



READ ME FIRST!!

UTM

UNIVERSAL TRUNK MODULE

PRODUCT / RELEASE NOTES

RELEASE 17.1

102 SW Orange Blossom
Lake City, Florida
32025-1613
Phone: 386-754-5700
email: sales@trdcusa.com
<http://www.trdcusa.com>

Manufacture & Distribution:



<http://www.datatekcorp.com>

TABLE OF CONTENTS

1	Introduction.....	5
2	Product Features	5
3	Release Changes	6
3.1	Release 17.1 Errata	6
3.2	Release 16.2 Errata	6
3.3	Release 16.1 Errata	7
3.4	Release 15 Errata	9
3.5	Release 14 Errata	10
3.6	Releases prior to 14.....	11
4	Installation Addendum	12
4.1	Obtaining Information from TeleComp R&D	12
4.2	Database Conversions	12
4.3	Software Registration	12
4.4	Utilities	12
4.5	Power	13
5	Documentation	13
6	Hardware Warranty.....	14
7	End-User License Agreement for Software.....	14
7.1	Software License	14
7.2	Intellectual Property Rights	14
7.3	Software Support	15
7.4	Export Restrictions	15
7.5	Limited Warranty.....	15
7.6	No Other Warranties	15
7.7	Special Provisions	16
8	Limitation of Liability	16
9	Sales & Distribution	17
10	Author.....	17

IMPORTANT !!

USER DOCUMENTATION IS AVAILABLE AT OUR WEB SITE.

Documentation:	http://www.trdcusa.com
Sales:	sales@trdcusa.com

The **UTM** is shipped from the factory with the inslot “magic” jumper disabled. This configuration assumes the UTM directly connects to another node. Refer to the UTM User’s Manual at <http://www.trdcusa.com> for instructions on changing this factory setting.

Special Installation and Upgrade Procedures

- **Database Conversion** – Release 16.1 and later will convert a UTM database that is on either build 14 or 15. If the present build on your UTM is build 13 or lower, then the UTM database must be converted to build 15 before the UTM can be upgraded to release 16.1 or higher. After upgrading from the older build to build 15, make one parameter change of anything to insure the database is converted. Then do a vfy mod, and send the result to keys@trdcusa.com so that the UTM can be properly registered before the installation of build 16.1 or higher. **Failure to install build 15 on a module currently running build 13 or lower will cause a problem to occur, and the module will have to be sent back to the manufacturer for repair at the customer’s expense.**
- **Telnet Console Address** – The telnet console port number has been changed from port 23 to port 1023 starting with build 16.1 in order to be consistent with other products. The current upgrade (18.4), backup (18.4), and reload (18.4) utilities still default to port 23. So therefore the “-t” option must be used to specify the telnet port of 1023 (“-t1023”) on the command line for each of the utilities after release 16.1 is installed.
- **Release Numbers** - Build numbers, beginning with release 16.1, consist of two parts: a release number and version level.

- **Activation Keys** – The UTM, when initially manufactured and delivered to the customer, *may* need a software key to fully activate the software¹. If so, when initially delivered, the equipment can be installed, but the module cannot be restored to service after it is configured until the keys are entered. In addition, when the UTM is upgraded with a new software build, a software key is required to activate the new software. The software initially is placed into a staging area and is not active. However, prior to the information being obtained for mechanized key generation, the device must be rebooted to make the new software active. When the reboot is executed without the new key being installed, the new software will execute, and the device will continue functioning as it did previously. However, no backup, reloads, or upgrades can be performed nor can any OA&M be performed or parameters, such as an IP address, be changed until the key(s) have been installed for the active software. If the module is taken out of service, the module cannot be restored until the new key(s) are installed.
- **Mechanized Key Procedure** – A mechanized key procedure is required starting with release 16.1. The mechanized procedure simplified the key installation and allows many devices to be installed at the same time.
- **Serial Port Upgrade Anomaly** – There is an anomaly when performing the upgrade of a UTM that is using a DTK41 I/O board through its console serial port. An upgrade via the normal TELNET console is not affected. Should the anomaly occur, the upgrade download will fail. In that event, the –slow option of the upgrade utility is required. The –slow option will require an extended period for downloading, but is a workaround to this anomaly.

