

PRCOSEEP

Version 103

Reference Manual

03. February 2005

The logo for greenHouse features the word "green" in a black, lowercase, sans-serif font, followed by a large red "H" with a green roof-like shape above it and a green underline below it, and the word "ouse" in a black, lowercase, sans-serif font.
greenHouse
Software & Consulting

Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg

**Trademarks or
Service Marks**

The following are trademarks or service marks of Tandem Computers Incorporated:

Atalla, Challenge/Response, Enform, Expand, Guardian, Guardiango, Inspect, Multilan, NonStop, TAOL, Tandem.

All brand names and product names are trademarks or registered trademarks of their respective companies.

The following are trademarks or service marks of *GreenHouse Software & Consulting*:

\$ARROW, \$AS, CRYSTAL, CURIOUS, FTPSERV-E, FUNCTRAC, MPWD, MPWD-L, PASSYNC, SECMAN, SECOM, GSTK, SSTK.

The following are trademarks or service marks of Jelinek EDV:

SECMAN

Copyright

Copyright © 2005 by *GreenHouse Software & Consulting*. All rights reserved. No part of this document may be reproduced in any form, including photo copying or translation to another language, without prior written consent of *GreenHouse Software & Consulting*.

Printed in Germany.

Please Comment

If you have questions or problems concerning the content of this document, please let me know! Send your comments to:

GreenHouse Software & Consulting

Karl-Heinz Weber

Heinrichstraße 12

D-45711 Datteln/Horneburg

Germany

Phone +49 (0)2363 72566

Fax +49 (0)2363 66106

Mobile +49 (0)172 23 18248

E-Mail: Info@GreenHouse.de

Internet: www.GreenHouse.de

PGP fingerprint: 3A32 D90A D125 5418
1150 2484 6629 2DD2



Process Control Security Event Exit Process

PRCOSEEP

Version 103

03Feb2005

GreenHouse is proud to announce a new product in its collection of products, preventing Denial of Service (DoS) attacks on a Tandem system.

And this is the DoS threat: Every user, allowed to create a process (any process), can crash the system by starting as many processes as possible. This exhausts all Process Control Blocks (PCB), and results in an inaccessible system.

The attack can be done

- by intention (a small TACL Macro), or
- by error (insufficient program stability and error handling)

and it can NOT be prevented by SAFEGUARD!

SAFEGUARD does not know anything about

- the number of processes a user is allowed to run in parallel
- the total number of process instances of a given program
- process create recursions

I also stumbled into the need to easily deny any program started from object files, residing outside a given set of locations, such as:

- \$SYSTEM.SYSTEM
- \$SYSTEM.SYSnn
- \$DATAoI.PROGRAMS

Or the other way around: Programs can not be started from object files matching e.g.

- \$DATA*.*.*
- \$TEMP*.*.*

And last but not least: What about restricting the parallel execution of programs such as VIEWSYS to e.g. one instance per user? Is there really the need to run multiple copies of VIEWSYS?

Controlling program execution from disk files can be solved with ACLs – but you need to have them on all subvols and/or object type files, may be even in default ACLs on all user records.

Installing ACLs in that depth can NOT be done ‘on the fly’, but requires a massive investment in time, work, and hassle. And it still does not solve controlling the number of process instances.

Is there help?

Yes - there is: The Security Event Authorization Exit (SEE) of SAFEGUARD gets all process create attempts! PRCOSEEP catches these events and rules on them, based on a configuration file.

Functionality

The PRCOSEEP supports these functions:

- Definition of object type files allowed to become executed (restriction of object files to specific locations)
- Restriction of users to execute an object file (this is on top of SAFEGUARD and GUARDIAN)
- Definition of maximum number of process instances per object file and user.
e.g. GHS.CARL is allowed to execute 10 SCLCI, while SUPER.OPERATOR can execute only 2 SQLCI in parallel
- Definition of maximum number of process instances per object file system wide.
e.g. GHS.CARL is allowed to execute 10 SCLCI, while SUPER.OPERATOR can execute only 2 SQLCI in parallel, but in total only 11 SQLCI are allowed on the system
- Deny of process recursions
A process can NOT start a copy of itself. E.g.: SCF can be prevented from starting itself, or a user written process no longer can create itself in a loop with the intention to crash the system.

