

SUMMARY - This document provides BlackTube commands and instructions supplemental to the *IP-Tube Users Guide* – detailing configuration of AES Encryption on the BlackTube systems. Consult the *IP-Tube Users Guide* for Serial over IP configuration and commands.

As you get started on testing and config, please contact Engage Technical Support - tel +1.831.688.1021, press '3' for Support, or support@engageinc.com - with any questions.

Genkey

A random 256 bit key is generated with the GenKey command. At the system level enter this command and it will create a key to input to a local and remote BlackTube. The Key must be identical at both ends for encryption to work.

EnterKey [N] XXXXXX.... (the actual key is 64 hex characters)

On both units issue the EnterKey command and provide the key generated by the output of the GenKey command. The output of the GenKey command can be copied into an editor and pasted onto the CLI when in configuration mode. Be sure to remove any linefeed or return characters in the key.

It is not required that the key be generated by GenKey if other means of generating a random value are available.

Multiple keys may be stored to have unique key relationships with multiple serial ports. N can be a number from 0 to 6 to identify the key. This number is used to specify the key in the serial port configuration.

Key 0 is the default used when N is not specified.

Serial Port Configuration

Tube [1 | 2] AES {On | Off}

Tube 1 refers to the configuration when LAN1 is the selected LANPort. Tube 2 refers to the configuration when LAN2 is the selected LANPort. When optional features such as Protector or Alternator are selected, both Tube 1 and Tube 2 configurations may be active at the same time.

On and Off turns encryption on or off.

Tube [1 | 2] Key N

Selects the key number to be used for this LANPort. The key is entered with the EnterKey command.

This key is used for authentication with the remote BlackTube. Once an encrypted session is established, a new secret key is exchanged and used for encryption of the BlackTube serial data.

Tube [1 | 2] RekeyPeriod {N [Days | Hours | Minutes]}

Sets the crypto period for how long a secret key should be used. When the crypto period has expired, a new secret key is exchanged and used.

The crypto period can be set to a maximum of 45 days. N is the number Days, Hours, or Minutes of the crypto period. N defaults to a unit of Minutes if Days or Hours are not specified.

If zero is specified, the initial secret key is established and no other key exchanges take place.

Show Security Info

Displays information about the keys. A valid key is one that does not have the same value for each byte. This is a good indicator whether or not a particular key has been set.

In use indicates the key is configured for use in the serial configuration.

Security Info

Key 0	Valid	Not in use
Key 1	Valid	In use
Key 2	Valid	In use
Key 3	Valid	In use
Key 4	Valid	In use
Key 5	Valid	In use
Key 6	Valid	In use

Show Black Statistics / Show Security Statistics

The Black and Security Statistics report errors and information regarding the crypto functions of the BlackTube. Only error statistics with nonzero values are displayed.

An AES Tunnel Not Ready statistic on the Serial Statistics indicates serial packets were received on the serial interface, but the encrypted session was not established and the packet was discarded. This may be common on startup or after reconfiguration of a line.

Show Info

The display of Show Info for a Serial Interface displays a line indicating the state of the encrypted path is Tube AES is On.

For example: AES LAN1: Tunnel State, 3 Rekeys

indicates LAN1 traffic is configured to be encrypted.

Tunnel State	indicates an encrypted session has been established.
Init State	would indicate an encrypted session has not been established.
3 Rekeys	indicates there have been 3 key exchanges since the serial port has been configured.