¹ It is the intent of the manufacturer, and its resellers, to have already installed the key(s) before receipt by the end-customer, so that the software is fully functional.

1 INTRODUCTION

These release notes highlight the product features, modifications, known caveats and any special considerations for the Universal Trunk Module (**UTM**) product. For detailed information on this product, reference the **UTM** User's Manual.

2 PRODUCT FEATURES

The **UTM** is a BNS² module that allows the customer to employ more cost-effective interconnection facilities between nodes and other BNS product family components. Facilities such as IP, ATM or Frame Relay can be used rather than traditional leased line services.

The **UTM** permits the movement of the BNS products toward the network edge. This is implemented by interconnecting BNS nodes, Remote Shelves and SAM devices over different backbone networks such as IP, ATM and Frame Relay.

The **UTM** supports an IP infrastructure, which is compatible with an IP-DSU³. It also supports a base protocol layer of HDLC, Frame Relay, and AAL5 ATM, all at rates up to E1. The transport layer is implemented using the BNS DDS, SWT, or PQ trunk protocols. UTM trunk interfaces can be duplexed for higher reliability as well.

The **UTM** is used in place of the CPM-HS module when the connection to a remote host is using IP-CommKit[®]. Using IP-CommKit and **UTM**, the host does not physically have to be collocated with the node but can be anywhere in a connected IP network, i.e. across the room or across the world. Throughput to the host is increased approximately 100% when the **UTM** is used. On the host side, the connection uses the resident host ethernet[™] module instead of a specially developed and costly hardware module that may slow down the host bus. Host CPU utilization is reduced to approximately 1/3 of its original value.

Consult the **UTM** User's manual for a complete enumeration of the features..

² In this document, BNS means any of the members of the BNS family of products which includes the BNS-2000 nodes and the BNS-2000 VCS nodes (a.k.a. Datakit® VCS nodes).

³ The IP-DSU allows router (IP) networks to carry both its original traffic and its new BNS-2000/BNS-2000 VCS trunk traffic simultaneously. The IP-DSU replaces an existing, conventional DSU on each end of the circuit and eliminates the interconnecting dedicated facility.

[®] IP-CommKit is a trademark of Lucent Technologies, Inc. licensed to Datatek Applications, Inc, a company independent of Lucent Technologies, Inc.

[™] Ethernet is a trademark of the XEROX Corporation.

3 RELEASE CHANGES

3.1 RELEASE 17.1 ERRATA

- Support for TACACS+ RADIUS servers is added. Two servers are supported, a primary and a secondary. Non-standard TCP ports are fully supported. Each server may be individually enabled. The syntax is as follows:

**Syntax: tac < PRI | SEC > [ipaddr=<IP Address>]
[port=<TCP Port>]
[key="Encryption Key" | NONE]
[ENABLE]
[DISABLE]**

- A BANNER page has been updated with up to 24 lines of 80 characters each. The syntax is changed as follows:
Syntax: banner [clear] [L#="Line # Message"]
- A correction is implemented to the TCP that prevents the potential for some additional packets, and a possible deadlock, at connection teardown.
- The SNMP agent has been updated to include protections from malicious attack. It should also be noted that access to the the SNMP agent can be restricted by closed user groups.
- The DBRESET command has been changed to prompt for the password rather than accepting it on the command line. This makes the command consistent with the other products in the product line; and enhances the security of the command.