Actions

In case a Process_Create_ is denied, one of the following actions can be performed by PrCoSEEP:

- Warning
In case the SEEP would deny the Process_Create_, it writes a message to the EMS system. The SEEP process does NOT prevent the process from being started, but hands the ruling to SAFEGUARD and/or GUARDIAN.
- Deny
A denied Process_Create_ is rejected with error 48.
NO EMS message is generated.
- Alarm
A denied Process_Create_ is rejected with error 48.
A message IS written to \$o like this:

```
05-02-07 10:53:49 \BEECH.$Z00W          GHS.21.100          007172 PRCOSEEP:
                                           $SYSTEM.SYSTEM.VIEWSYS was denied create
                                           access; User: GHS.CARL
```

The action type can be configured in the PRCOCONF file.

Interacting with SAFEGUARD

In addition, the following SAFEGUARD rules can be changed/overwritten:

- UNDENIABLE
PRCOSEEP obeys this by default, but this can be turned off, and a Process_Create_ even for SUPER.SUPER can be denied.
- CHECKONLY
SEEP messages can be 'check only' messages.
A check only causes the SEEP to skip its access right evaluation, and to give SAFEGUARD/GUARDIAN the ability to judge.
The check only can be switched off, and PRCOSEEP checks the access rights as well.

Wildcard support

To make the configuration as convenient as possible, user and file entries in the configuration file PRCOCONF support the GreenHouse extended wildcards.
For more details, please consult the explanations at the end of the document.

Log file

All check results are written into a log file, and can be evaluated by ENFORM queries, which are supplied along with the product.

PRCOSEEP supports these three log modes:

1. NONE no log is produced
2. FAIL only rejected Process_Creates_ are logged
3. ALL all Process_Create_ events are logged

Default is: NONE

The log mode, log file owner as well as the log file security can be defined in the PRCOCONF configuration file.

Environment

The SEEP environment consists of six items:

1. The configuration file (PRCOCONF)
2. The data loader program (PRCOLOAD)
3. The data file (PRCODATA)
4. The SEEP program (PRCOSEEP)
5. A data file, required by PRCOSEEP (PRCOUPDA)
6. The log file (PRCOLOGo .. PRCOLOG9)
7. A few ENFORM queries

1. PRCOCONF

The configuration file PRCOCONF is an EDIT type file.

All SEEP attributes and data is defined in this file.

The file is processed by the PRCOLOAD program (see topic 2), which checks and loads the configuration data into a file named PRCODATA (see topic 3).

The following entries are supported:

MODE <mode>

MODE defines the action, PRCOSEEP has to take when rejecting a Process_Create_.

The following attributes are supported:

- WARNING causes PRCOSEEP to send a warning message to the EMS system.
The final execution access is granted by SAFEGUARD or GUARDIAN.
- DENY causes PRCOSEEP to refuse from starting the process.
No message is generated.
- ALARM causes PRCOSEEP to deny the process creation AND to
send a message to the EMS system.

When MODE is not defined in PRCOCONF, the MODE attribute WARNING is assumed.

OBEYUNDENIABLE YES|NO

SAFEGUARD can be configured to grant access to SUPER.SUPER in any cse and independent of an ACL. This is set in the CONFTEXT file: SUPER_SUPER_IS_UNDENIABLE.

By default, PRCOSEEP obeys this setting, and grants access to the undeniable ID, but it also can be directed to ignore this setting and to deny the un-denied ID.

The action is defined by the OBEYUNDENIABLE attribute.

Two settings are supported:

1. YES PRCOSEEP obeys SUPER_SUPER_IS_UNDENIABLE
2. NO PRCOSEEP ignores any UNDENIED ID and rejects a process create when configured.

