IDG 9074® Secure Communications Controller®
U.S. Patent # 6,578,146
With SecureTN3270™ Software

Now technical support personnel can securely work from local or remote locations!

TOGETHER, THESE PRODUCTS PROVIDE THE COMPLETE SOLUTION FOR MAINFRAME MANAGEMENT

Replace 3174 Controllers

One IDG 9074 Secure Communications Controller replaces up to 128 IBM 3174 controllers providing 256 non-SNA or 1000 SNA sessions (or a combination of both) per ESCON or FICON adapter. This facilitates the use of multiple, easily scalable, common PC workstations in place of system dumb terminals. The IDG 9074 offers security for vastly more efficient LPAR, system and subsystem console management. The IDG 9074 supports all IBM mainframe system consoles. The IDG 9074 has at least two LAN cards that allow for independent networking, insuring reliability if one of the systems is not operating.

The IDG 9074 is the only controller that constantly monitors its own health, along with other IDG 9074s in an enterprise. In the event of an unexpected or threatening condition, the IDG 9074s can automatically issue SNMP alerts to any upper level system management tool, including SuperVision, TNG Unicenter, HP Openview, BMC Patrol, etc. In effect, the IDG 9074 controller can tell you about a system problem before members of your operations staff discover it!

Benefits of the IDG 9074 Secure Communications Controller

- Enables you to control users access level
- Provides technical support personnel the ability to securely work from local or remote locations
- Provides encrypted data streams
- Reduces operating and maintenance costs
- Integrates clients and improves reliability
- Extends secure, real-time corporate data access to a mobile workforce
- Offers COAX output for STK silos, printers and 3270-type terminals
- Provides 256 non-SNA and thousands of SNA sessions per ESCON or FICON adapter
- Compatible with existing TN3270E clients
- Increases floor space and efficiency to the data center

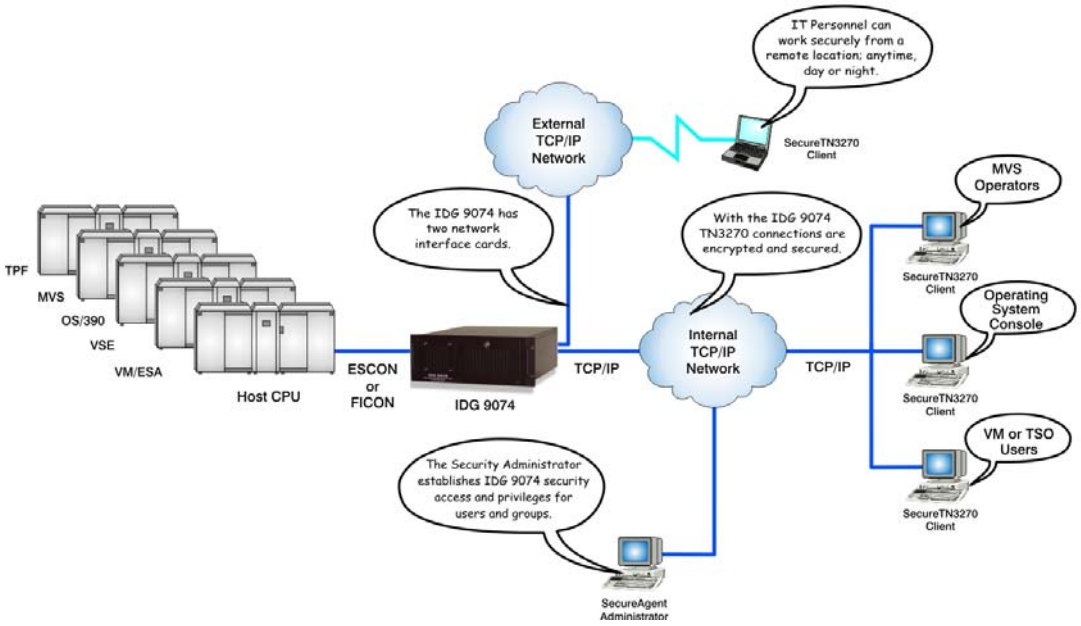
Features of the IDG 9074 Secure Communications Controller

- Offers DFT Support
- Patented data encryption technology
- ESCON or FICON channel attached

- Central user access control includes: administrator, read/write, read only and restricted
- Provides all console support functionality of the 3174, with complete security
- Includes SNA and non-SNA support allowing connection of master consoles and all sub-systems consoles (including: CICS, TSO, Omegamon, IMS, VTAM, etc.)
- Tightly integrated security options give unprecedented level of control
- Easy remote configuration and diagnostics
- Enables **Secure Remote Access** of 3270 sessions

Technical Profile… How the IDG 9074 Works

The IDG 9074 Secure Communications Controller connects to a host via ESCON or FICON adapter. The IDG 9074 provides continued support of SNA and non-SNA controllers. One IDG 9074 Secure Communications Controller replaces up to (128) one hundred twenty-eight 3174 controllers. The IDG 9074 enables enormous cost savings; while at the same time offers simplicity, convenience and security to the data center.