3.2 RELEASE 16.2 ERRATA

- A "Restore Module" command with an incorrect password would restore the UTM to service, but not effect the software reboot. As such, it was not ready for transport. A subsequent reboot command was a satisfactory workaround. The problem is corrected in this release.
- There was an error in the "Restore Passwords" command which prevented it's operation. This could lead to the inability to access the device should the passwords be misplaced as the command is the failsafe mechanism for recovery. The anomaly was corrected in this release.
- Support has been added for interproduct database conversions.
- The Console Timeout command has changed the semantics of the command from seconds to minutes. This allows a console inactivity timeout from one to 255 minutes, or roughly four hours. Previously, this was 15 to 255 seconds. The syntax of the command has not been changed. See the **UTM** user's manual for more information.

- Due to hardware changes in the AM7 series of modules, the memory test was executed on each reboot. The original intent was to execute the memory test only on a power-up. The AM1 through AM6 modules work that way. This release changes the hardware management such that the AM7 series behaves in the same manner as the other series. A memory test will occur only when the module is initially power cycled.

3.3 RELEASE 16.1 ERRATA

- Six new parameters have been added to the **SNMP** command: **COMM**, **PUBLIC**, **SYSCONTACT**, **SYSNAME**, **SYSLOC**, and **CUG**. The syntax of the command is now:

```
Syntax: snmp [ COMM="Double Quoted String" | NONE ]
          [ PUBLIC=< YES | NO > ]
          [ SYSCONTACT="Double Quoted String" | NONE ]
          [ SYSNAME="Double Quoted String" | NONE ]
          [ SYSLOC="Double Quoted String" | NONE ]
          [ CUG=<<+|->CUG Number> ]
          [ ipaddr=<trap manager address> ]
          [ port=< trap manager port> ]
```

The UTM allows the setting of an SNMP community in addition to the “public” community. When configured, the UTM will respond to SNMP manager requests in that community. The UTM will always respond to a request in the “public” community. The settable SNMP community is configured with the [**COMM**="Double Quoted String" | **NONE**] option. The community string may be in any case and up to 31 characters long, not including the double quotes that are used to enclose it. Setting **COMM=NONE** will clear the community.

The **PUBLIC** option allows the setting of whether or not the SNMP agent "public" community is recognized. The default is that the "public" community is recognized (YES). When the value is set to **NO**, the "public" community is not recognized. *After setting the option to YES or NO, the unit must be rebooted in order to have the value take effect.*

The MIB-II variables **sysName**, **sysContact**, and **sysLocation** may be initialized for the UTM non-volatile database using the **SNMP** command with the following parameters: **SYSCONTACT**, **SYSNAME**, and **SYSLOC**. The initial default values are strings that state that the initial values are not set. These variables are still volatile in that they may be over-written by an SNMP manager. However, any change made by the SNMP manager will not impact the UTM non-volatile database. Setting the value to **NONE** will clear the entries in the UTM non-volatile database. Each field may be in any case and up to 31 characters long, not including the double quotes that are used to enclose it. Any of the three parameters, **SYSCONTACT**, **SYSNAME**, and **SYSLOC**, may be cleared by setting the parameter keyword to the value **NONE**.

Any combination of the **CUGs** may be assigned to the SNMP interface using the SNMP command with the Closed User Group option (**CUG**). Packets that fail the SNMP Closed User Group test are discarded. An alarm is not displayed, but the failure is counted. The number of failures may be displayed with the **dmeas mod** command.

- The telnet console port number has been changed from port 23 to port 1023 starting with build 16.1 in order to be consistent with the other products. The current upgrade (18.4), backup (18.4), and reload (18.4) utilities still default to port 23. So therefore the “-t” option must be used to specify the telnet port of 1023 (“-t1023”) on the command line for each of the utilities.

- A banner message can be configured of up to 10 lines, where each line can have up to 29 characters. This banner is output upon execution of the login command after the prompt for the password.

Syntax: `banner [clear] [L#="Line # Message"]`

Where # is 1-9 and A (hexadecimal 10)

The **banner** command is only visible when the administrator is logging into the unit. This command is used to configure the security banner. The default is a NULL banner. If a security banner is configured, it is displayed at each user login. Use of the **clear** option will erase the entire message.

