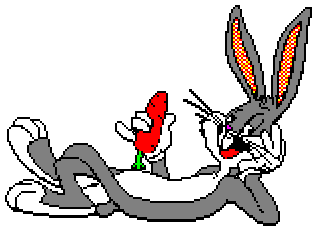
WhatsUp

Version 101

Reference Manual

16. January 2003



GreenHouse
Software & Consulting
Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg

Contents

What's Up

Introduction

Do you remember Bugs Bunny, asking his friends the question: What's up, Doc? And he always got an answer!
The original sound track is part of the product delivery (Whats Up Doc.wav).

Would you sometimes like to ask this question to SAFEGUARD to get an answer about the activities, filling up the Audit files?

While doing a Security Review I ended up with exactly this question: What is filling up 180 MB big SAFEGUARD Audit files within 10 hours, when there are literally no ACLs set, the general auditing was switched off, and only SUPER.SUPER activities were audited?
We had no clue.

Finally I decided to write a program that answers this question, and to name the product after the question of Bugs Bunny: WhatsUp.

WhatsUp evaluates incoming SAFEGUARD audit events in real time and displays them to the user.

The following execution modes are implemented:

1. Display accumulated event groups (compounds) every 10 seconds
2. Display up to 22 accumulated individual event types every 10 seconds
3. Display individual event types of an event group (compound) in real time
4. Display an individual event type in real time

My suggestion to look into the SAFEGUARD audit records is:

1. run WhatsUp with the BRIEF command
2. select the interesting compound events
3. select the most interesting detail event

or

1. run WhatsUp with the ALL command
2. select the most interesting detail event

Software Type

WhatsUp is ShareWare – a new type of software on the NSK systems. You are allowed to use the product for a two month period for free. When you use if on a regular basis after these two months, you are requested to register with GreenHouse (Info@GreenHouse.de), and to pay a one time fee of 1,000.00 € (for European users) or 1,000.00 US$ (all other users).
Paying the license fee entitles you to get unlimited product maintenance.

Maintenance

WhatsUp is a maintained product. Please report bugs, glitches and requests for enhancements to: Info@GreenHouse.de

Command Syntax

WhatsUp has the following command syntax:

```
[run] WHATSUP[/OUT <file>/] -H[ELP] [display-type] [;filter]
```

where

OUT allows to re-route the output to a disk file, or SPOOLER location.

-HELP display a help screen with the command syntax.

display-type is one of:

ALL Directs WhatsUp to display all audit event counters.
An example can be found at:
Display Individual Event Counters

BRIEF Causes WhatsUp to display accumulated compound event counters.
An example can be found at:
Display Compound Group

<event-type> Directs WhatsUp to display a specific event type only.
An example can be found at:
Display Individual Event Counters
and
Display Compound Group Details

When no parameter is given, ALL is assumed.

The display-type can be changed at run-time.

filter is one of:

USER <name> Defines a user; when present, only events of the given user are taken into account.
<name> supports wildcards.
Depending of the type of user, <name> is case sensitive.

DISKFILE <item> Defines a disk file; when present, only events, matching the given disk file, are taken into account.
<item> supports wildcards.
<item> is NOT case sensitive.

PROCESS <item> Defines a process name; when present, only events, matching the given disk file are taken into account.
<item> supports wildcards.
<item> is NOT case sensitive.

Multiple filters can be supplied.

Filters can NOT be changed at run-time.

Technical insights

When WhatsUp is started, it uses the SPI interface to talk to $ZSMP, the SAFEGUARD monitor process, to get the name of the currently used audit file. This file is opened, and WhatsUp positions to the EOF. It then establishes a READ that completes, when a new record is written into the audit file.

In case a new record is written, WhatsUp wakes up, reads the newly written audit record(s), analyses them, formats them, and displays the result. This is done until the EOF is reached again.

In case the audit file switches, WhatsUp takes care of the situation, closes the 'old' audit file, and opens the new one. This is totally transparent to the user.

