
Fast/CRAM Trusted Login for Model 204 Reference Manual



Sirius Software, Inc.
875 Massachusetts Avenue, Suite 21
Cambridge, MA 02139

Telephone: (617) 876-6677
FAX: (617) 234-1200
E-mail: support@sirius-software.com
World Wide Web: <http://sirius-software.com>

November 17, 2004

© 2004 Sirius Software, Inc.

Proprietary Notices

The following products:

- *Fast/Backup*
- *Fast/CRAM*
- *Fast/Reload*
- *Fast/CRAM Trusted Login for Model 204*
- *Sirius Mods*

are proprietary products of Sirius Software, Inc.:

Sirius Software, Inc.
875 Massachusetts Avenue, Suite 21
Cambridge, Massachusetts 02139
USA

Model 204™ is a proprietary product of Computer Corporation of America:

Computer Corporation of America
500 Old Connecticut Path
Framingham, Massachusetts 01701
USA

Model 204™ is a registered trademark of Computer Corporation of America.

Contents

Proprietary Notices **ii**

Contents **iii**

Summary of Changes **v**
 Fast/CRAM Trusted Login for Model 204 Version 4.2 v

Chapter 1: Introduction **1**
 Versions, Compatibility and Installation 1
 Related manuals 2

Chapter 2: Overview **3**

Chapter 3: Operation **5**

Appendix A: Date Processing **7**

Summary of Changes

This section describes significant changes to the documentation. In most cases these changes correspond to enhancements made to the underlying product.

Fast/CRAM Trusted Login for Model 204 Version 4.2

Conversion of this manual.

CHAPTER 1 *Introduction*

This document presents an enhancement to the *Model 204* Security Interfaces: ACF2, RACF, and Top Secret. This enhancement operates in conjunction with the Sirius Software *Fast/CRAM* program product to provide a trusted login facility for *Model 204*. This facility simplifies the management of *Model 204* security and also provides for increased security. With trusted login *Model 204* does not maintain its password for a user id, instead *Model 204* trusts the external authorizing facility to verify a users identity. For example, if a user logged on to TSO accesses *Model 204*, the trusted login facility allows *Model 204* to accept from TSO the id of the user as established by the system authorization facility. The user can then request a login to *Model 204* with the same id, without being prompted to enter a password. If the same user accesses *Model 204* from a VTAM session, *Model 204* will still prompt the user for a password.

1.1 Versions, Compatibility and Installation

Fast/CRAM Trusted Login for Model 204 is delivered as an object code enhancement to *Model 204* as part the *Sirius Mods* which also includes products such as *Fast/Backup* and *Fast/Reload* that do not require *Fast/CRAM Trusted Login for Model 204*. To install *Fast/CRAM Trusted Login for Model 204* the *Sirius Mods* must be installed. When the *Sirius Mods* are installed, all other products owned by the installing site that are part of the *Sirius Mods* will also be (re)installed. You must also install *Fast/CRAM* in order to receive the benefits of trusted login.

Since *Fast/CRAM Trusted Login for Model 204* is part of the *Sirius Mods* the version number of *Fast/CRAM Trusted Login for Model 204* is considered to be the version of the *Sirius Mods* in which it is contained. The current document describing *Fast/CRAM Trusted Login for Model 204* was first available in version 4.2 of the *Sirius Mods* and that version of *Fast/CRAM Trusted Login for Model 204* was called version 4.2. This document, the ***Fast/CRAM Trusted Login for Model 204 Reference Manual***, assumes that a site is running *Sirius Mods* version 4.2 or later.

Sirius Software has a strong commitment to backward compatibility with the *Sirius Mods*. What this means, is that any correct usage in any version of the *Sirius Mods* will continue to run correctly on subsequent versions of the *Sirius Mods*.

1.2 Related manuals

Since *Fast/CRAM Trusted Login for Model 204* requires the installation of the *Sirius Mods*, the person responsible for the installation of *Fast/CRAM Trusted Login for Model 204* should refer to the ***Sirius Mods Installation Guide***. The ***Sirius Messages Manual*** contains documentation on *Sirius Mods* error messages and so might be useful to programmers as well as installers. The *Fast/CRAM* installation procedures are described in the ***Fast/CRAM Installation Guide***.

CHAPTER 2 *Overview*

The *Model 204* Security Interfaces provide special support for certain types of batch users. With this support the user enters a LOGIN command without any user ID or account information. The login is then automatically completed with a user ID previously validated and the user is not prompted for a password. The ID of the user that submitted the *Model 204* batch job is used to satisfy this type of automatic login.

