SECURITY

The SECURITY command controls what security, if any, is provided for *TCP/IP for VSE* access.

Syntax:

```
SECURity [ON|OFF] [,BATCH={ON|OFF}] [,PHASE=member] [,XDATA=string]
         [,ADATA=string] [,ASMDATE=string] [,ASMTIME=string]
         [,VERSION=string] [,AUTO={ON|OFF}] [,EXIT={ON|OFF}]
         [,ARP={ON|OFF}] [,MODE={WARN|FAIL}]
         [,LOGGING={ALL|FAIL|NONE}] [,DUMP=ALL|FAIL|NONE}] [,LOCK]
```

Arguments

ON - Security processing will be globally enabled.

OFF - Security processing will be globally disabled. Be very careful with this option.

BATCH= - This parameter controls whether or not FTPBATCH processing will be under control of the stack's security processing, including calls to the security exit(s). This prevents using FTPBATCH as a convenient way of bypassing security.

- ON - Security processing will be enabled for FTPBATCH.
- OFF - Security processing will be disabled for FTPBATCH.

PHASE= - Specifies the name of an optional installation-supplied security exit. This value provides the phase name only. The phase is not loaded or its existence verified until EXIT=ON is specified.

XDATA= - Specifies a 40-byte character string to be passed to the installation-supplied security exit each time it is called.

ADATA= - Specifies a 40-byte character string to be passed to the Automatic security exit each time it is called..

ASMDATE= - Specifies a 1- to 8-byte character string to be compared with the assembly date of the installation-supplied security exit. This can be used to ensure that the exit has not been tampered with.

ASMTIME= - Specifies a 1- to 8-byte character string to be compared with the assembly time of the installation-supplied security exit. This can be used to ensure that the exit has not been tampered with.

VERSION= - Specifies a 1- to 8-byte character string to be compared with the version number of the installation-supplied security exit. This can be used to ensure that the exit has not been tampered with.

AUTO= - This parameter controls the enabling of the Automatic Security Exit.

- ON - Automatic security is enabled.
- OFF - Automatic security is disabled.

EXIT= - This parameter controls the loading and enabling of the installation-supplied security exit.

- ON - The installation-supplied security exit is loaded and its initialization routine is called.

OFF - The installation-supplied security exit's termination routine is called and the exit is then removed from storage.

ARP= - This parameter controls whether or not ARP requests will be examined before being processed. This might be useful if there is concern about unauthorized access or misrouting of data on the local network segment.

ON - ARP requests are passed to the Automatic security exit (if enabled) and the installation-supplied security exit (if enabled) for validation.

OFF - ARP requests are not checked.

MODE= - This parameter determines the severity of punishment for security violations.

WARN - Security failures are treated as "warnings" and all requests are allowed to complete. This is useful for testing security rules prior to enforcing them.

FAIL - Security failures result in the requested action being denied.

LOGGING= - Security requests may be logged minimally, aggressively, or not at all.

ALL - All security requests are logged.

FAIL - Failing security requests are logged.

None - Security requests are not logged unless the security exit explicitly indicates that logging should occur.

DUMP= - The Security eXit BLOcK (SXBLOK) contains all information on a particular security validation requests. It is created by the process requiring authorization and is passed to all validation processing and exits. Once complete, the SXBLOK will contain information that either permits or prevents the operation in question. This parameter permits you to dump a copy of a failed security request, either for logging or debugging purposes.

ALL - The SXBLOK of failed security requests will be dumped regardless of WARN or FAIL mode.

FAIL - The SXBLOK of failed security requests will be dumped.

None - SXBLOKs will not be dumped.

LOCK - Once issued, all security settings are locked to their current values. Security settings cannot be altered until the stack is cycled.

Example:

```
IPN237I security on,auto=on,batch=on
IPN759I Security status change: Security Processing Enabled
IPN759I Security status change: Automatic Security Enabled
IPN759I Security status change: Batch Security Enabled
```

Related Commands:

ACCESS	-	Control access to VSE by IP address
ASECURITY	-	Configure the Automatic Security Exit
DEFINE USER	-	Create a user ID and password.
QUERY SECURITY	-	Displays current security settings.
QUERY USERS	-	Displays a list of defined user IDs.