The display–type can be changed at run time by simply typing one of the key words:

- BRIEF
  (see: Display Compound Group Counters)
- ALL
  (see: Display Individual Event Counters)
- <event-type> as defined in Appendix A - Event Types
  (seet: Display Compound Group Details and Display Individual Event Details)

Filters can NOT be changed during runtime.

Display Compound Group Counters

To get an overview of the audit activities in SAFEGUARD, use the BRIEF mode: It displays all events, combined in so called event compound groups.

Command syntax:

```
[run] WHATSUP [/OUT <file>/] BRIEF [;filter]
```

BRIEF
The keyword **BRIEF** causes WhatsUp to display accumulated event compound groups, e.g. all disk file events (READ, WRITE, PURGE etc.) in one line. It gives a good first overview of the SAFEGUARD audit activities.
filter
A filter limits the output down to a user, disk file or process.
For more details refer to Command Syntax.

For more command syntax information, please refer to Command Syntax.

The following compound groups are implemented:

- `Authentication` includes all authentication events
- `AllDiskFile` includes all disk file events
- `AllOSS` includes all OSS events
- `AllProcess` includes all process events
- `AllSAFEGUARD` includes all SAFEGUARD events
- `AllSQL` includes all SQL events
- `AllTMF` includes all TMF events
- `AllOther` includes all events, not covered by one of the above compound groups

Fore more details re. The compound groups, please refer to Compound events.

WhatsUp accumulates all Audit events on a by compound group basis, counts them, and displays them as follows:

- 10 seconds number of events within the last 10 seconds
- One minute number of events within the last minute
- 10 Minutes number of events within the last 10 minutes
- One Hour number of events within the last hour
- Total total number of events since begin of measurement
- Pass total number of pass results
- Fail total number of fail results

WhatsUp displays the compound groups sorted in the following order

- Biggest number of 10 second
- Bigges number of one minute
- Biggest number of 10 minutes
- Biggest number of one hour
- Biggest total number

Start screen

When WhatsUp is started, the following screen is displayed:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2002,2003
User filter:     *
Process filter:  *
Diskfile filter: *
Positioning to EOF of actual Audit file $SYSTEM.SAFE.A0001324
Waiting for SAFEGUARD events. Stay tuned!
```

In case there are no SAFEGUARD events for 10 seconds, WhatsUp displays a time counter like this:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2002,2003
User filter:     *
Process filter:  *
Diskfile filter: *
Positioning to EOF of actual Audit file $SYSTEM.SAFE.A0001324
Waiting for SAFEGUARD events. Stay tuned!
No events since 00:00'09,999.096
No events since 00:00’19,999.003
```

Result screen

When SAFEGUARD audit record are detected, the output changes to this:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   18:33:23 10Feb2003  19:12:33 10Feb2003
     Event      Ten  Minu  10Mi   Hour    Total     Pass     Fail  Last Event
AllProcess        1     5     5      8        8        0        0   19:12:23
AllOther          0     2     2      8        8        0        0   19:11:47
AllDiskFile       0     0     0     17       17        0        0   18:40:28
Authentication    0     0     0      1        1        0        0   18:40:19
```

This screen is updated every 10 seconds.

Switching to a new Event Type

To switch to a new event type, press the RETURN key, and type in the new event you like to get displayed. Also refer to Changing the Display Mode.

Terminating WhatsUp

To terminate WhatsUp when OUT is a terminal:

- Press the BREAK key, or
- Type the CTRL-Y key combination

To terminate WhatsUp when OUT is a disk file:

- Stop the WhatsUp process.

Display Individual Event Counters

To get an overview about the audit activities of SAFEGUARD, use this mode.

Command syntax:

```
[run] WHATSUP [OUT <file>/] [ALL] [;filter]
```

WhatsUp accumulates all Audit events on a by event-type basis, counts them, and displays them as follows:

- 10 seconds number of events within the last 10 seconds
- One minute number of events within the last minute
- 10 Minutes number of events within the last 10 minutes
- One Hour number of events within the last hour
- Total total number of events since begin of measurement
- Pass total number of pass results
- Fail total number of fail results

WhatsUp displays up to 22 event types sorted in the following order

- Biggest number of 10 second
- Bigges number of one minute
- Biggest number of 10 minutes
- Biggest number of one hour
- Biggest total number

In case events have the same number profile, they are sorted in alphabetical order.

Event types with an event count of zero are NOT displayed.

Start screen

When WhatsUp is started, the following screen is displayed:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2002,2003
Positioning to EOF of actual Audit file $SYSTEM.SAFE.A0001237
Waiting for SAFEGUARD events. Stay tuned!
```

