DEFINE USER

The DEFINE USER command allows you to specify the user IDs of authorized *TCP/IP for VSE* users in the absence of a user-provided security exit.

Syntax:

```
DEFine USEr ID=name16 [,PASSword=name16] [,DATA=any] [,GID=snum]
            [,UID=snum] [,MAILbox=str] [,FTP={YES|NO}] [,LPR={YES|NO}]
            [,WEB={YES|NO}] [,TELNET={YES|NO}] [,ROOT=path]
```

Arguments:

ID= - This value will be used as the User ID. It will be converted to upper case.

PASSword= - If specified, the user must provide the matching value before logon is permitted. Passwords are from 1 to 16 characters long and always converted to upper case.

DATA= - This is an optional data string of up to 40 user-specified characters.

TCP/IP for VSE does not examine this field on input. Its contents are passed to the Automatic Security Exit (if active) and then to the installation-supplied security exit, if you provide one. No case conversion is performed on this field. If the field contains blanks or commas, it must be enclosed in single quotes.

When passed to the Automatic Security Exit, each position of the data string should contain either "Y" or "N" to indicate that functions are either allowed (Y) or disallowed (N). The positions within the data string correspond to the value passed in the SXBLOK DSECT's SXTYPE field. The values are shown below under “Automatic Security Exit”.

GID= - Signed numeric, -9999999 through +9999999

Defines this user as part of a group. *TCP/IP for VSE* does not use this field but passes it to the security exit.

UID= - Signed numeric, -9999999 through +9999999

Associates this user with a UNIX-style user ID. *TCP/IP for VSE* passes this field to the security exit.

FTP= - Determines whether or not the user is authorized to use FTP.

LPR= - Determines whether or not the user is authorized to use LPR.

WEB= - Determines whether or not the user is authorized to make HTTP requests. Note that the HTTP Daemon must also be configured to accept user IDs.

TELNET= - Determines whether or not the user is authorized to access Telnet menus. For this to be effective, the menu must make provision to poll for a user ID and password.

ROOT= - If specified and the user is authorized for FTP, the FTP session will begin in this directory. The user will be able to change to lower-level subdirectories, but will be prevented from accessing higher-level directories.

If this value contains special characters, it must be enclosed in apostrophes.

DEFINE USER *(continued)*

Example:

```
IPN237I define user,id=don,password=republican, data='Spills Coffee'
IPN237I define user,id=leo, data='Drinks Coffee' ftp=yes, -
IPN237I ++SUPRESSED++

IPN237I query users
IPN253I << TCP/IP User IDs >>
IPN475I  User ID: LEO
IPN476I    Data: Drinks Coffee
IPN883I    Valid for: FTP
IPN475I  User ID: DON
IPN476I    Data: Spills Coffee
IPN883I    Valid for: *All*
```

Notes:

- User IDs and passwords are case insensitive.
- Special characters should be avoided because a user may have difficulty in providing exactly matching values from some platforms.
- If the password is not specified, any value provided by the user is accepted unless the security exit (if any) determines otherwise.
- To modify an entry, you must delete and redefine it.
- In case of duplicate entries, the one entered first is used.
- The FTP Daemon, the Telnet Daemon (if a menu is supplied containing the appropriate fields), and the HTTP Daemon check user IDs and passwords. The HTTP Daemon checks user IDs if the SECURITY=ON parameter is specified in the DEFINE HTTPD command.
- If no limitation is placed on the user ID by FTP=, LPR=, WEB=, or TELNET=, then the user ID is authorized to be used with all services.
- See the *TCP/IP for VSE Installation Guide* for more information about user IDs and security.
- Any input statement whose first character is “+” is not echoed on the TCP/IP log. This includes each line of a “continued” command line.

Automatic Security Exit:

When activated by the SECURITY and ASECURITY commands, the Automatic Security Exit validates each user for the task being performed. User authorization is checked by examining specific field positions in the DATA= string supplied with DEFINE USER.
To permit a function, a “Y” should appear in its assigned position; To disallow the function, code “N”. The following table shows column numbers and their assigned functions. The values are those found in the SXTYPE field of the SXBLOK mapping macro.

1	Password Check
2	Read Check
3	Write Check
4	Update Check
5	Startup Security
6	Shutdown Security
7	Hardware Address Verify
8	IP Address Verify
9	SITE Command check
10	Delete check
11	Rename check
12	Create check
13	EXEC command check
14	APPEND check
15	OPDIR check
16	RDDIR check
17	CWD Check
18	SHELL Check
19	ICMP check
20	Daemon LOGIN request

21	RPC Request
22	Web Logon Screen Request
23	HTTPD SCANBLOCK request
24	Make directory
25	Remove directory
26	Last CWD
27	Auto exit startup
28	Auto exit shutdown
29	FTPD command

Related Commands:	ASECURITY	-	Configure the Automatic Security Exit
	DELETE USER	-	Remove a user ID and password entry.
	QUERY USERS	-	Displays a list of defined user IDs.
	SECURITY	-	Control TCP/IP security functions.