

# VILib

Version 311

## Reference Manual

19. March 2007

The logo for greenHouse features the word "green" in a black, lowercase, sans-serif font, followed by a stylized green house icon with a red roof and a green chimney. The word "House" is in a black, uppercase, sans-serif font, with the "H" being red and the "ouse" being black. The entire logo is centered above the text "Software & Consulting".  
**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, TACL, 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 © 2007 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](mailto:Info@GreenHouse.de)

Internet: [www.GreenHouse.de](http://www.GreenHouse.de)

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



## Visual Inspect Library – VILib

Version 311  
19Mar2007

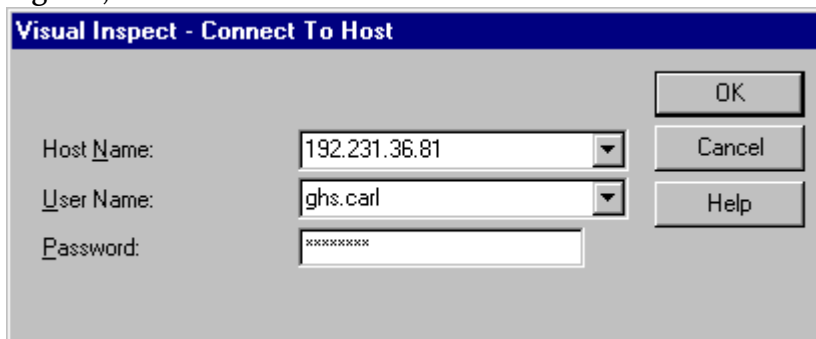
In a SECOM environment, access to all functional users is granted by SECOM WITHOUT the need to know the password. To run Visual Inspect for a functional user, actually the password of this user has to be known. This is - for a SECOM environment - a security breach, because it bypasses the SECOM security functions.

Knowing a password allows a 'logon from scratch', with losing the accountability.

The solution to this is a library, that replaces the original users authentication, and performs a mapping to a granted target ID.

The Visual Inspect authentication screen is enhanced to supply a target ID that has to be used.

Normally, the user types in his ID and password to get access to Visual Inspect. In case GHS.CARL logs on, it looks like this:

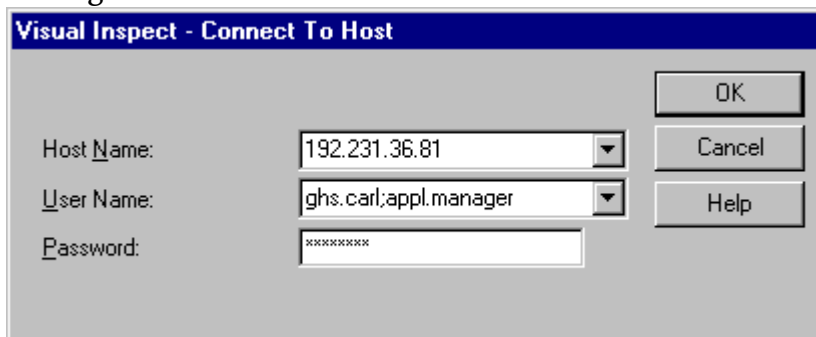


The screenshot shows a dialog box titled "Visual Inspect - Connect To Host". It contains three input fields: "Host Name" with the value "192.231.36.81", "User Name" with the value "ghs.carl", and "Password" with a masked value "\*\*\*\*\*". To the right of the input fields are three buttons: "OK", "Cancel", and "Help".

The enhancement by the VILIB product now allows GHS.CARL to ask Visual Inspect, not to logon to GHS.CARL, but to a target ID, e.g. APPL.MANAGER.

The user ID to be used in that case is: GHS.CARL, followed by a semicolon, followed by the target ID. The password is the one of GHS.CARL, NOT APPL.MANAGER!