Disaster Recovery

SecureAgent products are central to the disaster recovery plans of some of the largest organizations in the world and if a disaster occurs, instant access to your critical systems is needed to ensure that business disruptions are minimized and normal operations resume as quickly as possible. Today, where technology and business are converging, any disruption could be devastating. The use of Secure Agent technology can mean the difference between potential disaster and temporary inconvenience for your company.

SecureTN3270 software provides secure access to any remote disaster recovery site. At the same time, the IDG 9074 enables technical support personnel to work from local or remote locations. Combined these products provide the ultimate in continuous secure operations in the event of a disaster.

SecureTN3270

The SecureTN3270 client from SecureAgent Software provides additional functionality to the IDG 9074, such as Instant Replay. Instant Replay emulates all activity and enables the user to review each session to recreate and review any system condition or problem that may have occurred.

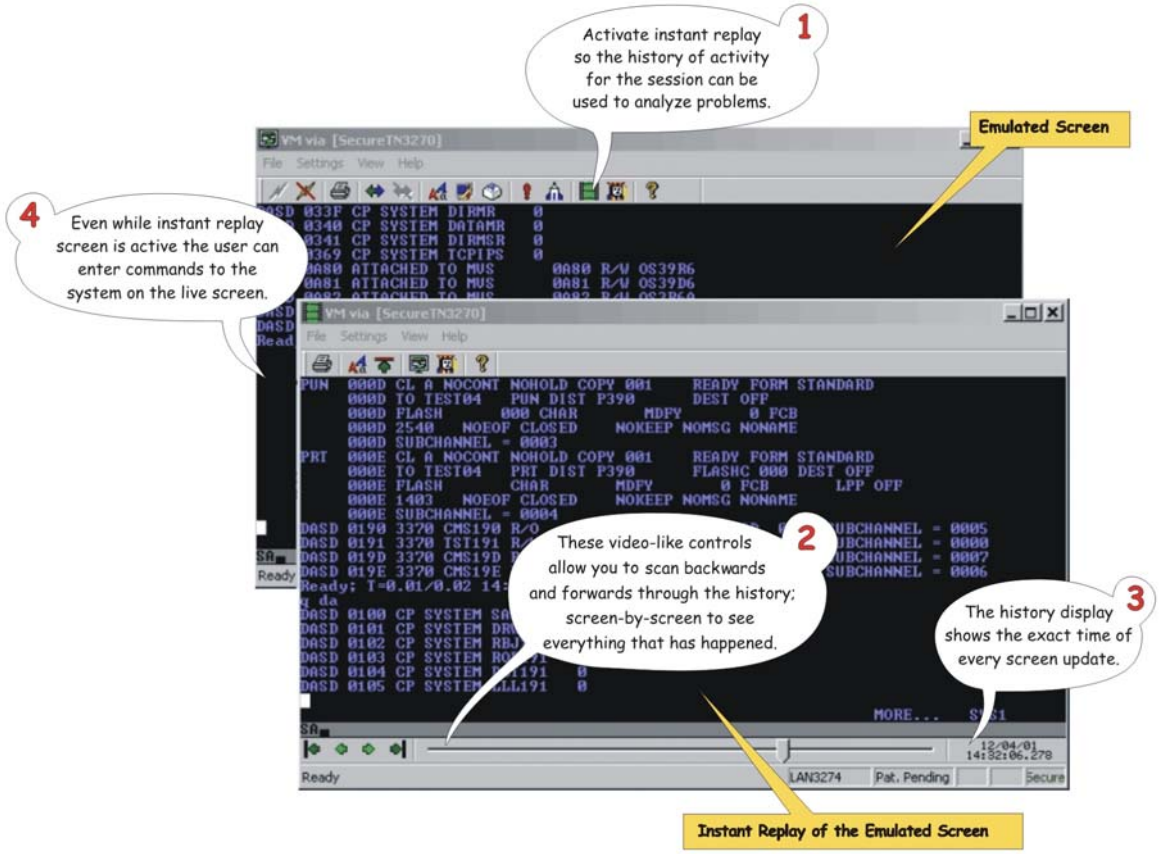
SecureAgent® Web Interface

The SecureAgent Web Interface enables users to make SecureTN3270 connections through a standard web browser with complete security! The use of your normal web browser can be more convenient than installing a client application. SecureTN3270 through the web interface has many features, including:

- Secure logon – authenticates the server and the client
- Encryption – provides the highest allowable encryption keys
- Instant Replay – allows the user to review all activity within a connected session

Instant Replay/TN3270 History

From the instant you make a connection to any mainframe system (z/MVS, z/VM®, z/VSE™, etc.) or subsystem (TSO™, IMS™, CICS®, Omegamon®, etc.) console, your Secure TN3270 client begins recording a log of system traffic. The Instant Replay feature emulates all activity and enables you to view screen-by-screen recreations of any connected session. This significantly reduces troubleshooting time, and allows you to easily recreate and review any system condition or problem that may have occurred.



