secure Agent®

*Secure Enterprise Solutions*

# Access Control



# The IDG 9074® Remote Access Controller™

**SecureAgent Software**
2448 E. 81st St, Ste 2000
Tulsa OK 74137-4271 USA
Tel: 918.971.1600
Fax: 918.971.1623

Printed in the United States of America



SecureAgent Software
2448 East 81st Street, Suite 2000
Tulsa OK 74137-4271 USA

Voice: 1.918.971.1600
Fax: 1.918.971.1623
Toll-free: 888.746.7735

www.secureagent.com

## Introduction

The IDG 9074® Remote Access Controller™ provides data center management with a one-stop, integrated hardware/software solution to controlling access to critical business IT systems. In today's business environment, access control can mean a company's life or death. Allowing the wrong person to access a system or allowing them to issue the wrong command can have disastrous consequences in lost data, lost business, or lost reputation. And if you can't prove you've done everything possible to control access and fail a security audit, government regulators may help you also lose sleep.

Whether you're running mainframes or mid-range systems, the IDG 9074 Remote Access Controller provides everything you need to assure that only the right people have access and that they can only do what they're supposed to do.

In this overview, we'll discuss how the IDG 9074 Remote Access Controller enables you to:

- Securely control access to systems.
- Once granted access, ensure a user can only issue appropriate commands. If a user tries to issue inappropriate commands, immediately and automatically notify security personnel by SNMP, e-mail, and/or digital pager; the security personnel can then monitor user activity keystroke by keystroke both in real time and since the user connected, and do so without the user's knowledge.
- Employ dual-party ("two-factor") authentication to ensure only authorized users are granted access.
- Take advantage of LDAP integration in user ID and password management.

The IDG 9074 Remote Access Controller allows you to mix and match these capabilities to your company's needs, ensuring a tailored and cost-effective solution.

No matter what type of system to which you need to connect, the IDG 9074 Remote Access Controller can handle it.

## Restricting user access

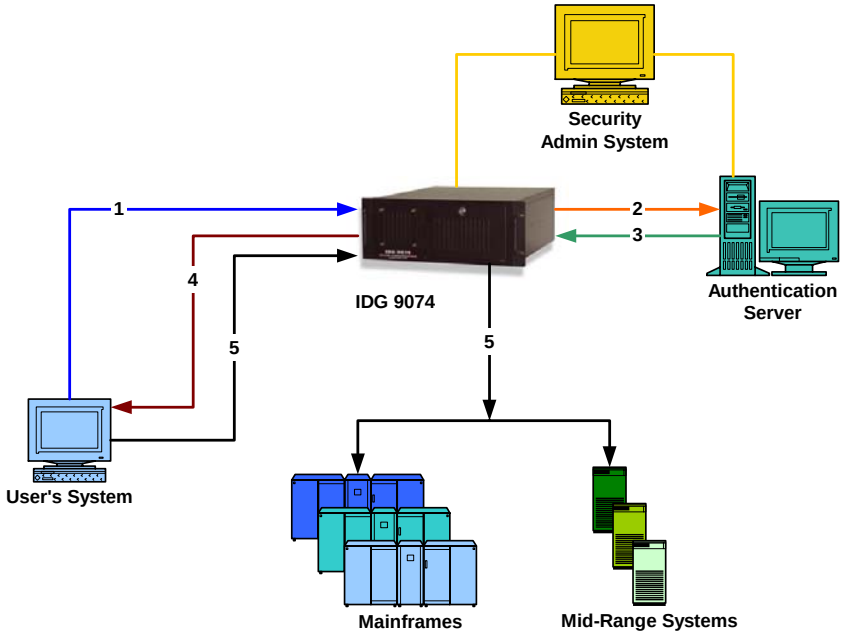
With the IDG 9074 Remote Access Controller, you can restrict an individual's access to particular systems, based on their duties; that is, the role they play—for example, if you have systems A, B, and C, you can ensure certain individuals can only access systems A and B, but not C. So, operators in training could connect to training systems but wouldn't be able to access those used in production.

User IDs and passwords have long been a mainstay in controlling access. But increasingly, we see that the "bad guys" are able to thwart them. Something more is needed—something that can't be compromised.

The IDG 9074 Remote Access Controller supports the latest in such security paradigms: dual-party authentication (sometimes called “two-factor authentication”). The user must supply two pieces of information (“factors”) before a connection will be allowed. One factor, known to the user, is the user ID/password combination. However, because this factor could be compromised, the user must also supply another factor, which that user alone has. A small device, often attachable to a key chain, supplies this second factor as a pseudo-random number, which changes automatically at pre-determined intervals (often, every minute).