Default is: YES

Entries are NOT case sensitive.

ALLOWCHECKONLY YES|NO

SAFEGUARD can be used to check an access right, not to perform anything.

PRCOSEEP gets this check only information, and can be directed to:

- let SAFEGUARD/GUARDIAN do the check
- perform the check itself when a matching file/user is found

Two settings are supported:

1. YES PRCOSEEP let SAFEGUARD/GUARDIAN do the check
2. NO PRCOSEEP performs an access check as well

Default is: YES

Entries are NOT case sensitive.

LOGFILEOWNER <owner>

Defines the owner of the PRCOLOGn files.

The log file owner has to be provided as a named user, e.g. GHS.CARL.

GUARDIAN as well as Alias user names are supported.

When this entry is missing, SUPER.SUPER is assumed to own the log files.

LOGFILESECURITY <rwep>

Defines the RWEP settings of the PRCOLOGn files.

Any valid GUARDIAN security string is supported.

Surrounding quotation marks (e.g. "AOO-") are optional.

When this entry is missing, a security string of "OOOO" is assumed.

LOGMODE ALL|FAIL|NONE

PRCOSEEP can log all Process_Create_ events. To customize the logging activities, three settings are supported:

- | | |
|------|---------------------------------|
| ALL | ALL events are logged |
| FAIL | only rejected events are logged |
| NONE | nothing is logged |

ProcessPair Entry <file>

To enable PRCOSEEP a correct interpretation of process create events it has to know, which program file names are used for NonStop process pairs.

A good example is VIEWSYS, PATHMON, PATHTCP2, the SPOOLER object files etc.

Up to 300 entries can be configured.

A configuration line looks like this:

PROCESSPAIR <file-name>

where

PROCESSPAIR Required keyword for each entry

<file-name> file name or file name template of an object file, that can be used as base for a NonStop process pair.
<file-name> has to be WITHOUT any node name, or part of, it.
e.g. \$SYSTEM.SYS*.VIEWSYS is OK, while
 \BEECH.\$SYSTEM.SYS*.VIEWSYS is NOT
<file-name> supports the GreenHouse extended wildcards.

Missing entries for NonStop processes cause PRCOSEEP to misbehave in counting the number of processes a user and the system is actually running.

File Entry <file> [<attribute> .. <attribute>]

Program file entries define objects which are allowed to be started as processes.

A file entry has this structure:

<file-name> [USER <user>] [DENY] [[NO]CHECK] [NOREC] [MAXU <nn>] [MAXT <nn>]

where:

<file-name> file name or file name template, e.g. \$SYSTEM.SYS*.SCF
A template beginning with \$SYSTEM.SYSNN is automatically resolved at runtime to the current SYSNN.
e.g. \$SYSTEM.SYSNN.FUP is resolved to \$SYSTEM.SYS03.FUP
<file-name> support the GreenHouse extended wildcards.
Entries are NOT case sensitive.
This entry is mandatory!

USER <user> defines a user, allowed to execute <file-name>.
USER is a required keyword to define <user>.
The key word is NOT case sensitive.
<user> is a user name or user template.
GUARDIAN user names or templates are NOT case sensitive, while
Alias names or templates ARE case sensitive.
<user> supports the GreenHouse extended wildcards.
This entry is optional. When missing, USER * is assumed.

DENY Keyword
When present causes PRCOSEEP to deny a process create from <file>, matching <user>.
The keyword is optional and NOT case sensitive.
When missing, the entry is NOT denied, but checked.