In case there are no SAFEGUARD events for 10 seconds, WhatsUp displays a time counter like this:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 2002,2003
Positioning to EOF of actual Audit file $SYSTEM.SAFE.A0001237
Waiting for SAFEGUARD events. Stay tuned!
No events since 00:00'10,002.217
No events since 00:00'20,001.918
.
.
```

Result screen

When a SAFEGUARD audit record is detected, the output changes to this:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   15:26:44 18Jan2003  15:29:34 18Jan2003
     Event      Ten  Minu  10Mi   Hour    Total     Pass     Fail  Last Event
Authentication    2     2     2      2        2        0        0   15:29:26
Logoff            1     1     1      1        1        1        0   15:29:26
VerifyUser        1     1     1      1        1        1        0   15:29:26
```

This screen is updated every 10 seconds, and might show something like this after a while:

```
WhatsUp (101) - T7172G06 - (16Jan2003)   15:26:44 18Jan2003  15:33:44 18Jan2003
     Event      Ten  Minu  10Mi   Hour    Total     Pass     Fail  Last Event
Purge             1     2     2      2        2        2        0   15:33:35
ReadWrite         0     2     2      2        2        2        0   15:33:22
Create            0     1     1      1        1        1        0   15:33:11
Execute           0     1     1      1        1        1        0   15:33:22
Read              0     1     1      1        1        1        0   15:33:31
Authentication    0     0     2      2        2        0        0   15:29:26
Logoff            0     0     1      1        1        1        0   15:29:26
VerifyUser        0     0     1      1        1        1        0   15:29:26
```

The maximum number of displayed events is limited to 22 – a 6530 type screen does not support more lines..

Switching to a new Event Type

To switch to a new event type, press the RETURN key, and type in the new event you like to get displayed. Also refer to Changing the Display Mode.

Terminating WhatsUp

To terminate WhatsUp when OUT is a terminal:

- Press the BREAK key, or
- Type the CTRL-Y key combination

To terminate WhatsUp when OUT is a disk file:

- Stop the WhatsUp process.

Display Compound Group Details

Beside displaying counters, WhatsUp can display so called compound events.
The following compound events are implemented:

Compound Group	Event
Authentication	Authentication
	Logoff
	Logon
	VerifyUser
AllDiskFile	ChangeOwner
	Create
	Execute
	Purge
	Read
	ReadWrite
	Rename
	Start
	Write
AllOSS	Access
	DirSearch
	Kill
	Link
	OSSResolve
AllProcess	ChangePRI
	ChangeSMom
	Debug
	Execute
	Start
	Stop
AllSAFEGUARD	NextFile
	Release
AllSQL	Grant
	Insert
	Reference
	Revoke
	Select
AllTMF	Abort
	Add
	Alter
	BackOut
	Enable
	Exclude
	Initialize
	Next
	OnlineDump
	Resolve
	RollForward
AllOther	all events, not covered by the compound events shown above.

Command syntax:

```
[run] WHATSUP [out <out-file>/] <compound> [;filter]
```

where

<compound> is one of the events shown above.

Switching to a new Event Type

To switch to a new event type, press the RETURN key, and type in the new event you like to get displayed. Also refer to Changing the Display Mode.

Display Individual Event Details

Command syntax:

```
[run] WHATSUP [out <out-file>/] <event-type> [;filter]
```

where

<event-type> is one of the definitions in SAFEGUARD events.

Switching to a new Event Type

To switch to a new event type, press the RETURN key, and type in the new event you like to get displayed. Also refer to Displayed Event Data.

