

InterSession

Installation & Customization Reference

Version 8.1

Åström Software AB

Fiskaregatan 5
SE-25270 Råå
Sweden

Web: www.astrom.se
Email: support@astrom.se

Document version: 8.1.9
Relates to InterSession 8.1.107 or higher

About this manual

This manual explains in full the installation and customization of InterSession.

If you are installing InterSession for the first time, we strongly recommend you to use the **Quick Start Guide**.

See the **Concepts and Facilities** for an introduction to the features of InterSession.

See the **User's Guide for 3270 Users** and the **User's Guide for Web Users** for a full description of how to use InterSession.

See the **Messages** manual for an explanation of the InterSession messages.

How Should I Use This Manual?

First review the sections on "Terminology" and "System and Memory Requirements".

Next, complete the installation steps contained in the chapter on "Getting Started".

The final installation step involves bringing up and using InterSession for the first time.

After you have used InterSession for a few of your applications, you may want to implement some of the optional facilities of InterSession. The chapter on "Application Session Considerations" will show you how to implement these features. This chapter also contains considerations that may be required or useful for using InterSession with some of your more complex applications.

The chapter on "The Maintenance Facility" describes all the features of InterSession and how they are customized. The maintenance facility is an internal application within InterSession.

The chapter on "Using an External Security Manager" describes how to interface with an External Security Manager, for example RACF, TopSecret or ACF2.

The chapter on "Sysplex functionality" describes the optional feature of how more than one InterSession system can run together in a z/OS sysplex.

The chapter on "The Web Gateway" describes the optional feature of being able to access applications defined in InterSession from a web browser.

InterSession provides several exit points that you can use to supply your own programs to assist with the normal processing functions. The chapter on "Installation-Written Exit Routines" contains information about each of these exits.

All trademarks, trade names and service marks referenced in this document belong to their respective companies.

Copyright © Åström Software AB.
Licensed materials. All rights reserved.

Contents

About this manual	3
How Should I Use This Manual?	3
Contents.....	5
Getting Started	13
Enhancements and new features in version 8.1	13
Features removed in 8.1	13
Evolutionary changes made in version 7.2.....	14
Terminology changes in version 7.2.....	14
Key Components and Terminology.....	14
System Requirements.....	16
New Installation	17
Upgrading from an earlier version	17
Step 1. The Installation File.....	17
Allocate files.....	17
FTP the XMT files to z/OS and RECEIVE them	17
Step 2: Authorize the 8.1 loadlib	18
Step 3. Preparations in your current version	18
Step 4. Running the Conversion program	18
Step 5. Start the upgraded system.....	19
Application Session Considerations	20
Overview.....	20
Relay Mode vs. Pass Mode Sessions	20
How to control which mode InterSession is using.....	20
How InterSession regains control after a pass mode session.....	21
Saving Terminal Data	21
Logging Off From InterSession	21
VTAM APPLid Usage for Application Sessions	22
Session APPLid Type = POOL.....	22
Session APPLid Type = GROUP	22
Session APPLid Type = UNIQUE	23
Using "Virtual terminal id" in the User Profile and in the Personal Application Profile	23
Session Portability	24
Inquire About APPL Status	24
Lock Pool APPLid To User	25
Appl Will Pass Session	25
Appl Sends First Screen	25
INTSMTAB Logmodes	26
3270 Data Compression	26
3270 Data Translation.....	26
TSO Considerations.....	27
zVM/CMS Considerations	28
z/VSE Interactive Interface Considerations	28
Ad-hoc Sessions.....	29
The timeout functions.....	29
Terminal Idle Timeout.....	30
Application Idle Timeout.....	30
Widow Session Timeout	30

Standby Screen Timeout.....	30
3270 Printer Support.....	30
Defining Virtual Printers	31
Using Printers for Hardcopies and Messages	31
Defining Printers for Users	31
Print Request Headers	32
Using TCPIP Printers.....	32
Write Print Data to System Spool	33
Customization	34
The System Options	34
VTAM APPL Statements.....	34
The Main APPLid.....	34
The Logon APPLid	34
The Batch APPLid	34
APPL Statements for Application Sessions, Type POOL	35
APPL Statements for Application Sessions, Type GROUP	35
VTAM Model Terminal Support.....	35
The VTAM USS Table	36
The Startup Parameters.....	38
How to Enter	38
Explanation	38
The Accounting Routines	41
Implementation	41
Accounting File Backup/Reset	42
The Wrap-Around Message Log File	42
Implementation	42
Printing Log Messages	43
//PRINTLG EXEC PGM=INTSUTIL.....	43
Copying Log Messages	43
The Spin-Off Message Log Files.....	44
Implementation	44
The JES2 Message Log File	44
Implementation	44
The HTTP Log File	45
Implementation	45
National Characters and Codepage Support.....	45
TCP/IP Stack Affinity.....	46
Selecting which stack to use	46
Using more than one stack	46
CICS outstanding work after a session termination	47
Security and Authorization	48
Overview.....	48
Internal Security Functions.....	48
Support for Long Passwords and Passphrases.....	48
Using an External Security Manager.....	50
RACF	50
Application Access.....	50
Improved Messages	50
ACF2	50
Running As a Started Task.....	51
Application Access.....	51
TopSecret.....	51
Running As a Started Task.....	52
Application Access.....	52
Controlling Application Access	52
Application Access Using Individual Applications	52

Application Access Using Models	52
Multithreaded Signon	55
PassTicket Support	55
RACF Definitions	56
TopSecret Definitions	57
ACF2 Definitions	58
Multi-Factor Authentication Considerations	59
General Considerations	59
MFA Server Verification Considerations	60
Sign On Screen Appearance	60
The MFA variables on the Sign On Screen	61
Identifying MFA messages	61
IBM MFA compound In-Band support	62
Analyzing the MFA messages	63
Debugging MFA signon	63
RACF IDentity Tokens	64
The Maintenance Facility	65
Overview	65
System Administrators	65
Distributed User Profile Maintenance	65
The Maintenance Selection Screen	66
User Profiles and Personal Application Profiles	67
Models	67
Shared Application Profiles	67
Session Scripts and Panels	68
Scripts are located in the InterSession INTSFLE VSAM file	68
Scripts and panels are located in a separate PDS	68
Panels (always in a separate PDS)	68
Screen Layouts	68
Printers	69
Interfaces	69
Services	69
Help Screens	69
System Options / APPLpools	69
The System Variables	70
Variables used in Scripts and in Screen Layouts	70
Variables used in Scripts only	74
Installation-defined Variables	75
Substrings in Variables	75
Getting Help on the Application Variables	75
User Profile Maintenance	76
User Profile Basic Data	76
User Application Access and Personal Application Profiles	84
Shared Application Access	85
Personal Application Profiles	85
User Application Sequence	86
Commands	87
User Profile Listing	87
Model Maintenance	88
Model Basic Data	88
Application access in Models	89
Application Profile Maintenance	90
New Application Profile	90
Application Types	90
Application Types for External Applications	91
Application Types for Internal Applications	91
Application Types for Miscellaneous Use	91

Main Menu Position	91
Application Profile Screen 1/2, type VTAM	92
Application Profile Screen 1/2, type TN3270.....	96
Application Profile Screen 2/2	97
Application Profile Screen, type SScript	100
Application Profile Screen, type Logoff	102
Shared Application Profiles Listing	103
Compressing the Application Security Keys.....	103
Session Script Maintenance.....	104
Script Residence.....	104
Scripts in the INTSFLE file.....	104
Scripts in a separate PDS.....	104
Script Editing.....	105
The Script Commands	105
The Script Statements.....	105
Script Commands.....	106
Notes on Variables	108
The TYPE (KEY) Command	109
The EEOF (EOF) Command	109
The Arrow Key Commands.....	110
The Tabulating Key Commands.....	110
The Terminal Key Command	110
The IFSTR Command	110
The IF Command	111
The ENDIF Command	111
The GOTO Command	111
The SRCH Command	112
The CMP Command	112
The BR Command.....	112
The WINP Command.....	112
The WSTR Command.....	113
The MSGBOX Command	113
The WAIT Command	114
The RESET Command	115
The TERM Command.....	115
The MENU Command.....	115
The XCTL Command	115
The CALL Command	115
The RETURN Command.....	116
The UPDACT Command.....	116
The UDEFINE/VDEFINE Commands.....	116
The UDELETE/VDELETE Commands	116
The LET (SET) Command.....	116
The ADD Command.....	117
The SUB Command	117
The START Command.....	117
The WTO Command	117
The SHOW Command.....	117
The NOP Command.....	118
The END (TERM) Command	118
The Comment Line.....	118
Example.....	118
Error messages.....	118
ISPF Panel Support.....	119
What is currently implemented	119
Session Script Listing.....	120
Session Script Recording.....	120
Screen Layout Maintenance	122
Screen Variables	122
Panel text attribute tags	122
Screen Layout, Selection.....	122

Screen Layout, Usage/Commands	123
Screen Layout, Language/Heading	126
Screen Layout, Sign On Screens	128
Screen Layout, Main Menu Screens	131
Screen Layout, Messages	135
Screen Layout, Terminal Lock Screen	136
Screen Layout, Message System Screens	137
Screen Layout, User Profile Screens	138
Screen Layout, Standby Screen	139
Screen Layout, Top Line Menu / Message Box	140
Screen Layout, Print Header Page Text	141
Screen Layout, Panel Tags	141
Screen Layout, Web Layout Settings 1/2	142
Screen Layout, Web Layout Settings 2/2	143
Screen Layout Listing	144
Screen Layout Examples	146
Printer Maintenance	148
New Printer	148
Printer type HARDCOPY	148
Printer type TN3270E	151
Printer type LPD	152
Printer type RAW or PJI	154
Printer type SPOOL	156
Printer Listing	157
Interfaces Maintenance	159
New Interface	159
Interface Type VTAM	161
Interface Type BPX	162
Interface type BPX (z/OS)	162
Interface Type BATCH	163
Interface Type ONLINE	164
Interface Listing	165
Services Maintenance	167
New Service	167
Service Types TN3270 and TN3270E	168
Service Type HTTP – The Web Gateway	169
Service Listing	171
Help Screen Maintenance	173
Help Screen Listing	175
System Options and APPLpools Maintenance	176
System Options Selection	176
System Options, Internal Security	177
System Options, External Security	179
System Options, Scripting	184
System Options, User/Application Profile Defaults	186
System Options, PF Keys Defaults	189
System Options, Other	190
System Options, User Exits	194
APPLid Pool List	195
APPLid Pool With a Mask	196
APPLid Pool With a List of APPLids	197
System Options that will Take Effect First After Next Startup	198
Problems with Exits etc. Causing System to Abend at Startup	198
The Web Gateway	199
The Web Server	199
Defining and Starting the Web Server	199

The File System	200
Folder names.....	200
Text Files	200
Binary Files	200
How the Files Are Kept	201
Special Files	201
The File Cache	201
The Application Menu	201
Accessing the Application Menu from Another Web Page	202
Accessing a Particular Application from Another Web Page	202
Redirect from InterSession Logoff to Another Web Page	202
The HTTP Log File	202
Changing the HTTPLOG file from YES to VSAM.....	203
Customization	203
Simple Customization	203
Replacing images.....	203
Language Support	204
Advanced Customization	204
Making Changes in the .html Files	204
Server Side Includes (SSI) Variables.....	204
Replacing the "menu.html" File	205
The CSS Files.....	205
The Entrances feature.....	206
User Profile settings.....	206
Setting up more VTAM entrances.....	206
Setting up TN3270 and HTTP entrances	207
Showing the Entrance id to the user	207
Sysplex Functionality.....	208
Prerequisites.....	208
Setting Up the VSAM Files.....	209
The INTSFLE VSAM File	209
The INTSLCL VSAM File	209
Defining the INTSLCL file	210
Defining the Startup Parameters	210
Using the VTAM Interface	211
Using the TCP/IP Services.....	211
Starting the InterSession Instances.....	211
Other Considerations	212
The IOS/Android Tablet App.....	213
Adding New Icon Files	213
Changing the Application Window Style.....	214
Installation-Written Exit Routines	215
The Sign On Exit.....	215
System Option Specification	215
Calls To The Interface	215
Sign On Screen Data Validation Call	215
External Security Model Call	216
Update User Profile Call	216
Sign Off Call	217
Contents of the UserFields Area	217
Contents of the ExtractInfo Area	217
The ApplicationList Information	218
Sample Sign On Exit	218
The Terminal Data Stream Exit.....	219
Writing the Exit	219
Other Exit Considerations	220

Activating the Exit.....	220
The System-Supplied Exit.....	220
Step 1: Create Translate Tables.....	220
Step 2: Set System Option Parameters	221
The Menu Screen Field Exit.....	222
Writing the Exit	222
The Security Maintenance Exit	224
External Security Exit.....	226
System Option Specification	226
Calls to the Exit	226
System Initialization	226
Start of User Verification.....	227
User/Application Profile Authorization Check	227
End of User Verification	228
Security Refreshing	228
Top Line Menu Exit.....	229
The Initial TLM Call.....	229
The "hardCopy" Call.....	230
The "Give" Call	230
The "shaRe" Call.....	230
Session Start Exit	231
Session Switch Exit	232
NETSPY Exit	232
User Written Session Switch Exit	232
The Telnet LU-name Exit	234
The default LU-names.....	234
The Exit	234
Entry parameters	234
Return parameters.....	235
The Batch Routines.....	236
Setting Up the VTAM Session.....	236
Retrieving User and Application Profiles—COPY.....	237
Creating Update Records for User and Application Profiles—UPDATE	238
Copying the log files—COPY LOG / COPY HTTPLOG	238
Maintaining User and Application Profiles—MAINT	240
Maintenance Records	240
Creating Reports on User and Application Profiles—LIST ..	243
Copying / moving application access list—COPYACC / MOVEACC	245
Sending MMS Messages—SEND.....	246
Closing and Opening System Files—CLOSE and OPEN....	247
Deleting Old MMS Messages—DELMSG	247
Printing the Log File—PRINTLOG	249
Inactivating/activating Application Profiles—INACT/ACT ...	249
Compressing Internal Security Keys—COMPRESS.....	250
Issuing VTAM Commands	250
Other Features.....	251
Initializing the VSAM File—FORMAT	251
Upgrading to a New Version—UPGRADE	251
Record Layouts.....	251
User Profile Record	251
Application Profile Record	251
Recovering from startup or sign on problems	252
Introduction	252
Securing TCP/IP traffic with AT-TLS	253
Introduction	253

Step 1A. AT-TLS is not used today	253
Activate RACF classes and define resources	253
Create a self-signed root certificate for testing purposes	254
Create a server certificate signed with your test root certificate	254
Export the test root certificate to a file	254
Step 1B. AT/TLS is already in use	255
Create a server certificate	255
Create a request file to send to your external CA	255
Add the signed certificate	255
Step 2. Create a keyring for your server and connect certificates to it	255
Step 3. Refresh RACF classes	256
Step 4. Configure and start the policy agent (PAGENT)	256
Step 5. Enable AT-TLS in the TCPIP stack	258
Step 6. Activate AT-TLS	258
Step 7. Debugging AT-TLS	259
Appendices	260
Appendix A: Accounting Record Layouts	260
The Record Prefix	260
The SMF record prefix	260
The VSAM record prefix	260
The "INTX" extra information	260
The Record Body	261
The Terminal Identifier	261
System Startup Record	261
Sign On / Sign Off Record	261
Session Start Record	261
Session Interval Record	262
Session End Record	262
System Shutdown or Midnight Record	262
Appendix B: Maintenance Record Fields	263
The User Profile / Model Record	263
The Shared or Personal Application Profile Record	265
The Screen Layout Usage Fields	266
Appendix C: Recognized Telnet Terminal Type Strings	268
Examples	268
Notes	268
Appendix D: The Host Table	269
Sample HOSTS table	269
Appendix E: TN3270E Printing Details	270
Supported Terminal Types	270
Supported Printer Modes	270
IP Address and Mask	270
Examples	270
Appendix F: Log File Record Layout	271
Appendix G: The InterSession Logon Component	272
Defining the INTSLOGN VTAM APPLid	272
Starting the Logon Component	272

Getting Started

Enhancements and new features in version 8.1

A number of enhancements and new features have been added in this version. The most significant are:

Improved support of MFA systems

Messages from MFA are now analyzed in closer detail and where appropriate shown to the user.

