

TL-150 Installation Instructions

Residential IP Alarm Communicator

THESE INSTRUCTIONS MUST BE USED WITH THE ALARM CONTROL PANEL INSTALLATION MANUAL

Power Draw: 65 mA

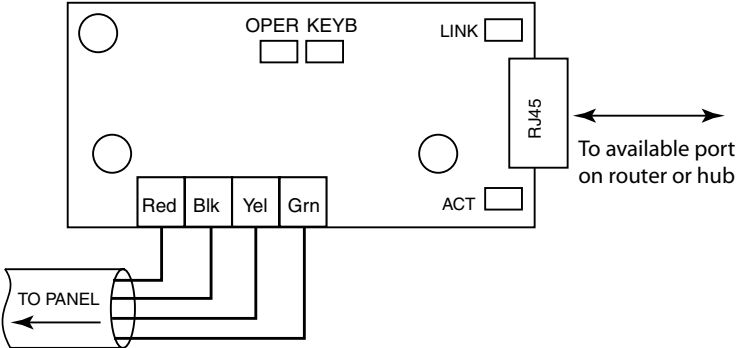
Terminal Connections

KEYBUS - The 4-wire KEYBUS connection is used by the panel to communicate with the module. Connect the RED, BLK, YEL and GRN terminals to the KEYBUS terminals on a PowerSeries™ panel.

RJ45 - Requires an 8-conductor UTP network cable with an RJ-45 connector on the end. This cable is required to plug into an available port on a router or other DHCP serving network.

To Connect Module to a Control Panel

- Connect module to the Keybus (with the panel powered down).
- Connect an 8-conductor UTP network cable with RJ-45 connector to an available router, switch or hub port with a DHCP server available.
- Power up the system.



NOTE: The TL-150 module automatically enrolls with the security system as PC5400/DVACS module.

Name	Color	Description
KEYB	Green	OFF - Security system is not connected Flashing - Security system detected but device does not have IP address Solid - Normal operation
OPER	Red	OFF - System is not powered Flashing - Normal operation Solid - Hardware fault
ACT	Red	Flashes - Upon Ethernet activity. Incoming packets only
LINK	Green	OFF - No Ethernet link ON - Ethernet link established

Administrator's Programming

- To enter Administrator's Programming: on a computer on the same network, launch a web browser and type "tl-150" in the URL entry line. You will be prompted for a user-name and password. The default administrative username is "admin" and the default password is "admin". This password can be changed any time. *The default homeowner username is "user" and the default password is "user".*
- From the main page choose the "Config" hyperlink in the top right corner.
- Enter the IP address of the DRL-IP where this module reports.

DRL-IP Reporting IP Address0.0.0.0MODIFY

OFFLINE

- Enter the new Receiver Port number (if required).

Receiver Port (MAX: 9999)3061MODIFY

- Enter the Encryption Key. Enter up to 32 HEX characters, unused characters are zero padded.

Encryption Key (HEX - up to 32 Characters)00000000000000000000000000000000MODIFY

- Enter the customer's account number.

Account Code (4-6 Digits)4566MODIFY

- Enter the test transmission period (Valid Entries: 0-99). The number you enter is the number of 15 minute increments the device will wait before sending a test transmission. A value of "0" will disable the test transmission. Enabling test transmissions also enables network supervision. See NOTE 3.

Test Transmission Period (X 15 minutes (0-99) - 0 to disable)1MODIFY

- Administrator password.

Administrator PasswordMODIFY

- Reboot the module using the "Reboot Module" link at the bottom of page.

Reset of Admin Password

If the installer forgets the administrator password, it is possible to default the module's administrator's password. Defaulting the password will send a signal to the central station of a password change (SIA - JV40) . This is to inform the central station of a possible "take-over" attempt. The installer must request the following URL to default the password: http://tl-150/8328641

NOTES:

- Only one TL150 can be enrolled on a local network
- If any of the DRL-IP Reporting IP, Cypher Key, Account Code fields are changed you must reboot the module using the "Reboot Module" link at the bottom of the page.

- Enabling test transmissions also enables network supervision. If the network connection is down at the time of a test transmission, a General System Supervisory Trouble will be triggered and the panel will go into trouble. The trouble will be restored on the next successful communication with the receiver. Setting this value to zero disables network supervision entirely.
- Only the following browsers are supported: Internet Explorer, Firefox/Mozilla, and Netscape.

LIMITED WARRANTY

Digital Security Controls warrants that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use and that in fulfillment of any breach of such warranty, Digital Security Controls shall, at its option, repair or replace the defective equipment upon return of the equipment to its repair depot. This warranty applies only to defects in parts and workmanship and not to damage incurred in shipping or handling, or damage due to causes beyond the control of Digital Security Controls such as lightning, excessive voltage, mechanical shock, water damage, or damage arising out of abuse, alteration or improper application of the equipment.

