

MDS SCADAcrypt™

Data Encryption Module



Installation and Operation Guide

05-4511A01, Rev. 01
JANUARY 2006

industrial/wireless/performance



***MDS SCADA*crypt™**

TABLE OF CONTENTS

SECTION 1 - DESCRIPTION	2
SECTION 2 - SPECIFICATIONS	4
SECTION 3 - INSTALLATION	5
SECTION 4 - CONTROLS AND INDICATORS	6
SECTION 5 – CONFIGURATION COMMANDS.....	7
SECTION 6 - INTERFACE SIGNALS AND CABLING.....	16
SECTION 7 - TROUBLESHOOTING	19
SECTION 8 – IN CASE OF DIFFICULTY	20

1. DESCRIPTION

The *MDS SCADAcrypt™* is an industrial rated serial data encryption device featuring two serial ports, a device port and a network port. The unit employs AES 256-bit encryption, 128-bit block size. AES is the U.S. Government standard, selected using an open selection process, to replace DES and 3DES encryption.

The unit provides a secure link between host and remote user sites. The two RS-232 serial ports operate at asynchronous speeds as low as 300 bps and as high as 57.6 Kbps. The serial interface can be RS-232, RS-422 or 2-wire or 4-wire RS-485.

The unit may be used point-to-point, linking two separate remote sites with radios, leased lines or dial-up connections, with one port used for the composite, and the other for user equipment. The unit may also be used on point-to-multi-point links. It is especially attractive for use over multi-point radios where high security is desired.

The *MDS SCADAcrypt* has a bypass mode (Block Mode Clear) for use during initial installation. When installing in a large multidrop network, it is desirable to have the remote units *not* encrypt data until the host unit is installed. This makes the scheduling of installation less critical, as the initial remote installation will not disable the drop if a host unit is not yet in service. The remote unit is temporarily just a “bump” in the serial cable.

The *MDS SCADAcrypt* is straightforward, easy to configure and maintain. Units can be configured via a serial port, or using the Ethernet port (via telnet or a web browser). The unit offers the most-needed features without undue complexities.



MDS SCADAcrypt Front View



MDS SCADAcrypt Rear View

2. SPECIFICATIONS

2.1 General

Two asynchronous RS-232 ports

- DE-9P (PC-9pin) connectors, DTE interface
- Speeds to 57.6 Kbps full or half duplex
- Can be configured via RS-232 serial port, or via Ethernet port for telnet or web browser management

Protocol Features

- 256-bit AES encryption
- 128-bit blocks
- Block Cipher – Cipher feedback mode

2.2 Environmental

- Operational Temperature: -40 to +70 C
- Storage Temperature: -50 to +75 C
- Humidity: <95% Non-condensing

2.3 Physical / Electrical

Power requirements: 9 Vdc, 500 mA

12, 24, 48, 125 Vdc and 240 Vac options are available

Supplied with 120 Vac external power supply

4_” wide x 5_” long x 1_” high

Weight: 1 lb./0.37 kg

2.4 Setup Commands

Cipher Configuration

Serial Port Configuration

LAN Configuration

Display Configuration Settings

Reset Configuration to Default

Save and Exit

Exit without Saving

3. INSTALLATION

3.1 Unpacking

The following is included with each unit:

- Unit and external power supply
- Cable for connection to a PC for initial configuration.
- Instruction Manual (this document)
- Information regarding warranty, maintenance contracts and repair

3.2 Setup

The *MDS SCADAcrypt* must be properly configured before use. See Section 5 for connection and configuration information.

3.3 Connections

The RS-232 serial ports on the *MDS SCADAcrypt* are configured as Data Terminal Equipment (DTE). This is the same configuration used on PC COM ports. To connect the *MDS SCADAcrypt* to peripheral equipment, use the same cable that would be used to connect that equipment to a PC COM port.

3.4 Using Block Mode Clear

In a multi-drop network it may be desirable to install the remote units configured for “Block Mode Clear.” In this mode, the *MDS SCADAcrypt* is merely a “bump” in the cable. The top rear panel LED will be OFF.

When ready to enable encryption, install the host end *MDS SCADAcrypt* and use the Cipher Configuration option 3, “Signal remotes to switch to Block Mode Cipher,” from the serial or Telnet setup menu. If using HTML and a browser, click on the red “Enable Block Mode Cipher” button.

4 CONTROLS AND INDICATORS

4.1 Controls

A pushbutton switch to invoke serial port setup is accessible through a small hole in the right side panel. Use a paper clip to press the switch. Use caution to push the clip straight in, and no farther than needed to activate the switch.