Problems with changing passwords have been corrected.

Models, previously named **Amaintainpplication** Access Profiles, is now separated from the User Profiles and are maintained separately. This change will improve the performance significantly of the sign on process.

Number of Models on a user has been increased from 10 to 200. This is especially important when converting from **certain competitive systems**.

Scripting enhancements

The scripting functionality has been greatly enhanced. The most important changes are:

- Maximum number of statements in a script is increased from 50 to 390
- Scripts can reside in a PDS instead of in the INTSFLE VSAM file
- Support of ISPF-like panels, residing in a separate PDS
- Dynamic variables
- Installation-defined, system-wide variables populated with data from External Security
- More commands that mimic competitive systems have been added, like SET, VDEFINE, ACLPGM etc.

Entrances

The Entrance feature means that a single InterSession system can act as a multiple of separate Instances with separate Screen Layouts but with the same applications. Active applications belongs to the instance, so if the user disconnects a terminal session and later reconnects to the same instance, the application sessions on that instance will reappear.

This feature will also be useful when a user has a need to have several instances of an application running simultaneously.

RACF IDentity Tokens

InterSession support RACF IDentity Tokens (IDT) to increase security.

IDTs are created and used by InterSession when a user changes his password or passphrase.

IDT requires z/OS 2.4 or higher. For detailed technical information see the IBM publication "Security Server RACROUTE Macro Reference", Appendix G.

Features removed in 8.1

Support for z/VSE and z/VM have been dropped in 8.1.

Existing z/VSE or z/VM customers are still supported using version 7.2.

A user exit can no longer be used for user sign on / sign off.

Evolutionary changes made in version 7.2

Since the first release of version 7.2, the following major changes have been made:

Conversion tools for conversion from the Network Director product (fixes 45-51)

Screen sizes - Support for all screen sizes with columns greater than 80 (fixes 91, 103)

Error messages - RACF new password error messages can now be greatly enhanced (fix 122)

Multi-Factor Authentication - Enhanced support for MFA products (fixes 127, 129 and 222)

Terminology changes in version 7.2

Two terms have been changed vs earlier versions:

System Profile has been changed to **Application Profile**

Session Procedure has been changed to **Session Script**.

The method BYNAME to obtain application access profile names from RACF/TopSecret is renamed to XSPROFILE (Fix 211).

Key Components and Terminology

The following components are parts of an InterSession installation. The terms below are used throughout the documentation:

External Security Manager

Security Manager

ESM

Your z/OS security system, RACF, ACF2 or TopSecret (TSS)

User Profile

Every user must be described in a User Profile. It can be explicitly defined by an administrator, or automatically from External Security data at user sign on. A User Profile contains all user-specific data, such as name, group code, authorized applications etc.

Model

A Model is similar to a User Profile but is only used as a container of Application Profile names, and optionally User options. The Model names are set in the User Profiles to simplify user maintenance. The Model names can also be obtained from the External Security Manager at user sign on.

A maximum of 100 Models can be defined on a user.

At user sign on, the options defined in a Model can optionally be copied to the User Profile.

Application Profile

Every application that you want to access directly from InterSession must be described in an Application Profile.

It contains all the necessary data about the application, such as VTAM APPLid or IP address, logon data, CICS transaction ID, Session Script IDs, etc.

There are two types of Application Profiles: Shared Application Profiles and Personal Application Profiles. A Personal Application Profile is unique to a certain user, whereas a Shared Application Profile may be shared by many users.

During the installation procedure, a number of predefined Application Profiles for various applications are automatically created. These can be modified as required to ease your implementation process.

Session Script

A Session Script is used together with an Application Profile to automate the logon/logoff sequences required for an application.

Session Scripts are based on the InterSession scripting language, containing a set of instructions to emulate a user's interaction with a 3270 application or to create simplifying tasks, such as starting several applications with one keystroke.

During the installation procedure, a number of predefined Session Scripts for various application systems are automatically created. These can be modified as required to ease your implementation process.

InterSession can also emulate most of the TPX Session Manager ACL commands, which will simplify a conversion from TPX to InterSession.

Panel

A panel is a description of a customer-created 3270 screen. Panels are invoked in a script with the DISPLAY command. Panels are created using the IBM ISPF panel language.

InterSession support a subset of the ISPF Panel protocol, where the commonly used Panel sections)ATTR,)BODY and)INIT sections are fully supported. InterSession can therefore emulate most features of the TPX Panels.

Screen Layout

A Screen Layout contains the text and format for all of the screens in InterSession.

A number of default Screen Layouts are generated during the installation procedure, with different screen appearance and/or languages. These layouts can be modified to fit your needs. You can also copy the standard layouts, creating different versions that can be specified for specific groups of users or terminals.

Interface

An interface describes the connections to the outer world, such as VTAM, TCPIP, batch job communication etc. At least one of the VTAM and TCPIP interfaces must be active for a user to connect to InterSession. During the installation procedure, a number of predefined interfaces are automatically created. These can be modified as required later.

Service

A service describes a subfunction of the TCPIP interface, such as TN3270 or HTTP access. During the installation procedure, a number of predefined services are automatically created. These can be modified as required later.

System Options

These are system-wide options that are maintained by an System Administrator.

Entrance

An Entrance is either a VTAM APPLid or a TN3270/HTTP Service name, used to log on to InterSession.

With more than one Entrance defined, a single InterSession system can act as multiple instances.

System and User Profile Administrator

A System Administrator is a user with the authority to maintain all parts of InterSession.

A user can also be given the authority to maintain User Profiles only, either all users or users in a specific group,

Master Operator

A Master Operator is a user who controls the operational aspects of InterSession, such as InterSession shutdown, closing/opening InterSession files, providing information on application availability, etc. Master Operator authority is set in the User Profile.

System Requirements

InterSession runs in its own z/OS region. The examples in this manual assume InterSession is running as an z/OS job, but it can also run as a started task if that is preferred.

VTAM should be installed and operational.

For IP support, a TCP/IP stack must be installed and operational.

You have most likely a security manager installed, i.e. RACF/ACF2/TopSecret. InterSession interacts closely with the security manager.

New Installation

You should use the manual **Quick Start Guide** to install InterSession.

If you need more information during the installation, you will find it in this manual.

Upgrading from an earlier version

This section covers each of the steps required to upgrade InterSession from the earlier versions 6.1, 6.2, 7.1 and 7.2.

Step 1. The Installation File

The system is shipped as a zip file that must be unzipped on a PC. The **Documents** folder contains all InterSession documentation, and the **Files** folder contains four z/OS PDS's, all in TSO XMIT format. The "nn" at the end is the fix level for the PDS:

- The load library, `LOADLIB_810_nn.XMT`
- The source library, `SOURCE_810_nn.XMT`
- The HTML text member library, `HTMLTXT_810_nn.XMT`
- The HTML binary member library, `HTMLBIN_810_nn.XMT`

Allocate files

All files should be about 10Mb in size.

- Allocate a work sequential file, `RECFM(FB) LRECL(80) BLKSIZE(n*80)`
- Allocate a PDS, `DSORG(PO) RECFM(U) BLKSIZE(6144)` directory blocks 40, with the name "`xxxx.VER810.INSTALL.LOADLIB`", where `xxxx` = `INTSESS` or any other appropriate high-level qualifier.
- Allocate two PDS's, `DSORG(PO) RECFM(VB) LRECL(256) BLKSIZE(4096)`, directory blocks 10, with the names "`xxxx.VER810.INSTALL.HTMLBIN`" and "`xxxx.VER810.INSTALL.HTMLTXT`"
- Allocate a PDS, `DSORG(PO) RECFM(FB) LRECL(80) BLKSIZE(3120)`, directory blocks 10, with the name "`xxxx.VER810.INSTALL.SOURCE`"

FTP the XMT files to z/OS and RECEIVE them

The files must be FTP'd binary and installed one at a time.

For each of the four files to be transferred, do as follows:

- FTP or IND\$FILE the .XMT file **binary** to the work sequential file in z/OS. If you use IND\$FILE, make sure the "crlf" option is unchecked.
- Enter the following command in TSO 6:
`RECEIVE INDSN(sequential.file)`

You will be prompted for the target PDS file name.

Enter the name of the appropriate PDS: **DA (xxxx.VER810.INSTALL.name)** according to the allocated file names above.

Step 2: Authorize the 8.1 loadlib

To use RACF or CA/TopSecret with InterSession, you must APF authorize the InterSession 8.1 loadlib to z/OS.

- For a static APF list, add the following statement to the **PROGxx** member, default **SYS1.PARMLIB (PROG00)** :

```
APF ADD DSNAME(name.of.intsess.loadlib) VOLUME(volser)
```

Then, issue the **SET PROG=xx** command to refresh.

- For a dynamic APF list, issue the **SETPROG APF** command:

```
SETPROG APF,ADD,LIB=name.of.intsess.loadlib,VOL=volser
```

Step 3. Preparations in your current version

If you are using Application Access User Profiles (Models in the 8.1 terminology) , these User Profiles must be converted to Models.

You can do that in your current version by giving the Application Access User Profiles group name(s) that are not used by normal User Profiles. The conversion program will then recognize these groups and do an automatic conversion to Models.

You can also do this work manually after upgrading by changing the “Access” field to “Model” in all such User Profiles.

Step 4. Running the Conversion program

In the source PDS you will find the UPGRADE member:

```
//INTSUPGR JOB   NNN,MSGCLASS=X,CLASS=A,REGION=2M  <--- ACCOUNT & CLASS
//IDCAMS1  EXEC  PGM=IDCAMS
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  *
DELETE INTS.VER810.FILE CL                      /* <--- NEW I/S FILE */
SET MAXCC=0
DEFINE CLUSTER (NAME(INTS.VER810.FILE)           /* <--- NEW I/S FILE */-
                VOL (XXXXXX)                     /* <--- VOLUME      */-
                KEY (10 0)                         -
                REC (NNNN NNN)                     /* <--- ALLOCATION   */-
                SHR (2 3)                           -
                RECSZ (4088 4088)                   -
                CISZ (4096))
/*
//UPGRADE EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER810.LOADLIB,DISP=SHR    <--- I/S LOADLIB
//INFILE  DD DSN=INTS.VERXXX.FILE,DISP=SHR       <--- OLD I/S FILE
//OUTFILE DD DSN=INTS.VER810.FILE,DISP=SHR       <--- NEW I/S FILE
```

```
//SYSIN DD *
UPGRADE
*MODELGROUP GRPNAME1          OPTIONAL SEE DOCUMENTATION
*MODELGROUP GRPNAME2
*MODELGROUP ....
/*
```

Make changes to file names etc. as needed. Note especially the allocation, it should be the same as you current INTSFLE.

If you have put your Models (Application Access User Profiles) into one or more groups, specify the group names in one or more MODELGROUP statements (the sample MODELGROUP statements are considered comments due to the asterisk in column 1).

When the job has completed you can start the upgraded system.

Step 5. Start the upgraded system

Take your current startup JCL and make a copy of it.

In the copy, change the file names of the LOADLIB, HTMLTXT and HTMLBIN files to point out the 8.1 PDSs.

If you run the 8.1 and your current version simultaneously, you need to add VTAM APPLids for 8.1, in order to not conflict with your current version. This is also true for the TN3270/HTTP servers regarding the port numbers.

When the 8.1 version is started you will see the following or similar log:

```
IS0001I  InterSession initializing, version 8.1.nn
IS0310I  Executing under z/OS 2.5.0
IS0311I  Vtam level is 625
IS0315I  Jobstep is APF-authorized
IS0313I  Region size Below: 9192kB Above: 1531MB
IS0016I  002 External Security subtasks started
IS0018I  RACF security interface active
IS0019I  External Security passwords are case sensitive
IS0019I  External Security passphrases are case sensitive
IS0020I  Internal security passwords are case sensitive
IS0020I  Internal security passphrases are case sensitive
IS1300I  License key: Obtained from SYSIN parameters
IS1301I  License key: Expiration date is mmm dd, yyyy
IS0061I  Loading application profiles
IS0062I  Loading user and model profiles
IS0064I  xxxx user and yyy model profiles loaded
IS2404I  VTAM interface started for APPLid xxxxxxxx
IS0090I  InterSession initialization complete
IS0306I  Accepting operator commands
IS1504I  TCPIP BPX API successfully initiated
IS2601I  HTTP service started on interface TCPIP port nnnn
IS2601I  TN3270E service started on interface TCPIP port mmmmm
```

You can now log on to InterSession version 8.1 and start exploring the new features.

If you use Application Access User Profiles (Models) and you have not done the “Change to Model” step before the conversion (see Step 3 above) you must change all these User Profiles now.

This is done in Maint, User Profiles. In each Model you should set the “Access” field to “Model”.

The profile is then removed from the Users list and added to the “Models” list.

Note that this process is not reversible. If you have changed a User Profile by mistake, you have to delete the Model and create a new User Profile.

Application Session Considerations

Overview

This section discusses various considerations that may be important when using InterSession with various application hosts such as CICS, ICCF, TSO, IMS, CMS, etc.

This section also discusses the various options and features that can be defined in the Application Profile for each application system.

Review this section prior to beginning the customization process.

Relay Mode vs. Pass Mode Sessions

When a user starts an application session, it will be started in Relay Mode or Pass Mode.

- Relay Mode means that a session is started between InterSession and the application. All terminal interactions to the application and all data sent from the application is relayed via InterSession. This is the most common mode and gives the user the possibility to have more than one application session active simultaneously. Session Scripts can also be used to automate application logon.
- Pass Mode means that InterSession will pass the terminal session from itself to the selected application environment. When the user logs off the application, InterSession will regain control over the terminal.

This mode is rarely used today but exist for backward compatibility purposes.

How to control which mode InterSession is using

There are a number of settings that affects InterSession's choice of Relay Mode or Pass Mode. These are:

- The System Option **Use pass mode**. If set to **NO**, relay mode is always used.
- The User Profile setting **Number of sessions**. If set to **01** and **Use pass mode** is set to **YES**, the sessions for the user will always start in pass mode. If set to a higher value, the sessions for the user will always start in relay mode.
- The commands defined in the Screen Layout **S/relay** and **S/pass**. When these commands are used to start a session, the mode indicated by the command is used.

Exceptions:

If the Application Profile setting **Session APPLid type** is set to **NONE** then pass mode must be used.

If a logon Session Script is defined in the Application Profile, then relay mode must be used.

How InterSession regains control after a pass mode session

If a pass mode session is started, control of the terminal is taken by the application. If no action is taken regarding which application that should regain control when the pass mode session is ended, the VTAM USS screen will be sent to the terminal.

Since we want InterSession's menu screen to be shown instead, InterSession can send a SIMLOGON request to VTAM when a pass mode session has been started. VTAM will then queue a session with InterSession, which will be activated when the application session ends.

Use this setting in the System Options, Other System Options:

Use SIMLOGON w pass mode ==> YES

If this option is set to NO, interSession will use the VTAM command VARY NET,LOGON=applid where "applid" is InterSession's VTAM APPLid. VTAM will then initiate a session with InterSession when no other application session exist with the terminal. This connection can be removed when a user logs off from InterSession if you have set **Remove VTAM LOGAPPL** to YES in the Logoff Application Profile.

However, this method will not work in a multi-domain environment or for terminals using IBM's TCPIP for access and is therefore not recommended.

Saving Terminal Data

Whenever an application session is not active, that is, it is not the application session that is currently being displayed on the terminal screen, InterSession must maintain an image of the screen in virtual storage, so that it can be redisplayed when the session is reactivated. InterSession can maintain these images in one of two ways:

- A copy of the terminal image is saved within InterSession
- Whenever a user leaves a session (going to the menu or to another session), InterSession can send a Read Terminal Buffer request to the terminal which send the screen image back to InterSession for saving.

