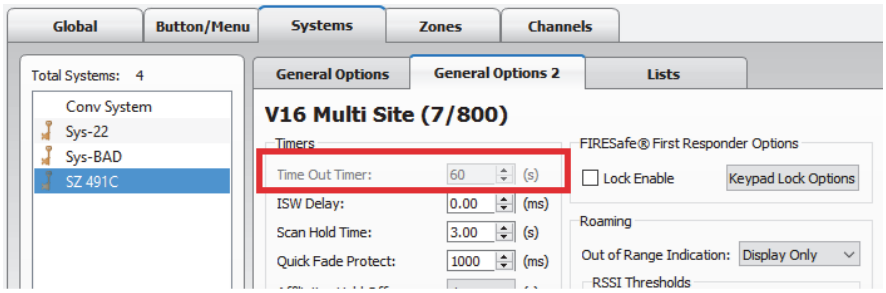


Figure 18 Restricted/Critical V16 System List Parameters

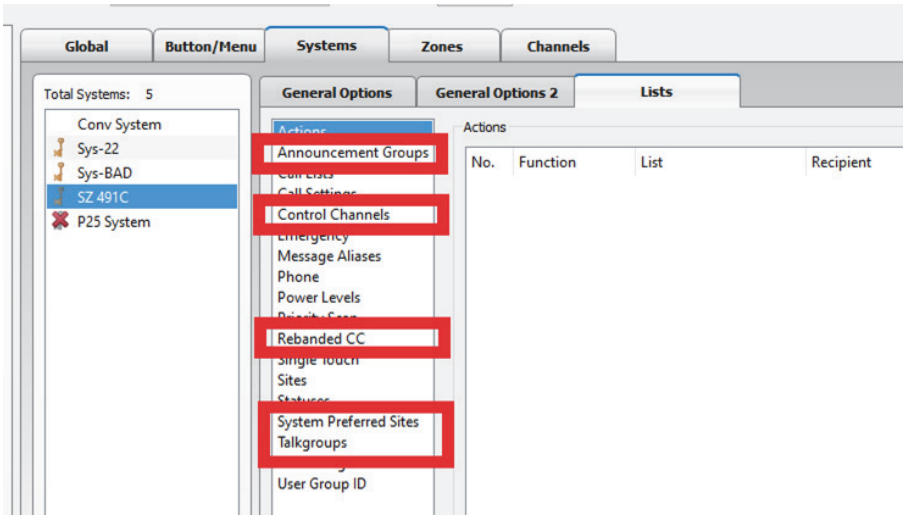
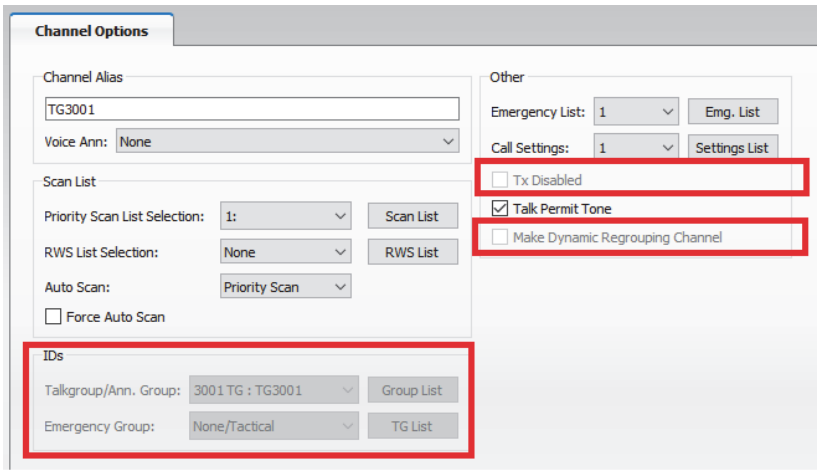


Figure 19 Restricted/Critical V16 Channel Parameters



Zone/Channel - System Key rules that are modeled after lenient rules, but also allow channels to be assigned to the system or have channels' group changed to any Talkgroup (but not AG) present on the system without a System Key. Talkgroups themselves may not be edited or added without a valid key though. A system key is still required to link a radio with **Zone/Channel** systems to a template as a Unit ID must be specified. This setting cannot be chosen if **Require ESK to Edit** is checked.