4.2 Indicators

Front

<u>Indicator</u>	<u>Condition</u>	<u>Meaning</u>
Top	ON	Port 2 TxD active
Bottom	ON	Port 1 TxD active

Rear

<u>Indicator</u>	<u>Condition</u>	<u>Meaning</u>
Top (Mode)	ON	Normal Encrypted Mode
	OFF	Clear Mode
	Flashing	Serial Setup Mode
Bottom	OFF	No LAN Connection
	ON	LAN Valid
	Flashing	LAN Active

5. CONFIGURATION COMMANDS ---

5.1 Introduction

Initial setup of the *MDS SCADAcrypt* is accomplished using serial port 1 (right). After initial configuration, a web browser or Telnet connection may be used if the unit was configured for LAN operation.

5.2 Connections and Setup

The unit can be set up through serial port 1. Connect a PC to serial port 1 using the cable provided. If an asynchronous terminal is used, a null modem cable is required.

Use an asynchronous terminal or a PC using a communications program such as HyperTerminal. Set the terminal to 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Press the button through the hole in the right side of the case of the case. Pressing the button will bring up the following screen:

5.3 Serial Mode and Telnet Setup Screens

Serial Encryption Module V1.2

Configuration setup.

[Press any key to continue]

After pressing any key:

Main Menu

1 Cipher Configuration
2 Serial Port Configuration
3 LAN Configuration
4 Username/Password Configuration
5 Display Configuration Settings
6 Reset Configuration to Default
7 Save and Exit
0 Exit without Saving

Choose a Number =>

5.3.1 Cipher Configuration

CIPHER CONFIGURATION:

Operational Mode: Block Mode Cipher

Passphrase: *****

SET CIPHER CONFIGURATION:

- 1 Operational Mode [0=Block Mode Cipher, 1=Block Mode Clear]
- 2 Secret Passphrase [1 to 62 characters]
- 3 Signal remotes to switch to Block Mode Cipher.
- 0 -- Return to previous menu

EXAMPLE: To set the secret passphrase to "my secret!"

=> 2 my secret!

Enter Command =>2

5.3.2 Serial Port Configuration

SERIAL PORT CONFIGURATION:

Baud Rate: 9600, Parity: NONE, Data: 8-Bits, Stop: 1-Bit

Port 1 RS485: 4-wire (jumper set for RS-232)

Port 2 RS485: 4-wire (jumper set for RS-232)

Rx Idle Time: 12 character times

Tx Idle Time: 2 character times

SET SERIAL PORT CONFIGURATION:

- 1 Baud Rate [0=57600, 1=38400, 2=19200, 3=9600
4=4800, 5=2400, 6=1200,]
- 2 Parity bit [0=None, 1=Odd, 2=Even]
- 3 Data bits [0=7bits, 1=8bits]
- 4 Stop bits [0=1bit, 1=2bits]
- 5 Port 0 RS485 Mode [0=4-wire, 1=2-wire]
- 6 Port 1 RS485 Mode [0=4-wire, 1=2-wire]
- 7 Rx Idle Time [5 - 1000 character times]
- 8 Tx Idle Time [1 - 1000 character times]
- 0 -- Return to previous menu.

EXAMPLE: To set the baud rate to 19200

=> 1 2

5.3.3 LAN Configuration

LOCAL UNIT CONFIGURATION:

```
Local Address: 205.166.54.181      Serial NO:  
00:60:E9:00:D7:11  
Gateway Address: (NOT SET)        Subnet Mask: 255.255.255.0  
Ethernet Mode: Auto
```

LAN CONFIGURATION:

- 1 Local IP Address
- 2 Gateway IP Address
- 3 Subnet Mask
- 4 Ethernet Mode [0=Auto, 1=100Mb-Full, 2=100Mb-Half, 3=10Mb-Full, 4=10MB-Half]

0 -- Return to previous menu

EXAMPLE: To set local IP address to 192.168.1.57
=> 1 192.168.1.57

Enter Command =>

5.3.4 Username/Password Configuration

USERNAME/PASSWORD CONFIGURATION:

```
UserName: (not set)  
Password: (not set)
```

SET USERNAME/PASSWORD CONFIGURATION:

- 1 Username [1 to 16 characters]
- 2 Password [1 to 16 characters]
- 3 Clear Username and Password
- 0 -- Return to previous menu

EXAMPLE: to set username to "admin"
=> 1 admin

Enter Command =>

5.3.5 Display Configuration Settings

Serial Encryption Module: V1.2

CIPHER CONFIGURATION:

Operational Mode: Block Mode Cipher

Passphrase: *****

[Press any key to continue]

SERIAL PORT CONFIGURATION:

