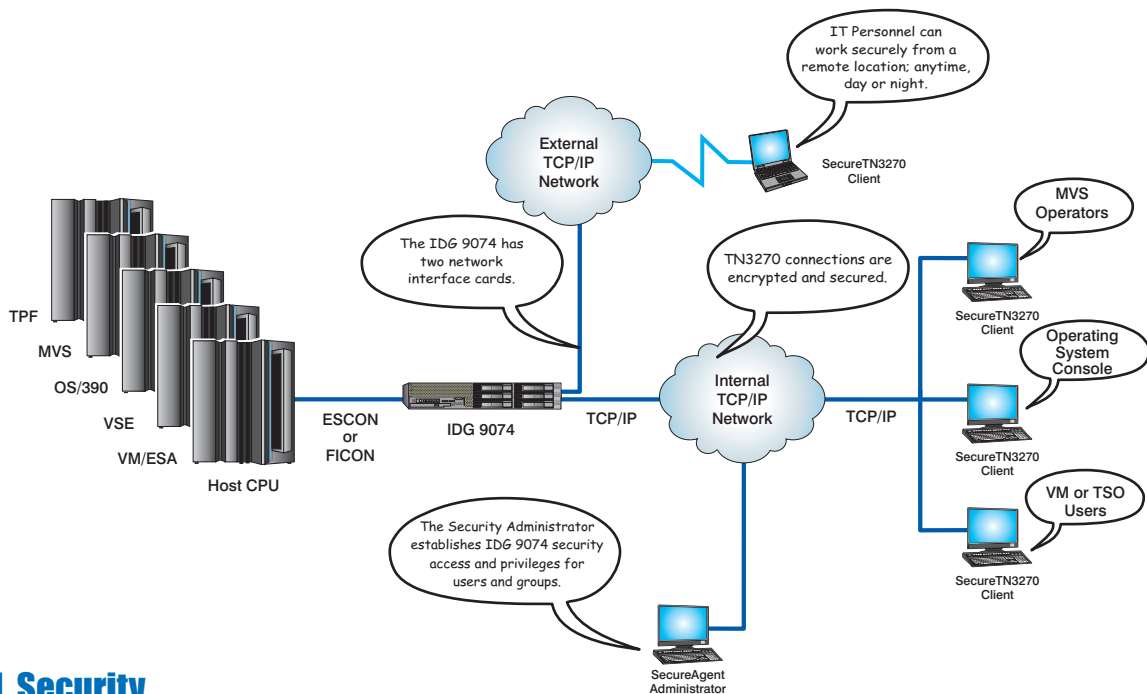


SecureTN3270™

Enables Technical People to Work from Local or Remote Locations with Encryption



Unparalleled Security

SecureAgent Software® has developed revolutionary enhanced features for TN3270 users, such as Instant Replay, REXX Execs, SNMP alerts/traps, email notifications and a dialogic voice response system. Combined with IDG's 9074® Secure Communications Controller®, these products provide the complete solution for your mainframe management needs, both local and remote!

SecureTN3270 offers these unique features:

- **Instant Replay** - enables users to view screen-by-screen playback of sessions
- **REXX** - automates command sequences
 - Automate Entry
 - Watch display from host
 - Send SNMP traps/alerts
- **SNMP** - REXX sends alerts to TNG, Tivoli, BMC
- **E-Mail** - REXX notifies personnel of alerts or problems
- **Pages** - REXX sends a page via modem or email indicating alerts or problems
- **Dialogic Voice Response System** - ability to interact with the Dialogic telephone support card
- **Data Security** - enhanced security logon and patented encryption process

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 – enables the user to review all activity within a connected session

The IDG 9074® Secure Communications Controller®

One IDG 9074 replaces up to 32 (thirty-two) 3174 or 3172 controllers and provides data encryption, data compression and a request-challenge-response user authentication process. SecureAgent® technology enables technical personnel [Remote Access](#) to manage any system in the enterprise from any local or remote location with [complete security](#).

Benefits of Secure Remote Access

- Remote access is secured by encryption of data and user authentication
- Increased system uptime by enabling technical support personnel to work from any location, remote or internal
- Security administrator can setup and maintain user privileges from any location
- Convenience to access critical data and perform work functions at any time

Instant Replay/TN3270 History

The Instant Replay feature enables users to view screen-by-screen playback of any connected session. This significantly reduces the time needed for any type of troubleshooting and enables the user to recreate and review any system condition that previously occurred on any mainframe system, i.e., CICS, TSO, Omegamon, etc.

1 Click on the icon and activate instant replay so the history of activity for the session can be used to analyze problems.

2 These video-like controls allow you to scan backwards and forwards through the history; screen-by-screen to see everything that has happened.

