Changes and Enhancements

Introduction

Information about changes and enhancements that were implemented in Version 8 is preceded by V8. All other changes and enhancements described in this section were implemented in Version 7. If your site upgraded directly from Version 6 to Version 8, then all of the changes and enhancements described here are new to you. If you upgraded from Version 7 to Version 8, then only the items preceded by V8 are new to you.

New SAS/CONNECT Remote Host Spawners Available

A spawner program resides on a SAS/CONNECT remote host and listens for client requests for connection to the remote host. After the spawner program receives a request, it invokes the remote SAS session.
New spawner programs support these remote host types:

□ OpenVMS Alpha

□ OS/390.

Both of these spawners support only the TCP/IP access method for communicating with a supported local host.

New SAS/CONNECT TCPPORTFIRST and TCPPORTLAST System Options

The TCPPORTFIRST and TCPPORTLAST options restrict the range of TCP/IP ports through which local hosts can connect to remote hosts when using the TCP/IP access method.
These options can be used only with SAS/CONNECT running on a platform that supports the TCP/IP access method. These options can be set on the remote host only.

New SAS/SHARE AUTHSERVER System Option

The AUTHSERVER option specifies the location of the database that contains the username and password pairs that are used for validation. You specify the name of either an NT domain or an NT server at which the database resides.

This option is supported by all access methods that support security.

Windows 98 Is Supported

Microsoft Windows 98 is a supported host for Version 8 SAS Software. SAS behavior is identical on both Windows 98 and Windows 95.

Windows NT Domain Name Can be Specified in the Username

V8 Introduced in Version 8 for Windows NT hosts only, specifies the location of the database that contains the username and password pairs that are used for validation. You may specify the name of either an NT domain or an NT server at which the database resides.

This Version 8 feature replaces the Version 7 requirement to define a single NT domain according to the product. Version 7 SAS/CONNECT provided the -AUTHSERVER option to the PC spawner. Version 7 SAS/SHARE provided the AUTHSERVER system option. In Version 8, you may bypass these options and specify the domain name in the form *domain\username* when you supply your username in the Windows NT environment. Here is an example of how you might specify this information in the SAS/CONNECT SIGNON statement:

```
signon user=apex\bass password=time2go;
```

Here is an example of how you might specify this information in the SAS/SHARE LIBNAME statement:

```
libname test 'prog2 a' user="apex\bass" password=_prompt_  server=share1;
```

The domain name **apex** identifies the location of the username and password database. The username **bass** and the password **time2go** will be verified against those in the identified domain's username and password database.

Version 8 Method to Provide User Identification

V8 Version 8 offers a new method to provide user identification to a SAS/CONNECT remote host and a SAS/SHARE server by means of the USER= and PASSWORD= options in the SIGNON or RSUBMIT statements in SAS/CONNECT and in the LIBNAME, Remote SQL Pass-Thru (RSPT), or PROC OPERATE statements in SAS/SHARE.

These security options can be set on any Version 8 local host accessing a remote host that runs any version of SAS. The USER= and PASSWORD= options to these statements are recommended and take precedence over the applicable security option, which varies by host and access method. SAS/CONNECT and SAS/SHARE security options are APPCSEC, APPC_SECURE, TCPSEC, and SASUSER and SASPASS.

If a Version 7 security option remains set on the local host, the Version 8 specification of USER= and PASSWORD= in a SAS/CONNECT statement overrides the previously set security option on the local host. For example, the Version 8 USER= and PASSWORD= options in the SIGNON statement will override the TCPSEC= _PROMPT_ option set on a local host for a non-scripted sign on to a spawner.

If a Version 8 local host does not set USER= and PASSWORD= options, the communications access method or host security option would remain in effect. If both the USER= and PASSWORD= options and a security option are specified, then the USER= and PASSWORD= options would take precedence.

Syntax and definitions are:

USER | **USERNAME** | **USERID** | **UID**= *username* | _PROMPT_

PASSWORD | **PASSWD** | **PASS** | **PWD** | **PW**= *password* | _PROMPT_

Specifying these options allows local hosts whose usernames and passwords have been verified to access the remote host.

Username is a valid userid on the remote host being accessed. On Windows NT only, the username can also include the domain name, which locates the specified username in a domain.

Password is a valid password on the remote host being accessed.

Supplying a userid and password by using the USER= and PASSWORD= options is more secure than assigning them by means of a security option (such as TCPSEC), which can be inadvertently publicized in a configuration file or in a log.

PROMPT specifies that the SAS System prompts for *userid* and *password*. Hardcoding a username and password value to the USER= and PASSWORD= options limits the assignment to a single user whereas prompting permits any user to supply a username and password that are valid. Specifying only USER=_PROMPT_ implies that the SAS System will prompt for both a username and a password.

The values supplied for the USER= and PASSWORD= options are valid for the duration of the remote host connection. Subsequent local host connections to the same remote host or to a different remote host require you to specify these options again. By contrast, as an example, the values assigned to TCPSEC in a local host configuration file endure for subsequent connections to the same remote host and to different remote hosts.

Here is a Version 8 example for SAS/CONNECT:

```
signon user=joeblack password=born2run;
```

Here is a Version 8 example for SAS/SHARE:

```
libname test 'prog2 a' user=joeblue password='2muchfun' server=share1;
```

As a security precaution, PASSWORD= field entries echoed in the local host log are replaced with Xs. See the naming conventions identified in the *SAS/SHARE User's Guide* for guidelines on quoted passwords.

If _PROMPT_ is specified, when presented with the prompt for *password* during a remote host connection, the value entered would not be displayed on the screen.