Baud Rate: 9600, Parity: NONE, Data: 8-Bits, Stop: 1-Bit

Flow Control: NONE

Port 0 RS485: 4-wire

Port 1 RS485: 4-wire

Rx Idle Time: 12 character times

Tx Idle Time: 2 character times

[Press any key to continue]

LOCAL UNIT CONFIGURATION:

Local Address: 192.168.1.1

Serial NO:

00:60:E7:00:D7:0B

Gateway Address: (NOT SET)

Subnet Mask: 255.255.255.0

Ethernet Mode: Auto

[Press any key to continue]

CURRENT STATISTICS:

Serial clear bytes received: 0

Serial clear bytes transmitted: 0

Network packets received: 0

Network packets transmitted: 0

Network packet errors: 0

CONFIG Mode

[Press any key to continue]

5.4 Ethernet Management

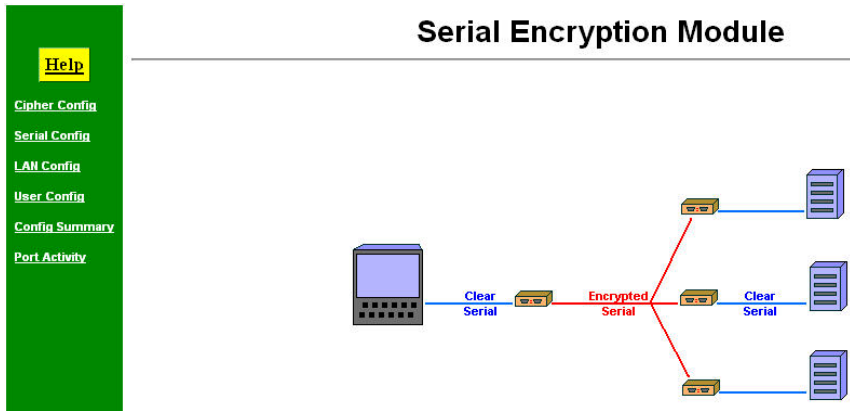
For a connection directly to a PC, use an Ethernet crossover cable, part number 9500097. If plugged into an Ethernet hub or switch, use a straight through Ethernet cable.

5.4.1 Telnet

Telnet screens are identical to the serial screens

5.4.2 Browser screens:

Front page screen:



Help box common to every HTML page:



Cipher Configuration screen minus the help box:

One to 62 characters for the passphrase. Any combination of symbols, numbers, letters, upper and lower case. Not useable are CR, LF,

Click on Enable Block Mode Cipher to trigger the remote units and put them in cipher mode.

Cipher Configuration

Operational Mode: ☒ Block Mode Cipher
☐ Block Mode Clear

Passphrase :

Save

Cancel

Press the following button to switch local and remote units to

Block Mode Cipher.

Enable Block Mode Cipher

When saving a configuration message:

Server Status Message

Saving new configuration!

Back

When enabling block cipher mode:

Enabling Block Cipher Mode

Sending command to enable **Block Mode Cipher**. Please wait for screen to refresh in 15 seconds.

Back

Serial Configuration page minus the help box:

Serial Configuration

Baud Rate:

Parity bit: ☒ NONE ☐ ODD ☐ EVEN

Data bits: ☐ 7 bits ☒ 8 bits

Stop bits: ☒ 1 bit ☐ 2 bits

Rx Idle Time : [5 to 1000 char time]

Tx Idle Time : [1 to 1000 char time]

Serial Configuration

Baud Rate:

Parity bit: ☐ ODD ☐ EVEN

Data bits: ☒ 8 bits

Stop bits: ☐ 2 bits

Rx Idle Time : [1 to 1000 char time]

Tx Idle Time : [1 to 1000 char time]

LAN configuration page:

LAN Configuration

TCP/IP

IP Address:	205	166	54	175
Network Mask:	255	255	255	0
Gateway IP Address:	0	0	0	0
Ethernet Mode:	<input checked="" type="radio"/> Auto <input type="radio"/> 100Mb-Full <input type="radio"/> 100Mb-Half <input type="radio"/> 10Mb-Full <input type="radio"/> 10Mb-Half			

Save

Cancel

User Configuration page:

User/Password Configuration

Username :	<input type="text"/>
Password :	<input type="password"/>
Verify Password :	<input type="password"/>

Save

Cancel

Configuration Summary page:

Serial Encryption Module V1.0

Serial Configuration

Baud Rate (bps)	9600
Parity	NONE
Data Bits	8 bits
Stop Bits	1 bit
Port 1	RS232
Port 2	RS232
Rx Idle Time (char time)	12
Tx Idle Time (char time)	2

LAN Configuration

IP Address	205.166.54.175
Network Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Ethernet Mode	Auto

Set to Defaults

Port Activity page:

Port Activity

Serial

Clear Bytes received: 0


Clear Bytes transmitted: 0

Network

Packets received: 102

Packets transmitted: 88

Packet errors: 0

After entering the data using the HTML method (browser), there is no need to press a save and exit key. There is a "SAVE"  button on every page.