Displayed Event Data

WhatsUp displays the following data from the zSFG^DDL^Primary^Record SAFEGUARD audit record:

- [event type]
- zObject.zObject^Name
- zSubject.zProcessName
- zOutcome
- zSubject.zUserName

e.g.

```
Read  $GHS1.WHATSUP.WHATSUPS by $SYSTEM.SYSTEM.EDIT (1,105)  NoRec  SA.CARL
```

where

Read	[event type]
$GHS1.WHATSUP.WHATSUPS	zObject.zObject^Name
$SYSTEM.SYSTEM.EDIT (1,105)	zSubject.zProcessName
NoRec	zOutcome
SA.CARL	zSubject.zUserNamed

Changing the Display Mode

Once WhatsUp is started, the display-mode can be changed during run time. This allows you to switch back and forth between different display modes and allows you to see various counters and events while WhatsUp keeps its counter history.

To change the display mode of WhatsUp, simply type in any known event type.
A list of legal event types can be found at: Appendix A - Event Types.

WhatsUp can be in a mode, where you don't have enough time to type in a new event type, because it displays events faster than you can type. In this case, switch to the ALL mode by pressing the RETURN key.
When in ALL mode, WhatsUp refreshes the screen every 10 seconds. This is enough time to then e.g. type a key word, such as ALLDISKFILE to switch WhatsUp into a mode, where all disk file events are displayed.

Advise: To change the display mode, first type RETURN, followed by the event key word.

Changing Filters

Filters can NOT be changed at run time!

Installation

WhatsUp comes as a program with a file code of 100. It is accelerated, and stripped.
It can be located anywhere on the system.
What about putting it in $SYSTEM.GHSTOOLS.*, and making this location available in the search path (TACLLOCL), AND protecting this location with an ACL against Trojan horses (foreign create)?

Security Settings

Owner:	SUPER.SUPER
GUARDIAN security:	OOOO
SAFEGUARD ACL:	owner 255,255, access 255,255 *
License Flag:	No
ProgID:	Can be set to allow non SUPER.SUPER users access. A better solution would be to control WhatsUp through a command level security tool such as SECOM.
Location:	Any; but what about $SYSTEM.GHS.WHATSUP?

Appendix A - Event Types

The following is a list of SAFEGUARD event types, known by WhatsUp. These event types can be used at start-up time, or to re-focus WhatsUp during run-time.
A detailed description of the event types is available at Event Description.

General events

General events are a collection of events:

`All`	Displays up to 22 SAFEGUARD events along with their counters.
`Brief`	Displays all Compound events along with their counters.

Compound events

Compound events combine individual events into groups as follows:

`Authentication`	`Authentication`
	`Logoff`
	`Logon`
	`VerifyUser`
`AllDiskFile`	`ChangeOwner`
	`Create`
	`Execute`
	`Purge`
	`Read`
	`ReadWrite`
	`Rename`
	`Start`
	`Write`
`AllOSS`	`Access`
	`DirSearch`
	`Kill`
	`Link`
	`OSSResolve`
`AllProcess`	`ChangePRI`
	`ChangeSMom`
	`Debug`
	`Execute`
	`Start`
	`Stop`
`AllSAFEGUARD`	`NextFile`
	`Release`
`AllSQL`	`Grant`
	`Insert`
	`Reference`
	`Revoke`
	`Select`
`AllTMF`	`Abort`
	`Add`
	`Alter`
	`BackOut`
	`Enable`
	`Exclude`

	Initialize Next OnlineDump Resolve RollForward
AllOther	all events, not covered by the compound events shown above.

SAFEGUARD events

Abort
Accept
Access
Add
Alter
Authenticate
BackOut
Change
ChangeOwner
ChangePriority
ChangeStepMom
Close
Composite
Create
Debug
Delete
DirSearch
Enable
Exclude
Execute
Give
Grant
Initialize
Insert
Kill
License
Link
Logoff
Logon
NewProcess
Next
NextFile
NextTape
OnlineDump
Open
OSSResolve
Other
ProgID
Purge
Read
ReadWrite

Reference
Reject
Release
Rename
Reset
Resolve
Revive
Revoke
Rollforward
Scratch
Security
Select
Set
Start
Stop
Suspend
Update
UseTape
VerifyUser
Write
Unknown