To change the strictness rules of a system, you must have valid soft key, a Parent ESK, or a Child ESK with **Allow Change of "System Key Rules"** present.

Prior to the 1.36.14 release of Armada, trunking system are automatically treated with the Strict rules regardless of this setting. Armada releases 1.36.14 through 1.36.20 automatically treated all trunking systems using Lenient system key rules regardless of this setting. Starting with Armada 1.36.21, this setting is observed. Though Armada releases 1.36.21 through 1.40.13 will treat Zone/Channel system key rules as Lenient.

Note *Armada releases 1.4.x through 1.8.x allow viewing of trunking system data without a key, but not editing.*

5.2 Soft System Key

Soft System Keys are encrypted .akey files that provide full edit access to the corresponding trunking system on a profile. They are only created by EFJohnson but may be copied and distributed by anyone that has the file. To use a soft system key in Armada put it in a directory on your computer then go to **Tools > Preferences…** and select the **Directories** tab and browse for that directory. If you add or remove system keys in that directory while Armada is running, go to **Tools > Reload System Keys** to refresh.

5.3 Parent ESK

Parent ESKs are Hard System Keys that live on an RSD created by EFJohnson. They can create Child ESKs on other RSDs. Parent ESKs themselves cannot be duplicated. You can view all ESKs on a Parent RSD. Refer to Section 4.1 for more information.

5.4 Child ESK

Child ESKs are created in the Enhanced System Key Dialog, shown in Figure 8 above. To add a Child ESK, first have two RSDs plugged in, one must have the corresponding Parent System Key. Then click the **New** button and choose which Parent Key to use. Newly added Child Keys have no restrictions, but these may be configured at this time; see Table 8 for a list of all parameters, also shown in Figure 20. To delete a Child ESK, its Parent ESK must be present. You must click **Write** to commit any changes you make.