6. INTERFACE SIGNALS AND CABLING

6.1 Introduction

The serial ports on the *MDS SCADA*crypt can be either *RS-232* or *RS-422/485*. The configuration is changed using internal jumpers.

To change the setting, remove the board from the case by removing 2 screws from the front panel and sliding the circuit board assembly out of the case. There is a row of jumpers and three rows of pins behind each serial connector. For *RS-232* operation, the jumpers should cover the two pins nearest the connector. For *RS-422/485* operation, move the jumper block to cover the two rows of pins away from the connector.

The default setting is *RS-232*.

6.2 RS-232 Port Interface (DE-9P)

<u>Pi</u> <u>n</u>	<u>Signal</u>	<u>In/Out</u>
1	Carrier Detect	IN
2	Receive Data	IN
3	Transmit Data	OUT
4	Data Terminal Ready	OUT
5	Signal Ground	--
6	Data Set Ready	IN
7	Request to Send	OUT
8	Clear to Send	IN
9	NOT USED	

6.2.1 RS-232 Signals Through *MDS SCADA*crypt

Port 1	Port 2
TxD -----	>RxD
RxD< -----	TxD
RTS -----	>CTS
CTS< -----	RTS
DTR-----	>DCD
DCD<-----	DTR
DSR	Ignored DSR

6.3 RS 422/485 4-Wire Interface (DE-9P)

<u>Pi</u> <u>n</u>	<u>Signal</u>	<u>In/Out</u>
1	NOT USED	
2	NOT USED	
3	Receive Data Return (RxD-)	IN
4	Transmit Data Return (TxD-)	OUT
5	--	----
6	NOT USED	
7	NOT USED	
8	Receive Data (RxD+)	IN
9	Transmit Data (TxD+)	OUT

6.4 RS 485 2-Wire Interface (DE-9P)

<u>Pi</u> <u>n</u>	<u>Signal</u>	<u>In/Out</u>
1	NOT USED	
2	NOT USED	
3	Data Return -	IN/OUT
4	NOT USED	
5	Signal Ground	--
6	NOT USED	
7	NOT USED	
8	Data +	IN/OUT
9	NOT USED	

6.5 Cables

The RS-232 serial ports on the *MDS SCADA*crypt are configured as Data Terminal Equipment (DTE). This is the same configuration used on PC COM ports. To connect the *MDS SCADA*crypt to peripheral equipment, use the same cable that would be used to connect that equipment to a PC COM port.

To connect the *MDS SCADA*crypt to a DCB SR/SR 4 Series Multiplexer Composite port, use the following cable wiring:

(Adapter available as P/N 9802067)

RJ-45		DE-9S
1	BLU	NC
2	ORG	NC
3	BLK	7
4	RED	5
5	GRN	2
6	YEL	3
7	BRN	1,8
8	WHT	4

7. TROUBLESHOOTING

When troubleshooting problems, a rational plan can save considerable time. The following is a brief outline of standard troubleshooting procedures.

1. Gather the facts to determine the exact nature of the problem.
2. Draw a picture of the system showing the equipment at both the host and remote ends and the phone lines or in-house wiring. Use this as a reference to note your observations, test steps and test results. A picture keeps you focused and often saves duplicate effort.
3. Record the front panel indications before changing anything. This is an important part of fact-gathering.
4. If you change anything, change only one thing at a time.
5. Record your results.

8. IN CASE OF DIFFICULTY

MDS products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for MDS products is available from our Technical Support Department during business hours (8:00 A.M.—5:30 P.M. Eastern Time). When calling, please give the complete model number of the unit, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved over the telephone, without the need for returning the unit to the factory. Please use one of the following means for product assistance:

Phone: 585 241-5510
FAX: 585 242-8369

E-Mail: TechSupport@microwavedata.com
Web: www.microwavedata.com

FACTORY SERVICE

Component level repair of equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your unit to its proper operating specifications.

If return of the equipment is necessary, you will be issued a Service Request Order (SRO) number. The SRO number will help expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the SRO number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an SRO number.

A statement should accompany the unit describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to it. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

The unit must be properly packed for return to MDS. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

Microwave Data Systems
Product Services Department
(SRO No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Product Services Group at 585-241-5540 (FAX: 585-242-8400), or via e-mail at ProductServices@microwavedata.com.