The foregoing warranty shall apply only to the original buyer, and is and shall be in lieu of any and all other warranties, whether expressed or implied and of all other obligations or liabilities on the part of Digital Security Controls. Digital Security Controls neither assumes responsibility, nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

In no event shall Digital Security Controls be liable for any direct, indirect or consequential damages, loss of anticipated profits, loss of time or any other losses incurred by the buyer in connection with the purchase, installation or operation or failure of this product.

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

Important Information: Changes or modifications not expressly approved by Digital Security Controls could void the user's authority to operate this equipment.

Warning: Digital Security Controls recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

FCC COMPLIANCE STATEMENT

CAUTION: Changes or modifications not expressly approved by Digital Security Controls could void your authority to use this equipment.

This equipment generates and uses radio frequency energy and if not installed and used properly, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for Class B device in accordance with the specifications in Subpart "B" of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in any residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to television or radio reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient the receiving antenna
 - Relocate the alarm control with respect to the receiver
 - Move the alarm control away from the receiver
 - Connect the alarm control into a different outlet so that alarm control and receiver are on different circuits.
- If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the FCC useful: "How to Identify and Resolve Radio/Television Interference Problems". This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, Stock # 004-000-00345-4.



TL-150 Instrucciones de Instalación Comunicador Residencial Del Alarmer del IP

Este manual se debe utilizar junto con el Manual de instalación del panel de control

Consumo: 65 mA

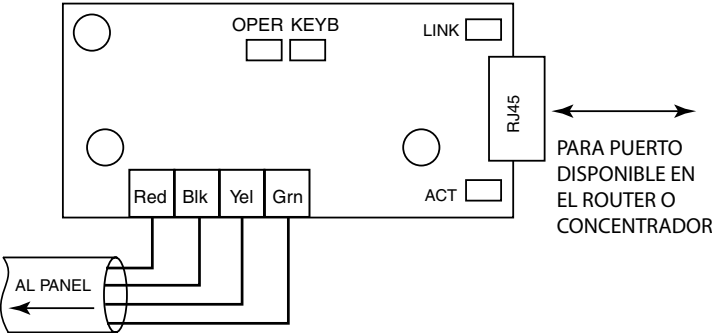
Terminación de Conexiones

KEYBUS - La conexión de KEYBUS de 4 cables es utilizada por el panel para comunicarse con el módulo. Conecte los terminales RED, BLK, YEL y GRN en los terminales KEYBUS en un panel PowerSeries™.

RJ45 - Requiere un cable UTP de 8 conductores con un conector RJ-45 en el extremo. Este cable es necesario para conexión en una puerta disponible en un enrutador u otra red servidora DHCP.

Para Conectar un Módulo a un Panel de Control

- Conecte el módulo al Keybus (con el panel desconectado de la electricidad).
- Conecte un cable UTP de 8 conductores con un conector RJ-45 en un puerto disponible de un router, conmutador o concentrador con un servidor DHCP disponible.
- Energice el sistema.



NOTA: El módulo TL-150 se conecta automáticamente al sistema de seguridad como un módulo PC5400/DVACS.

Nombre	Color	Descripción
KEYB	Verde	APAGADO - sistema de seguridad no conectado INTERMITENTE - sistema de seguridad detectado, pero el dispositivo no tiene dirección IP LIGADO - operación normal
OPER	Rojo	APAGADO - sistema no energizado INTERMITENTE - operación normal ENCENDIDO - falla en el hardware
ACT	Rojo	PARPADEA bajo actividad Ethernet. Solamente entrada de paquetes
LINK	Verde	APAGADO - sin conexión Ethernet ENCENDIDO - conexión Ethernet establecida

Programación del Administrador

- Para entrar en la Programación del Administrador: en una computadora en la misma red, inicie un navegador de Internet y digite "tl-150" en la línea de entrada de URL. Será solicitado un nombre de usuario y contraseña. El nombre de usuario administrativo estándar es "admin" y la contraseña estándar es "admin". Esta contraseña podrá alterarse a cualquier momento. *El nombre de usuario residencial estándar es "user" y la contraseña estándar es "user".*
- En la página principal, seleccione el hyperlink "Config" en el rincón superior derecho.
- Digite la dirección IP del DRL-IP para el cual este módulo deberá transmitir.

DRL-IP Reporting IP Address 0.0.0.0

OFFLINE

- Entre el nuevo numero del puerto para el Receptor (Si es necesario).

Receiver Port (MAX: 9999) 3061

- Digite la llave de codificación (Encryption Key). Digite hasta 32 caracteres HEX, caracteres no utilizados serán completados con ceros

Encryption Key (HEX - up to 32 Characters) 00000000000000000000000000000000

- Digite el número de cuenta del cliente.

Account Code (4-6 Digits) 4566

- Digite el período de transmisión de prueba. El número informado es un incremento de 15 minutos en que el dispositivo esperará antes de enviar una transmisión de prueba. Un valor de "0" deshabilitará la transmisión de prueba. La habilitación de la transmisión de prueba también habilitará la supervisión de red. Ver la Nota 3.