Figure 20 Armada's ESK Dialog shown with a Child System Key Selected

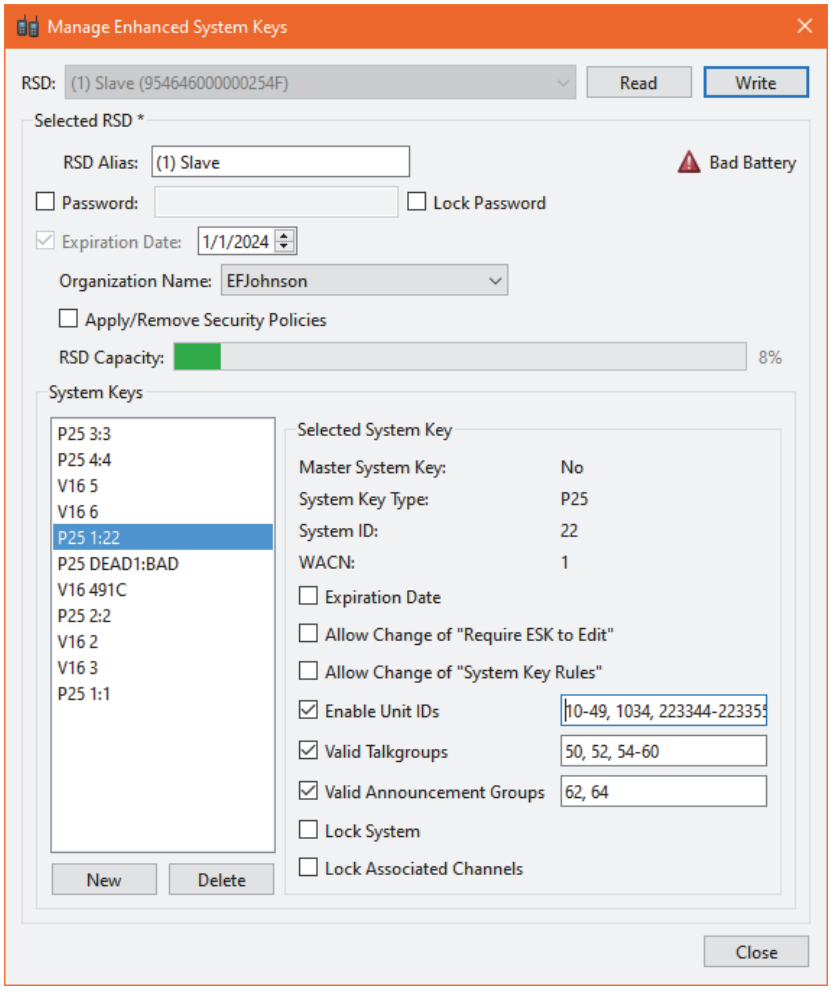


Table 8 Child System Key Parameters

Parameter	System Type	Description	Armada Release
Expiration Date	V16, P25	If configured, once this date is passed, the Child Key is expired and ignored. A Parent Key can extend the date. But if the Parent Key has an expiration date, the Child Key must have one as well and it cannot be set to expire later than the Parent's.	1.4.x and Later
Allow Change of "Require ESK to Edit"	P25	When checked, a system's "Require ESK to Edit" setting may be enabled (or disabled). If this is checked, all Unit IDs, TGs and AGs will be enabled and system and channel will not be locked.	1.40.15 and Later
Allow Change of "System Key Rules"	V16, P25	When checked, people with this Child key may select a more lenient (or stricter) "System Key Rule" setting. If this is checked, all Unit IDs, TGs and AGs will be enabled and system and channel will not be locked.	1.40.15 and Later
Unit IDs	V16, P25	The range of valid Unit IDs[1]. If unchecked, no unit IDs may be assigned which means this key cannot link templates to radios.	1.4.x and Later
Valid Talkgroups	V16, P25	The range of valid Talkgroups[1]. This controls which Talkgroups may be assigned to channels and announcement groups. When linking templates to radios, all assigned talkgroups must be in this list. This setting is meaningless if a system is configured with "Zone/Channel" rules.	1.4.x and Later
Valid Announcement Groups	V16, P25	The range of valid Announcement Groups[1]. This controls which Announcement Groups may be assigned to channels. When linking templates to radios, all assigned AGs must be in this list.	1.4.x and Later
Lock System	V16, P25	When set, depending on your system key rules, either no system parameters or no critical system parameters may be edited. Radios may still be linked to templates and systems pasted while obeying the Unit ID, TG and AG restrictions.	1.4.x and Later
Lock Associated Channels	V16, P25	When set, depending on your system key rules, either no channel parameters or no critical channel parameters may be edited. Radios may be linked to templates, but channels may not be pasted to other profiles.	1.10.x and Later

1. Multiple ranges and individual values may be entered, for example "1-3, 5, 6-10".

ESKs written by newer Armada versions are backwards compatible as long as they do not use newer features. If newer features are used that key (and others on the RSD) may not be read by older versions of Armada.

5.5 System Keys and Armada Server

Currently, all System Keys are local to each client. Armada Server does not deal with or have any need for system keys. This means each radio programmer will need their own system keys.

6 Use Cases

The following subsections outline a few common use cases of security policies and system keys to secure fleets of Viking radios using Armada programming software.

This section contains information on the following topics:

6.1 Protecting Your Radios from Unauthorized Access & Modification

Scope: A fleet administrator uses a security policy to keep unauthorized people from changing their radio's programming.

Primary Actor: Fleet administrator

Secondary Actor: Fleet programmer

Preconditions:

- Fleet administrator and programmer work for the same organization with Viking radios.
- Fleet administrator and programmer both have accounts on Armada Server.

Postconditions:

- Only fleet administrator and programmer can update the programming of their Viking radios.

Workflow:

1. Fleet administrator orders a Parent RSD with their organization name.
2. Fleet administrator creates a Child RSD with that Parent RSD when it arrives and gives it to fleet programmer.
3. Fleet administrator creates a security policy locked by the Parent RSD with these restrictions:
   a. Access Mode: **RSD to Edit**
   b. **Require RSD to Upload** checked

4 Fleet administrator applies this security policy to all radios in the fleet.

5 Fleet programmer can edit profiles, read, and write to these radios.

6 If someone picks up one of these radios and connects it to their Armada, they will not be able to read it in.

6.2 Share System Programming with Child ESKs

Scope: A system owner would like to share their system's programming with another organization but avoid the hassle of managing their codeplugs.