[NO]CHECK Keyword
When set to NOCHECK, causes PRCOSEEP to skip the check for all matching <file-name>/<user> entries.
When set to CHECK, PRCOSEEP checks the number of running processes with each process stop message. This ensures, that stopped backup processes

	are counted OK. CHECK is the most expensive attribute. When missing, the <file-name>/<user> entry IS checked on an estimate basis. The key word is optional and NOT case sensitive.
NOREC	Keyword When present causes PROSEEP to deny all processes from creating themselves when matching <file-name>/<user>. The key word is optional and NOT case sensitive. When missing, process recursions are OK.
MAXU nn	MAXU is a keyword and defines the maximum processes, derived from <file-name> for a user, matching <user> (Max User). MAXU is a required keyword to define <nn> The keyword is not case sensitive. <nn> is any positive number between 0 and 1,000,000: o allows any number of process instances > 0 number of max. process instances for <file-name>/<user> This entry is optional. When missing, 0 is assumed.
MAXT nn	MAXT is a keyword and defines the maximum processes, derived from <file-name> independent of <user> for the system (Max Total) MAXT is a required keyword to define <nn> The keyword is not case sensitive. <nn> is any positive number between 0 and 1,000,000: o allows any number of process instances > 0 number of max. process instances for <file-name>/<user> on the system This entry is optional. When missing, 0 is assumed.

All lines have to begin with a file name or file name template.
The following keywords and attributes may follow in any order.

An example PROCONF file can be found at the end of this documentation.

2. PRCOLOAD

The PRCOLOAD program is a TAL program.

It reads the PRCOCONF configuration file, parses and checks the data, converts it into a binary format, that can be used by PRCOSEEP, and loads it into the PRCODATA file.

The following two execution modes are supported:

CHECK The CHECK command causes PRCOLOAD to read, parse and check the PRCOCONF configuration file. Errors are displayed to the user.

No changes are done to the PRCOSEEP process.

LOAD The LOAD command directs PRCOLOAD to read, parse and check the PRCOCONF configuration file and to create the file PRCODATA, which is used by PRCOSEEP.

As soon as PRCOSEEP is active, it detects the changes data file, and re-reads it.

This means: A changed PRCOSEEP configuration is taken into account by PRCOSEEP WITHOUT a re-start!

SWITCH PRCOSEEP writes all actions into a log file. This file is kept open until it runs full. The SWITCH command directs PRCOSEEP to close the current log file, and to open a new one.

Command syntax is:

PRCOLOAD CHECK | LOAD | SWITCH

```
$GHS1 PRCOSEEP 68> prcoload check
PRCOLOAD (100) - T7172G06 - (19Jan2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2004
3 MODE attributes recognized
10 FILE attributes recognized
PRCOData NOT loaded
$GHS1 PRCOSEEP 69>
```

```
$GHS1 PRCOSEEP 73> prcoload load
PRCOLOAD (100) - T7172G06 - (19Jan2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2004
3 MODE attributes recognized
10 FILE attributes recognized
13 PRCOData records loaded
$GHS1 PRCOSEEP 74>
```

```
$GHS1 PRCOSEEP 75>prcoload switch
$GHS1 PRCOSEEP 76>
```

3. PRCODATA

The PRCODATA file is created/updated by the PRCOLOAD program, when processing the configuration file PRCOCONF.

PRCODATA is a key-sequenced file.

This file is automatically read by the PRCOSEEP process when ever it is changed.

Do NOT touch this file.

4. PRCOSEEP

The Security Event Exit program PRCOSEEP is a TAL program. To activate it, it has to be attached to SAFEGUARD as a Authorization Security Event Exit Process (SEEP).

The following TACL-Macros are supplied:

- Start to add and start the PRCOSEEP function to SAFEGUARD
- Stop to stop and delete the PRCOSEEP function from SAFEGUARD
- Restart to re-start the PRCOSEEP function
- Info to display the PRCOSEEP attributes

Beside running as SEEP, the PRCOSEEP program can be used interactively to

- list the PRCODATA contents
- evaluate the access right on a <file-name>[<user>] base.

