

Dataatek



ENHANCED SECURITY GUIDE

ISSUE 2

379 Campus Drive, Suite 100
Somerset, NJ 08873
fax: 732.667.1091
phone: 732.667.1080
email: sales@datatekcorp.com
<http://www.datatekcorp.com>



TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	What is the IP-CommKit Enhanced Security Feature?	3
2	REGISTRATION	5
3	CONFIGURATION	6
4	TROUBLESHOOTING	7
4.1	Check the UTM	7
4.2	Check /var/opt/dk/log/dkipdlog.....	7
5	END-USER LICENSE AGREEMENT FOR SOFTWARE	9
5.1	SOFTWARE LICENSE	9
5.2	INTELLECTUAL PROPERTY RIGHTS.....	9
5.3	SOFTWARE SUPPORT.....	10
5.4	EXPORT RESTRICTIONS	10
5.5	LIMITED WARRANTY	10
5.6	NO OTHER WARRANTIES	10
5.7	SPECIAL PROVISIONS.....	11
5.8	LIMITATION OF LIABILITY	11



1 INTRODUCTION

This document describes the IP-CommKit™ Enhanced Security Feature, and is written as a supplement to the *IP-CommKit Installation and Administration Guide*. If you are not familiar with IP-CommKit, please read it first.

1.1 WHAT IS THE IP-COMMKIT ENHANCED SECURITY FEATURE?

The IP-CommKit Enhanced Security Feature protects the communications between your host computer and BNS-2000/BNS-2000 VCS endpoints from eavesdroppers in the IP network. IP-CommKit allows you to connect a host computer to a BNS network through an IP network. While the closed architecture of BNS networks make eavesdropping exceptionally difficult, the open architecture of IP networks can expose your data to a large group of unauthorized listeners. Using inexpensive, commercially available test equipment, an eavesdropper with access to the IP network can easily observe the data that the host and BNS endpoints exchange. The IP-CommKit Enhanced Security Feature automatically encrypts the data that passes through the IP network, making it useless to eavesdroppers.

The IP-CommKit Enhanced Security Feature is transparent to both the host application and the BNS network endpoints. No changes to your host application or BNS node configuration are required. Data leaving the host computer is encrypted by the IP-CommKit software and decrypted when it enters the BNS network at the UTM module. Similarly, data leaving the BNS network is encrypted by the UTM module and decrypted when it reaches the host computer by the IP-CommKit software. The host application and BNS endpoints are unaware of the process.

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



The IP-CommKit Enhanced Security Feature also makes it more difficult for an unauthorized host computer to gain access to the BNS network through the UTM module. In *IP-CommKit Security Analysis*, the effect of IP-CommKit on the vulnerability of BNS networks to unauthorized access is examined. The conclusion is that several layers of protection make a successful attack unlikely. The IP-CommKit Enhanced Security Feature adds another layer of protection, further reducing the probability of a successful attack.

The IP-CommKit Enhanced Security Feature uses a proprietary encryption algorithm. While Datatek does not describe the algorithm in the documentation, it has the following properties:

- ❑ The host computer and UTM module use different encryption keys.
- ❑ Every host computer and UTM module uses a different encryption key.
- ❑ The host computer generates the encryption key used by the UTM from IP-CommKit configuration data, and vice versa, so there is no need for the host computer and UTM module to exchange keys through the IP network.
- ❑ The encryption algorithm is efficient, and results in a negligible increase in CPU utilization on the host computer.
- ❑ The encryption algorithm does not increase the size of the messages exchanged by the host and UTM module. Thus, there is no increase in the IP network traffic load.

The encryption algorithm used in the IP-CommKit Enhanced Security Feature is not powerful enough to thwart sophisticated cryptographic attacks, such as those mounted by government agencies or organized crime groups. As a result, the IP-CommKit Enhanced Security Feature is not suitable for protecting financial or military information in public networks. For these applications, contact Datatek for information about using IPsec with IP-CommKit.