You select which method to use for each application via the Application Profile setting

Read terminal buffer ==> NO/YES

Logging Off From InterSession

To disconnect a terminal from InterSession, returning to VTAM's normal USS screen, the predefined Application Profile OFF can be used. To permit users to disconnect from InterSession directly from the sign-on screen, the following procedure can be used :

- Create an Application Profile of type Logoff, with **Authorization check** set to NO. Set **Cancel all sessions** and **Remove VTAM LOGAPPL** to YES or NO, as desired.
- Create a User Profile with a suitable user ID, such as LOGOFF, VTAM, or USS. Specify NO in the field **Can change password**, and make sure that the **New password** field is set to blanks. Set

the field **Password duration days** to **999**. Specify the name of the Application Profile created above in the **Autostart application** field.

When a user enters this user ID on the sign-on screen, his terminal will immediately be logged off InterSession and returned to the control of VTAM.

Note1: This procedure can be used by all users. You may prefer to specify a password for the user ID, and make this known only to certain users.

Note2: When this procedure is used from a terminal connected via the InterSession TN3270 server, the terminal will just be disconnected.

VTAM APPLid Usage for Application Sessions

Unless the TN3270 client is used for an application session, InterSession uses a VTAM APPL name for each application session established by a user (the “virtual terminal” name). These APPL names must be defined to VTAM. The APPL statements are used for all application sessions started by Multiple Session users and for all application sessions using a session start or end script.

To minimize the amount of storage required, InterSession will only use one APPL for each user. However, if more than one session is to the same VTAM application, a separate APPL is used for each.

There is a System Option that you can specify to control the number of open APPLs, “Close inactive VTAM ACBs”. See section “The System Options” for more information.

InterSession has four methods on how to use the VTAM APPL statements. The method you choose is usually based on the needs of the particular VTAM applications.

Session APPLid Type = POOL

This is the most common method of using APPL names.

You define one or more application pool of APPL names in the System Options. When a user starts a session, InterSession will select a free APPL from the specified pool.

The number of APPL statements in each pool determines the maximum number of concurrent sessions that can be started in each pool.

In the Application Profile you define as follows:

```
Session APPLid type ==> POOL
Session applid/Pool no ==> 1 (1-99)
```

You need also to define the names and numbers of the APPLids, in the **System Options and Applpools** section.

Session APPLid Type = GROUP

For some types of VTAM application hosts, like TSO, one ACB (application ID) can be used for all application sessions between InterSession and that particular VTAM application. In such a case, a single APPLid can be defined to VTAM and InterSession.

A unique application ID name must be used for each of these VTAM applications. If, for instance, you have two TSO systems in two CPUs, you must use two different application IDs, one for each TSO system.

This is defined in each Application Profile as follows:

```
Session APPLid type ==> GROUP
Session applid/Pool no ==> applname
```

Session APPLid Type = UNIQUE

When establishing application sessions, it is sometimes desirable for the application to know who or from where the session has been started, i.e. to know the user id or physical terminal id (or parts of it). With the UNIQUE option, this information can be used when creating the VTAM application ID for the application session.

Example 1:

The application IDs are to begin with an X, followed by the first seven characters of the User ID. In the Application Profile, the session fields are defined as follows:

```
Session APPLid type ==> UNIQUE
Session applid/Pool no ==> X%UI
```

When creating the VTAM application ID for the session, InterSession will expand any System Variable, in this case the User ID. For a User ID of **STEVE233**, the resulting application ID will be **XSTEVE23**.

Example 2:

The application IDs are to begin with an M, followed by the second, third, and fourth characters of the VTAM netname of the terminal. In the Application Profile, the session fields are defined as follows:

```
Session APPLid type ==> UNIQUE
Session applid/Pool no ==> M***
```

When creating the VTAM application ID for the session, InterSession will replace the asterisks with the corresponding positions from the terminal name. For a terminal with the VTAM netname **DK53D**, the resulting application ID will be **MK53**. The mask can contain any combination of characters and asterisks, up to the maximum length of eight characters.

Using “Virtual terminal id” in the User Profile and in the Personal Application Profile

In the User Profiles there is a setting “Virtual terminal id”. If you specify a VTAM APPLid here, it will be used for all application sessions started for this user, and the APPLids defined in the Application Profiles will be ignored.

In the Personal Application Profiles there is also such a setting. If you specify a VTAM APPLid here, it will be used for this particular application session, and the APPLids defined in the Application Profiles will be ignored.

The APPLid coded in these fields may be manipulated in two ways before it is used:

- If you code some of the eight positions as asterisks (*), these will be replaced by the corresponding positions of the terminal id the user is signed on to.

- If you have coded the Startup Parameter VTERMMASK, the characters coded in this mask will replace the corresponding positions in the “Virtual terminal id” field.

You can combine the use of asterisks coded in the “Virtual terminal id” field and the use of the VTERMMASK parameter.

Example:

“Virtual terminal id” is coded “ABCD****” and the terminal id is “SCP0345”. The resulting APPLid will be “ABCD0345”.

If you also have coded “VTERMMASK=**YZ” in the Startup Parameters, the resulting APPLid would have been “ABYZ0345”.

Note that the VTERMMASK parameter is normally used in a sysplex environment, but it can be used in all environments. Also, the parameter only affects “Virtual terminal id” of the User Profile, not the APPLids defined in the Application Profiles.

Session Portability

This option specifies whether or not application sessions can be transferred by InterSession from one terminal to another. The default is to allow the transfer.

In some cases though, it may not be advisable to transfer the session. This can be true, for instance, in a CICS environment where the CICS Terminal ID is created based on the physical Terminal ID. The following would then happen:

- A user starts a CICS session on Terminal A. A CICS TCT entry is used based on the Terminal A name.
- The user then moves to terminal B and issues an InterSession sign on, porting the session to terminal B. Since the session remains active in CICS, it keeps the name derived from Terminal A.
- If another user tries to start a CICS session on terminal A, it will be rejected because the Terminal A name is already in use by the ported session.

In such a case, specify NO in the Application Profile:

Session portability ==> NO

It means that the session will be canceled if a user tries to move it to a terminal other than the one where it was started. Also, if a user starts a session and leaves the terminal, and another user signs on to that terminal, the session for the first user will be canceled by InterSession.

Inquire About APPL Status

By default, InterSession will ask VTAM every two minutes about the application status (if the application is active or inactive). Normally, this should be done for all applications. However, in a cross-domain environment, VTAM may not respond to the inquiry. InterSession will then issue messages MS17I and MS18I, and the inquire mechanism will remain locked for this application.

If this happens frequently for an application, change this option to NO in the Application Profile:

Inquire about appl status ==> NO

The application will then always be shown as active on the menu. A Master Operator can still manually set the application as inactive, if desired. A change of this parameter will also affect all other Application Profiles with the same VTAM APPLid.

Lock Pool APPLid To User

Certain application systems, like IMS, will require this field to be set to YES in the Application Profile:

Lock pool APPLid to user ==> YES

This means that once a new application ID has been selected from a pool for a user, it will be assigned solely to that user. The reason for this being required in IMS is that the application ID (which is seen as the IMS PTERM) can be temporarily disconnected from the IMS LTERM at session logoff. If another user uses the same application ID, that user enters the first user's transaction.

InterSession will automatically release all application ID "locks" at midnight.

Appl Will Pass Session

Many VTAM application systems, like TSO or NetView, issue a CLSDST PASS, which results in the session being switched from one VTAM application ID to another.

If no data has been exchanged on the session when this switch occurs, InterSession will handle the situation automatically. However, some application systems (typically, another session handling system) will issue a CLSDST PASS after data has been exchanged on the session. If you experience problems in connecting to such a system, code YES in this field:

Appl will pass session ==> YES

TSO and NetView do not require this option to be set to YES.

Appl Sends First Screen

Normally, the application system will send the first data on the session to the terminal, and InterSession will wait for it, leaving the terminal locked until the first data arrives. If you have a VTAM application that waits for the user to send the first data of the session, you must specify NO in this field:

Appl sends first screen ==> NO

INTSMTAB Logmodes

When InterSession initiates an application session, a logmode entry from INTSMTAB is selected based on the terminal logmode. See Step 5 of the installation process.

Certain applications will require a specific logmode to be used. An example of such an application is IBM's Host Command Facility, used to communicate with AS/400 computers.

Consult the documentation for the application, review the INTSMTAB source module for an appropriate entry, and code the name of this logmode into the appropriate Application Profile fields:

```
SNA logmode name ==> xxxxxxxx
Non-SNA logmode name ==> xxxxxxxx
```

If the required logmode does not exist in INTSMTAB, you have to add a new logmode entry with a suitable name.

Note that it is not necessary for InterSession to use the INTSMTAB logmode table. You can define another logmode table in the System Options.

3270 Data Compression

InterSession has an option that you can specify to automatically compress the 3270 data stream from an application before it is sent to the terminal.

The compression consists of replacing repeated characters with a 3270 Repeat-to-address string. This feature can improve your response times and decrease the load on your terminal network.

The percentage reduction resulting from the compression is shown on the Session Status Screen and in the Accounting Records.

In the Application Profile for each system or application where you want Data Compression to be performed, set the following field:

```
3270 data compression ==> YES
```

3270 Data Translation

InterSession has an option that you can specify to automatically translate the 3270 data stream each time it is sent to or received from a terminal.

This facility can be used if you have a need to translate special characters such as for certain national character sets for your terminals.

On the User Exits screen of the System Options, specify:

```
Term. data stream exit name x) ==> XLATE
```

This will indicate to InterSession that the system supplied exit is to be used.

Generate one or more translate tables using the Assembler Language macro IXLATE supplied with InterSession. Refer to the section on "The Terminal Data Exit" for more information.

The translation may be done on terminal ID level, on Application Profile level, or both.

- To perform translation on specific terminals, use the System Options / User Exits / XLATE parameters.
- To perform translation on specific applications, enter the name of the translate table in the appropriate Application Profile:

3270 data trans. table ==> xxxxxxxx

Instead of the system-supplied translation exit, the installation may provide its own translation-routine. See the section on "The Terminal Data Exit".

TSO Considerations

Use the GROUP type of VTAM ACB (application ID) usage when interfacing TSO. Refer to the section on "VTAM ACB (application ID) Usage" for more information.

The easiest way to enter a TSO application is to use the session concept with start/end scripts to define automatic logon and logoff from TSO.

- First, specify the Application Profile as application type SESS.
- Second, code a Session Script similar to the following, and give the name of the script in the "Session start script" field of the Application Profile. The following script is supplied with the name TSOON and can be used to take a user to the first TSO/ISPF screen:

```
TYPE %UI          Type user id
ENTER             Press ENTER key
IFSTR IKJ56420     User not defined ?
    TERM 'You are not defined to TSO'
TYPE %PW          Type password
ENTER             Press ENTER key
IFSTR IKJ56421     Invalid password ?
    TERM 'Invalid TSO password'
IFSTR IKJ56425     Reconnect ?
    TYPE 'LOGON %UI' Yes, repeat logon
    ENTER          Press ENTER
    TYPE %PW        Type password
    TABL            Tab to last
    TABB 1          Tab backward
    TYPE S           S for reconnect
    ENTER           Press ENTER
ENDIF             End reconnect
IFSTR 'NO BROADCAST MESSAGES' Any bc messages ?
    CLEAR           No, clear screen
    TYPE ISPF
    ENTER           Get to ISPF panel
ENDIF             End broadcast
END               Successful logon
```

zVM/CMS Considerations

You should use the session concept, where you can code a number of interactions in a Session Script in order to reach a specific point within your CMS application.

- First, specify the Application Profile with application type VTAM.
- Next, code %UI in the "Data to pass to application" field. This causes InterSession to send the user ID as part of the VTAM logon process to CMS.
- Then, use a Session Script similar to the following, and specify the name of the script in the "Session start script" field of the Application Profile.

```

                IFSTR 053E          User id incorrect ?
                TERM 'You are not defined to z/VM'
CHECKCP IFSTR 'CP READ'          CP READ sent ?
                GOTO PSWD
                WINP                No, wait for more
                GOTO CHECKCP        Continue loop
PSWD  TYPE %PW                    Yes, type password
                ENTER              Press ENTER key
CHECKRC IFSTR Ready              "Ready" sent ?
                GOTO FINISH        Yes, finished
                IFSTR 050E          Invalid password ?
                TERM 'Invalid password in z/VM'
                IFSTR 054E          Already in session ?
                TERM 'You have already a session with z/VM'
                IFSTR RECONNECT     Reconnect ?
                TYPE B              Yes, type "B"(egin)
                ENTER              Press ENTER key
                GOTO FINISH        End RECONNECT
                WINP                No, wait for more
                GOTO CHECKRC       Check again
FINISH END                      Successful logon

```

This script is provided with the name CMSON.

z/VSE Interactive Interface Considerations

To achieve an automatic logon to z/VSE, use a start script to perform the logon and an end script to perform the logoff.

1. Use a Session Script like the following, and specify the name of the script in the "Session start script" field of the z/VSE Application Profile:

```

TYPE %UI      VSE User ID
TAB
TYPE %PW      VSE Password
ENTER        Press ENTER key

```

This script assumes that you are using the same user ID and password in InterSession and z/VSE. If this is not the case, use two of the data fields of the User Profile for the z/VSE user ID and password. (code %D1—%D8 instead of %UI and %PW).

2. It is important that the z/VSE session be terminated properly. Use a second Session Script like the following, and specify the name of this script in the "Session end script" field of the z/VSE Application Profile:

```

PF3                incase blank screen

```

CHECK	IFSTR	IESADM	Inside z/VSE ?
	GOTO	VSELOOP	
	TERM		No, just terminate
VSELOOP	IFSTR	IESADMS01	Yes, Sign on screen ?
	GOTO	SIGNOFF	
	PF3		No, press PF3
	GOTO	CHECK	Continue check
SIGNOFF	PF4		Yes, logoff z/VSE

Ad-hoc Sessions

Users who are properly authorized can start ad-hoc sessions with 3270 applications. Ad-hoc sessions are sessions to applications not defined among the Shared or Personal Application Profiles.

To enable a user for ad-hoc sessions, set the following option in the User Profile:

Use ad-hoc sessions ==> YES

To start an ad-hoc session, enter the start command and a VTAM APPLid or an IP address in the command field of the menu screen. Examples:

S A12TSO

S 192.168.24.32

The ad-hoc sessions will show as selectable items at the end of the menu application list until they are removed by the user or until InterSession is brought down.

When an ad-hoc session is started, InterSession creates an Application Profile internally. This profile does not show and can not be maintained. The profile is deleted when the user removes the item.

However, the System Administrator can define a specific Application Profile to be used as a Model when starting an ad-hoc session. In this way, specific defaults for ad-hoc sessions can be set up.

See the parameter "Ad hoc Model profile" in the section "System Options and APPLpools maintenance", screen User/Application Profile Defaults..

The timeout functions

InterSession has a number of inactivity timeout functions as follows:

- **Terminal idle timeout**
- **Application idle timeout**
- **Widow session timeout**
- **Standby Screen timeout**

The timeout values are set in minutes. They are set globally in the System Options and per user in the User Profile. A user profile setting overrides the global values.

A general recommendation is to use the global timeout settings as far as possible and minimize the user profile settings, to simplify the maintenance.

All timeout values are set in the MAINT application.

Terminal Idle Timeout

This timeout starts to count down as soon as a screen is sent to the terminal / terminal emulator. When the timeout occurs, the Sign On screen is sent to the terminal.

For example, if this timeout is set to 20 (minutes), then the terminal is signed off after 20 minutes of inactivity.

Application Idle Timeout

This timeout starts to count down as soon as the user has sent something to the application. When the timeout occurs, the application session is terminated.

For example, if this timeout is set to 15 (minutes), then the application session is terminated after 15 minutes of inactivity.

Widow Session Timeout

An application session is considered a "widow" when there is no terminal associated with it (the terminal is signed off, either by the user or by inactivity). This timeout starts to count down as soon as the application session has become a "widow".