Appendic B - SAFEGUARD Events

Event Description

Abort	Refers to a TMF ABORT operation.
Accept	Refers to the acceptance of a request.
Access	Refers to OSS operations to check the user's access permissions for a given object.
Add	Refers to a TMF ADD operation.
Alter	Describes a TMF ALTER operation.
Authenticate	Refers to an identity check of a user ID requested by a client subsystem. This does not imply that a logon action occurred or was attempted following a successful authentication.
BackOut	Refers to a NonStop TMF BACKOUT operation.
Change	Refers to an attempted change to one or more object attributes. Unlike Update, Change implies that the attempt involved reading and overwriting the attributes.
ChangeOwner	Refers to an explicit change in object ownership made by a command such as the FUP GIVE command.
ChangePriority	Refers to a change of the priority of a process or process pair.
ChangeStepMom	Refers to a change of the step mom of a process or process pair.
Close	Refers to the termination of a connection between an object and a subject when an object is closed.
Composite	No documentation
Create	Refers to the creation of an object or record.
Debug	Refers to a request to put the process in debug mode.
Delete	Refers to the deletion of part of an object or a portion of its contents. On completion of this operation, the affected object remains in existence.
DirSearch	Refers to directory search operation performed by an OSS Name Server while resolving a path name to ensure that the subject has search authority for that directory.
Enable	Refers to a TMF ENABLE operation.
Exclude	Refers to a TMF EXCLUDE operation.
Execute	Refers to opens of program files for execution.
Give	Reserved for future use.
Grant	Refers to an SQL grant or transmission of access rights to an SQL object by one user to another.
Initialize	Refers to a TMF INITIALIZE operation.
Insert	Refers to an operation, not exclusively by SQL, involving the insertion of a record or other collection of values into an object, such as a file or table.
Kill	Refers to OSS operation to terminate an existing process or group of processes.
License	Reserved for future use.
Link	Refers to OSS operation to terminate an additional directory entry for an existing file on the same file set.
Logoff	Refers to a logoff that occurs if a user successfully logs on at a terminal where another user has not logged off. The previous user is automatically logged off. Logoff also refers to logoffs that occur from Safeguard terminals.

Logon	Refers to a user authentication that is followed by either the creation of a new process that executes as the authenticated user or the transformation of an existing process that executes as the authenticated user.
NewProcess	Reserved for future use.
Next	Refers to a TMF NEXT operation.
NextFile	Refers to an audit file rollover resulting from a NEXTFILE command.
NextTape	Refers to a next tape operation.
OnlineDump	Refers to a TMF online dump operation.
Open	Refers to the establishment of a connection between an object and a subject when an object is opened. This value is not used for audited Safeguard events. More specific descriptions, such as READ and WRITE, are used for Safeguard events.
OssResolve	Refers to a Resolve record generated by an OSS Name Server to audit the mapping of the path name used to access a file and the internal name.
Other	Refers to an event other than one of those described here.
Progid	Reserved for future use.
Purge	Refers to the deletion of an object after which the object ceases to exist.
Read	Refers to object opens for read access.
ReadWrite (Update)	Refers to object opens for read/write access. Update does not imply that the accessed object was actually changed. It implies only that the requested access was read/write.
Reference	Refers to an SQL operation in which an SQL object is implicitly read during the course of some other operation performed on a related object.
Reject	Refers to the rejection of a request.
Release	Refers to an audit file release resulting from a RELEASE command.
Rename	Refers to the renaming of an object.
Reset	Refers to the action of resetting a flag or condition.
Resolve	Refers to a TMF RESOLVE operation.
Revive	Refers to a change of state of an object from inactive to active.
Revoke	Refers to an SQL revocation of a user's access rights to an SQL object by another user.
RollForward	Refers to a TMF roll forward operation.
Scratch	Refers to the action of expiring a labeled tape.
Security	No documentation
Select	Refers to an SQL selection operation applied to an SQL table or view.
Set	Refers to the action of setting a flag or condition.
Start	Refers to a change of state of an object to an active state.
Stop	Refers to a change of state of an object to an inactive state in which the object might cease to exist.
Suspend	Refers to a change of state of an object from active to inactive. In this state, the object continues to exist but is otherwise dormant.
UseTape	Refers to a use tape operation.
VerifyUser	Refers to a user authentication and subsequent logon performed by the operating system or the Safeguard subsystem.
Write	Refers to object opens for write access.