After entering the user ID/password factor, the user enters the random-number factor. The IDG 9074 sends this to a secure server for authentication. If this is successful, the connection is completed—otherwise, the user is not allowed to connect.

In combination with RSA, a leader in authentication technology, SecureAgent has incorporated dual-party authentication into the IDG 9074, providing both mainframe and mid-range systems with extra assurance that only authorized users have access.




1. User sends user ID, password, and authentication factor to IDG 9074.
2. IDG 9074 passes factor to authentication server.
3. Authentication server authenticates user and sends confirmation to IDG 9074.
4. IDG 9074 presents user with list of systems to which they are allowed access.
5. User selects and connects to desired system.

## Restricting user actions

You can also restrict the commands that an individual is allowed to issue. Based on the security groups you define, group members can be restricted from issuing particular commands.

Additionally, using the included REXX scripting language, commands can be restricted based on prompts. A user presented with one system prompt will be allowed to issue commands unavailable to a user presented with a different system prompt. If a user attempts to issue an illegal command for the presented prompt, an alert can be sent to security personnel via any combination of SNMP, e-mail, or digital voice pager.

Using REXX, the IDG 9074 Remote Access Controller can watch for keystroke patterns and issue alerts to security personnel via any combination of SNMP, e-mail, or digital voice pager if it detects specified patterns.

With REXX scripting, a problem user's connection can even be terminated automatically.

The IDG 9074 provides security personnel with an additional tool to assist them; they can use its patent-pending Instant Replay feature to watch a user's actions keystroke-by-keystroke, both in real time and since the user connected, and take appropriate action to prevent or minimize problems.

In all cases, audit logs capture root-level access and activity and provide evidence of compliance to both business requirements and governmental regulations.

## Centralized password management

Companies often have disparate computer systems and software applications that each requires managing its user IDs and passwords. Instead of dealing with them on a one-by-one basis, companies often use a Lightweight Directory Access Protocol (LDAP) server to centralize user ID/password management. The IDG 9074 Remote Access Controller can communicate with an LDAP server in the course of verifying user IDs and passwords, ensuring that their management stays in one place. Whether you're running a mainframe or mid-range system, you don't have to change how you manage user IDs and passwords to enjoy the IDG 9074's advantages.

## Mainframe connectivity

For mainframe systems, the IDG 9074 can directly connect via ESCON or FICON channels. It can also connect over a network to an OSA-ICC or via a browser to the host's HMC, the latter allowing remote hardware configuration.

## Secure root access for mid-range systems

For mid-range systems running Linux® or Unix®, the IDG 9074 controls root access. Since root access gives the user total system control, both unintended mistakes and deliberate maliciousness can cause catastrophic interruptions in system availability and busi-

ness continuity (or even survival). The concerns inherent in granting root access on Unix and Linux systems are magnified as the computers are distributed geographically (for example, a production data center in one location and the associated disaster recovery site in another) or as the number of systems increases. Root access is not granted lightly.

Acting as a secure root-access control for a mid-range system, the IDG 9074 Remote Access Controller ensures that there is no blanket access with a global password. Root access requires each individual to have a unique user ID/password combination, which the IDG 9074 Remote Access Controller uses to verify root-access permission. Security audits can thus tie actions back to a particular individual, instead of a ubiquitous "super user."

## About SecureAgent Software

SecureAgent Software has been helping customers manage sensitive data for more than 20 years. Many of the largest companies across the United States and throughout Europe use SecureAgent products in mission-critical areas of their daily operations. They play an integral role in secure remote console access, data backup and recovery, advanced automation, integrated tape management, and disaster recovery.

SecureAgent Software is playing a pioneering role in the implementation of role-based access controls, and is used extensively by both commercial customers and the governmental sector to comply with evolving regulatory guidance.

Among the companies using SecureAgent Software are three of the four largest US banks, the two largest credit card processing companies, the nation's two largest communications companies, the world's largest stock exchange, the largest US airline, and the largest airline reservations companies in the US and Europe.

For additional information or to arrange an on-site trial, please contact:

**SecureAgent Software**
2448 East 81st Street, Suite 2000
Tulsa, OK 74137-4271
Voice: 918.971.1600 Fax: 918.971.1623
Toll-free: 888-746-7735

www.secureagent.com