For example, if this timeout is set to 10 (minutes), then the application session is terminated 10 minutes after the session has become a "widow".

Note that if "Number of terminals" for a user is greater than one, and "Use multiple entrances" is set to NO, then the widow timeout should be zero. If not, a user could end up after a new signon with two or more application sessions with the same name. In this case InterSession will cancel all but one application session.

Standby Screen Timeout

This timeout starts to count down as soon as the Standby Screen is sent to the terminal. When the timeout occurs, the Sign On screen is sent to the terminal.

For example, if this timeout is set to 30 (minutes), then the terminal is signed off after 30 minutes of inactivity.

Note: If a user has signed on to InterSession with a PassTicket or with an MFA product, the Standby Screen will not be sent to the terminal. Instead, the Sign On Screen will be sent.

3270 Printer Support

With the InterSession Printer Support, you can:

Print screen hardcopies and messages to a physical 3270 printer owned by VTAM

Print screen hardcopies and messages to a TCPIP printer via a "virtual" VTAM printer, defined as an APPLid

Write screen hardcopies and messages to a system spool queue entry via a "virtual" VTAM printer, defined as an APPLid

Capture 3270 print from other VTAM applications and print to a TCPIP printer via a "virtual" VTAM printer, defined as an APPLid.

Capture 3270 print from other VTAM applications and write to a system spool queue entry via a "virtual" VTAM printer, defined as an APPLid.

All print requests to a TCPIP printer are queued as part of a "spool file" contained within the InterSession LPRQUE VSAM file. This ensures that no print requests are lost, even if InterSession is brought down before the actual printing takes place.

Defining Virtual Printers

InterSession can utilize 3270 printers that are owned by VTAM, either as a physical printer or as a virtual printer (VTAM APPLid). Using a virtual printer enables you to further process the print data, either by the InterSession TCPIP printer support, or by an external print product.

A virtual printer is defined by a VTAM APPLid. You can either use one of the two printer logmodes from INTSMTAB, or a logmode from any other logmode table. Examples:

```
INTSVPR  APPL  ACBNAME=INTSVPR,MODETAB=INTSMTAB,PARSESS=YES, *  
                                DLOGMOD=PRTL3  
                                INTSSCSP APPL  
ACBNAME=INTSSCSP,MODETAB=INTSMTAB,PARSESS=YES, *  
                                DLOGMOD=PRTSCS
```

To print to an IP printer using InterSession, the VTAM APPLids for the virtual printers must also be defined in a IP printer profile, see below.

When a user specifies one of these VTAM APPLids as a printer name (either from InterSession or from any other VTAM application), the print data is captured and spooled by InterSession. It will then be printed to the defined destination - to the system spool or to the IP printer as soon as the printer is available.

Using Printers for Hardcopies and Messages

For hardcopy screen prints, and for printing messages from the Mail/Message System (MMS), you define your 3270 printers to InterSession using the MAINT screens for "Printers", and with a printer type of "HARDCOPY".

These types of printers can be defined both for physical 3270 printers or for virtual 3270 printers.

InterSession is shipped with a "DEFAULT" printer profile that will be used for any 3270 printers not specifically defined. This profile should be changed to match the majority of your printers. You then only need to define those printers that differs from the default definition.

Each printer profile can be defined with the VTAM network name or with any other name. When using the printer, either the VTAM network name or the printer profile name can be given.

Defining Printers for Users

You define which 3270 printer to use for each user's print requests using the maintenance facility screen for "User Profiles":

Printer id ==> name

```

      Print header ==> YES
Form feed after header ==> NO

```

Each end user can change these values using the PROF screen:

```

      Printer id ==> name
      Print header ==> YES
Newpage after header ==> NO

```

At time of the print request, each end user can override these specifications, using any printer name.

Print Request Headers

InterSession can generate a heading page prior to each Hardcopy screen or Mail/Message printed. Heading data can be printed on a separate page, or on the same page as the actual print request.

This feature is controlled by individual user, using the PROF (user's own profile) facility.

The following is a sample of the Heading data. The format of the headers can be changed by using the maintenance facility, in the "Screen Layout" section.

```
* * * * * INTERSESSION PRINT REQUEST * * * * *
```

```
Distribute to: userid/user name
```

```
Terminal: netname
```

```
Type: Hardcopy
```

```
Application: MAINT
```

```
Printer: netname
```

```
Date: yymmdd
```

```
Time: hhmmss
```

Using TCPIP Printers

Both internally generated VTAM print (hardcopies, messages) and VTAM print from any other application can be passed from a virtual VTAM printer through InterSession to a TCPIP printer.

A TCPIP interface must be defined and active.

InterSession supports four types of TCPIP printers:

- TN3270E printers (a feature found in many TN3270 emulators)
- Using the LPD protocol, providing the ability to spool jobs to a UNIX system
- Using the RAW protocol and a direct connection to a LAN printer
- Using the HP PJI protocol and a direct connection to a LAN printer

All TCPIP printers must be defined to InterSession using the MAINT screens for "Printers", and with a printer type of "TN3270E", "LPD", "RAW" or "PJI".

See the section on "Printer Maintenance" later in this manual for further explanation.

Write Print Data to System Spool

By specifying a printer profile with type SPOOL, all print data directed to the associated VTAM APPLid will be written to system spool (JES, POWER or RSCS). In the printer profile you can define the spool entry characteristics, such as class, job name, forms number etc.

See the section on "Printer Maintenance" later in this manual for further explanation.

Customization

The System Options

System Options control InterSession. These options are maintained with the MAiNT application, see “The Maintenance Facility” later in this manual.

VTAM APPL Statements

If VTAM is used, InterSession is defined to VTAM via a standard VTAM APPL statement. InterSession itself requires from one to three APPLids to be specified in each VTAM host, depending on which components of InterSession you are using. InterSession also requires one or more APPL statements that it uses to establish individual application sessions.

The Main APPLid

The following APPL statement must be specified in the VTAM host where you are running the InterSession system:

```
intsess APPL AUTH=(ACQ,PASS),PARSESS=YES
```

The name (intsess) is the name of InterSession, and should be known as a cross-domain resource to all VTAM hosts that own terminals (via a CDRSC statement). The recommended name is INTSESS.

The Logon APPLid

This is optional and not used by new installations. However, if used, the following APPL statement must be specified in all VTAM hosts where you are running the InterSession logon component:

```
logonname APPL AUTH=(ACQ,PASS,SPO),PARSESS=YES
```

This APPLid is used when you log on to InterSession from a terminal and want InterSession to be the logon application for your terminal. The name (logonname) should be the same in all VTAM hosts, for consistency. This name must also not be specified as a cross-domain resource. The recommended name is INTSLOGN.

See Appendix G for more information.

The Batch APPLid

The following APPL statement must be specified in all VTAM hosts where you intend to use the batch program:

```
utilname APPL AUTH=(ACQ,SPO)
```

The name (utilname) is specified as a parameter to the INTSUTIL batch program. Refer to the section on “The Batch Routines” for more information. The recommended name is INTSUTIL.

APPL Statements for Application Sessions, Type POOL

For each application session, InterSession will open a VTAM ACB, which is defined via an APPL statement. There are two types of ACBs/APPLids, the first being used for applications specified as using a POOL type of APPLid:

```
abc***** APPL MODETAB=INTSMTAB
```

The “abc” part can be 1-7 characters and the number of asterisks 1-7. The same generic name defined in VTAM must be specified for each pool in the System Options.

For instance, **INTS******* will generate up to 9999 APPLids with the names **INTS0000** to **INTS9999**.

In the System Options you can specify the generic APPLids as above by using type MASK.

You may also use type LIST if the APPLids are not in sequence, like CIC10AA, CIC10BC, CICF0CF etc. With type LIST, you have to define all APPLids one by one.

You can have up to 99 pools of APPLids.

APPL Statements for Application Sessions, Type GROUP

The second type of APPLids that is used for application sessions, is the GROUP type. With this type, code one unique APPLid statement for each application you have specified as using a GROUP type of ACB/APPLid in an Application Profile:

```
groupnam APPL MODETAB=INTSMTAB, PARSESS=YES
```

The GROUP type implies that all sessions to a specific VTAM application can make use of a single APPLid instead of one APPLid per session.

Note: You cannot use the same GROUP APPLid for more than one VTAM application.

VTAM Model Terminal Support

The VTAM Model Terminal Support (MTS) concept is used to supply an application host system, like CICS, with a terminal Model name when an application session is started. This Model name must be defined in the application host system with the appropriate parameters. With MTS you will be able to control for example some aspects of CICS Autoinstall.

If you specify “Model terminal support ==> YES” in an Application Profile, then InterSession will use the selected VTAM logmode entry name as a Model name when starting the application sessions for this Application Profile. If you use the default logmode table INTSMTAB, the Model names will be S2480N1, S2480E5, B2480N1 etc. depending on the current terminal characteristics, and if any override logmode names have been specified in the Application Profile.

In the InterSession installation source library for CICS you will find CICS RDO definitions to support these Model names, in the member RDOMODEL. It contains the TYPETERM and TERMINAL definitions corresponding to all entries in the INTSMTAB logmode table.

You use MTS since you want to control the Models used by the application host. You will therefore most likely need to change these TYPETERM and TERMINAL definitions to achieve the desired result, for instance to set the USERAREALEN parameter in the TYPETERM entries.

The VTAM USS Table

The following USS table can be used to cause an automatic connection to InterSession, simply by pressing enter. This example assumes that the default APPL names is used.

```

USSTAB  USSTAB
        SPACE 3
INTSLOGN USSCMD CMD=INTSLOGN,REP=LOGON,FORMAT=PL1
        USSPARM PARM=APPLID,DEFAULT=INTSLOGN
        USSPARM PARM=LOGMODE
        USSPARM PARM=DATA
        SPACE 3
LOGON    USSCMD CMD=LOGON,FORMAT=BAL
        USSPARM PARM=APPLID
        "      "      (more USSCMD stmts)
        "      "
        SPACE 3
MESSAGE  USSMSG MSG=0,BUFFER=OKMSG
        USSMSG MSG=1,BUFFER=ERRMSG
        USSMSG MSG=2,BUFFER=ERRMSG
        USSMSG MSG=3,BUFFER=ERRMSG
        USSMSG MSG=4,BUFFER=ERRMSG
        USSMSG MSG=5,BUFFER=ERRMSG
        USSMSG MSG=6,BUFFER=ERRMSG
        USSMSG MSG=7,BUFFER=ERRMSG
        USSMSG MSG=8,BUFFER=ERRMSG
        USSMSG MSG=7,BUFFER=ERRMSG
        USSMSG MSG=8,BUFFER=ERRMSG
        USSMSG MSG=9,BUFFER=ERRMSG
        USSMSG MSG=10,BUFFER=INITMSG
        USSMSG MSG=11,BUFFER=ERRMSG
        USSMSG MSG=12,BUFFER=ERRMSG
        SPACE 3
        DS    0F
INITMSG  DC    Y(INITMSG-INITMSG-2)
        DC    X'F5C3'      WE + K/M
        DC    X'115D7F1DF0' L24 P80 SF PAN
        DC    C'PRESS ENTER FOR InterSession'
        DC    X'11C47F1DF8' L4 P80 SF PAH
        DC    C'SYSTEM ===>'
        DC    X'1DC113'      SF UANM IC
        DC    CL50'INTSLOGN'
        DC    X'1DF0'      SF PAN
INITMSGGE EQU  *
        SPACE 3
        DS    0F
OKMSG    DC    Y(OKMSG-OKMSG-2)
        DC    X'F160'      W
        DC    X'115D7F1DF0' L24 P80 SF PAN
        DC    CL80'OK, LOGON IN PROGRESS'
OKMSGGE  EQU  *
        SPACE 3
        DS    0F
ERRMSG   DC    Y(ERRMSG-ERRMSG-2)
        DC    X'F1C6'      W + K/A
        DC    X'115D7F1DF0' L24 P80 SF PAN
        DC    CL80'THE SYSTEM IS NOT AVAILABLE'
        DC    X'11C47F1DF8' L5 P1 SF PAH
        DC    C'SYSTEM ===>'
        DC    X'1DC113'      SF UANM IC
ERRMSGGE EQU  *
        SPACE 3
END       USSEND
        END

```

For SNA/SDLC terminals, you cannot use the 3270 mapping characters (x'11'-SBA, x'1D'-SF etc.). The only allowed control character is x'15' (NL, new line), so you have to change the USS message buffers accordingly:

```

          DS      0F
INITMSG  DC      Y(INITMSG-INITMSG-2)
          DC      C'TYPE "INTSLOGN" + ENTER FOR SIGN-ON'
          DC      X'15401540154015'          4 * NL
          DC      C'SYSTEM ==> '
INITMSG  EQU      *
          SPACE 3
          DS      0F
OKMSG    DC      Y(OKMSG-OKMSG-2)
          DC      X'40154015'                2 * NL
          DC      CL80'OK, LOGON IN PROGRESS'
OKMSG    EQU      *
          SPACE 3
          DS      0F
ERRMSG   DC      Y(ERRMSG-ERRMSG-2)
          DC      X'40154015'                2 * NL
          DC      CL80'THE SYSTEM IS NOT AVAILABLE'
          DC      X'40154015'                2 * NL
          DC      C'SYSTEM ==> '
ERRMSG   EQU      *
          SPACE 3
END       USSEND
          END

```

The Startup Parameters

Optionally, you can specify InterSession startup parameters in the system input file (SYSIN) in the startup JCL. These parameters define the following, of which none is mandatory:

- The InterSession License Key
- Parameters to activate interfaces and services, that is to describe how you want to connect to InterSession (via VTAM, TN3270 or web browser)
- Debugging parameters.

How to Enter

```
[LICENSEKEY=key]
[PASSWORD=key]
[CPUIDn=cupid]
[INTERFACE=]
[SERVICE=]
[APPLID=mainappl]
[LGAPPLID=logonappl]
[EXTSEC=]
[SYSPLEXGROUP=group name]
[SYSPLEXMEMBER=member name]
[VTAMGNAME=generic resource name]
[VSAMRLS=YES/NO]
[VTERMMASK=mask]
[VPRINTMASK=mask]
[SPOOLUNITS=(cuu,cuu...)]
[FAILSAFE=]
[DEBUG=]
[SNAPMAX=]
[MIGRATE=module]
```

Explanation

```
LICENSEKEY=key
PASSWORD=key
CPUIDn=cupid
```

These parameters are optional. They provides InterSession with data on how long you are authorized to use InterSession and on which CPU. See “Step 5” in the Installation section earlier in this manual.

PASSWORD is an alias of **LICENSEKEY**.

```
INTERFACE=name,type,START|STOP[,applid|trmchar][,lgapplid|tcpname]
```

This parameter is optional. If you need to start certain interfaces at InterSession startup, which is either not defined or not started, you can use this parameter. You can also use it to stop a defined interface.

name is the name of the interface, 1-8 characters.

type can be any of the following: VTAM, BATCH, OPER, BPX.

applid must be given for type VTAM and BATCH.

lgapplid can only be given for type VTAM.

trmchar is the first char in the generated termid and can be used for BPX.

tcpname is the tcpip stack name for BPX (optional).

Example:

```
INTERFACE=TCPIP,BPX,START
```

Note that specifying

```
INTERFACE=VTAM,VTAM,START,INTSESS
```

is equivalent to specifying the parameter card **APPLID=INTSESS**. See section “The Maintenance Facility”, “Interfaces Maintenance” for more information.

```
SERVICE=name,type,START|STOP,interface,port,[mhomeip][,HTTPLOG=YES|NO|VSAM]
```

This parameter is optional. If you need to start certain services at InterSession startup, which is either not defined or not started, you can use this parameter.

name is the name of the service, 1-8 characters.

type can be any of the following: TN3270, TN3270E, HTTP.

mhomeip is the optional multihomed ip address.

HTTPLOG=YES|NO|VSAM is the optional parameter to control the use of the HTTPLOG file. This is for HTTP service type only.

