



H893V USER-Access[®]
for Stratus OpenVOS Operating Systems

Release 4.1

Memo to Users

December 14, 2011

© 2011 Network Executive Software, Inc.
6420 Sycamore Lane N #300
Maple Grove, MN 55369

Introduction

This memo-to-users contains information for H893V, and should be reviewed before beginning the installation process.

H893V is a new product that provides USER-Access for Stratus V Series platforms. It is functionally equivalent to H893C, which was the comparable USER-Access product that ran on the Stratus Continuum platform. H893V uses H897IPV NetEx/IP Requester, which uses a TNP component that is part of NetEx/IP for z/OS (H210IPZ Release 7.1), rather than using a DXE HYPERchannel adapter or NESi-Gate-LO adapter.

H893V is available by download.

The following manuals are available for the H89x Stratus products:

H892TV Print File Transfer (PFX) for Stratus OpenVOS Systems Software Reference Manual

H893V USER-Access for Stratus OpenVOS Systems Software Reference Manual

H897IPV NetEx/IP Requester for Stratus OpenVOS Systems Software Reference Manual

Note: these manuals may not be available at time of release, but will be available shortly thereafter. Since the OpenVOS versions of these products are logically equivalent to the Continuum versions, the Continuum versions of the manuals can be used as a reference until the OpenVOS versions are available. However, the complete installation instructions for the OpenVOS versions are contained in this “Memo to Users” document.

These manuals, along with this “Memo to Users” document can be downloaded from www.netex.com by selecting the ‘Support’ tab then navigating to the ‘Products, and then selecting the ‘Stratus’ link on the left side of the window, then clicking on ‘Docs’ in the ‘USER-Access [H893V]’ for the appropriate version.

Support

Support for NetEx/IP and its associated products is available via:

- Telephone (24x7) at (800) 854-0359 (+1 763-694-4350)
- The worldwide web at <http://www.netex.com>
- E-mail to support@netex.com

Notice to the Customer

Comments about this documentation may be submitted via e-mail to pubs@netex.com or by visiting our website, <http://www.netex.com>. Always include the complete title of the document with your comments.

Information on Network Executive Software's general software support policy (e.g., alternate contact methods, support severity level descriptions, and service status definitions) may be found at <http://www.netex.com/support/software-support-policy>.

Software Modification Policy

Modifications to H893V that are not specifically authorized by NESi are prohibited.

Any unauthorized modifications to H893V may affect its operation and/or obstruct NESi's ability to diagnose problems and provide corrections. Any work resulting from unauthorized modifications shall be paid by the customer at NESi's then-current support rates and may result in the immediate termination of warranty/support coverage.

New Features

Release 4.1

OpenVOS support on Stratus V Series

This release supports the Stratus V Series platform running the OpenVOS Release 17 operating system.

Installation

Installation Notes

A product release bundle for H893V is available as a downloadable distribution. The file has the name “H893V_Rel4.1.save.evf.gz”. Download instructions can be obtained by contacting support@netex.com.

The following are prerequisites for installing H893V Release 4.1 USER-Access:

- Stratus V Series processor running OpenVOS Release 17.
- H897IPV NetEx/IP Requester must be fully installed, tested, and running.
- The installer must have modify access to the (*master_disk*)>*system* and the directory into which USER-Access will be installed.
- The installer must be logged in as a “privileged” user.
- A process directory entry must exist for Stratus USER-Access users. Temporary files for command execution are created in this directory.
- The user that starts the USER-Access Service Initiator must have read access to the system registration file >*system*>*change_password_sysdb*. If the user is registered in either the SysAdmin or System group, then the required access rights already exist.
- Refer to the “H893 (Rel 2.0) USER-Access for Stratus Continuum Software Reference Manual” until the H893V Software Reference Manual is available.

Installation Steps

The installation of USER-Access, whether the initial installation or a subsequent update, consists of the following steps:

1. Create the release directory
2. Load the distribution file set
3. Install the distribution file set
4. Start the Service Initiator
5. Verify USER-Access

The steps required to install the H893V USER-Access product on Stratus V Series are as follows:

Step 1. Create the Release Directory

The USER-Access release is loaded into a DISTRIBUTION directory and is then installed into the TARGET directory. Existing files in the TARGET directory are replaced with the new release files.