Secure Remote Access

Increase productivity with telecommuting and reduce downtime by enabling off-site technical support personnel to immediately access systems and troubleshoot anytime from anywhere, with complete security. Secure Remote Access is convenient to access critical data and perform work functions at anytime.

Hot Console Support

Another feature of the IDG 9074 is Hot Console support. Hot console support creates a virtual terminal within the IDG 9074, ensuring that the mainframe always has a terminal with which to communicate.

COAX Connections

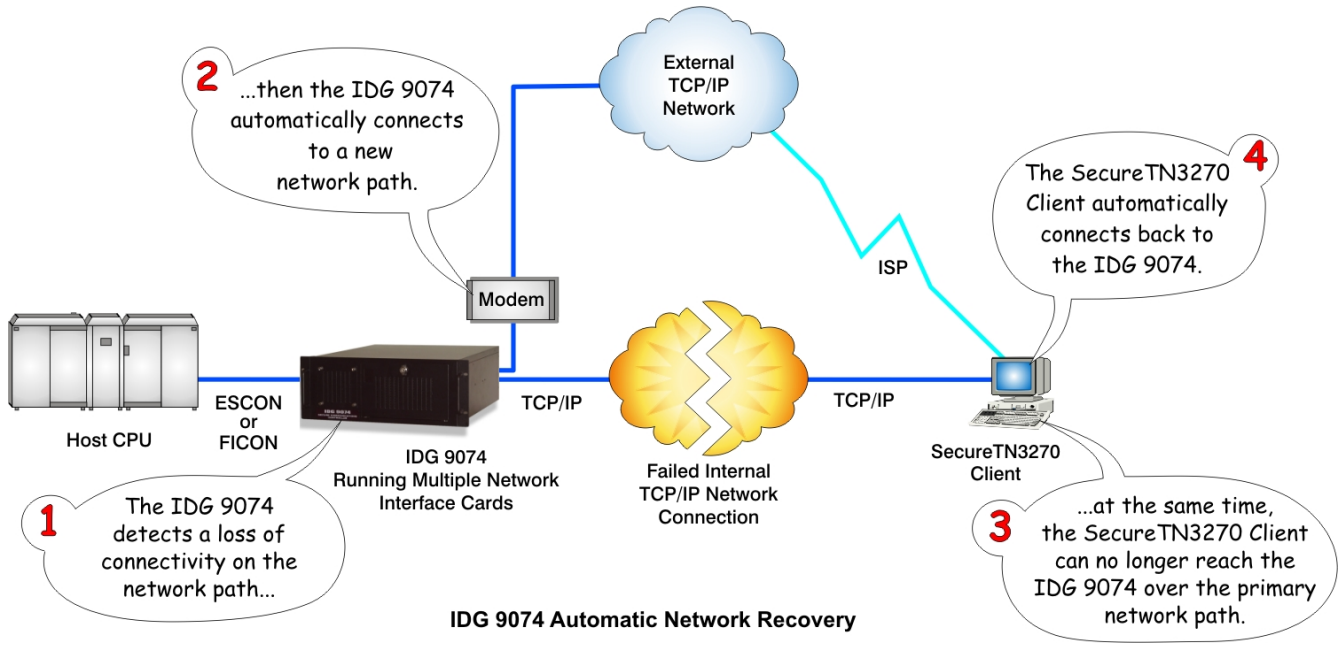
In addition to providing TCP/IP connectivity, the IDG 9074 Secure Communications Controller also provides COAX output. COAX output enables the IDG 9074 the ability to support up to 32 COAX devices such as: STK tape silos, COAX printers and 3270 type terminals.

Printer Support

The IDG 9074 supports HP laser printers connect either directly to PC or via Ethernet. The printer is connected directly to the host and can communicate required events from the printer to the host, etc. Printer status can be checked to ensure job completion.

Automatic Network Recovery

The IDG 9074 Secure Communications Controller detects loss of connectivity on the network path and can immediately connect to an alternate network path.