Examples:

```
SERVICE=TN3270,TN3270E,START,TCPIP,9923
```

```
SERVICE=HTTP,HTTP,START,TCPIP,8080,,HTTPLOG=VSAM
```

See section “The Maintenance Facility”, “Services Maintenance” for more information.

```
APPLID=mainappl
```

This parameter is optional. It provides InterSession with the name of the VTAM APPLid. If specified, the VTAM interface will always be activated with this APPLid. If not specified, the VTAM interface can be either active, inactive or non-existent. This parameter can be used instead of the **INTERFACE=VTAM** parameter.

```
EXTSEC=RACF|ACF2|TSS
```

This parameter is optional; it is mainly used during the first installation of InterSession. See the Quick Start Guide manual.

```
SYSPLEXGROUP=group name
```

```
SYSPLEXMEMBER=member name
```

```
VTAMGNAME=generic resource name
```

```
VSAMRLS=YES/NO
```

These parameters are optional. See the chapter “Sysplex Functionality” for details

VTERMMASK=mask
VPRINTMASK=mask

These parameters are optional and normally used in a sysplex environment, but can be used in all environments. See the chapter “Sysplex Functionality” for details.

FAILSAFE={NO,APF,EXTSE,TCPIP,USEREXIT,NOABEXIT,AMODE24,SYSDADMIN:userId,SCRLAYOUT,YES,APPLINQ}

This parameter is optional. If you encounter problems that prevents InterSession to start properly, you can use one or more of these parameters to disable certain functions:

NO	No functions are set. This is the default.
APF	The system does not test for APF authorization. z/OS only.
EXTSEC	External Security support will not be activated.
TCPIP	The TCPIP interface will not be activated.
USEREXIT	No user exits will be activated.
NOABEXIT	The InterSession abend exit will not be activated.
AMODE24	InterSession will run in 24 bits addressing mode.

SYSDADMIN:userId At system startup, the “userId” will be set as a System Administrator. This can be needed when all users with System Administrator privileges has been deleted by mistake, for instance with a user written program.

SCRLAYOUT If your Screen Layout has been corrupted for some reason, preventing you from signing on to InterSession, this function will restore the contents of the DEFAULT Screen Layout to its original appearance. Also, as long as this function is in effect, all users will be forced to use the DEFAULT Screen Layout, regardless of the settings in other Screen Layouts or in the User Profiles.

YES All of the above functions are set.

APPLINQ The application status inquire mechanism of InterSession will be disabled at startup. This means that all applications will show as available, regardless of status. Note that the inquire mechanism can be enabled by the REFRESH INQ=YES operator command.

DEBUG=option[,option....]
SNAPMAX=value

See the section “The InterSession Debugging Facility” in the *User’s Guide for 3270 Users* manual for information on these parameters.
 You can specify more than one DEUG statement.

MIGRATE=module

This parameter is optional and may be used when migrating to InterSession from certain competitive products. See the appropriate conversion / migration documentation for details.

The Accounting Routines

InterSession can be customized to generate accounting records on a VSAM ESDS file, or for z/OS users, directly to SMF. For the layout of the accounting records, see Appendix A. Accounting records will be written for the following events:

- At InterSession startup
- At user sign-on
- At user sign-off
- At application session start
- At application session end
- Interval session records (optional)
- At InterSession shutdown
- At midnight

Implementation

In the System Options, “Other System Options” screen, the following fields are used to specify accounting:

```
Accounting x) ==> {NO|YES|SMF}
Account record SMF no. ==> [nnn]
Account record layout x) ==> {INTS|INTX|TV|TVX}
Interval record interval ==> [minutes]
```

Set “Accounting” to YES or SMF.

If you choose to write records to SMF, set the “Account record SMF no.”

InterSession can create account records either in its own format or in a format that resembles Teleview account records. Specify INTS, INTX, TV or TVX.

INTS and INTX creates records that are described in Appendix A.

Specifying TVX creates records that are extensions of the Teleview records. TVX differs from TV as follows:

- The SMFREASN field will always contain X'FE' in the terminal logon and application logon records. SMFREASN will always contain X'FF' in the terminal logoff and application logoff records.
- The terminal logon/logoff records will be appended with the following fields:

SMFMDL	DS	CL8	MODEL PROFILE NAME
SMFTRNSF	DS	CL1	"Y" IF TRANSFER FROM ANOTHER TERMINAL
SMFIPAD	DS	XL4	TERMINAL IP ADDRESS IF ANY
	DS	XL12	RESERVED FOR IPV6
SMFPORT	DS	XL2	TERMINAL IP PORT NUMBER IF ANY

For InterSession's own format, session account records written at a specified interval can be created. These records can be used, for example, to monitor fluctuations in application response times over the

day. At the end of each time interval, session account records are written, equal to the session end record but containing only data related to the latest interval. Such a record is written for each active session. The interval in minutes is to be specified in the field "Interval record interval". A value of zero (default) disables the function.

Note: Be careful when you specify the interval. Specifying a low interval will result in an excessive amount of records being written. For this reason, it is not recommended to use this option permanently.

If **Accounting** ==> **YES** is specified, the VSAM file must be defined using IDCAMS:

```
DEFINE CLUSTER (NAME(name.of.file)           -
              NIXD                           -
              VOL(volume)                     -
              REC(pri sec)                    -
              SHR(2 3)                        -
              RECSZ(60 200)                   -
              CISZ(512))
```

You must also add the following JCL to your startup job:

```
//INTSACC DD DSN=name.of file,DISP=SHR
```

Accounting File Backup/Reset

To backup and reset the Accounting File while InterSession is running, use the following procedure:

1. The account file must first be closed. It can be done with the INTSUTIL command CLOSE ACCOUNT. You can also use the Master Operator command /CLOSE ACCOUNT on the menu screen..
2. Copy the contents of the VSAM file by means of IDCAMS REPRO or a user-written program.
3. Delete/Define the file by means of the IDCAMS DEFINE statements as shown above.
4. Reopen the log file with the INTSUTIL command OPEN ACCOUNT, or use the command /OPEN ACCOUNT on the menu screen.

You must be defined as a "Master Operator" to perform these functions.

The Wrap-Around Message Log File

All messages that InterSession writes to the system log can also be written to a VSAM RRDS file. InterSession will also write more detailed information messages to this file, and all messages will be time stamped. When the file becomes full, InterSession will wrap-around and continue from the beginning.

You can browse this file from the STAT internal application. You can also use the INTSUTIL program to print portions or all of the file, or to copy the log records to a sequential file.

Implementation

In the System Options, "Other System Options" screen, set the following parameter:

Use wrap-around log file x) ==> YES

The log file must be defined to VSAM by means of the following IDCAMS parameters. Note the lack of secondary allocation:

```
DEFINE CLUSTER (NAME(name.of.file)           -
                NUMBERED                       -
                VOL(volser)                    -
                REC(pri 0)                     -
                SHR(2 3)                       -
                RECSZ(100 100)                 -
                CISZ(512))
```

You must also add the following JCL to the InterSession startup job:

```
//INTSLOG DD DSN=name.of.file,DISP=SHR
```

Printing Log Messages

To print messages from the log file, use the following procedure:

1. The log file must first be closed. It can be done with the INTSUTIL command CLOSE LOG. You can also use the Master Operator command /CLOSE LOG on the menu screen.
2. Use the INTSUTIL command PRINTLOG.
3. Reopen the log file with the INTSUTIL command OPEN LOG, or use the Master Operator command /OPEN LOG on the menu screen.

Item 1 and 3 requires that an interface of type BATCH is active in InterSession. In the following examples, INTSUTIL will print all IS0101- and IS0103- messages. If you do not specify any ISnnn message numbers, all messages will be printed. You may enter as many numbers as can fit on one card. Note also that you will need a CONNECT card before each CLOSE and OPEN.

```
//PRINTLG EXEC PGM=INTSUTIL
//INTSLOG DD DSN=INTS.LOG.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
APPLID=INTSUTIL
CONNECT APPLID=INTSESS
CLOSE LOG
PRINTLOG IS0101 IS0103
CONNECT APPLID=INTSESS
OPEN LOG
/*
```

Copying Log Messages

You may copy the log messages from the VSAM file to a sequential file with variable length records.

For more information, see the section “The Web Gateway” later in this manual.

The Spin-Off Message Log Files

All messages that InterSession writes to the wrap-around log file can also be written to a sequential file. As with the wrap-around log file, InterSession will also write more detailed information messages to this file, and all messages are time stamped. For each day of week a unique file is used. At mid-night, the current log file is closed and the log file for the new day is opened.

When a file becomes full, InterSession will discontinue logging until midnight, when the new file is opened.

It is the user's responsibility to handle the information on the old file and to reallocate it for next week's use.

Note that the use of the wrap-around log file is a prerequisite for the spin-off log files to work.

Implementation

In the System Options, "Other System Options" screen, set the following parameter:

Use spin-off log files x) ==> YES

The log files must be pre-allocated with the following parameters and with an appropriate allocation. Note that secondary allocations can be used, in contrast to the wrap-around log file.

```
Organization . . . : PS
Record format . . . : FB
Record length . . . : 100
Block size . . . . : 4000
```

You must also add the following JCL to the InterSession startup job:

```
//INTSMON DD DSN=ints.spinoff.MONDAY,DISP=SHR
//INTSTUE DD DSN=ints.spinoff.TUESDAY,DISP=SHR
//INTSWED DD DSN=ints.spinoff.WEDNSDAY,DISP=SHR
//INTSTHU DD DSN=ints.spinoff.THURSDAY,DISP=SHR
//INTSFRI DD DSN=ints.spinoff.FRIDAY,DISP=SHR
//INTSSAT DD DSN=ints.spinoff.SATURDAY,DISP=SHR
//INTSSUN DD DSN=ints.spinoff.SUNDAY,DISP=SHR
```

The JES2 Message Log File

All messages that InterSession will write to the wrap-around and spin-off log files can be written to a JES2 spool file. This type of log file can be used in addition, or as a replacement to, the other log files.

Implementation

In the System Options, "Other System Options" screen, set the following parameter:

Use JES2 log file ==> YES

You must also add the following JCL to the InterSession startup job, if not already there:

```
//JES2LOG DD SYSOUT=*
```

You can specify any other parameter allowed for a spool file.

The HTTP Log File

Accesses to the Web Gateway can be logged to the HTTPLOG file.

The log records are written in the *Combined Log Format*, a common format used by most other web servers and which can be used by many log analysers.

The log records can be written to a sequential file or to a wrap-around VSAM file.

You can use the INTSUTIL program to copy the log records to a sequential file.

You can also browse the VSAM file from the STAT internal application.

Implementation

See the section “The Web Gateway” later in this manual.

National Characters and Codepage Support

If you have applications and/or terminals with different national character sets, you need to use InterSession’s codepage support.

From the 3270 terminal Query Reply, InterSession will record the codepage number that is used by the 3270 terminal.

The Web Gateway will by default use codepage 1148 (Multilingual with Euro sign) on the web browser side. If needed, you can set a national codepage in the Screen Layout and/or in the Application Profiles. You can also use the %CP variable, see the section “The Web Gateway” for more information.

On each Application Profile you can define which codepage the application is using. In the System Options, you can define the default value to be used for all applications that do not have a codepage explicitly defined in the Application Profile.

For InterSession screens, including the internal applications, you can set a codepage on each Screen Layout.

If a codepage number exist on both the terminal / web browser side and on the application side, InterSession will translate between the codepages if they are not the same.

The following codepages are supported by InterSession. The second codepage number on each line is equivalent to the first, but with added support for the Euro character:

037 1140 United States

273 1141 Germany

277	1142	Denmark
278	1143	Sweden / Finland
280	1144	Italy
284	1145	Spain
285	1146	United Kingdom
297	1147	France
500	1148	International
871	1149	Iceland

TCP/IP Stack Affinity

If you have more than one TCP/IP stack defined in your system, InterSession will support this. You may have a need to select which stack InterSession shall use, or you may want InterSession to use more than one stack.

Selecting which stack to use

Method 1: In the InterSession TCPIP Interface Profile, you can define which stack to use with the parameter “TCP/IP ident”. Here you should give the TCPIP stack name for BPX, the address space id for TLI, the TCPIP user id for IUCV or the TCPIP for VSE identification.

Method 2 (z/OS BPX only): You can use the IBM-supplied program BPXTCAFF in your InterSession startup procedure to select the stack. Insert the following JCL before the execution of INTSESS:

```
//*          SELECT TCPIP STACK
//*
//STACK      EXEC PGM=BPXTCAFF,PARM=stack name
```

Using more than one stack

To use more than one stack, you will need to define one Interface Profile and at least one Service Profile for each stack.

Example: In a z/OS system, we have two stacks defined with the names TCPIP1 and TCPIP2. We want InterSession to accept TN3270 requests on port 1023 for stack TCPIP1 and on port 1123 for stack TCPIP2:

The Interface Profiles:

```
Interface id TCPIPA
    Interface type ==> BPX
    TCP/IP ident ==> TCPIP1
    Termid 1st char ==> T
    Active ==> YES

Interface id TCPIPB
    Interface type ==> BPX
    TCP/IP ident ==> TCPIP2
    Termid 1st char ==> U
```

Active ==> YES

The Service Profiles:

```
Service id TN3270A
  Service type ==> TN3270E
    Interface ==> TCPIPA
      Port ==> 01023
Multi-homed IP address ==> 0.0.0.0
  Queue length ==> 005
    Active ==> YES
```

```
Service id TN3270B
  Service type ==> TN3270E
    Interface ==> TCPIPB
      Port ==> 01123
Multi-homed IP address ==> 0.0.0.0
  Queue length ==> 005
    Active ==> YES
```

CICS outstanding work after a session termination

When a CICS session is terminated abnormally (for example, via the idle timeout option), there may be work outstanding on the session, such as BMS paging requests or EXEC CICS START requests that have not yet been executed.

If the CICS terminal ID is based on the VTAM netname of the pool application IDs, another user may later start a CICS session using the same pool application ID. CICS uses the same terminal entry, and the outstanding requests are then executed, possibly causing application screens to be displayed that the user should not see.

This problem is solved by setting the Application Profile option “Lock pool APPLid to user” to YES. The pool application id will then be unique for each user, and this problem will never occur.

As an alternative, you can install the InterSession version of DFHZNEP, the CICS node error program. This program can be found in the installation source library. When a session is ended, DFHZNEP cancels all outstanding BMS paging and START requests.

Security and Authorization

Overview

If you do not have any External Security Manager installed, the InterSession security functions can replace many of the features found in a External Security Manager, see “Internal Security Functions” below.

InterSession supports all of the popular External Security Managers. They are used for InterSession sign-on and Application Profile authorization.

In addition, InterSession supports the use of an installation-written security exit for InterSession sign-on and Application Profile authorization.

Internal Security Functions

The following security functions are available:

- Users can change their own passwords.
- Passwords can be required to be reset after a specified period of time.
- Password content rules can be specified.
- InterSession keep a history of prior passwords and check that users specify genuinely new ones.
- Users can be revoked after a specified date or after a specified period of inactivity.
- Users can also be revoked after too many unsuccessful signon attempts and at will by a security administrator.

The ability for a user to change his own password is specified in the User Profile. All other functions are defined in the System Options, Internal Security Options. See the “The Maintenance Facility” chapter for how to specify.

Support for Long Passwords and Passphrases

InterSession supports long passwords and passphrases, both when using the built in security or when using an External Security Manager. In the following, the term “passphrase” is used both for long passwords and for passphrases.

Passwords are 1-8 characters in length and passphrases are 9-100 characters in length.

For any user, both an 8-character password and a 9-100 character passphrase can be used at the same time.

After the installation, the DEFAULT Screen Layout is used by InterSession. This layout has only 8-character password fields defined on the Sign On screen.

If you want to use longer passwords or passphrases, you should use the following Screen Layout instead (or copy the appropriate parts on the Sign On screen definition from these layouts to your own):

- If you want to use the same screen field for both 8-character passwords and passphrases, use the DEFLPW Screen Layout.
- If you want to use separate screen fields for 8-character passwords and passphrases, use the DEFPWPP Screen Layout.