Nothing is modified in the DISTRIBUTION directory during the installation process, allowing repeated installations into different TARGET directories, each with different install options. To preserve disk space, the DISTRIBUTION directory can be deleted once USER-Access is fully installed into the TARGET directory. Once it has been deleted, the DISTRIBUTION directory must be restored again if a subsequent rebind is required.

The installation procedures and examples assume a DISTRIBUTION directory of:

(master_disk)>nsc>ua_r4 and a TARGET directory of *(master_disk)>nsc>sicom*.

However, any valid directory (with adequate space) can be selected. If an alternate directory is chosen, be sure to replace *(master_disk)>nsc>ua_r4* or *(master_disk)>nsc>sicom* with the alternate directories in the commands that follow.

At this point, you should create your DISTRIBUTION directory:

```
create_dir (master_disk)>nsc>ua_r4
```

Step 2. Load the Distribution File Set

After creating the release directory, load the contents of the product release bundle to the release directory created in Step 1:

```
change_current_dir (master_disk)>nsc>ua_r4
```

Copy the H893V product release bundle to the current directory:

```
copy_file [H893V_Rel4.1.save.evf.gz from ftp server] -keep_dates
```

Extract the files from this bundled file to the current directory:

```
unbundle H893V_Rel4.1.save.evf.gz -keep_dates
```

The entire H893V distribution file set will be restored to the current directory and the lib subdirectory. The file set includes command macros, object modules, and numerous other “ua” files to support the operation of the USER-Access Client, Server, Service Initiator, and Control program modules.

Step 3. Install the Distribution File Set

The USER-Access installation macro (“install.cm”) prompts for valid install options including the TARGET directory. If the install macro is invoked with the -bind option, the macro will attempt to rebind the executables only if the product has already been installed. If the -bind option is specified the path of the NetEx/IP library will also be requested.

As stated above, the install macro prompts for the USER-Access TARGET directory. If USER-Access is installed in a directory other than *(master_disk)>nsc>sicom*, an appropriate link must be created so USER-Access can find help files and startup files.

Invoke the “install.cm” macro to perform the installation procedure. The following shows an example of a typical install:

```
install

*****
install macro invoked on Thursday, October 20, 2011  1:52 pm edt
*****

=====
Starting USER-Access install
=====
You need to know the following:

o   The USER-Access install option (ALL)
o   The target directory for the install ((master_disk)>nsc>sicom)
o   The USER-Access network (NETEX)
o   The NETEX product (H897IPV)

Are you ready to install USER-Access?  (yes, no) yes

For each of the requests that follow, the default value
is designated by [].  To select the default value, simply
press the return key in response to the request.

The USER-Access install options are:
    ALL      - full USER-Access

Enter install option [ALL]? _____

The TARGET root directory defines where USER-Access is
installed.

Enter the target directory [(master_disk)>nsc>sicom]? _____

USER-Access network choices are:
    NETEX    - NETEX connection

Enter the desired network [NETEX]? _____

You have selected the following install parameters:
OPTION      = ALL
TARGET      = %mkt2#m2_d01>nsc>sicom
NETWORK     = NETEX

Do you wish to proceed with the install?  (yes, no) yes
=====
Create USER-Access target directories
=====
.
.
=====
```

```

Copying USER-Access executables
=====
.
.
=====
Copying USER-Access control files
=====
.
.
=====
Editing TARGET in command macro files
=====
.
.
Please check INSTALL_4.1.log for any errors which may have
occurred during the install.  If this is a new release or you
have configuration changes, consult the USER-Access Memo To
Users for further instructions before proceeding.

NOTE: If USER-Access was previously installed, several control
files in the user sub-directory may have been copied to
similarly named files with the suffix "_save". Review
these files and merge any required changes into the new
versions.

=====
USER-Access install complete.
=====

```

Note that between the reply to proceed with the install and the “USER-Access install complete” message, the following steps are performed:

- Create the USER-Access TARGET directories and copy the distribution object libraries.
- Copy the USER-Access executable files and control files to the TARGET directory. Any previous control files that were modified are preserved.
- Edit the command macros “user.cm” and “uaserver.cm” in the TARGET user subdirectory so that the TARGET directory is given as the USER-Access root directory parameter. In the same manner, the “si_input” script and “start_si.cm” command macros in the TARGET “si” subdirectory are also edited.
- Set the file security on the USER-Access executable files and command macros.