For example, if TSO user GARY submits a BATCH204 job and the User Zero stream has a LOGIN command with no arguments, the result is the same as if the User Zero stream had contained "LOGIN GARY", followed by the password for GARY. This is a secure facility because the *Model 204* batch job is executing under the security profile for GARY; the system security facility (ACF2, RACF, or Top Secret) propagated the already validated ID of the submitter to the BATCH204 job. Each MVS batch job executes using the security profile of its submitter. The current *Model 204* User Zero login feature just lets User Zero run under the same profile that is currently used for the batch job itself, without requiring that the password be reentered.

Fast/CRAM understands the security structure of an MVS address space. Whenever a TSO user or batch job opens a *Fast/CRAM* connection to *Model 204*, that user's previously validated User ID and terminal ID is copied from a protected system control block to a protected *Fast/CRAM* control block associated with the connection. This information is maintained in storage that is key zero and fetch protected, so the mechanism cannot be "fooled" by an impostor. A new *Fast/CRAM* function is provided to retrieve the ID associated with a thread. *Fast/CRAM Trusted Login for Model 204* uses the new function for IODEV=29, IODEV=11, and IODEV=23 threads.

When a connection is made over a *Fast/CRAM* thread, the validated ID of the conversation partner is passed by the Trusted Login support to the external security interface (ACF2, RACF, or TOPS). This extends the support for a LOGIN command with no ID or password to users of IODEV=11 (TSO interface), IODEV=29 (BATCH2), and IODEV=23 (IFAM2) connections. IFAM2 programs pass ';' to IFSTRT(N), without needing to include a user ID and password.

The ACF2 Trusted Login facility is invoked by a *Model 204* LOGIN command that does not provide a user ID. An optional account may be specified, preceded by a comma:

```
LOGIN
LOGIN , account
```

If the LOGIN command is issued through an IODEV=11 or IODEV=29 connection, and if *Fast/CRAM* is installed, then the LOGIN will be completed using the User ID that owns the "other end" of the *Fast/CRAM* conversation.

A similar facility is provided for IFAM2 programs. The IFSTRT(N) call should be passed a string with two semi-colons for a login with the default account or a semi-colon followed by a comma, the account, and a semi-colon to assign an optional account:

```
';;'
';,account;
```

The standard form of the LOGIN command may still be used at any time to request a login with the specific ID. Once a LOGIN command has been issued for a thread, whether or not the login was successful, the thread's auto-login information is cleared. Thus, a LOGOUT command must be issued to return the thread to a trusted login state. For example, the following sequence is necessary to switch accounts in a session:

```
LOGIN , account1
.. processing
LOGOUT
LOGIN , account2
```

If the LOGOUT command is left out of the sequence above, the second LOGIN command will request a password and then the LOGIN command will be rejected.

For example, if a BATCH2 job is submitted by the TSO user "GARY", then the *Model 204* login will be processed as if it contained "LOGIN GARY", followed by the password for "GARY". Similarly, if the TSO user "GARY" invokes the *Model 204* TSO interface and enters a LOGIN command with no arguments, then the login will be completed as if the ID of GARY had been present and a password was provided.

Note: The current version of *Fast/CRAM Trusted Login for Model 204* does not distinguish between the various users of a CICS address space. Thus, if an IFAM2 CICS transaction attempts a trusted login (i.e., no ID is provided in the login string), the

login will be attempted using the owner ID of the CICS address space. For this reason the owner ID's for all CICS address spaces should not be authorized for *Model 204* login.

APPENDIX A *Date Processing*

This chapter presents date processing issues for *Fast/CRAM Trusted Login for Model 204*. The only use of dates within *Fast/CRAM Trusted Login for Model 204* is to examine the CPU clock (as returned by the STCK hardware instruction) to determine the current date, in case *Fast/CRAM Trusted Login for Model 204* is under a rental or trial agreement. Other than that, there are no date processing considerations for using *Fast/CRAM Trusted Login for Model 204*; *Fast/CRAM Trusted Login for Model 204* itself does not produce any results which depend on the content of any data which may be date values.

To correctly use *Fast/CRAM Trusted Login for Model 204* past the year 1999, *Sirius Mods* version 4.6 or later is required.

Above and beyond the post-1999 requirements specific to *Fast/CRAM Trusted Login for Model 204*, you must examine all uses of date values in your applications to ensure that each of your applications produces correct results. Furthermore, both the operating system and *Model 204* must correctly process and transmit dates beyond 1999 in order for *Fast/CRAM Trusted Login for Model 204* to operate properly.