System Variables used in Screen Layouts for passwords and passphrases are %PW, %PP, %NPW %NPP, %VNP and %VNPP.

System Variables used in Session Scripts for passwords and passphrases are %PW, %PP and %LP (other password related variables exist for special purposes).

Note specifically the %LP variable in Session Scripts.

It will expand to either the user's password or the user's passphrase, depending on which was used when the user signed on to InterSession.

See the section "The System Variables" in "The Maintenance Facility" chapter for more information.

Using an External Security Manager

The following External Security Managers are supported for InterSession sign-on and Application Profile authorization:

- RACF
- ACF2
- TopSecret

Note that InterSession will attempt to keep in memory the most recent External Security data, in order to speed up the security processing. This retained data will automatically be refreshed every 30 minutes. To force a refresh at any time, use the REFRESH operator command.

RACF

The following steps should be performed to activate the InterSession interface for RACF. Note that the RACF support uses the SAF interface via the RACROUTE macro.

Make sure that the library in which your InterSession load modules reside is APF authorized.

In MAINT, System Options, External Security, specify **"Security manager = RACF"**. Restart InterSession.

InterSession will now use RACF for user sign on verification. This includes also support for PassTickets and MFA factors. To be able to enter these on the sign on screen, your Screen Layout will need changes.

Application Access

To let RACF control which applications a user is authorized for (which applications that are shown on the menu screen) a number of methods can be used. See the section "Controlling Application Access" below.

Improved Messages

When a user defines a new password and RACF detects some kind of password error, RACF returns a generic error code to InterSession regardless if the error is related to the password contents, password history etc. The error message shown to the user is therefore of little help. However, if you specify your RACF password rules in the System Options also, InterSession will perform the same password contents checks as RACF and will be able to give the user a detailed error message. See MAINT, section "System Options, External Security" for more information.

ACF2

The following steps should be performed to activate the interface for ACF2:

Select an ACF2 resource type to be used for authorizing access to your InterSession Application Profiles. It can be any of the ACF2 predefined resource types, such as CKC (CICS transactions), ITR (IMS transactions), or it can be a user-defined resource type.

In MAINT, System Options, External Security, specify "**External Security = ACF2**" and specify the resource type in the "**External Security class**" field.

Define InterSession to ACF2 as a "MUSASS". This is accomplished by the following:

Create an ACF2 logon ID record. This logon ID must have the following attributes: MUSASS, JOB, NO-SMC, NON-CNCL.

To achieve fast-path processing (not required) also insert a MUSASS macro in the ACF2 Field Definition Record generation.

The name and password of the InterSession logon ID must be defined in the InterSession startup job card.

Running As a Started Task

If you prefer to run InterSession as a started task, then in Step 6, the name of the Logon Id created must be the same as the name of the started task.

If no such profile is found when the task is started, ACF2 will look for a default logon ID with a name given in the ACF2 definition table (if not changed, the default name for started tasks is DFTSTC). If found, this logon ID will be used to validate that the task is authorized to issue ACF2 requests. Finally, if no such logon ID is found, then the task will not be able to issue any ACF2 requests.

Application Access

To let ACF2 control which applications a user is authorized for (which applications that are shown on the menu screen) a number of methods can be used. See the section "Controlling Application Access" below.

TopSecret

The following steps should be performed to activate the InterSession interface for TopSecret. Note that the TopSecret support uses the SAF interface via the RACROUTE macro.

Make sure that the library in which the InterSession load modules reside is APF authorized.

Select a TopSecret facility name to be used for InterSession. The facility name can be any name; in the following we have chosen the name INTS.

Update the facility table in the SYS1.PARMLIB member TSSPARM with the following statements:

```
FACILITY (USERn=NAME=INTS)  
FACILITY (INTS=PGM=INTSESS)  
FACILITY (INTS=MODE=FAIL)  
FACILITY (INTS=LOCKTIME=00 , LOG (MSG) , SIGN (S) , AUTHINIT)  
FACILITY (INTS=ACTIVE , LUMSG , NOABEND , NOINSTDATA , NONPWR)  
FACILITY (INTS=NORES , NORNDPW , NOSTMSG , MULTIUSER , SHRPRF)
```

Replace USERn with any of the USER facilities defined in TopSecret (for example, USER1 or USER2).

Examine also the TopSecret-supplied facility INTERACT. This facility may have a PGM specification which conflicts with InterSession. If so, change the INTERACT PGM specification to a name that does not conflict with InterSession.

In MAINT, System Options, Security, specify

External Security ==> TSS

and the selected facility name in the field

External Security class ==>

Running As a Started Task

If you are running InterSession as a started task, define in TopSecret:

```
TSS CREATE (INTSESS) NAME ('INTERSESSION')
FACILITY (STC)
MASTFAC (INTS)
PASSWORD (NOPW, 0)
DEPARTMENT (dept)

TSS ADDTO (STC) PROCNAME (procname) ACID (INTSESS)
```

Restart InterSession.

Application Access

To let TopSecret control which applications a user is authorized for (which applications that are shown on the menu screen) a number of methods can be used. See the section “Controlling Application Access” below.

Controlling Application Access

It is strongly recommended that you use External Security for Application Access.

InterSession supports control either by authorizing the individual applications or by using Models. Models is the preferable way, since the effort to implement the Model approach is significantly less.

Application Access Using Individual Applications

It is defined in the System Options, External Security, by setting the parameter “**Obtain application access from**” to “**APPL**”.

Set the name of an External Security Manager CLASS name in the field “**Security manager class**”.

In the field “**Class profile access needed**”, specify whether READ or UPDATE access is required to gain access to the PROFILES defined in External Security.

In External Security, all application names in InterSession must be defined as PROFILES in the CLASS specified above.

Each user that should have access to an application must be connected in External Security to the PROFILE with the application name.

Application Access Using Models

Instead of authorizing individual applications for each user, there are a number of methods to let the External Security Manager control application access via one or more InterSession Models.

Create a number of Models, where each Model represents a logical group of applications.

Give each Model access to the applications that belong to this logical group. Use the normal way of setting + (plus) signs in front of the application id's.

In a User Profile you can define up to 100 Model id's in the Model fields of the second User Profile screen. The individual user will now have access to the sum of the applications defined in these Models.

For users defined to External Security you may use the External Security Manager to define which Models that should be assigned to an individual user.

There are five different ways of this setup. It is defined in the System Options, External Security, parameters "**Obtain application access from**" and "**Select model names from**".

1) Using the security manager's PROFILES

Specify "**Obtain application access from** ==> **MODELS**"

Specify "**Select model names from** ==> **XSPROFILE**"

in the field "**Security manager class**" type the name of a Security Manager CLASS

In the field "**Access required**", specify whether READ or UPDATE access is required to gain access to the PROFILES in External Security.

In External Security, all Model profile id's must be defined as PROFILES under the External Security CLASS specified above.

In External Security, the users should be connected to the PROFILES they should have access to.

At sign on time, InterSession will check the names of all Model profiles against the user's access to the PROFILES in External Security with the same name. Access will be given to the Models that matches, and the user will get access to the applications defined in these Models. A maximum of 100 Models can be assigned to a user.

This method can be used with RACF, Top Secret and ACF2.

2) Using the security manager's GROUP names

Specify "**Obtain application access from** ==> **MODELS**"

Specify "**Select model names from** ==> **XSGROUP**"

In External Security, the Model names should be defined as GROUP names.

In External Security, each individual should be connected to the GROUPs he should use.

For Top Secret, use IBMGROUP to assign group names to users.

At sign on time, InterSession will locate all Model profiles by the External Security GROUP names connected to this user. The individual user will then get access to the applications in the Models that matches these group names.

To restrict the search for unwanted group names you can set a group name prefix in the field "**XSGROUP' prefix**" from one to seven characters. InterSession will match the External Security group names against this prefix to determine what group names to select. A maximum of 10 Models can be assigned to a user.

This method can be used with RACF and Top Secret.

3) Using the security manager's default GROUP for the user

Specify “**Obtain application access from ===> MODELS**”

Specify “**Select model names from ===> XSDEFGRP**”

In External Security, each individual should be connected to a default group name.

XSDEFGRP works the same as XSGROUP except that InterSession will use the user's RACF/Top Secret default group name to find the Model. Only this Model is used.

This method can be used with RACF and Top Secret.

4) Using the security manager field INSTDATA

Specify “**Obtain application access from ===> MODELS**”

Specify “**Select model names from ===> INSTDATA**”

If you have more types of data in the INSTDATA field, you may give a search string that identifies the Model name in the '**INSTDATA**' **model prefix string**', for example **TELEVIEW(**.

If your Model names are not always eight characters long, you may specify a character which ends the name in the '**INSTDATA**' **stop character**' field.

In External Security, specify the name of a Model in the **INSTDATA** field for each user.

At sign on time, InterSession will locate the Model profile with the name set in the **INSTDATA** field for this user. The individual user will then get access to the applications in this Model.

This method can be used with RACF and Top Secret.

5) Specify “**Obtain application access from ===> modelName**”

All users defined to External Security will get access to this Model's applications. Only one Model can be specified. Note that this approach is mainly used to give External Security users certain attributes, defined in this Model, not for giving access to applications.

Apply Model at every signon

When set to NO (the default) the Model(s) will only be applied if the user does not exist in InterSession. When set to YES, the Model will be applied to the User Profile every time the user signs on to InterSession. This can be useful if you want to add or remove applications from the Model and have these changes propagated to the User Profiles.

Note 1: When set to YES, any sign on exit will be called with a type “2” call every time a user signs on.

Note 2: When set to NO and only one Model is used, the Model name is not set in the User Profile field “Appl access profiles”.

Copy Model attributes

Copying other attributes from the Model profiles

This is defined in the System Options, External Security, parameter “**Copy Model attributes**”.

When this parameter is set to “YES” (the default), then for each Model, the following User Profile attributes will be examined. If the Model information is of higher priority than what is currently set in the individual's User Profile it will be replaced by the Model information. If this parameter is set to “EXT”, additional information is copied from the Model, see below.

Please also note that the attributes will be updated regardless of this setting if the user's profile is not stored in the data base (the setting "**Store extsec users in data base**" is NO). The reason for this is that such a profile can not be updated via MAINT.

If "**Copy Model attributes**" is set to **YES** or **EXT**, the following attributes in the individual User Profile will be updated:

- System administrator
- Update user profiles
- Only with group code
- Maintain own profile
- Master operator
- Update info screens
- Change own password
- Terminal lock administrator
- Can start adhoc sessions
- Number of sessions
- Number of terminals.

When set to **EXT**, the following additional attributes will also be updated:

- Jump key
- Attention key
- Command key
- Command chars.

The Hot keys are also copied from the first Model profile, if the System Option, User Profile Defaults, "**Hot keys from Syst. acc. Profile**" is set to **YES**.

Multithreaded Signon

When using an External Security Manager (RACF, ACF2, TopSecret), InterSession will by default execute all External Security requests in two z/OS subtasks. This will be sufficient for the majority of installations. However, in a system with several thousands of users, the performance of the sign on process may be noticeably decreased. You may then define InterSession to use more z/OS subtasks. Many External Security requests can then be processed simultaneously, and the sign on bottleneck be eliminated.

The feature is controlled by a parameter in the System Options, "**Number of extsec subtasks**". See the Maintenance Facility, System Options, later in this manual.

PassTicket Support

InterSession can use PassTickets to sign on to other applications. This is done by using one of the variables **%PT**, **%PTU** or **%PTT** instead of **%PW** in an Application Script or in the "**Data to pass to app1**" field of an Application Profile.

The **%PT** and **%PTU** variables generates PassTickets based on the user id, whereas the **%PTT** variable generates PassTickets based on the terminal id. Which to use is dependent on the External Security Manager you use. RACF for instance generates PassTickets based on the user id. At session establishment time the variable will be substituted with a PassTicket obtained from External Security.

Use of PassTickets requires a proper setup in External Security. To use PassTickets with an application, the VTAM APPLid of the Application Profile is used for most applications. For TSO however a

specific string is used. This application unique string should be set in page 2 of the InterSession Application Profiles, "**PassTicket application name**". If this field is not filled in, the VTAM APPLid of the Application Profile is used. See below.

Automatic replacement of the %PW variable with a Pass Ticket, %PT

InterSession will attempt to replace a %PW variable in an Application Script with a PassTicket if any one of the following options is true:

- If the "**PassTicket application name**" field is filled in
- If sign on to InterSession was made with a PassTicket or by using MFA (Multiple Factor Authentication)
- If the **PassTicket application name** is defined in the PTKTDATA class (RACF only).

If PassTicket generation fails, InterSession will fallback by trying a password or pass phrase, if a password or phrase was used earlier when signing on to InterSession (after the latest InterSession startup). Since no password information is stored in the INTSFLE file for users defined to External Security, any such information will be lost when InterSession is recycled.

Other considerations

InterSession also accepts a PassTicket instead of a password during user sign on to InterSession, for example if the sign on is made by another application. InterSession will recognize the PassTicket and validate it via External Security. Note that the Standby Screen will not be sent to the terminal at terminal idle timeout, but instead the Sign On Screen will be sent.

Instead of entering the PassTicket in the normal password field on the Sign On screen, you may want to use a specific field to enter a PassTicket. The field should contain the %PT variable. This is an example how to code in the Screen Layout:

```

;
#      User id ==> %UI      #
#      Password ==> %PW     #
#      New password ==> %NP  #
#      Passticket ==> %PT    #
%IMSG                                     %TI
F1-help  F3-return  F7/8-bwd/fwd

```

RACF Definitions

First, you must activate the PTKTDATA class if not already done:

```

SETROPTS CLASSACT (PTKTDATA)
SETROPTS RACLIST (PTKTDATA)
SETROPTS RACLIST (PTKTDATA) REFRESH

```

Then, for each VTAM application that should use PassTickets, you must define a profile in the PTKTDATA class:

```

RDEFINE PTKTDATA profile-name
        SSIGNON(key-description)
        UACC (NONE)

```

profile-name is one of the following, depending on application type:

TSO: The characters "TSO" plus four bytes as follows:

If a VTAM generic name is used, the GNAME value in the TSOKEYxx member of SYS1.PARMLIB, or the GNAME= operand of the START command issued to start TSO.

If a VTAM generic name is not used, the SID= value of the SMFPRMxx member of SYS1.PARMLIB. For example if SID=SYSA, the profile name is TSOSYSA.

Other applications: The VTAM application id used to logon to the application.

The profile name must not be suffixed by any group or user id.

key-description can be either **KEYMASKED (16-digit-hex-string)** for RACF to mask (obscure) the key, or **KEYENCRYPTED** for using an encryption algorithm.

UACC (NONE) should be used. This is also the default.

You must also set the **profile-name** in each InterSession Application Profile that will use pass tickets.

Example:

```
RDEFINE PTKTDATA TSOSYSA
        SSIGNON (KEYMASKED (34A1708DEE420581) )
```

Passticket External Security id ==> TSOSYSA

You can then use the **%PT** variable instead of the **%PW** variable, either in an InterSession script, or in the Application Profile as data to pass to the application at logon time, for example

Data to pass to appl ==> %UI/%PT

As mentioned, any **%PW** variable will expand as a pass ticket.

For more information, see the IBM manual *"Security Server RACF Security Administrator's Guide"*.

TopSecret Definitions

If not already done, update the resource descriptor table (RDT) to define the PTKTDATA class:

```
TSS ADD (RDT) RESCLASS (PTKTDATA) RESCODE (n)
        ACLST (ALL, READ, UPDATE) MAXLEN (37)
```

Include **RESCODE (n)** in the range of 101 to 13F to make PTKTDATA a prefixed resource class.

Assign ownership for the PassTicket resource (IRRPTAUT):

```
TSS ADD (department) PTKTDATA (IRRPTAUT)
```

For each VTAM application that should use PassTickets, you must define a profile in the PTKTDATA class and permit access to the profile for InterSession:

```
TSS ADDTO (NDT) PSTKAPPL (profile-name)
        SESSKEY (16-digit-hex-string)

TSS PERMIT (userid-of-stc)
        PTKTDATA (IRRPTAUTH.profile-name) ACCESS (UPDATE)
```

profile-name See the RACF Definitions above.

userid-of-stc specifies the uid of the InterSession started task user ID.