- The DTK41 **HPIO** command now allows each wire (10/100) physical interface (**PHY**) to be configured into a static mode. The default is the same as before; auto-negotiate. The PHY can be set into a static mode of 10Mbps Half Duplex (**10HDX**), 10Mbps Full Duplex (**10FDX**), 100Mbps Half Duplex (**100HDX**), and 100Mbps Full Duplex (**100FDX**). This feature was implemented in order to overcome a problem with auto-negotiation on some (but not all) Cisco Catalyst switches.

Syntax: `HPIO RESET`

`ENABLE < ALL | FIBER | <10/100 PHY RANGE> >`

`DISABLE < ALL | FIBER | <10/100 PHY RANGE> >`

`AUTO < ALL | <10/100 PHY RANGE> >`

`10HDX < ALL | <10/100 PHY RANGE> >`

`10FDX < ALL | <10/100 PHY RANGE> >`

`100HDX < ALL | <10/100 PHY RANGE> >`

`100FDX < ALL | <10/100 PHY RANGE> >`

Because of problems with etherswitches recognizing the static modes, the implementation of this feature is actually done by selective advertisement during autonegotiation. That is when a "static" configuration of 10FDX is selected; the HPIO will only advertise 10Mbps Full Duplex to the peer. That will force the link to become that state (if the other peer is capable).

IMPORTANT: Not configuring a "static" mode properly, such as 100Mbps into a 10Mbps only hub, will result in unpredictable network problems. It is *HIGHLY RECOMMENDED* that the default of AUTO be always used unless a specific special situation exists.

The **hpio** commands can only be entered via the UTM consoles. The **hpio** commands cannot be executed on the BNS/Datakit[®] nodes.

The HPIO database (DB) is backed up when the UTM undergoes a database backup, and restored when the UTM undergoes a reload. There is no separate command for these functions. Note that the DB files created have a new version ID and format. Files created by prior versions of the UTM will not be accepted during the reload process.

- The **reboot** command has been changed to prompt for a password before it is executed, similar to the other products.

[®] Datakit is a registered trademark of Lucent Technologies, Inc. licensed to Datatek Applications, Inc, a company independent of Lucent Technologies, Inc.

- The report generated by the command **vfy mod** now includes the hardware serial number. This number is required for module registration for the generation of keys.
- The report generated by the command **vfy mod** has been modified to show the status of the "public" community, the user specified community and the CUGs assigned to the SNMP interface.
- The report generated by the command **vfy mod** has been modified to show the type of I/O board used on the backplane: **CEY5** or **DTK41**.
- The **traceroute** command when issued from an IP-CommKit host would not terminate when the host was the peer to the **UTM**. The **traceroute** command would work properly when the host was not the peer. Other peers, such as a DT-SAM or DT-4000, or even another **UTM** would work fine. The IP-CommKit host uses UDP packets for tracing the route and not ICMP "ping" packets. This is legal, but the implementation allowed these to be queued in the UTM queues. The host then considered them lost. This has been corrected.
- Qwest reported that SNMP traps were being sent as a broadcast. Some routers are having trouble with that form of addressing as address screens are applied. The UTM will now ARP for the next hop before sending any trap. The ARP for the MAC will occur only until it is acquired. It is saved for subsequent use.
- The database reload operation using the **reload** utility now prevents the following fields from being overwritten by the utility: **MAC** address, **local ipaddr** and **submask**, and **gateway ipaddr**.
- Should the telnet console be closed by the administrator issuing the **disc console** command two times consecutively, the telnet console would be removed from the active lists of sockets and not respond. This problem was corrected.
- The UTM now requires a key to activate its software. In order to obtain a key, the module must be registered. For registration of the software, support has been added in this release for a mechanized key generation. This procedure will alleviate administrators of the tedious process of getting key generation information for each device by running a command on that device after logging into it, and then having to go back later and enter the new key manually.