2 REGISTRATION

The IP-CommKit Enhanced Security Feature was incorporated into the IP-CommKit software starting with release 1.0.13 (a.k.a. Build 13). However, you must purchase a license to use the IP-CommKit Enhanced Security Feature for a small additional cost. Datatek manages all IP-CommKit licenses with the software registration process described in the *IP-CommKit Installation and Administration Guide*. If you have purchased a license to use the IP-CommKit software with the Enhanced Security Feature, the software key that Datatek supplies will enable the Enhanced Security Feature. Otherwise, the Enhanced Security Feature will not operate.

If you are using an earlier release of the IP-CommKit software, and want to use the Enhanced Security Feature, you must upgrade to release 1.0.13 or any later release. When you purchase a license to use the Enhanced Security Feature, Datatek will provide you a new software key for your host computer. You must repeat the registration procedure using the new key and your current software certificate number.



3 CONFIGURATION

It's easy to configure IP-CommKit to use the Enhanced Security Feature. If you are installing the IP-CommKit software, follow the procedures in the *IP-CommKit Installation and Administration Guide*. When you have completed these procedures, enter the following command on the UTM console port.

```
<TRK-UNIV> trk encrypt=on
```

If your host uses several UTM modules, you should enter this command on the console port of each. The host will automatically detect that a UTM is using encryption, and will start using it as well. There are no configuration changes required on the host computer.



4 TROUBLESHOOTING

The follow procedures show how to check if the IP-CommKit Enhanced Security Feature is operating correctly.

4.1 CHECK THE UTM

To check if encryption is enabled on the UTM module, enter the following command on the UTM console port:

```
<TRK-UNIV> vfy
```

You should see the following line in the report:

```
IP-DSU Data Encryption Status ==> Enabled.
```

4.2 CHECK /VAR/OPT/DK/LOG/DKIPDLOG

To check if the host has automatically determined that the UTM is using encryption, enter the following command on the host computer:

```
$ tail /var/opt/dk/log/dkipdlog
```

This displays the end of the log file created by *dkipd* (1M). The last line of the output should be similar to the message below:

```
Jun  5 15:27:21 (10202) UTM module utm_ip_address encryption  
enabled
```



Here, ***utm_ip_address*** is the address assigned to the UTM. Note that *dkipd* will use the name associated with the address, if possible. If your host connects to several UTMs, you should see this message repeated for each UTM IP address.

If you did not enable encryption on the UTM, you will see the following message:

```
Jun  5 15:27:21 (10202) UTM module utm_ip_address encryption
disabled
```

If you did not purchase a license to use the IP-CommKit Enhanced Security Feature, or did not register your software with a software key that enables the feature, you will see the following output:

```
Jun  5 15:27:21 (10202) Software key does not have encryption
feature enabled
```

If you see no messages containing the word *encryption*, you are probably running a release of IP-CommKit that does not support the Enhanced Security Feature. Follow the procedure in the *IP-CommKit Installation and Administration Guide* for checking the release number of the IP-CommKit software. If the release is not 1.0.13 or greater, you must upgrade your IP-CommKit software to use the Enhanced Security Feature.



5 END-USER LICENSE AGREEMENT FOR SOFTWARE

This License Agreement ("License") is a legal contract between you and the manufacturer ("Manufacturer") of the software product(s) you acquired identified as ("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.

5.1 SOFTWARE LICENSE

You may only install and use one copy of the SOFTWARE on one host computer (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 host computer. You may not rent, lease or lend the SOFTWARE in any manner. You may permanently transfer all of your rights under this LICENSE 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.

5.2 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).



5.3 SOFTWARE SUPPORT

SOFTWARE support is provided by Manufacturer, or its affiliates or subsidiaries separate from the host computer on which it may be installed. 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 SOFTWARE.

5.4 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.

5.5 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 Datatek Applications, Inc. Software support is limited to the hours of 9 AM to 5 PM ET Monday through Friday excluding Datatek-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.

5.6 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.

5.7 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 Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Datatek Applications, Inc., 379 Campus Drive, Suite 100, Somerset, NJ 08873

If you acquired the SOFTWARE in the United States of America, this Software License are governed by the laws of the State of New Jersey, 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 supercedes any and all prior or other communications, statements, documents, agreements or other information between the parties with respect to the subject matter hereof.

5.8 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. 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.

©Copyright 2002, 2006 Datatek Applications, Inc.

All Rights Reserved

Printed in USA