Command syntax is:

```
PRCOSEEP LIST|<prog-file> [<user>]
```

where

LIST directs PRCOSEEP to display the configuration data it is working with. e.g.:

```
$GHS1 PRCOSEEP 51>prcoseep list
PRCOSEEP (100) - T7172G06 - (19Jan2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2004
```

Program	File Name	User	NoCh Deny	Max Use/Total	No ReCu
\$SYSTEM.SYSTEM.VIEWSYS	*			1/ 10	
\$SYSTEM.SYSTEM.SQLCI	*			5/ 100	NORE
\$SYSTEM.SYSTEM.SCF	*			2	NORE
\$SYSTEM.SYS03.TACLH	*		NC		
\$SYSTEM.SYS03.TACL	*		NC		
\$SYSTEM.SYS03.SAFECOM	*				NORE
\$GHS1.SECOM600.*	*			5/ 20	
..TANDUMP	*		DE		
..DIVER	*		DE		
..*	*			10/ 100	NORE

PRCOSEEP executes in ALARM ActionMode

CheckOnly is supported

Undeniable is supported

```
$GHS1 PRCOSEEP 52>
```

<prog-file> directs PRCOSEEP to evaluate execution rights on <prog-file>, e.g.:

```
$GHS1 PRCOSEEP 54> prcoseep $system.system.scf
PRCOSEEP (100) - T7172G06 - (19Jan2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2004
PRCOSEEP executes in ALARM ActionMode
CheckOnly is supported
Undeniable is supported
Program file in question: $system.system.scf
User in question: SA.CARL
Supplied program file will be started!
Matching file entry: $SYSTEM.SYSTEM.SCF
Matching user entry: *
MaxNum user instances: 2
MaxNum total instances: 0
Process recursion NOT allowed
$GHS1 PRCOSEEP 55>
```

<user> directs PRCOSEEP to evaluate execution rights on <prog-file> for user <user>, e.g.:

```
$GHS1 PRCOSEEP 54> prcoseep $system.system.scf sa.carl
PRCOSEEP (100) - T7172G06 - (19Jan2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2004
PRCOSEEP executes in ALARM ActionMode
CheckOnly is supported
Undeniable is supported
Program file in question: $system.system.scf
User in question: SA.CARL
Supplied program file will be started!
Matching file entry: $SYSTEM.SYSTEM.SCF
Matching user entry: *
MaxNum user instances: 2
MaxNum total instances: 0
Process recursion NOT allowed
$GHS1 PRCOSEEP 55>
```

5. PRCOUPDA

To minimize the need to scan the system for the number of processes a user has running, PRCOSEEP uses some estimations, which are stored in the PRCOUPDA data file. Please do NOT change this file while it is open.

6. PRCOLOGo .. PRCOLOGg

All results of PRCOSEEP are written into an entry sequenced file. The information can easily be extracted by ENFORM. Some pre-designed queries are shipped along with the product.

7. ENFORM queries:

LISTLOG lists the PRCOLOG file
LISTPROC list the PRCOUPDA file
LISTSUM lists process summaries

To make ENFORM run, PRCODDL has to be compiled with the DDL compiler to get the DICT-files created.

Installation

Follow the installation guideline as explained in the CD-Install document.

Because PRCOSEEP is system software, it should reside on a system drive, such as \$SYSTEM. Choose a location that makes it easy to have multiple versions available, e.g. \$SYSTEM.PRCO100 for version 100. When the product is installed, the following files should be available:

	CODE	
INFO	101	TACL Macro to get SEEP information from SAFEGUARD
LISTLOG	101	ENFORM query to list the PRCOLOG0 file
LISTPROC	101	ENFORM query to list the PRCOUPDA file
LISTSUM	101	ENFORM query to list process start summaries
PRCOCONF	101	PRCOSEEP Configuration file
PRCODATA	18248	Binary version of PRCOCONF
PRCODDL	101	DDL description of data files
PRCOLOAD	100	Loader program to check and load PRCOCONF
PRCOLOG0	18248	Log file
PRCOSEEP	100	Process Control SEEP
PRCOUPDA	18248	Information file of PRCOSEEP
RESTART	101	TACL Macro to re-start the SEEP
START	101	TACL Macro to start the SEEP
STOP	101	TACL Macro to stop the SEEP

Security settings

The entire PRCOSEEP location should be owned by the system owner, which is SUPER.SUPER. The installation process sets the most secure GUARDIAN attributes automatically.