The logon screen looks like this:



The screenshot shows a dialog box titled "Visual Inspect - Connect To Host". It contains three input fields: "Host Name" with the value "192.231.36.81", "User Name" with the value "ghs.carl;appl.manager", and "Password" with a masked value "\*\*\*\*\*". To the right of the input fields are three buttons: "OK", "Cancel", and "Help".

In this case, the user GHS.CARL and his password is checked, and after a successful authentication, the library takes over: It checks, if GHS.CARL is allowed to become mapped to the requested user ID, and in case he is, the Inspect Server becomes logged on to APPL.MANAGER automatically WITHOUT the need to know any password, except the one of GHS.CARL!

# greenHouse

---

- The mapping is defined in a small EDIT type file.
- The EDIT type configuration list allows wild cards, as well as the DENY keyword.
- Target IDs can be GUARDIAN as well as Alias users.
- It can be used to restrict access to VI on a 'by user basis'
- All actions will be logged in a file.

## VICONFIG file

The User/target-ID pairs are stored in an EDIT type file:

```

!
!           Visual Inspect Library Configuration
!           =====
!
!
! This configuration file has to be named VICONFIG and it has to
! reside in the same location as VILIB.
!
! It defines the
! - evaluation method
! - user
! - user/target-ID pairs
!
! This file should be owned by SUPER.SUPER, or the security administrator, and
! secured to "0000" or the SAFEGUARD equivalent.
!
!-----
! Evaluation Method
! =====
! The normal access right evaluation on a NSK system is done according
! to: Deny takes precedence (DTP). This means: In case the requesting
! user is denied access anywhere in the access right list, she/he is
! denied. This method is used e.g. in SAFEGUARD.
! But this may be a problem.
! When evaluating the following user/target-ID list according to DTP,
! GHS.CARL is denied access to ANY SUPER-ID.
!
!   User           TargetID           DENY
!   -----
! GHS.CARL        *
! GHS.CARL        SUPER.*           DENY
! GHS.CARL        SUPER.SUPER
!
! Changing the evaluation method from 'deny takes precedence' (DTP) to
! 'most complete' (MCO), the access evaluation outcome would allow GHS.CARL
! to assume SUPER.SUPER, because entry SUPER.SUPER is 'more complete' than
! SUPER.*.
!
! Mode  DTP = Deny Takes Precedence (default)
! ===== MCO = Most Complete
!
! In case this entry is missing, DTP is the assumed default evaluation
! method.
! A given Mode is used to evaluate the user/target-ID pairs, following
! the Mode entry.
! A second and next Mode entry changes the evaluation right for those
! user/target-ID entries, following the new Mode entry.
!
!-----
!
! DTP

```



```
!-----  
! User list  
! =====  
! VILib controls access to VI.  
! This can be used to grant access to VI to specific users.  
! These are the rules:  
! 1. A user, NOT mentioned in this list, gets access. This makes it  
!    upwards compatible.  
! 2. A user with an entry of: <user-name> <NONE> DENY does NOT get access.  
!    <NONE> is a required key word.  
!  
!  
!   User          Target-ID      DENY  
! -----  
! GHS.CARL                               gets access  
! GHS.MANAGER <NONE>                   gets access  
! CarlWeber    <NONE>          DENY     does NOT get access  
!  
! According to the rules, sysdamin.carl gets access, while CarlWeber does not.  
!
```

```
!-----
! User/target-ID pairs
! =====
! The User/target-ID pairs define, which user is allowed to become
! mapped to which target ID.
! To add more flexibility, the keyword DENY allows to deny a specific
! User/target-ID pair mapping rights.
!
! User as well as target-ID entries allow wildcards.
!
! User as well as target-ID names allow GUARDIAN as well as Alias user
! entries:
! - GUARDIAN user entries are NOT case sensitive, while
! - Alias user entries are case sensitive.
! This is also true when names contain wild card characters (? and *).
!
!
! The following list allows GHS.CARL to become mapped to ANY
! requested ID, GHS.MANAGER to become mapped to GHS.CARL only,
! GHS.COMFORTE to become mapped to SUPER.SUPER only, and CarlWeber to
! become mapped to comForte.
!
!   User          TargetID      DENY
! -----
! GHS.CARL       *
! GHS.MANAGER    GHS.CARL
! GHS.COMFORTE   SUPER.SUPER
! CarlWeber      BakerStreet
!
!
! This list allows GHS.CARL to assume any ID, except
! a SUPER-ID:
!
!   User          TargetID      DENY
! -----
! GHS.CARL       *
! GHS.CARL       SUPER.*      DENY
!
!
!
```



```
!
!-----
!
! User/TargetID pairs
! =====
! Defines the functional user IDs a user is allowed to access through
! Visual Inspect.
! The number of entries is unlimited.
!
!-----
!   User           Target ID           Deny
!-----
!
!   *             *
!
!-----
! To speed up the evaluation of this file, you can delete all lines
! beginning with an exclamation mark.
!-----
```



