

Software operating system RouterOS version 6 («RouterOS 6») encryption details

SIA MikroTiks developed RouterOS 6 to use for management of network (telecommunication) devices.

SIA MikroTiks informs, that:

1. RouterOS 6 includes encryption features (components), intended for data (information) security, passed through telecommunication channels and device control channels.
2. All encryption features (components) are an integral part of RouterOS 6 and can not be changed by the end-users.
3. RouterOS 6 is intended for installation by end-users without significant support from the vendor.
4. RouterOS 6 uses the following security protocols:

Supported security protocol	Encryption algorithm	Maximum key length
IPSec	DES	56 bit
	3DES	168 bit
	AES	128 bit
		192 bit
		256 bit
	Blowfish	448 bit
	Twofish	256 bit
	Camelia	128 bit
		192 bit
256 bit		
PPTP (with MPPE)	RC4	128 bit
L2TP (with MPPE)	RC4	128 bit
SNMP	DES	56 bit
	AES	128 bit
SSH	Blowfish	128 bit
	3DES	192 bit
	AES	128 bit
		192 bit
		256 bit

Supported security protocol	Encryption algorithm	Maximum key length
SSTP	AES	256 bit
	RC4	128 bit
Used in WinBox connection (nameless)	AES	128 bit
WEP	RC4	104 bit
WPA-TKIP	RC4	128 bit
WPA2-TKIP	RC4	128 bit
WPA-AES	AES	128 bit
WPA2-AES	AES	128 bit

Interfaces are traditional - graphical interface and command line. Detailed description of interfaces usage is available at <https://wiki.mikrotik.com/wiki/Manual:TOC>.