Performance

PRCOSEEP consumes 0,0463 seconds per Process_Create_ event on an S7000 system, running Go6.23.

Other GreenHouse products to prevent DoS attacks

- PurgeTMP
Purges outdated temporary disk files.
This product is FreeWare.
- LISTLIB
Listner Library, controlling the number of
- started
- logged of
- logged on
FTPSERV processes.
This product is ShareWare.

Availability

The PRCOSEEP product is available as of today. Please contact us at: Info@GreenHouse.de to get a fully functional copy of the product for a two month evaluation period for free.

PRCOCONF File

```
!
!           Process Control Configuration File  PRCOCONF
!           =====
!                               Version 102
!                               -----
!                               02Feb2005
!
!
! Any change of the PRCOCONF file is automatically detected by the
! PRCOSEEP process, causing it to re-read the configuration file PRCODATA.
! NO re-start of the PRCOSEEP process is needed!
!
! Lines, beginning with
! - an exclamation mark  (!)
!
! - a double minus sign  (--)
! - a double equal sign  (==)
! as well as empty lines are treated as comment lines.
!
! Entries in this configuration file - except Alias user names -
! are NOT case sensitive.
!
! PRCOCONF processing
! =====
!
! 1. EDIT this file (PRCOCONF), and adjust the following entries
!    according to your needs:
!    - MODE
!    - OBEYUNDENIABLE
!    - ALLOWCHECKONLY
!    - file entries at the bottom if this file
!
! 2. Run the PRCOLOAD program with the CHECK command to check the entries
!    in the PRCOCONF file:
!
! $GHS1 PRCOSEEP 74> prcoload check
! PRCOLOAD (101) - T7172G06 - (26Jan2005) System \BEECH, running NSK G06
! Copyright (c) GreenHouse Software & Consulting 2005
!     3 MODE attributes recognized
!     10 FILE attributes recognized
!     7 PROCESSPAIR files recognized
! PRCOData NOT loaded
! $GHS1 PRCOSEEP 75>
!
! 3. When everything worked out similar to the shown above, run the
!    PRCOLOAD program with the LOAD command.
!    This loads the PRCOCONF data into file PRCODATA, which is used by
!    PRCOSEEP:
!
! $GHS1 PRCOSEEP 76> prcoload load
! PRCOLOAD (101) - T7172G06 - (26Jan2005) System \BEECH, running NSK G06
! Copyright (c) GreenHouse Software & Consulting 2005
!     3 MODE attributes recognized
!     10 FILE attributes recognized
!     7 PROCESSPAIR files recognized
```



```
! Matching user entry:      *
! MaxNum user instances:    5
! MaxNum total instances:  100
! Process recursion NOT allowed
! $GHS1 PRCOSEEP 79>
!
! -----
! MODE
! =====
! MODE defines the action, PRCOSEEP takes when it rejects a
! Process_Create_
!
! - WARNING causes PRCOSEEP to send a warning message to the EMS
!           system.
!           The final execution access is granted by SAFEGUARD or
!           GUARDIAN.
!
! - DENY causes PROCSEEP to refuse from starting the process.
!         No message is generated.
!
! - ALARM causes PROCSEEP to deny the process creation AND to send
!         a message to the EMS system.
!
! Entries are NOT case sensitive!
!
! When missing, or not correctly defined, WARNING is assumed.
! Default is: WARNING
!
MODE      ALARM
!
! -----
! OBEYUNDENIABLE
! =====
! SAFEGUARD can be configured to grant access to SUPER.SUPER
! INDEPENDENT of any ACL.
! This is set in the CONFTEXT file:  SUPER_SUPER_IS_UNDENIABLE
! It specifies that Safeguard security must ignore explicit denials of
! access authority to the super ID.
! PRCOSEEP can be directed to ignore this setting, and to deny
! Process_Create_ to even SUPER.SUPER.
! This is done by using the OBEYUNDENIABLE attribute.
!
! Two attributes are available:
!   YES = PRCOSEEP obeys SUPER_SUPER_IS_UNDENIABLE
!   NO  = PRCOSEEP rejects a SUPER.SUPER action when needed
!
! Entries are NOT case sensitive!
!
! Default is: YES
!
OBEYUNDENIABLE  YES