Example:

```
TSS ADDTO (NDT) PSTKAPPL (TSOSYSA)
        SESSKEY (34A1708DEE420581) )
```

```
Passticket External Security id ==> TSOSYSA
```

You can then use the %PT variable instead of the %PW variable, either in an InterSession script, or in the Application Profile as data to pass to the application at logon time, for example

```
Data to pass to appl ==> %UI/%PT
```

For more information, see the appropriate TopSecret manuals.

ACF2 Definitions

First, you must activate the pass ticket support for InterSession::

```
SET RESOURCE(PTK) RECKEY IRRPTAUTH
  ADD(applid UID(userid-of-stc)
  SERVICE(UPDATE,READ) ALLOW)
```

applid is used for PassTicket validation. Specify the InterSession VTAM APPLid.

userid- of-stc specifies the uid of the InterSession started task user ID. InterSession can then generate PassTickets for any user.

For each VTAM application that should use PassTickets, you must define a profile in PTKTDATA:

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
  INSERT profile-name
  SSKEY(16-digit-hex-string)
```

profile-name See the RACF Definitions above.

When you have created the profile records, rebuild the directory:

```
REBUILD(PTK) CLASS(P)
```

You must also set the profile-name in each InterSession Application Profile that will use pass tickets.

Example:

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
  INSERT TSOSYSA SSKEY(34A1708DEE420581)
```

```
Passticket External Security id ==> TSOSYSA
```

You can then use the %PT variable instead of the %PW variable, either in an InterSession script, or in the Application Profile as data to pass to the application at logon time, for example

```
Data to pass to appl ==> %UI/%PT
```

For more information, see the appropriate ACF2 manuals.

Multi-Factor Authentication Considerations

Multi-Factor Authentication (MFA) is a technique to enhance the security for User Sign On. It is based on multiple authentication factors that are to be presented during logon in order to verify a user's identity. Each authentication factor must be from a separate category of credential types. A card is one type (something you have) and a pin code another (something you know).

A number of vendors have MFA products. Only a few have mainframe support though, among them IBM. These products interfaces with the External Security Manager (RACF, ACF2 or TopSecret) by using exits, and requires that all users enabled for MFA is defined to the External Security Manager.

Depending on the product, one or more MFA codes (pin codes, one-time passwords etc.) should be entered by the user on the sign on screen. For example, a user of one MFA product generates a one-time password (OTP) by using a USB stick and a PC program. This OTP is then entered in the password field. Other solutions may require more than one MFA code, for example to be entered in the password and new password fields.

In the following, MFA codes entered by the user are named *PassCodes*.

General Considerations

The common way of entering the PassCode(s) in a mainframe application is to use the password field(s) of the sign on screen. However, InterSession can not distinguish between passwords and PassCodes. Each time a PassCode is used to sign on, InterSession considers this to be a new password, since it does not match the current InterSession password for that user. The password in the InterSession data base is therefore updated with the PassCode. When later the %PW variable is used, it will be substituted with the latest PassCode, which is most likely invalid at that time.

You should therefore consider the following:

- 1) The MFA product may work in such a way that if a user is MFA enabled, he can not use passwords.
- 2) InterSession can distinguish between passwords and PassCodes by using separate fields for passwords and PassCodes on the sign on screen. See **Sign On Screen Appearance** below.
When InterSession recognizes a PassCode the following will occur:
 - a) After some time where only PassCodes are used for sign on to InterSession, the user's password known by InterSession may be outdated and therefore not usable in application sign on scripts.. Any %PW variables in application sign on script will therefore be replaced by a PassTicket for this user and this terminal session. It is not needed to manually change the %PW variable to %PT in the scripts.
 - b) The Standby Screen will not be sent to the terminal at terminal idle timeout. Instead the Sign On Screen will be sent.

We strongly recommended that PassTickets are used instead of passwords in the application sign on scripts, either by InterSession's automatic password / PassTicket replacement, or by hard-coding the %PT variable.

For PassTickets, see above in the section **PassTicket Support**.

MFA Server Verification Considerations

In general, the MFA product has a server separate from the mainframe. Depending on product type, server load and server communication speed, a delay may occur when a PassCode is validated by the MFA server. If this delay is longer than a fraction of a second, you should consider the following.

- 1) **Number of subtasks.** InterSession uses one or more subtasks to interface with the External Security Manager, in order to not delay the processing for other users not currently signing on. If the MFA delay is noticeable, you may have to increase the number of subtasks to allow for multiple users to sign on concurrently. This is done in MAINT, System Options, External Security. The number of subtasks may be up to 255. You can monitor the use of subtasks in the STAT application.
- 2) **“Waiting for MFA” message to the user.** If the MFA delay sometimes is longer than one or two seconds, InterSession can send a message to the user while waiting for the sign on to complete. In MAINT, System Options, External Security you can set how long the delay should be before sending the message. A value of zero indicates that the message should never be sent. The message itself can be customized in the Screen Layout, Messages 7/7. The default message is *“Waiting for external authentication”*.

Sign On Screen Appearance

Entering the PassCode(s) in the normal fields for password / new password fields etc. will work, with the exception that the %PT variable must be used instead of the %PW variable in sign on scripts for the applications.

If you want InterSession to be able to distinguish between passwords and PassCodes, and so automatically replace the %PW variable with %PT in the scripts when needed, you should define one or more separate field(s) to be used for the PassCode(s). The changes are made in MAINT, Screen Layout, Sign on screen.

There is one predefined Screen Layout named DEFMFA. The Sign On Screen in DEFMFA contains one extra field for a PassCode:

```
InterSession ----- Maintenance, Screen Layout 4/23 -----
Screen Layout DEFMFA      Sign On Screen 2/2

      Line start column 80/01/02 ==> 0
Number of lines at bottom of screen ==> 6
Lines 9-24 (line command I/R/D):
; $IIII$nn; $nn; $tttt; $eeee;$rr;          #Julian:<<<%Y.%JD
;
;          [SSSSS;[EEEEEEE;[SSSSS; [SSS;  [IIIII;[00000;[NNN;[NNN;
;          [SSS[SSS[EEE;/[E[SSS[SSS[SSS[SSS;[III;[000[000[NNNN[NNN;
;          [SSS;///[EEE;/[SSS;///[SSS;/// [III;[000[000[NNN[NNNN;
;          /[SSSSS;[EEEE;/[SSSSS;/[SSSSS; [III;[000[000[NNN;[NNN;
;          ///[SSS[EEE;/;  ///[SSS;///[SSS; [III;[000[000[NNN;[NNN;
;          [SSS[SSS[EEE;[E[SSS[SSS[SSS[SSS;[III;[000[000[NNN;[NNN;
;          /[SSSSS;[EEEEEEE;[SSSSS;/[SSSSS;[IIIII;[00000;[NNN;[NNN;
;          //IIII //IIIIII //IIII //IIII //IIII //IIII //IIII //IIII
;
;          User id ==> %UI      Å
;          Password ==> %PW      Å
;          New password ==> %NP      Å
;          MFA/PIV passcode ==> %MFA1      Å
;          %IMSG                      Å
;          %TI
F1-help  F3-return  F7/8-bwd/fwd
```

You can either set this Screen Layout as the default, or you can change your own Screen Layout accordingly. The DEFMFA layout will work as is with MFA products that only uses one PassCode.

When using the DEFMFA Screen Layout the sign on screen looks as follows:



The user can then enter his normal password in the “**Password**” field or the PassCode in the “**MFA/PIV passcode**” field, so that InterSession will be able to distinguish between passwords and PassCodes.

The MFA variables on the Sign On Screen

There are five MFA PassCode fields that can be defined on the Sign On Screen. The data entered in each field will be presented to the External Security Manager as specific data depending on the variable. The variables associated with the different PassCode types are as follows.

Variable	External Security Manager field
%MFA1	Password
%MFA2	New password
%MFA3	Passphrase
%MFA4	New passphrase
%MFA5	Group

To choose which MFA variables to use, consult your MFA product documentation where TSO logon is discussed.

The variables can all be used with RACF and TopSecret. With ACF2 only the first two can be used.

Note that a screen field with an %MFA or %PT variable by default is visible, due to the short life of a PassCode. If you want the field to be dark/invisible, go to the Screen Layout page 3 and set

Hide MFA and PT fields ==> YES

Identifying MFA messages

The security manager works closely with the MFA product. For most MFA products the security manager relays any MFA messages to InterSession. Since any return code is often not detailed, InterSession will analyze the MFA messages.

To distinguish what messages coming from MFA, you must specify the message prefix the MFA product uses. Also the error/information message number suffixes must be specified. For example, IBM MFA has a message prefix of AZF and error/info suffixes E and I.

This is defined in the System Options, third page of External Security settings:

```
InterSession ----- Maintenance, External Security Options 3/3 -----
MFA options:
  Message number prefix ==> ZF
  Msg number error suffix ==> E
  Msg number info suffix ==> I

  Compound In-Band factors ==> %MFA1:%PW

  Show MFA messages to user ==> YES

  Show waiting msg after nn secs ==> 00 00 - no msg

F1-help  F3-return  F7/8-bwd/fwd
```

IBM MFA compound In-Band support

The IBM MFA product has a function named “MFA compound In-Band”.

This means that a user shall enter both an old-fashioned password and a PassCode.

They should be combined with a separation character and passed on to IBM MFA via the Passphrase field.

This combination can be done by InterSession from separate fields.

Example:

The user enters the password **TSECR672** and the PassCode **56QSH897** (for example, from an OTP generator gadget).

The separation character is set to **:**.

InterSession will then combine the information to **56QSH897:TSECR672** and send it to IBM MFA as a Passphrase.

To know which factors to use, you have to specify this information in the field **Compound In-Band factors** in the System Options, third page of External Security settings.

In this case it would be

```
Compound In-Band factors ==> %MFA1:%PW
```

On the Sign on screen, the input fields containing these factors must exist, for example

```
User id ==> %UI      Ä
Password ==> %PW     Ä
MFA passcode ==> %MFA1      Ä
```

If a user only enters his password but not the PassCode, InterSession will ignore the MFA compound setting and call External Security with just the password. Depending on this user's setting in External Security the signon will be accepted or fail.

Analyzing the MFA messages

At some occasions InterSession has a need to analyze MFA messages to determine which action to take. If the MFA messages prefix (like AZF for IBM MFA) differs from regular extsec messages, you should supply this information to InterSession. This is set in the System Options, External Security. Example:

```
----- MFA options -----  
  Message number prefix ==> AZF  
Msg number error suffix ==> E  
  Msg number info suffix ==> I
```

With this information, InterSession will be able to detect MFA related errors and give the user a better error / informational message.

Debugging MFA signon

The debugging facility of InterSession has a special feature for debugging the sign on settings. To use it you must have a DD card in the InterSession startup JCL:

```
//DEBUG    DD    SYSOUT=*
```

To start the debugging, enter `/debug *,sign` on the application selection screen, or on the system log with the command `f intsess,debug *,sign`

You can then view the debug file directly with TSO SDSF.

RACF IDentity Tokens

InterSession support RACF IDentity Tokens (IDT) to increase security.

IDTs are created and used by InterSession when a user changes his password or passphrase.

IDT require z/OS 2.4 or higher.

The use of IDT is controlled in the System Options, External Security 3/3, "Use IDT when changing passwords".

The password change process in InterSession for an MFA user follows:

1. The user has entered a new password on the sign on screen, either by will or when the current password is expired.
2. Due to internal design, RACF can not handle both current and new passwords when MFA items are parts of the request. InterSession then requests an IDT by logging on to RACF with the current password and no MFA items. Even if expired, the current password is enough to verify the user. Provided that the user is authorized in RACF for IDT, the IDT is given back to InterSession for use in next step.
3. If the IDT was created, the original RACF MFA call is reissued but with the IDT for identification. RACF will change the password and the process is completed.
4. If the IDT creation fails, InterSession writes a message to the log file and issues a sign on with the new password and the RACROUTE parameter PASSCHK=NO. If PASSCHK=NO is allowed for the user, RACF will change the password, and InterSession immediately signs off the user. If compound is used, a new compound is created containing the new password. The original RACF MFA call is reissued and the process is completed.

For more information see the IBM publication **Security Server RACROUTE Macro Reference**, Appendix G and the **IBM Z Multi-Factor Authentication User's Guide**.

The Maintenance Facility

Overview

InterSession provides an maintenance facility that you use to add, modify, and/or delete the following:

- User Profiles
- Models
- Application Profiles
- Session Scripts
- Screen Layouts
- Printers
- Interfaces
- Services
- Help screen text
- System Options and APPL pools

The maintenance facility can only be accessed by users defined to InterSession as System Administrators.

Note: The following text assumes that the PF key assignments have not been changed from their default values. If they have been changed, use the corresponding keys as appropriate.

System Administrators

A user defined as a System Administrator can access the maintenance facility. There must be at least one System Administrator defined for your installation, but there can be as many System Administrators as you want. This authorization is specified in the User Profile.

Distributed User Profile Maintenance

In a large organization, the largest maintenance task will be to keep the User Profiles up to date. InterSession allows you to distribute the responsibility for User Profile maintenance without having to assign complete System Administrator authority.

You can authorize one or more users to be able to update User Profiles only. The scope of authorization may also be restricted to only being able to modify User Profiles belonging to a specific group (or number of groups). This authorization is specified in the User Profile.

You can also restrict User Profile maintenance so that users cannot authorize another user for any InterSession feature that they themselves are not authorized for. The following features are restricted:

- Master Operator
- Update info screens
- Terminal lock admin
- Can change password
- Number of sessions
- Number of terminals

In addition to the above types of user administrators, a user may be given the authority to update his own User Profile.

The Maintenance Selection Screen

To enter the maintenance routines, type MAINT on the menu. The following screen will be displayed:

```

InterSession ----- Maintenance, Selection ----- Version 8.1.00
Users:
  New/List ==> █   User or Group ==>           Copy ==>
Models:
  New/List ==>           Model ==>           Copy ==>
Shared Applications:
  New/List ==>           Application ==>       Copy ==>
Session Scripts:
  New/List ==>           Script ==>           Copy ==>
Screen Layouts:
  New/List ==>           Screen Layout ==>     Copy ==>
Printers:
  New/List ==>           Printer ==>           Copy ==>
Interfaces:
  New/List ==>           Interface ==>         Copy ==>
Services:
  New/List ==>           Service ==>           Copy ==>
Help Screen Sets:
  New/List ==>           Help Screen Set ==>   Copy ==>
System Options and APPLpools:
  Password ==>
F1-help  F3-return
  
```

You use this screen to select any profile or specification that you want to add, maintain, or delete. When you create a new item, you can make the new one a copy of an existing one.

If you do not know the exact name of the item you want, you can request a list of all item for a particular type. You can then select the item you want from the list.

Note that this screen will look slightly different if your scripts and panels are located in PDS's, see below.

User Profiles and Personal Application Profiles

To display an existing User Profile, enter the user ID in the "User or Group" field.

To create a new User Profile, enter 'N' in the "New/List" field and the new User ID in the "User or Group" field. Optionally, you may enter the ID of an existing user in the "Copy" field. The new user/model will then start with the same profile information as the existing.

To obtain a listing of all Users, enter an 'L' in the "New/List" field.

To restrict the listing to certain IDs, enter one or more characters from the User id in the "User or Group" field, followed by an asterisk (*). For example, if you enter the letters CFG* in the "User or Group" field, the listing will contain all users with an id starting with the letters CFG.

To restrict the listing to certain group(s) of users/models, enter the group ID in the "User or Group" field, without any trailing asterisk. For example, if you enter the letters AV in the "User or Group" field, the listing will contain all users/models with a group code starting with the letters AV.

Note that a specific User Profile id cannot also be a Model id.

Models

To display an existing Model, enter the ID in the "Model" field.

To create a new Model, enter 'N' in the "New/List" field and the new Model ID in the "Model" field. Optionally, you may enter the ID of an existing model in the "Copy" field. The new model will then start with the same profile information as the existing.