3 The history display shows the exact time of every screen update.

4 Even while the instant replay screen is active the user can enter further commands to the system on the live screen.

Emulated Screen

Instant Replay of the Emulated Screen

**INSTANT REPLAY Speeds
Problem Determination
& Problem Resolution -
EVEN if the System is Down!**

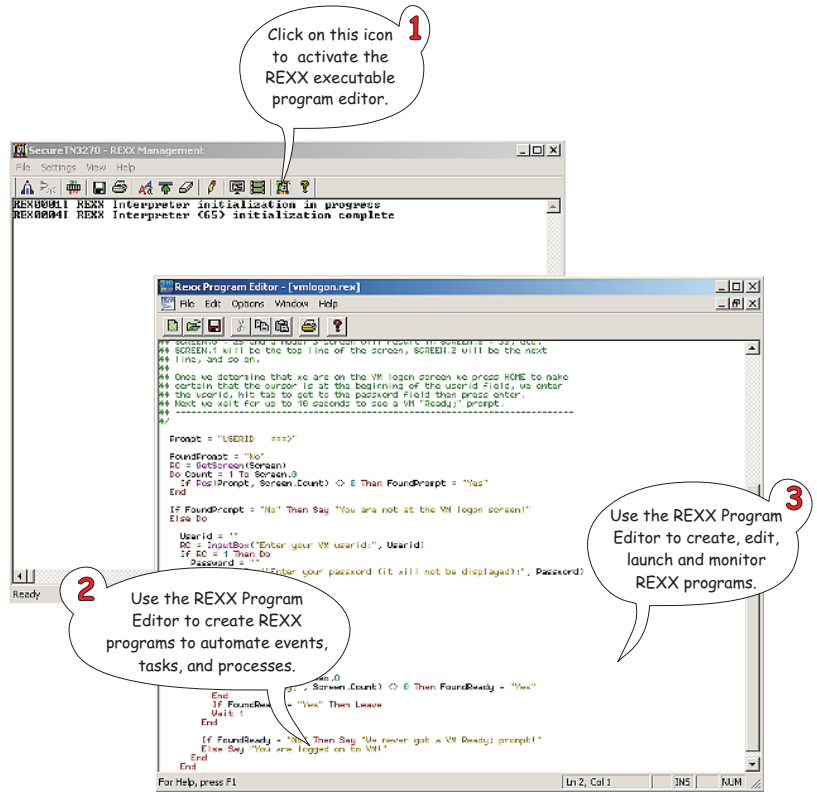
REXX

The REXX programming language is widely used to automate operating system command sequences. Some of the features of REXX with SecureAgent Software are:

- REXX Editor
- Debugging Wizard
- Launch any number of REXX Execs

Benefits of REXX with SecureAgent Software:

- Ease of use
- Enables automated responses
- Provides true multi-tasking
- Incorporated REXX capabilities



SNMP Alerts/Traps

SNMP facilitates communication alerts to high level alert monitors (i.e. TNG, Tivoli and BMC). SecureAgent Software utilizes a variety of REXX methods to trap and evaluate information, and then generates SNMP alerts/traps. Such alerts can be forwarded to any location on the network for further analysis, display or other appropriate action.

E-mail Notification

E-mail notifications are communicated through REXX Execs. Personnel can be notified of alerts or problems within the system immediately through email transfer.

Pager Notification

Pager notifications are sent via REXX Execs. Personnel can be paged via modem or E-mail to indicate alerts or problems within the system.

Dialogic-Interactive Voice Response System

SecureTN3270 includes the ability to interact with the dialogic telephone support card via REXX. SecureAgent REXX voice messaging capabilities enable the system to send alerts to telephone numbers for notification of system problems/changes as they are occurring. Using an intelligent and interactive process, REXX determines who is on the contact list then continues to call down the list until it reaches a technician. The technician then determines if they can assume responsibility for the call or whether another technician should be contacted. At that time, the technician informs REXX as to what action to take next. This process flexibly and efficiently streamlines duties that need to be performed immediately.



Central User Administration and User Defined Access

The Secure Domain Server provides logon security, controls user privileges, and manages access rights from a central point. Users can be limited to particular sessions. All access, authority, privileges, and security functions can be securely administered from a central point of control.

SecureAgent Administrator (SAA)

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

SecureAgent® Technology

This software layer protects remote and networked communications with a 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 helps reduce communication delays over networks, including the Internet, as well as enhancing data security.

Login Process / User Authentication

In a communication system, authentication verifies that messages really come from their stated source. The SecureAgent® handshake, or contentious logon protocol, authenticates the server and the client. It uses 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 Challenge and Response process

Security Request - Administration

All aspects of SecureAgent technology can be set up by your own security administrator from any location.

For additional information regarding SecureAgent Software, 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