This procedure requires a site to have a support host connected to the network that can connect to the individual devices over IP. The support host must use the Solaris[®], HP-UX[®] or the Linux operating system.

3.4 RELEASE 15 ERRATA

- The output of the **vfy mod** command was changed in order to display the hardware serial number. The hardware serial number is used for module tracking and registration purposes.
- A potential flow control issue that could affect service with the serial console was corrected.
- Logic was added to use the TCP probe method for keep-alives. If there is no response to a TCP probe from the distant end after an initial time-out period of 200 seconds, additional probes are sent up to 8 times at 12-second intervals. If there is still no response during the probing period, then the connection is dropped with a RST+ACK.

[®] Solaris is a registered trademark of Sun Microsystems, Inc.

[®] HP-UX is a registered trademark of Hewlett Packard, Inc. Systems Division.

3.5 RELEASE 14 ERRATA

- The **label** command has new syntax:

Syntax: `label ["Console Label" | none]`

Now a label is allowed to be up to 31 characters. The label may be a mixture of alpha characters, digits, and spaces, but *MUST* be enclosed in double quotes. Both upper and lower case are now allowed. However, a colon ":" is not allowed in the label string. If the command is issued without arguments, the current label is displayed. When issued with an argument of "none", the label becomes a NULL label.

- A new command has been added to define Closed User Group (CUG) security:

Syntax: `cug < cug num > [ipaddr=< ip address >]
[submask=< ip submask >]`

The **cug** command is only visible when the unit is logged in. The **cug num** parameter is the closed user group identifier used to assign the CUG to the telnet console (with the **console** command – see below). The **cug num** may be a value between 1 and 16, inclusive. A single IP address and subnet mask pair specifies each CUG. The **ipaddr** parameter is an address of an endpoint (or base address of a group of endpoints) to be allowed into the group. The **ipaddr** value *AND'ed* with the **submask** value must agree with the caller's IP address *AND'ed* with the same submask for a call to be allowed to the destination user port on which the CUG is assigned. Depending on the **submask** value, this allows an individual (submask=255.255.255.255), intermediate, or network-wide level of authorization. Setting the **ipaddr** value to 0.0.0.0 deletes any prior configuration for the **<cug num>**. A **<cug num>** may not be deleted if it is currently assigned to the telnet console port. However, the administrator may change the value of the **ipaddr** or **submask** for a CUG dynamically. It is not necessary to delete the **cug num** from the console first unless it is the CUG that allows the administrator's access. (See the **console** command below for more details.)

- The **vfy** command now has a new format. An argument is now required:

Syntax: `verify mod or verify cug`

- Security has been added for the telnet console. A new command, **console**, allows the assigning of CUGs to it.

Syntax: `console cug=<+ | - > < cug num>`

Where **cug num** is a number from 1 to 16 and initially defined by the **cug** command described above. Any combination of CUGs may be assigned to the telnet console. Only those users that have a compatible IP address with an administered CUG will be able to use the telnet console. If the value of a CUG is set equal to the UTM's IP address and assigned to the console, then the telnet console is disabled. The only way to enable it again is to change the CUG security via the serial console port.

CUG security is checked dynamically. Initially, when an administrator uses the telnet console, and no CUGs have previously been assigned to the console, the administrator must specify the **cug num** that matches his IP address as the first assigned CUG. If the administrator attempts to assign as the first assigned CUG a **cug num** for a CUG that won't allow access by the administrator, the assignment will be denied. Otherwise, the administrator would have been denied any further access. Similarly, when an administrator is deleting a **cug num** from the

console list, the **cug num** of the CUG that allows his access must be deleted last. Attempts to delete it prior to other **cug num**'s will be denied. If it were allowed, the administrator would have been denied any further access. After an administrator deletes all the **cug num**'s, CUG security is disabled, and his telnet session continues.