### VICONFIG example

The VICONFIG file, which describes the possible ID mappings, may look like this:

```
!
! Visual Inspect Library Configuration
!
!
! Mode
!
DTP
!
! User      Allowed Mapping    Deny
!-----
!
! ghs.carl  *1
! ghs.carl  super.super          deny
!-----
```

In the above example, user GHS.CARL can request ANY other ID, EXCEPT SUPER.SUPER.

```
!
! Visual Inspect Library Configuration
!
!
! Mode
!
MCO
!
! User      Allowed Mapping    Deny
!-----
!
! ghs.christi <NONE>          deny
! ghs.carl   *              deny
! ghs.carl   super.super
!-----
```

In this example, user GHS.CARL can request ONLY SUPER.SUPER, while GHS.CHRISTI is not allowed to get access to VI at all.

```
!
! Visual Inspect Library Configuration
!
!
! Mode
!
DTP
!
! User      Allowed Mapping    Deny
!-----
!
! CarlWeber  app*.man*
! super.*    app*.man*
!-----
```

This example allows Alias user CarlWeber as well as all SUPER-Group members to run a Visual Inspect session with any ID, matching app\*.man\*.

<sup>1</sup> GUARDIAN user IDs are NOT case sensitive, while Alias user IDs are!



## CHECK program

VILIB comes with a CHECK program, which evaluates the defined User/target-ID pairs based on the configured mode.

The command syntax is:

```
[run] CHECK [/IN viconfig/] user [[,] targeted]
```

To get the answer to the question:

```
Is GHS.CARL allowed to become mapped to SUPER.SUPER
```

execute the CHECK program as follows:

```
$GHS1 VISUAL 135> check ghs.carl,super.operator  
User allowed to become mapped  
$GHS1 VISUAL 136>
```

```
$GHS1 VISUAL 136> check ghs.carl,super.super  
User NOT allowed to become mapped  
$GHS1 VISUAL 137>
```

## Log file

All events, controlled by VILib, are recorded in a log file named VILOGo.

When this file runs full, it is renamed to VILOGI, and a new VILIGo is created.

This procedure is used, until VOLIGo exists, and VILOGo runs full. In this case, VILOGo will be deleted.

A log file has a size of ~ 90 MB, holding a few thousand events, which makes the VILOG stack 900 MB large.

VILib is delivered with the DDL file, where the log file structure is defined. It can be used to compile a dictionary, which then can be used by ENFORM and the as well delivered query named LISTLOG.

A typical LISTLOG may look like the following:

```

1      * !
2      * ! ENFORM query to list all entries from the log file VILOG0, create
3      * ! by the Visual Inspect library VILIB.
4      * !
5      * ! GreenHouse Software & Consulting
6      * ! -----
6.1    *
7      * ?Assign VL,VILOG0
8      *
9      * open VL;
10     *
11     * list  EventTime          heading "Event Time"
12     *
13     *      User              as A15  heading "Requesting/User"
14     *
15     *      MappedUser       as A15  heading "Mapped/User"
16     *
17     *      (If Event = "O" then "User mapped to Target ID OK"
18     *      else
19     *      (If Event = "M" then "User not allowed to map to Target ID"
20     *      else
21     *      (If Event = "L" then "LicenseToken invalid, or missing; no ma
22     *      else
23     *      (If Event = "T" then "Invalid Target ID specification"
24     *      else
24.1   *      (If Event = "D" then "User denied access"
24.2   *      else
24.3   *      (If Event = "A" then "User allowed access"
24.4   *      else
25     *      ("???"))))))          heading "Outcome"
26     * ;