Be sure to scan the generated output, looking for any errors or warning messages. If USER-Access was installed in some directory other than the default root directory of *(master_disk)>nsc>sicom*, then create a link under the *(master_disk)>nsc* root directory which points to where USER-Access is installed. For example, if USER-Access was installed in the directory *(master_disk)>prod>sicom*, a link called *(master_disk)>nsc>sicom* can be created with the command:

```
link (master_disk)>prod>sicom (master_disk)>nsc>sicom
```

Step 4. Start the Service Initiator

The Service Initiator is a program that services USER-Access CONNECT or LOGIN requests from hosts on the network. It runs as a started process under the name “svcinit”. Before proceeding, make sure that you meet the requirements outlined in the “Prerequisites” section above. Also make sure that a previous copy of the Service Initiator is not running.

To start a new Service Initiator, issue the following commands:

```
change_current_dir (master_disk)>nsc>sicom>si
start_si
```

To verify that the Service Initiator is running, the process named svcinit should display when the following command is issued:

```
list_users
```

The Service Initiator will log messages to *(master_disk)>nsc>sicom>si_output*. Use the following command to look at the file:

```
display_file si_output
```

The last message in the file should be:

```
USER Service offered.
```

This confirms that the USER-Access service “USER” is being offered by the Service Initiator. If “svcinit” is not running, check to make sure the protections on the “si” subdirectory allow you to have read/write access. Also check the input and log files for errors (“si_input” and “si_output”).

Step 5. Verify USER-Access

A simple verification script has been supplied as part of the USER-Access release. This verification procedure prompts you for the local NetEx/IP network host name of your system, and a valid username and password on this host (for verification purposes, the username and password specified should at least have the privileges you do - specify your username and password to be safe). It attempts to connect back to your host, login, and perform basic USER-Access functions.

To invoke the verification script, set your directory to the ‘user’ subdirectory and invoke USER-Access with the script “verify.ua”:

```
change_current_dir (master_disk)>nsc>sicom>user
user verify.ua
```

In addition to being prompted for the host and login parameters, you will see numerous messages displayed on your terminal followed by a final “Verification Successful” message. If an error is encountered during verification, the script will terminate with the display of an error message.

This completes the formal installation of USER-Access on your V Series system. However, it is important to continue on through this document in order to set up your environment properly.

Making USER-Access Available to Other Users

To make the various program modules in the user directory available to users on your system, you may do so by executing the following command in the file “(master_disk)>system>module_start_up.cm” at the place indicated for “adding library paths”.

```
add_library_path command (master_disk)>nsc>sicom>user
```

Other arguments should be provided to this command at your discretion.

Stratus USER-Access users should have a process directory entry beneath the (*master_disk*)>*process_dir_dir* directory. Temporary files for command execution are created in the process directory of the user.

Automatically Starting the Service Initiator

The Service Initiator may be automatically started when the local Stratus module starts by placing a command to start it in the “module_start_up.cm”. To modify the “module_start_up.cm”, you must have modify access to the (*master_disk*)>*system* directory on your system. To automatically start the Service Initiator, edit the file “(master_disk)>system>module_start_up.cm” using any Stratus editor. Move to the end of this file and enter the following lines:

```
&  
&      Command to invoke USER-Access Service Initiator  
&  
(master_disk)>nsc>sicom>si>start_si
```

In order to verify your changes to the system startup file, you should reboot your system. This is not a requirement of USER-Access but strongly recommended to ensure the Service Initiator gets started successfully when the system is booted.