Outcome Description

Denied	Permission to attempt the requested operation was denied.
Failed	The requested operation was unsuccessfully completed.
Granted	Permission to attempt the requested operation was granted.
Maybe	The outcome was unknown when the audit request was made.
NoRecord	The outcome was undetermined when the audit request occurred because the authorization record for the accessed object could not be found or did not exist. This outcome occurs in audit requests originated by the Safeguard subsystem.
Other	This value refers to an outcome other than those defined here.
PartialSuccess	The operation was successful for the primary partition of a file but might have failed for one or more secondary partitions.
Passed	The requested operation completed successfully.
Pending	The outcome is only partially complete and requires additional processing before final authorization can be made.
UserExpired	The authentication attempt failed because the user expired. Occurs only if operation is Authenticate or VerifyUser.
UserFailed	The authentication attempt failed because the number of failed attempts by the user exceeded the configured maximum. Occurs only if operation is Authenticate or VerifyUser.
UserFrozen	The authentication attempt failed because the user was frozen. Occurs only if operation is Authenticate or VerifyUser.
UserInvalid	The authentication attempt failed because the user was invalid or unknown to the system. Occurs only if operation is Authenticate or VerifyUser.
UserPwExpired	The authentication attempt failed because the user's password expired. Occurs only if operation is Authenticate or VerifyUser.
UserPwInvalid	The authentication attempt failed because the user supplied an incorrect password. Occurs only if operation is Authenticate or VerifyUser.
UserValid	The user was successfully authenticated. Occurs only if operation is Authenticate or VerifyUser.
Warning	The operation would have been denied, but the system was in Safeguard warning mode.