IDG 9074 Automatic Network Recovery

DFT Support

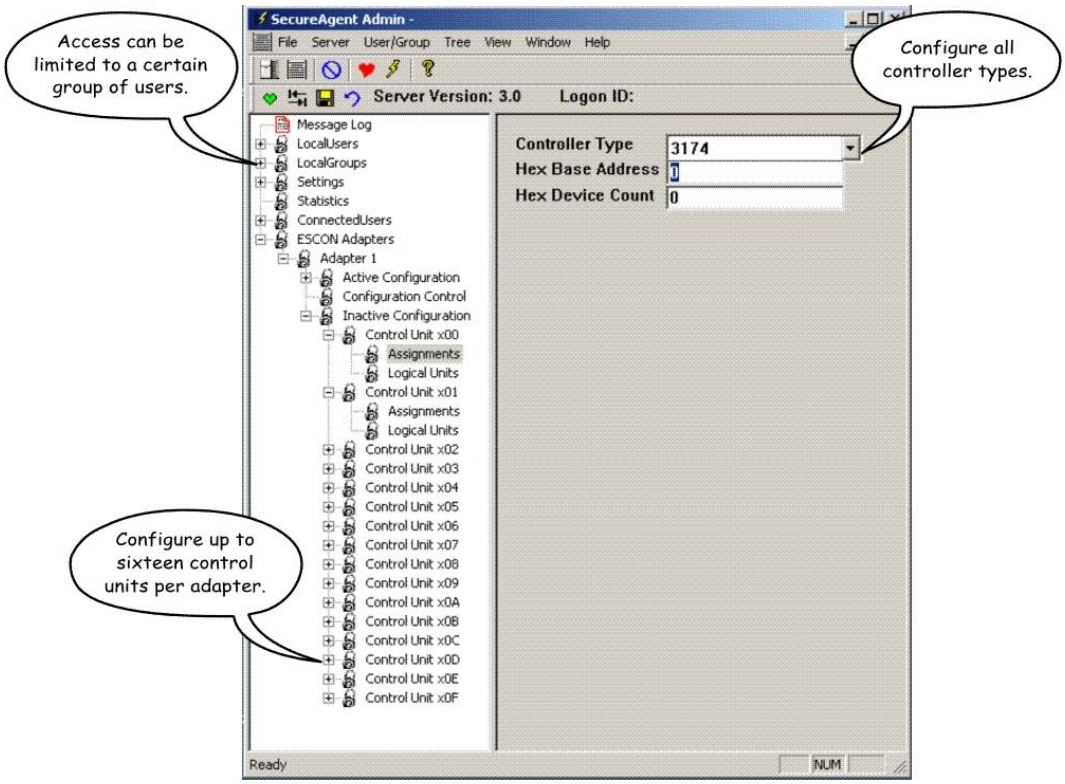
In addition to providing support for legacy control unit terminal (CUT) devices, the IDG 9074 supports legacy DFT devices, such as 3290 plasma displays and PCs with 3270 adapters, having the ability to display up to five simultaneous sessions across a single coaxial cable connection.

Extended OMA Support

Extended Optical Media Attached (Extended OMA) enables the IDG 9074 the ability to transfer files and data from the host to an emulated tape and archive the information on removable media (i.e. DVD).

SecureAgent Administrator (SAA)

SecureAgent Administrator (SAA) enables data center personnel to administer, from one or several workstation(s), all IDG 9074 machines in the enterprise from their workstations, regardless of the physical location of the machines. Use SecureAgent Administrator to set up user ID's, groups and privilege levels, as well as for configuring IDG 9074 control units, addresses and Logical Units.



Supported Connectivity

The IDG 9074 supports connectivity via TCP/IP over LAN, WAN, the Internet, dial-up or direct serial connection. The product supports any physical pathway that can provide TCP/IP connectivity to the host operating system.

SecureAgent® Technology

SecureAgent is a software layer that protects remote and networked communications with a special combination of patented and patent-pending processes including: encryption, compression and user authentication.

Encryption

SecureAgent's encryption is transparent to the user, easy-to-use and requires no special training. It is a simple matter of logging on and working as normal.

- Provides the highest allowable encryption keys
- Provides protection against attacks

Compression

SecureAgent delivers data between the connected machines in an optimized and compressed format. This reduces communication delays over networks, including the Internet, as well as enhancing data security.

Proprietary Login Process / User Authentication

The SecureAgent® handshake, or contentious logon protocol, authenticates the server and the client. Authentication of both client and server is an intrinsic property of SecureAgent. It utilizes a "Request-Challenge-Response" process that authenticates the user.

- Passwords are never sent between SecureAgent and the remote machine.
- Recording of user logon data sent by remote machines is rendered virtually worthless with an aggressive "Request-Challenge-Response process.
- Inability to bombard the SecureAgent server with logon requests by timing or not responding to requests, rendering the next attempt invalid.

For additional information regarding SecureAgent products, please contact us at:

SecureAgent Software

2448 East 81st Street, Suite 2000

Tulsa, OK 74137-4271 USA

Phone: (918) 971-1600

Fax: (918) 971-1623

www.secureagent.com