- A new command has been added which can have only one parameter: **console**

Syntax: disc console

If the telnet console is connected to the UTM, the session is terminated. This is useful in IP networks when the remote peer vanishes due to a remote reboot or network error. The effect of the command is to reset the telnet console. The user must initiate another telnet session after using this command in order to use the telnet console again.

- An attempt is made to detect a duplicate IP address by listening for ARP broadcasts that may contain this unit's IP address. If a duplicate is found, a MAJOR alarm is issued, and the MAC address of the offending device is presented.
- Changes were made that now enables a UTM module to respond properly to a UNIX[®] "traceroute" command when connected to an IP network.
- Changes were made for better compatibility when a UTM is used with an MPC. These changes reduce the chance of "Poorly Formed Status Packets" resulting in the module being removed from service automatically.

3.6 RELEASES PRIOR TO 14

Contact support@trdcusa.com with specific questions on releases older than 14.

[®] UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company, Ltd.

4 INSTALLATION ADDENDUM

4.1 OBTAINING INFORMATION FROM TELECOMP R&D

Load modules for all the TeleComp R&D products are obtained by sending email to support@trdcusa.com. All other documentation, including release notes, user manuals, “white-papers”, etc. can be accessed on the TeleComp R&D web site and downloaded for your use.

To insure that the correct version of the binary load modules have been retrieved and has not been corrupted during the transmission process, the UNIX® **sum** command can be used.

On some hosts, the “-s” flag must be used with the **sum** command. On X86 linux hosts, the **-sysv** flag must be used with the **sum** command.

Key-in **sum** < name of load module file>.

The values returned must match the numbers shown below:

For example:

Key-in: **sum -sysv univ_pp.17.1**
Response: **35207 1159 univ_pp.17.1**

4.2 DATABASE CONVERSIONS

When moving from one release or version to the next, the database is usually automatically converted. Therefore, **do not attempt** to perform a **backup** on an earlier release/version and then do a **reload** on the new release/version. The database structures may not be the same. For safety reasons, do a **backup** on the earlier release/version in case you need to revert back to this release/version. Then upgrade to the new release/version, and do a backup again which will now be the converted database for use with this release/version. Backups and restores should only be used with the same release/version, not across releases or versions.

4.3 SOFTWARE REGISTRATION

The **UTM** must be registered when it is upgraded with new software. The **UTM** will continue to operate without registration, but **various OA&M functions, including placing the module into service, will not operate until registration is complete.** See the **UTM** User’s Manual for the registration procedure.

4.4 UTILITIES

The current version of the upgrade, backup, and reload utilities are 18.4 respectively. The getinfo, devrep, and setreg utilities have a current version of 1.2. All of the utilities are available by contacting support@trdcusa.com. Please note that the TCP port for the console is 1023.

® UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company, Ltd.

4.5 POWER

The **UTM** may be powered via the node backplane. For planning purposes, a maximum consumption of 20 Watts is to be used. This is a worse case value. The actual power consumption will be substantially less than the planning value. -48VDC or 5VDC via an AC power adapter.

5 DOCUMENTATION

The current version of the **UTM** User manual, and this release letter, may be downloaded from the support area of <http://www.trdcusa.com>.

6 HARDWARE WARRANTY

The warranty period for hardware shall be ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Replacements and repairs are guaranteed for the longer of the remaining original warranty period or 30 days.

7 END-USER LICENSE AGREEMENT FOR SOFTWARE

This License Agreement ("License") is a legal contract between you and the manufacturer ("Manufacturer") of the system ("HARDWARE") with which you acquired software product(s) identified above ("SOFTWARE"). The SOFTWARE may include printed materials that accompany the SOFTWARE. Any software provided along with the SOFTWARE that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this LICENSE. If you do not agree to the terms of this LICENSE, Manufacturer is unwilling to license the SOFTWARE to you. In such event, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) for a refund.