!
! -----
! ALLOWCHECKONLY
! =====
! SAFEGUARD can be used to only check an access right, NOT to really
```

```
! reject an action.
! The PRCOSEEP knows about this and can be directed to
! - let SAFEGUARD/GUARDIAN do the check
! - performs a check as well
!
! Two attributes are available:
!   YES = PRCOSEEP lets SAFEGUARD/GUARDIAN do the check
!   NO  = PRCOSEEP performs an access checks as well
!
! Entries are NOT case sensitive!
!
! Default is: YES
!
ALLOWCHECKONLY  YES
!
! -----
!
! LOG File Owner
! =====
! PRCOSEEP logs all its actions to a log file named PRCOLOG0.
! This file belongs by default to SUPER.SUPER.
! The owner can be changed by this entry.
! The LOGFILEOWNER has to be an existing GUARDIAN or Alias user.
! In case the entry is missing, SUPER.SUPER is assumed to be the log
! file owner.
!
LOGFILEOWNER    sa.carl
!
! -----
!
! LOG file security
! =====
! The log file security is set to "0000" by default.
! This can be changed with this entry.
! Any valid RWEP combination is allowed.
! Surrounding quotation marks, e.g. "0000" can be omitted.
! In case this entry is missing, "0000" is assumed to be the log file
! security.
!
LOGFILESECURITY uooo
!
! -----
!
! LOG mode
! =====
! To minimize the number of log entries, PRCOSEEP allows these log mode
! settings:
! - NONE  no log is produced
! - FAIL  only rejected Process_Creates_ are logged
! - ALL   all Process_Create_ events are logged
!
! Default is: NONE
!
LOGMODE all
!
! -----
!
! Process Pair program files
```

```
! =====
! Some program files are the base for NonStop process pairs.
! PROCOSEEP should know about these file names to ensure, it performs a
! proper counting.
! Program File names have to be delivered WITHOUT a node name extension.
! GreenHouse extended wildcards are supported.

!
! The maximum number of entries is limited to 300.
!
! In case no PROCESSPAIR entries are defined, no PROCISPAIR file
! names are taken into account.
!
! The following program file names are delivered by default:
!
PROCESSPAIR  $system.system.viewsys
PROCESSPAIR  $system.system.spool
PROCESSPAIR  $system.system.cspool
PROCESSPAIR  $system.sysnn.tacl
PROCESSPAIR  $system.sysnn.taclh
PROCESSPAIR  $system.system.pathmon
PROCESSPAIR  $system.system.pathtcp2
!
! -----
!
! Program File Names and attributes:
! =====
! Program file entries define the object file names allowed to be
! started as processes.
!
! A file entry has this structure:
!
! <file-name> [USER <user>] [DENY] [NOCHECK] [NOREC] [MAXU <nn>] [MAXT <nn>]
!                                     [CHECK]
! where
!
! <file-name>      is a file name or file name template.
!                  e.g. $SYSTEM.SYS*.SCF
!
!                  $SYSTEM.SYSNN.<file> is automatically adjusted to the
!                  current SYSnn.
!                  $SYSTEM.SYSNN.FUP is automatically adjusted to e.g.:
!                  $SYSTEM.SYS03.FUP
!
!                  GreenHouse extended wildcards are supported.
!                  Entries are NOT case sensitive.
!
!                  This entry is mandatory.
!
! USER <user>     Defines a user, allowed to execute <file-name>.
!                  USER is a required key word to define <user>.
!                  The key word is NOT case sensitive.
!
!                  <user> is a user name or user name template.
!
!                  GUARDIAN user/template entries are NOT case
!                  sensitive, while Alias user/template entries ARE
!                  case sensitive!
```

```
!
!           GreenHouse extended wildcards are supported.
!
!           This entry is optional.
!           When missing, a user template of "*" is used.
!
! DENY      Keyword
!           When present, causes PRCOSEEP to deny all
!           processes, created from <file> and matching <user>.
!
!           The key word is NOT case sensitive.