```



Event Time	Requesting User	Mapped User	Out
03/17/2007 14:18'35	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 14:33'08	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 14:33'24	SA.CARL	SUPER.TEST	User not allowed to map
03/17/2007 15:01'57	sa.carl		User allowed access
03/17/2007 15:03'03	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:04'46	SA.CARL	SUPER.TEST	User not allowed to map
03/17/2007 15:12'46	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:13'08	sa.carl		User allowed access
03/17/2007 15:13'34	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:22'05	sa.carl		User allowed access
03/17/2007 15:25'43	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:26'12	SA.CARL	SUPER.TEST	User not allowed to map
03/17/2007 15:33'29	SA.CARL	SUPER.TEST	User not allowed to map
03/17/2007 15:34'55	SA.CARL		User allowed access
03/17/2007 15:38'37	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:38'57	SA.CARL	SUPER.TEST	User not allowed to map
03/17/2007 15:45'18	SA.CARL		User allowed access
03/17/2007 15:45'44	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:49'37	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 15:55'17	SA.CARL		User allowed access
03/17/2007 15:58'24	SA.CARL		User allowed access
03/17/2007 15:58'24	SA.CARL		User denied access
03/17/2007 16:00'52	SA.CARL		User allowed access
03/17/2007 16:01'05	GHS.CARL		User denied access
03/17/2007 16:18'34	GHS.CARL		User denied access
03/17/2007 16:18'44	SA.CARL		User allowed access
03/17/2007 16:19'20	GHS.CARL		User allowed access
03/17/2007 16:19'37	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 16:19'47	SA.CARL	SUPER.SUPER	User mapped to Target ID
03/17/2007 16:20'11	SA.CARL	SUPER.TEST	User not allowed to map
03/19/2007 08:10'35	SA.CARL	SUPER.TEST	User not allowed to map
03/19/2007 09:31'38	SA.CARL		User allowed access
03/19/2007 09:32'07	SA.CARL		User allowed access

27 \* !

\*\* END-OF-ENFORM-RUN \*\*

## Installation hints

1. Check, if the VILIBTOK LicenseToken file is in the same location as VILIB, and that it is a valid one.

This can be checked with the CHECKTOK program, which is part of the product delivery. You as well can get the mosg recent version from the FreeWare section of [www.GreenHouse.de](http://www.GreenHouse.de):

```
CHECKTOK file VILIBTOK
```

You should get something like this:

```
$GHS1 VISUAL 7> checktok file vilibtok
*** Actual system date and time is: 19Mar2007 09:16 ***
LicenseToken file $SYSTEM.GHSTOKEN.VILIBTOK checked OK
ShortCut re-built
No options available
Token granted to:   TO:                GreenHouse
Token age in days: 0
Expiration date is: 31Dec2008
CheckFlag:         OK (-14733)
$GHS1 VISUAL 8>
```

2. For Itanium systems:

Use `eld` to bind VILIB to `$SYSTEM.SYSnn.INSPSVR`:

```
eld -change libname <$vol.subvol.VILIB> $SYSTEM.SYSnn.INSPSVR
```

or

```
BINDLIB <$vol.subvol.VILIB> WITH $SYSTEM.SYSnn.INSPSVR
```

Check the successful bind using the SHOWLIB tool:

```
SHOWLIB $SYSTEM.SYSnn.INSPSVR
```

3. For Itanium systems:

Make sure the library file VILIB is licensed, while the server `$SYSTEM.SYSnn.INSPSVR` is **NOT**.