7.1 SOFTWARE LICENSE

You may only install and use one copy of the SOFTWARE on the HARDWARE (unless otherwise licensed by Manufacturer). The SOFTWARE may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device ("Devices"). Notwithstanding the foregoing and except as otherwise provided below, any number of Devices may access or otherwise utilize the services of the SOFTWARE. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE. The SOFTWARE is licensed with the HARDWARE as a single integrated product. The SOFTWARE may only be used with the HARDWARE as set forth in this LICENSE. You may not rent, lease or lend the SOFTWARE in any manner. You may permanently transfer all of your rights under this LICENSE only as part of a permanent sale or transfer of the HARDWARE, provided you retain no copies, you transfer all of the SOFTWARE (including all component parts, the media and printed materials, any upgrades, this LICENSE and, if applicable, the Certificate(s) of Authenticity), and the recipient agrees to the terms of this LICENSE. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE. Without prejudice to any other rights, Manufacturer may terminate this LICENSE if you fail to comply with the terms and conditions of this LICENSE. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.

7.2 INTELLECTUAL PROPERTY RIGHTS

The SOFTWARE is licensed, not sold to you. The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. You may not copy the printed materials accompanying the SOFTWARE. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property

laws and treaties. This LICENSE grants you no rights to use such content. All rights not expressly granted under this LICENSE are reserved Manufacturer and its licensors (if any).

7.3 SOFTWARE SUPPORT

SOFTWARE support is not provided by Manufacturer, or its affiliates or subsidiaries separate from the HARDWARE. For SOFTWARE support, please contact your supplier of the HARDWARE. SOFTWARE support is limited to the warranty period stated below unless either a separate contract has been consummated between you and the manufacturer or the manufacturer has agreed in writing at the time of purchase by you of the software to an extension of the warranty. Should you have any questions concerning this LICENSE, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the HARDWARE.

7.4 EXPORT RESTRICTIONS

You agree that you will not export or re-export the SOFTWARE to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the SOFTWARE: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to know will utilize the SOFTWARE or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

7.5 LIMITED WARRANTY

Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Software support is limited to the hours of 9 AM to 5 PM ET Monday through Friday excluding TeleComp R&D observed holidays. Other coverage and extended warranty may be purchased at additional cost. Any implied warranties on the SOFTWARE are limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

7.6 NO OTHER WARRANTIES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MANUFACTURER AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE AND THE ACCOMPANYING WRITTEN MATERIALS. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

7.7 SPECIAL PROVISIONS

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and HARDWARE Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial HARDWARE Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is TeleComp R&D or it's designee manufacturer., 102 SW Orange Blossom, Lake City, Florida, 32025-1613.

If you acquired the SOFTWARE in the United States of America, this Software License are governed by the laws of the State of Florida, excluding its choice of laws provisions. If you acquired the SOFTWARE outside the United States of America, local law may apply. This LICENSE constitutes the entire understanding and agreement between you and the Manufacturer in relation to the SOFTWARE and supersedes any and all prior or other communications, statements, documents, agreements or other information between the parties with respect to the subject matter hereof.

8 LIMITATION OF LIABILITY

To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this License shall be limited to the amount actually paid by you for the SOFTWARE and/or the HARDWARE. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

9 SALES & DISTRIBUTION



Communications Technology Solutions

CBM of America, Inc.
Mr. Mike Stephens
1455 West Newport Center Drive
Deerfield Beach, Florida
33442

800-881-8202
954-698-9104 Fax: 954-360-0682

www.cbmusa.com



Datatek Applications, Inc.
Mr. Dan Conklin
379 Campus Drive, Suite 100
Somerset, New Jersey
08873

732-667-1080 Fax: 732-667-1091

www.datatekcorp.com

10 AUTHOR

Comments and Questions regarding this document or the products covered within this document should be addressed to the author Angel Gomez via email at angel@trdcusa.com or via telephone at 386-754-5700.

©Copyright 2003, 2008 TeleComp R&D Corp.
©Copyright 1998, 2002 TeleComp, Inc.
All Rights Reserved
Printed in USA