Test Transmission Period (X 15 minutes (0-99) - 0 to disable) 1

- Contraseña del Administrador.

Administrator Password

- Reinicie el módulo utilizando el enlace "Reboot Module" (Reiniciación del Módulo) en la parte inferior de la página.

Restablecer el Contraseña del Administrador

Si se le olvida al administrador el contraseña, es posible restablecer el contraseña del módulo del administrador. Al restablecer el contraseña se mandara una señal a la estación central del cambio de contraseña (SIA JV40). Esto se hace para informar a la estacion central de un posible "asumir cargo de" cuenta por otro instalador.

NOTAS:

- Solo un TL150 puede ser instalado en el red local.
- Si el campo de IP de Transmisión DRL-IP, Contraseña Cifrada, o Código de Cuenta fuere alterado, se debe reiniciar el módulo utilizando el enlace "Reboot Module" en la parte inferior de la página.
- La habilitación de la transmisión de prueba también habilitará la supervisión de red. Si la conexión de red estuvo fuera del aire en el momento de la transmisión de prueba será generado un Problema en la Supervisión General del Sistema (General System Supervisory Trouble), y el panel estará en estado de problema. El problema será solucionado en la próxima comunicación bien sucedida con el receptor. Ajustando este valor en cero la supervisión de red será totalmente deshabilitada.
- Solo los siguientes buscadores son apoyados : Internet Explorer, Firefox/Mozilla, Netscape.

Garantía Limitada

Digital Security Controls garantiza que por un período de doce meses desde la fecha de adquisición, el producto estará libre de defectos en materiales y mano de obra bajo condiciones de uso normal y que, en cumplimiento de cualquier violación de dicha garantía, Digital Security Controls podrá, a su opción, reparar o reemplazar el equipo defectuoso al recibo del equipo en su local de servicio. Esta garantía se aplica solamente a defectos en componentes y mano de obra y no a los daños que puedan haberse presentado durante el transporte y manipulación o a daños debidos a causas fuera del control de Digital Security Controls Ltd. tales como rayos, voltaje excesivo, sacudidas mecánicas, daños por agua, o daños resultantes del abuso, alteración o aplicación inadecuada del equipo.

La garantía anterior se aplicará solamente al comprador original y sustituye a cualquier otra garantía, ya sea explícita o implícita, y todas las otras obligaciones y responsabilidades por parte de Digital Security Controls. Esta garantía contiene la garantía total. Digital Security Controls no se compromete, ni autoriza a ninguna otra persona que pretenda actuar a su nombre, a modificar o cambiar esta garantía ni a asumir ninguna otra garantía o responsabilidad con respecto a este producto.

En ningún caso, Digital Security Controls será responsable de cualquier daño o perjuicio directo, indirecto o consecuente, pérdidas de utilidades esperadas, pérdidas de tiempo o cualquier otra pérdida incurrida por el comprador con relación a la adquisición, instalación, operación o fallo de este producto.

Los detectores de movimiento solamente pueden detectar movimiento dentro de las áreas designadas como se muestra en las respectivas instrucciones de instalación. Los detectores de movimiento no pueden discriminar entre intrusos y los que habitan el local o residencia. Los detectores de movimiento no proporcionan un área de protección volumétrica. Estos poseen múltiples rayos de detección y el movimiento solamente puede ser detectado en áreas no obstruidas que están cubiertas por estos rayos. Ellos no pueden detectar movimiento que ocurre detrás de las paredes, cielo rasos, pisos, puertas cerradas, separaciones de vidrio, puertas o ventanas de vidrio. Cualquier clase de sabotaje ya sea intencional o sin intención tales como encubrimiento, pintando o regando cualquier tipo de material en los lentes, espejos, ventanas o cualquier otra parte del sistema de detección perjudicará su correcta operación.

Los detectores de movimiento pasivos infrarrojos operan detectando cambios en la temperatura. Sin embargo su efectividad puede ser reducida cuando la temperatura del ambiente aumenta o disminuye de la temperatura del cuerpo o si hay orígenes intencionales o sin intención de calor en o cerca del área de detección. Algunos de los orígenes de calor pueden ser calentadores, radiadores, estufas, asadores, chimeneas, luz solar, ventiladores de vapor, alumbrado y así sucesivamente.

ADVERTENCIA: Digital Security Controls recomienda que el sistema sea probado en su integridad con la debida regularidad. Sin embargo, a pesar de pruebas frecuentes y debido a interferencia criminal o cortes eléctricos, pero no sólo limitado a ellos, es posible que este producto deje de operar en la forma esperada.

INFORMACIÓN IMPORTANTE: Los cambios o modificaciones no aprobadas expresamente por Digital Security Controls, pueden cancelar la autoridad del usuario para operar este equipo.

DSC



©2005 Digital Security Controls
Toronto, Canada • www.dsc.com
Tech. Support: 1-800-387-3630 (Canada & U.S.), 905-760-3036

Printed in Canada