Primary Actor: System administrator

Secondary Actor: Organization programmer

Preconditions:

- System administrator has a Parent ESK for their system.
- System administrator has a template with their system's parameters. Including **Require ESK to Edit** checked and **Strict** rules as desired.
- Organization programmer belongs to a separate organization.

Postconditions:

- Organization programmer has a Child ESK for system administrator's system.
- Organization programmer's radios are programmed with the system administrator's system as given (unmodified) and using only the allowed unit IDs, TGs and AGs.

Workflow:

1 System administrator uses their Parent ESK to create a Child ESK specifying:

   a Valid Unit ID, Talkgroups and Announcement Group ranges

   b Checking **Lock System**

2 System administrator exports and emails their template and mails the Child ESK to organization programmer.

3 Organization programmer imports the system and plugs in the ESK.

4 Organization programmer copies the system off the imported template and to their template.

5 Organization programmer updates all unit IDs (within limited range) and writes to each radio.

6.3 Share System Programming without Sharing ESKs

Scope: A system owner would like to share their system's programming with another organization but avoid the hassle of managing their codeplugs and avoid sharing system keys.

Primary Actor: System owner

Secondary Actor: Organization programmer

Preconditions:

- System administrator has a template with their system's parameters
- Organization programmer belongs to a separate organization

Postconditions:

- Organization programmer's radios are programmed with the system administrator's system with unchanged “critical” parameters, but other changes have been made (e.g. customer scan lists).

Workflow:

1. System owner sets their system to use **Lenient** rules.
2. Organization programmer gets system owner's system on their radios; this is the tricky part of avoiding using ESKs; here is one possible set of steps:
   a. Organization programmer emails their fleet (including linked templates) to system administrator.
   b. System administrator puts their system (and channels) on the imported profiles; including assigning unit IDs to all radios; then exports and emails back.
   c. Organization programmer imports their fleet, now with system administrator's system.
3. Organization programmer updates channel aliases, scan lists, etc. as desired, but cannot change critical system parameters.
4. Organization programmer writes to all their radios.

6.4 Moving From Soft Keys to ESKs

Scope: A system owner has been using soft keys but would like to switch to requiring hard keys.

Primary Actor: System administrator

Preconditions:

- Soft system keys for a system have been distributed and are in the wild

Postconditions:

- All radios that can authenticate to the system were programmed with ESKs

Workflow:

1 System administrator orders a Parent Key for their system and blank ESKs.

2 System administrator checks **Require ESK to Edit** on their system in Armada.

3 System administrator distributes this change and Child ESKs (see other use cases).

4 System administrator loads authentication keys only on updated radios requiring ESK to edit.

5 System administrator enables authentication on their system.

6.5 Using a Child RSD as a Parent RSD

Scope: An office has multiple programmers who need to configure radios' security policies

Primary Actor: Supervisor

Secondary Actors: Programmer 1 and programmer 2

Preconditions:

- Supervisor has a Parent RSD with their organization name and two blank RSDs

Postconditions:

- Programmer 1 and programmer 2 can assign security policies
- Programmer 1 and programmer 2 cannot modify the policy or create more Child RSDs

Workflow:

1. Supervisor creates a security policy with their Parent RSD's organization name and shares this with programmer 1 and programmer 2.
2. Supervisor creates two Child RSDs with that organization name and checks **Apply/ Remove Security Policy** and shares them with programmer 1 and programmer 2.
3. Programmer 1 and programmer 2 can now assign that security policy to their radios or templates.

6.6 Using a Child ESK as a Parent ESK

This is the same use case as above, but when creating Child ESKs, check either **Allow Change of "Require ESK to Edit"** or **Allow change of "System Key Rules"** based on what behavior is desired. Again, these Child ESKs cannot create additional Child ESKs.