

RunCTRL

Version 200

14. February 2000


GreenHouse

Software & Consulting

Karl-Heinz Weber

Heinrichstraße 12

D-45711 Datteln/Horneburg

Note:
This product is freeware from GreenHouse Software & Consulting.
It does not contain trap doors, Trojan horses, or other damaging code.
No warranty is given for its functionality.
Use it at your own risk.

Some TANDEM supplied programs, e.g. SAFECOM, SCF etc. allow the user to start a new program through a RUN command from within e.g. SAFECOM. The RUN feature is intended to makes the use of the tools easier. But this feature might be a security problem: In case e.g. SAFECOM runs with the SUPER.SUPER ID, any program, started through SAFECOM by the RUN command, executes with the SUPER-ID.

Controlling the RUN-ability of Tandem supplied programs is demanded since a long time.

The library code RUNCTRL (RUN Control) is able to control all RUN commands, initiated from within any program (Tandem supplies, as well as user written).

To control the RUN command, the library RUNCTRL has to be bound to the program(s), where the RUN command should be controlled. It intercepts the three procedure calls:

1. PROCESS_CREATE_
2. NEWPROCESS
3. NEWPROCESSNOWAIT

and checks the following three parameters:

1. The program, executing the RUN command (Originator), e.g. SAFECOM, SCF etc.
2. The user of the program, executing the RUN command (User)
3. The resource that has to be started by the RUN command (NewProgram), e.g. EDIT, FUP etc.

These parameters are compared with a list, that is provided through the EDIT type file named **RUNCONF**. The following format in **RUNCONF** is expected:

```
!
!           User of
! Calling Program   Calling Program   Called Program   DENY
! -----
! $*.*.*           *                   $*.*.*
! $*.*.*           super.super         $*.*.*          deny
! -----
```

Each line, beginning with an exclamation mark, is treated as comment.

All parameters must be separated by at least one blank character.

Calling Program	File name of program, that issues the RUN command, e.g. \$SYSTEM.SYS*.SAFECOM This entry is NOT case sensitive. Wild cards are supported.
User of Calling Program	Name of user of Originator in named form, e.g. GHS.CARL GUARDIAN as well as Alias user names are supported. GUARDIAN names are NOT case sensitive. Alias names ARE case sensitive! Wild cards are supported.

Called Program	File name of program that is allowed/denied for execution from Originator by User. e.g. \$SYSTEM.SYSTEM.FUP This entry is NOT case sensitive. Wild cards are supported.
DENY	Keyword, that denies the corresponding entry. This entry is NOT case sensitive. Optional entry.

In case RUNCONF does NOT exist, or is empty, the library code RUNCTRL is not activated, and no RUN command is restricted!

In the above example, all users can execute all RUN commands, except the user SUPER.SUPER: All his attempts to start a new process through the RUN command, are rejected with an error 48 (security violation).

The following programs have to be allowed for SQLCI to make it work OK:

- `$system.sys*.sqlcomp`
- `$system.sys*.sqlci2`
- `$system.sys*.sqlcat`
- `$system.sys*.sqlutil`

The Library comes in two flavors:

1. Type 100 file (for non native programs)
2. Type 700 file (for native programs)

To install the RUNCTRL files on your system, perform these steps:

1. Upload the file RUNCTRL.100 or RUNCTRL.700 in binary format onto your Tandem system into an empty subvol, e.g. \$SYSTEM.RUNCTRL and name it RUNCTRL.

1. Change the file code of RUNCTRL to 100 or 700:

```
FUP ALTER RUNCTRL, CODE 100/700
```

Secure RUNCTRL to NOOO:

```
FUP SECURE RUNCTRL, NOOO
```

2. Upload the files

- RUNCONF
- BSCF
- USCF
- BSQLCI
- USQLCI
- BSAFECOM
- USAFECOM

in ASCII mode into the same location as RUNCTRL.

RUNCON is the configuration file. Set its security to: NOOO

These files are TACL Macros, performing the necessary steps to bind/unbind the RUNCTRL library to the corresponding programs.
Set the security to: OOOO

3. Give all files to SUPER.SUPER:
FUP GIVE*, -1

By now, all files are installed on e.g. \$SYSTEM.RUNCTRL.

To activate RUNCTRL on your system, perform these steps:

1. Edit RUNCONF and change it according to your needs, e.g.:

```
!
! Configuration file of RUNCTRL library.
!
!
!           User of
! Calling Program      Calling Program      Called Program      DENY
! -----
! $system.sys*.scf      ghs.carl          $*.*.*
! $system.*.*          Carlito           $*.*.*
! $system.sys*.safecom  super.*          $system.sys*.edit
! $*.*.*              super.super      $*.*.*              Deny
! -----
```

- Each line, beginning with an exclamation mark, is treated as comment.
- Entries are NOT case sensitive, except Alias names.
- All entries 'understand' wild cards.
- The shown entries are just examples. Add your own restrictions!
- In case this file is empty, or does NOT exist, no checks take place.
- Secure RUNCONF to: "NOOO", and give it to a trustworthy person.
- RUNCONF has to reside in the same location as the RUNCTRL library file.

Note:

To successfully execute the RUN command from within a program, that has the library activated, the user must be positively mentioned in RUNCONF!

2. Bind the library file RUNCTRL to the program(s) in question. This has to be done once. To bind RUNCTRL to e.g. SAFECOM, perform the following command:
[RUN] \$SYSTEM.SYSnn.SAFECOM/LIB \$vol.subvol.RUNCTRL/
You must have read/write access to SAFECOM to perform the library binding.
SAFECOM should be secured to: OONO
RUNCTRL should be secured to: NOOO

From now on, every RUN command from SAFECOM is controlled by the library. Unauthorized RUN commands are rejected with error 48 (security violation).

3. To un-bind the library, execute the following command:
[RUN] \$SYSTEM.SYSTEM.SAFECOM/LIB/
This brings SAFECOM back to its original behavior.

To make life easier, a few TACL macros are provided that do all this (Bxxx = BIND, Uxxx = UN-BIND):

- BSCF activates the RUNCTRL library for SCF
- USCF de-activates the RUNCTRL library for SCF
- BSQLCI activates the RUNCTRL library for SQLCI
- USQLCU de-activates the RUNCTRL library for SQLCI
- BSAFECOM activates the RUNCTRL library for SAFECOM
- USAFECOM de-activates the RUNCTRL library for SAFECOM

To execute them successfully, you must have read/write access to the programs in question!

Hope this nifty tool makes life easier to you!

Please report any error and/or request for enhancements to:

GreenHouse Software & Consulting

Karl-Heinz Weber

Heinrichstraße 12

D-45711 Datteln/Horneburg

Germany

Phone +49 (0)2363 72566

Fax +49 (0)2363 66106

AOL Fax +49 (0)40 3603 044706

Mobile +49 (0)172 23 18248

E-Mail: Info@GreenHouse.de

Home page: <http://www.GreenHouse.de>

PGP fingerprint: 3A 32 D9 0A D1 25 54 18
 11 50 24 84 66 29 2D D2