Stopping the Service Initiator

The Service Initiator can be stopped by using the Service Initiator control program. To run this program to stop the Service Initiator, execute the following commands:

```
change_current_dir (master_disk)>nsc>sicom>si  
control stop -h host -s service
```

where ‘host’ is the host name of the local netex host and ‘service’ is the name of a network service being offered by the Service Initiator (“USER” is generally the service name being offered).

Providing a Guest LOGIN

The Service Initiator provides for a default (or guest) login when no username and password are provided on the USER-Access CONNECT command. If you want a guest login for USER-Access, edit the file “(master_disk)>nsc>sicom>si>si_input”. Remove the comments from the following lines:

```
# USERNAME guest
# PASSWORD netex
```

Change the username ‘guest’ and the password ‘netex’ to correspond to a valid username/password for your system. In doing so, this username/password account becomes a USER-Access guest account. Alternatively, add ‘guest’ as a valid account on your Stratus system. The username/password account specified becomes the default account if none is given on the CONNECT command.

Service Initiator Keywords

The Service Initiator startup input file “(master_disk)>nsc>sicom>si>si_input” contains a list of keywords that can be set to alter the way the Service Initiator operates for a given SERVICE being offered. Each keyword is listed below along with a brief description of the value that can be assigned to it:

SERVER	specifies the command that is to invoke or run the USER-Access server.
OPERATOR	specifies a password that is required when issuing commands through the CONTROL program “(master_disk)>nsc>sicom>si>control”. This is used for shutting down the Service Initiator.
LOGTIMEOUT	specifies the login timeout in seconds. This is used to terminate a login request that, for some unknown reason, is hanging around.
MINIMUM	specifies the minimum session number that will be offered for this service. For example, a MINIMUM value of 5 would result in SERVICE “USER” being offered as “USER005” up to a MAXIMUM (below). Specifying MINIMUM and MAXIMUM do nothing to limit the number of USER-Access sessions that are allowed. They are simply provided as a naming tool.
MAXIMUM	specifies the maximum session number that will be offered for this service. For example, a MAXIMUM value of 30 would result in the last offer of “USER” being “USER030” before starting over at MINIMUM.
USERNAME	specifies the default username value. This is provided for guest logins.
PASSWORD	specifies the default password value. This is provided for guest logins.

TRACE allows different levels of tracing of the Service Initiator. Refer to the startup input file “(master_disk)>nsc>sicom>si>si_input” for a description of the different trace levels.

USER-Access Site Startup Files

Site startup files are supported for the USER-Access client and server modules. These files allow the installer to establish site parameters (command defaults, alias definitions, etc.) for both the client (Initiator) and server (Responder). Two sample site files are provided with this release. You should edit your changes into them:

```
(master_disk)>nsc>sicom>user>sclient.ua  
(master_disk)>nsc>sicom>user>sserver.ua
```

For example: To include site specific modifications in the site startup file “sclient.ua”, the following change can be made:

```
#      Site XYZ changes for USER-Access Initiator  
#  
Set connect blocksize 8140  
Set alias printline text
```

The first command changes the default connect blocksize to 8140, and the second command defines an alias called “printline”.

Any USER-Access command may be included in the SCLIENT startup files. A restricted command set (excluding CONNECT, DISCONNECT, SEND, RECEIVE, LOCAL, and REMOTE) may be included in the SSERVER startup file. Refer to the “H893V USER-Access for Stratus OpenVOS Systems Software Reference Manual” for more startup file information.

Update Summary

Release 4.1

This section describes the updates in Release 4.1 that have been made since the initial Beta Release 4.0.1. Updates in this release include:

- The product was rebuilt after the version level was changed to Release 4.1.
- Shortened the `destination_file` component of the H893V release bundle file name in order to ensure that the length of the entire bundle file name does not exceed 32 characters. This was done to prevent a problem copying the H893V release bundle to an OpenVOS system on which extended-names support has been disabled.

Beta Release 4.0.1

Updates in this Beta release, made after porting the product from the previous H893C 3.0.8 M0 release on Stratus Continuum platforms include:

- Removed support of the CAM backup facility by removing the `uabackup.cm` and `uarestore.cm` command macros from the product.
- Removed support of the CART facility by removing `cart.*` modules from the product.

Known Problems

There are no known problems at the time of this release.