Appendix C - List of Event Relations

SAFEGUARD Event	WhatUp Internal Event	WhatsUp Event	WhatsUp Compound Type
ZSFG^VAL^OPER^ABORT	Oper^Abort	Abort	ALLTMF
ZSFG^VAL^OPER^ACCEPT	Oper^Accep	Accep	AllOther
ZSFG^VAL^OPER^ACCESS	Oper^Access	Access	ALLOSS
ZSFG^VAL^OPER^ADD	Oper^Add	Add	ALLTMF
ZSFG^VAL^OPER^ALTER	Oper^Alter	Alter	ALLTMF
ZSFG^VAL^OPER^AUTHENTICATE	Oper^Authenticate	Authenticate	Authentication
ZSFG^VAL^OPER^BACK^OUT	Oper^Back^Out	BackOut	ALLTMF
ZSFG^VAL^OPER^CHANGE	Oper^Change	Change	AllOther
ZSFG^VAL^OPER^CHANGE^OWNER	Oper^Change^Owner	ChangeOwner	AllDiskfile
ZSFG^VAL^OPER^CHANGEPRIORITY	Oper^ChangePriority	ChangePriority	AllProcess
ZSFG^VAL^OPER^CHANGESTEPMOM	Oper^ChangeStepMom	ChangeStepMom	AllProcess
ZSFG^VAL^OPER^CLOSE	Oper^Close	Close	AllOther
ZSFG^VAL^OPER^COMPOSITE	Oper^Composite	Composite	AllOther
ZSFG^VAL^OPER^CREATE	Oper^Create	Create	AllDiskfile
ZSFG^VAL^OPER^DEBUG	Oper^Debug	Debug	AllProcess
ZSFG^VAL^OPER^DELETE	Oper^Delete	Delete	AllOther
ZSFG^VAL^OPER^DIRSEARCH	Oper^DIRSearch	DIRSearch	ALLOSS
ZSFG^VAL^OPER^ENABLE	Oper^Enable	Enable	ALLTMF
ZSFG^VAL^OPER^EXCLUDE	Oper^Exclude	Exclude	ALLTMF
ZSFG^VAL^OPER^EXECUTE	Oper^Execute	Execute	AllDiskfile AllProcess
ZSFG^VAL^OPER^GIVE	Oper^Give	Give	AllOther
ZSFG^VAL^OPER^GRANT	Oper^Grant	Grant	ALLSQL
ZSFG^VAL^OPER^INITIALIZE	Oper^Initialize	Initialize	ALLTMF
ZSFG^VAL^OPER^INSERT	Oper^Insert	Insert	ALLSQL
ZSFG^VAL^OPER^KILL	Oper^Kill	Kill	ALLOSS
ZSFG^VAL^OPER^LICENSE	Oper^License	License	AllOther
ZSFG^VAL^OPER^LINK	Oper^Link	Link	ALLOSS
ZSFG^VAL^OPER^LOGOFF	Oper^Logoff	Logoff	Authentication
ZSFG^VAL^OPER^LOGON	Oper^Logon	Logon	Authentication
ZSFG^VAL^OPER^NEWPROCESS	Oper^NewProcess	NewProcess	AllOther
ZSFG^VAL^OPER^NEXT	Oper^Next	Next	ALLTMF
ZSFG^VAL^OPER^NEXTFILE	Oper^NextFile	NextFile	AllOther
ZSFG^VAL^OPER^NEXTTAPE	Oper^NextTape	NextTape	AllOther
ZSFG^VAL^OPER^ONLINE^DUMP	Oper^Online^Dump	OnlineDump	ALLTMF
ZSFG^VAL^OPER^OPEN	Oper^Open	Open	AllOther
ZSFG^VAL^OPER^OSSRESOLVE	Oper^OSSResolve	OSSResolve	ALLOSS
ZSFG^VAL^OPER^OTHER	Oper^Other	Other	AllOther
ZSFG^VAL^OPER^PROGID	Oper^PROGID	PROGID	AllOther
ZSFG^VAL^OPER^PURGE	Oper^Purge	Purge	AllDiskfile
ZSFG^VAL^OPER^READ	Oper^Read	Read	AllDiskfile
ZSFG^VAL^OPER^READWRITE & ZSFG^VAL^OPER^UPDATE	Oper^ReadWrite	ReadWrite	AllDiskfile
ZSFG^VAL^OPER^REFERENCE	Oper^Reference	Reference	ALLSQL
ZSFG^VAL^OPER^REJECT	Oper^Reject	Reject	AllOther
ZSFG^VAL^OPER^RELEASE	Oper^Release	Release	AllOther
ZSFG^VAL^OPER^RENAME	Oper^Rename	Rename	AllDiskfile
ZSFG^VAL^OPER^RESET	Oper^Reset	Reset	AllOther
ZSFG^VAL^OPER^RESOLVE	Oper^Resolve	Resolve	ALLTMF
ZSFG^VAL^OPER^REVIVE	Oper^Revive	Revive	AllOther
ZSFG^VAL^OPER^REVOKE	Oper^Revoke	Revoke	ALLSQL
ZSFG^VAL^OPER^ROLLFORWARD	Oper^RollForward	RollForward	ALLTMF

ZSFG^VAL^OPER^SCRATCH	Oper^Scratch	Scratch	AllOther
ZSFG^VAL^OPER^SECURITY	Oper^Security	Security	AllOther
ZSFG^VAL^OPER^SELECT	Oper^Select	Select	ALLSQL
ZSFG^VAL^OPER^SET	Oper^Set	Set	AllOther
ZSFG^VAL^OPER^START	Oper^Start	Start	AllDiskfile AllProcess
ZSFG^VAL^OPER^STOP	Oper^Stop	Stop	AllProcess
ZSFG^VAL^OPER^SUSPEND	Oper^Suspend	Suspend	AllOther
ZSFG^VAL^OPER^USETAPE	Oper^UseTape	UseTape	AllOther
ZSFG^VAL^OPER^VERIFYUSER	Oper^VerifyUser	VerifyUser	Authentication
ZSFG^VAL^OPER^WRITE	Oper^Write	Write	AllDiskfile
Otherwise	Oper^Unknown	Unknown	AllOther