!
!           This entry is optional.
!           When missing, no DENY is assumed.
!
! NOCHECK   Keyword (No Check)
!           When present, causes PRCOSEEP to skip the SEEP logic
!           for the matching user/file entry.
!           The key word is NOT case sensitive.
!
!           This entry is optional.
!           When missing, a check is done on estimations.
!
! CHECK     Keyword (Check)
!           When present, causes PRCOSEEP to perform the SEEP
!           logic for the matching user/file entry and to
!           update the estimation counters at every STOP event.
!           The key word is NOT case sensitive.
!
!           This entry is optional.
!           When missing, a check is done on estimations.
!
!           This option allows a better control for processes,
!           being stopped from the outside, and for stopped
!           backup processes.
!           This option increases the CPU time PRCOSEEP uses on
!           a STOP event.
!
! NOREC     Keyword (No Recursions)
!           When present, causes PRCOSEEP to deny all
!           processes, creating itself when
!           created from <file> for matching <user>.
!
!           The key word is NOT case sensitive.
!
!           This entry is optional.
!           When missing, recursions are not checked.
!
! MAXU <nn> MAXU is a key word (Max processes per User)
!           Defines the number of instances of a process,
!           started from <file> for matching <user>.
!           MAXU is a required key word to define <nn>.
!
!           The key word is NOT case sensitive.
!
!           <nn> is any number between 0 and 1,000,000.
!           0 = allow any number of instances
!           > 0 = number of allowed process instances
```

```
!
!           This entry is optional.
!           When missing, 0 is used (= any number of instances)
!
! MAXT <nn>      MAXT is a key word
!                 (Max Total = max processes system wide)
!                 Defines the total number of instances of a process,
!                 started from <file> INDEPENDENT of <user>.
!                 MAXT is a required key word to define <nn>.
!
!           The key word is NOT case sensitive.
!
!           <nn> is any number between 0 and 1,000,000.
!           0 = allow any number of instances
!           > 0 = number of allowed process instances
!
!           This entry is optional.
!           When missing, 0 is used (= any number of instances)
!
! A <file> entry has to start with a file name or file name template.
! The order of the file attributes is irrelevant.
!
! The maximum number of currently supported <file> entries is limited
! to 20,000.
! The PRCOLOAD program currently works on systems, where no more than
! 100,000 system users are configured.
! In case you like to have these limits extended, please let us know
! your requirements, and we enhance the product.
!
! PRCOSEEP uses a file name evaluation mechanism, that is based on
! the 'most complete' algorithm developed by GreenHouse. This ensures,
! that templates are evaluated in the correct order.
! e.g.:
! - $A.B.C is more complete than $A.B.*
! - $*.*.* is less complete than $*.*.C
!
! Use fully qualified file names when ever possible.
!
! To get the sorted list of program file names, execute the LIST
! command when running PRCOSEEP interactively:
!
!   RUN PROCSEEP LIST
!
! Object file names, not mentioned in this file, or having the DENY
! attribute, can not be started and are rejected with error 48.
!
! Missing file entries make PRCOSEEP assume this default entry:
!
!   $*.*.* USER * MAXU 0 MAXT 0
!
! where
!
!   $*.*.* = all program file names
!   USER * = all GUARDIAN as well as Alias users
!   MAXU 0  = no limit on process instances per user
!   MAXT 0  = no limit on process instances system wide
!
!
```