To obtain a listing of all Models, enter an 'L' in the "New/List" field.

To restrict the listing to certain IDs, enter one or more characters from the Model id in the "Model" field, followed by an asterisk (*). For example, if you enter the letters CFG* in the "Model" field, the listing will contain all users with an id starting with the letters CFG.

To restrict the listing to certain group(s) of models, enter the group ID in the "Model" field, without any trailing asterisk. For example, if you enter the letters AV in the "Model" field, the listing will contain all models with a group code starting with the letters AV.

Note that a specific Model id cannot also be a User Profile id.

Shared Application Profiles

To display an existing profile, enter the application ID in the "Application" field.

To create a new Application Profile, enter 'N' in the "New/List" field and the new application ID in the "Application" field. Optionally, you may enter the ID of an existing application in the "Copy" field. The new application will then start with the same profile information as the existing application ID.

For a new Application Profile, you will receive a second screen where you must enter the "Application Type" and the position on the menu, relative to the other Applications already defined. The position is set by typing an existing application ID in the "Insert After ID" field. The new application will appear after the old application on the menu. If nothing is entered in this field, the new application will be placed at the end.

To obtain a listing of all applications enter an L in the "New/List" field.

You may rearrange the order in which applications are displayed on the menu screen by using this list of Application Profiles.

Session Scripts and Panels

Scripts are located in the InterSession INTSFLE VSAM file

To display an existing script, enter the script ID in the "Script" field.

To create a new script, enter N in the "New/List" field and the new script ID in the "Script" field. Optionally, you may enter the ID of an existing script in the "Copy" field. The new script will then be an exact copy of the existing script.

To obtain a listing of all scripts, enter L in the "New/List" field.

Scripts and panels are located in a separate PDS

```
Shared Applications:
  New/List ==>      Application ==>      Copy ==>
Session Scripts:
  Refresh/List ==>      Script ==>      Panel ==>
Screen Layouts:
  New/List ==>      Screen Layout ==>      Refresh only
                                     Copy ==>
```

To get a list of all script names, enter L in the "Refresh/List" field.

To view the script, enter the script name in the "Script" field.

When a script has been changed in the PDS, you need to refresh the script to get the changed script into InterSession. Type R in the "Refresh/List" field and the script name in the "Script" field.

Panels (always in a separate PDS)

If you use panels, both the panels and the scripts must reside in separate PDS's. The only command related to panels is when a panel has been changed in the PDS. To get the changed panel into InterSession, type R in the "Refresh/List" field and the panel name in the "Panel" field.

Screen Layouts

To display an existing Screen Layout, enter the layout ID in the "Screen Layout" field.

To create a new Screen Layout, enter N in the "New/List" field and the new layout ID in the "Screen Layout" field. Optionally, you may enter the ID of an existing layout in the "Copy" field. The new Screen Layout will then be an exact copy of the existing layout.

To obtain a listing of all Screen Layouts, enter L in the "New/List" field.

Printers

To display an existing printer, enter the printer id in the "Printer" field.

To define a new printer, enter N in the "New/List" field and the printer id of the new printer in the "Printer" field. Optionally, you may enter the ID of an existing printer in the "Copy" field. The new printer will then be a copy of the existing printer. You will see a second screen where you have to specify the printer type.

To obtain a listing of all printers currently defined, enter L in the "New/List" field.

Interfaces

To display an existing interface, enter the interface name in the "Interface" field.

To define a new interface, enter N in the "New/List" field and the id of the new interface in the "Interface" field. Optionally, you may enter the ID of an existing interface in the "Copy" field. The new interface will then be a copy of the existing printer. A second screen will be displayed where you have to specify the interface type of the new interface.

To obtain a listing of all interfaces currently defined, enter L in the "New/List" field.

Services

To display an existing service, enter the service name in the "Service" field.

To define a new service, enter N in the "New/List" field and the id of the new service in the "Service" field. Optionally, you may enter the ID of an existing service in the "Copy" field. The new service will then be a copy of the existing. A second screen will be displayed where you have to specify the service type of the new service.

To obtain a listing of all services currently defined, enter L in the "New/List" field.

Help Screens

To display existing help screens, enter the ID in the "Help Screen ID" field.

To create a new set of help screens, enter N in the "Type" field and the new ID in the "Help Screen ID" field. Optionally, you may enter the ID of an existing help screen set in the "Copy Help Screen" field. The new set of help screens will then be an exact copy of the existing set.

To obtain a listing of all sets of help screens, enter L in the "Type" field.

System Options / APPLpools

To display / alter the System Options or the Application Pools, enter your current InterSession password in the "Type your password" field.

The System Variables

A number of variables can be used in the screen panels of a Screen Layout, in a Session Script or in the field “Data to pass to system” of an Application Profile. They are all of read-only nature.

A variable must be prefixed by a meta character, which is the percent sign (%), or in Session Scripts also an ampersand (&) or “at” sign (@).

Not all variables are applicable everywhere. If not, they will be replaced by the string “n/a”.

Note that some variables have an alias for backward compatibility reasons:

Variables used in Scripts and in Screen Layouts

VER	InterSession version
ML	InterSession maintenance level
APPLID	InterSession APPLid , ie INTSESS
SITE	InterSession site id
MVSI	z/OS system name
SNM	z/OS system name
TI	Terminal id
NETNAME	Terminal id
LM	Terminal logmode
TT	Terminal type
IP	TN3270 client ip address
IPHEX	TN3270 ip address in hex
CP	Terminal codepage
PTT	PassTicket based on the terminal id
TD	Data from main menu command
C	Century, two chars
Y	Year, two chars
M	Month, two chars
D	Day, two chars
JD	Julian day, three chars
DN	Day name, three chars
MN	Month name, three chars

YMD[s]	YY/MM/DD [s] = separator char, ex "%YMD-" => YY-MM-DD
DMY[s]	DD/MM/YY [s] = separator char
MDY[s]	MM/DD/YY [s] = separator char
HO or H	Hour
MI or I	Minute
SE or S	Second
TIME	HH.MM
HMS[s]	HH:MM:SS [s] = separator char
HL	Help key
V1	Misc key
RT	Return key
V2	Misc2 key
BW	Bwd key
FW	Fwd key
CA	Cancel key
BW/FW	Bwd/fwd key
(nn,nn)	Screen row/col
(nnnn)	Screen position
UI	User id
UU	User id on the sign on screen, first char = underscore
USERID	User id
UG	InterSession user group
RG	RACF user group
UN	User name
PW	8-char password
PWO	8-char password, obscured with User Id
PSWD	8-char password
PP	9-100 char passphrase
PPO	9-100 char passphrase, obscured with User Id
LP	Logon password or passphrase, depending on which was used to sign on to InterSession
LPO	As LP, but obscured with User Id

LPLEN	Logon password / passphrase length Example: IF %LPLEN > 8
NP	New 8-char password
NPP	New 9-100 char passphrase
VNP	Verify new 8-char password
VNPP	Verify new 9-100 char passphrase
MFA1	Multi-factor PassCode given as the user's password
MFA2	Multi-factor PassCode given as the user's new password
MFA3	Multi-factor PassCode be given as the user's passphrase
MFA4	Multi-factor PassCode given as the user's new passphrase
MFA5	Multi-factor PassCode given as the user's group
EPW	Encrypted password
OPW(n)	Old password, n=1-3
OPW	Old password 1
OPSWD	Old password 1
OPP(n)	Old passphrase, n=1-3
OPP	Old passphrase 1
PT PTU	PassTicket based on the user id
PI	Printer id
PRINTER	Printer id
CI	CICS opid
UD	User data from exit
D1-8	User Profile data field 1-8
TC	Heading text center
TS	Heading text start
HDLINE	Heading line
IMSG	Instruction/error message
EMSG	Error message
LN	Language number
AC SC	Application line command. Valid command codes are the codes defined for start, termination and removal of sessions.
AU SU U	Application line command as above, first char = underscore
V	Application line command as U above, except that %V only

	occupies one screen position. Note that this is not WYSIWYG.!
AN SN	Application name
ANP SNP	Application name protected
AD SD	Application description
ADC AD	Application description centered
AH SK	Application hot key
ASK SP	Application start PF key. Each application on the menu screen will be assigned a PF key from 1 and upwards. The PF key can only be used on the menu screen.
ASKND	As ASK, Network Director style
ASN SR	Application start number. Each application on the menu screen will be assigned a number from 1 and upwards. The numbers can be used for application selection. For numbers 1-24 the corresponding PF key can also be used. Can only be used on the menu screen.
AS SS	Application status. The application status texts can be changed in the Screen Layout.
AI SI	Application info. Can be "??" if not available, an availability time set by a Master Operator or "!!" if a background session update is pending.
AX SX	Application comment. If the Master Operator has entered a commentary text, this variable contains an asterisk "*".
DP	Application Profile field "Data to pass to application"
AP SA	Session applid/ipaddr
APN SY	Main menu command, where the user enters the name of an application, or a command
APNND	As APN, Network Director style
AK AKP	Attention key Attention key, protected
JK JKP	Jump key Jump key, protected
CK CKP	Command key Command key, protected
CC	Command prefix

CCP	Command prefix, protected
IFA1-4	MSGBOX input fields 1-4, characters as is, in Session Script command MSGBOX only
IFU1-4	MSGBOX input fields 1-4, characters in upper case, in Session Script command MSGBOX only

Variables used in Scripts only

AID	The 3270 key used to send data when on the native application screen, ie ENTER, CLEAR, PF1 etc
A1 A1 A2 A4	Predefined numeric variables used for arithmetic operations (not read-only)
CURSOR	Cursor position on the native application screen, 1-max screen size, ie 1920 for a 24x80 screen
CURSROW	Cursor row number on the native application screen 1-max line
CURSCOL	Cursor column number on the native application screen, 1-max col
LrOC	Screen position after a search, 1-max screen size, ie 1920 for a 24x80 screen
LOCROW	Screen row number after a search 1-max line
LOCCOL	Screen column number after a search 1-max col
LOOPCNT	Number of statements executed in a script
MAXWAIT	Max number of seconds the script will wait for application input
SCREEN	Without substring, the entire screen contents, size=screen size, ie 1920 bytes With substring,,ie SCREEN((81,240) contains lines 2—3.
SCRNSIZE	Real terminal screen size, ie 1920
SCRNROW	Real terminal number of rows, ie 24
SCRNCOL	Real terminal number of columns ie 80
SCRNFLD	After a search, SCRNFLD contains screen data from the found position to the end of the screen field.
TAID	The 3270 key used to send data when on a Panel screen, ie ENTER, CLEAR, PF1 etc
TCURSOR	Cursor position on the Panel screen, 1-max screen size, ie 1920 for a 24x80 screen
TCRSROW	Cursor row number on the Panel screen 1-max line

TCRSCOL	Cursor column number on the Panel screen, 1-max col
ZPANEL	Panel name as specified in the DISPLAY command

Installation-defined Variables

In the InterSession installation, up to ten variables can be defined, for use in Session Scripts and in the InterSession Screen Layouts. They are system-wide read-only variables populated with data from External Security. The variables defined here will be populated at user sign on time.

Note that if you are using the Sysplex functions, these variables must be defined in all instances, since they belong to the System Options.

See the section **System Options, Scripting** for more information.

Substrings in Variables

In Session Scripts and in the Application Profile field "Data to pass to application" you can substring variables.

Example:

%AN(3,4)

If the %AN variable (Application name) contains **VCICS32** the above spec will result in the string **ICS3**.

Note that substrings can not be used in the Screen Layouts.

Getting Help on the Application Variables

Anywhere in the maintenance routines you can press the help key (default PF1) to get help on the current screen. While on any help screen, press PF1 again to get help on the application variables:

```

InterSession ----- Help -----
Variables

The variables may be specified on the screen panels, in the System Profile
field Data to pass to system and in session procedures.
They must be prefixed by a meta character, which can be a percent sign %
and in session procedures also an ampersand &.
Not all variables are applicable everywhere. If not they will expand as "n/a".

VER      System version      UI UU  User id
ML       System maint level  USERID User id
APPLID   System applid      UG     User group
SITE     System site id     UN     User name
PW       Password
PP       Passphrase
TI       Terminal id        NP/NPP New password/phrase
NETNAME  Terminal id        VNP/VNPP Verify new password/phrase
LM       Terminal logmode   EPW    Encrypted password
TT       Terminal type      OPWL-3 Old password 1-3
IP       TN3270 client ip address OPSWD  Old password 1
IPHEX    TN3270 ip address in hex PT     Pass ticket
CP       Terminal codepage  RG     RACF user group
TD       Data from main menu cmd

F3-return  F7/8-bwd/fwd

```

User Profile Maintenance

User maintenance is composed of three types of information:

- Basic data contained on three screens
- Shared application access and personal Application Profiles
- Application sequence as seen on the user's menu screen.

User Profile Basic Data

If you want to maintain a User Profile, enter the user ID in the "User/Group ID" field on the maintenance selection screen. A screen like the following will be displayed:

```

InterSession ----- Maintenance, User Profile -----
User Id ADCDMST          Basic Data 1/3

      User Name ==> first user          Access ==> External
      Group ==> GROUPCC          Last access date ==> 060824
      CICS opid ==> ADC          Revoke date ==>
      Screen Layout ==> DEFAULT          Two-level menu ==> DEF
Check user with extsec ==> YES          Max application sessions ==> 010
Password duration days ==> N/A          Max terminal sessions ==> 005
System administrator ==> YES          Terminal idle timeout ==> DEF
Update user profiles ==> YES          Standby at timeout ==> DEF
  Only with group ==>          Standby idle timeout ==> DEF
Maintain own profile ==> YES          Application session timeout ==> DEF
  Master Operator ==> YES          widow session timeout ==> DEF
Terminal lock admin. ==> YES          Use multiple entrances ==> DEF
  Only with group ==>          Background update action ==> ALARM
Can change password ==> YES          Mailbox open ==> YES
Update info screens ==> YES          Show immediate messages ==> YES
Use ad-hoc sessions ==> YES          Print receiver profile ==> NO
  New password ==>

'Delete' for removal ==>
F1-help  F2-applications  F3-return  F7/8-bwd/fwd

```

An explanation of the fields follows:

User Name

The full name of the user.

Group Code

It is recommended that every user is assigned to a group. This allows the maintenance responsibilities for User Profiles to be split among multiple users or administrators, each being responsible for one or more groups.

When assigning group codes, remember that a single user can be allowed to maintain several groups, as long as the group codes all begin with the same letter or letters.

CICS opid

The operator ID that InterSession will establish for the user for sessions within a CICS environment.

Screen Layout

Normally, the Screen Layout to be used is based upon the user's terminal ID. However, if a user always wants a specific layout, no matter which terminal he or she is using, the layout ID may be given here.

Check user with extsec

Specify YES or NO. If set to NO, InterSession will not check this user against External Security, but rather use all the internal specifications for this user, like password rules, application access etc.

Password duration days

Each user can have their own password expiration interval. Specify DEF here to use the default specified in the System Options.

System Administrator

Specify YES or NO to indicate whether or not this user is a System Administrator.

Update User Profiles

Specify YES, NO or RES (restricted). If you specify YES, you have assigned the authorization to update User Profiles only. This user can alter and create new User Profiles just like a System Administrator. If you specify RES, this user may only authorize other users to applications that this user is authorized to use.

Only with group code (Update User Profiles...)

If this user is authorized to update User Profiles only (YES or RES), this authorization may be restricted to one or more groups of users. For instance, if you specify TE (or TE*) here, this user can only update users that belong to groups beginning with the letters TE.

Maintain own profile

Specify NO, YES, RES or SEQ. Unless already authorized (as a System Administrator or with Update User Profiles), the user may be allowed to update his own profile, which is done via the normal MAINT application.

YES means that the user will go directly to his own User Profile screen when MAINT is selected, where all aspects of the user's own profile may be viewed and changed.

RES is a more restrictive setting than YES, where the user will not be allowed to change some of the more sensitive settings. Also, it is not possible to view or alter the application access list.

SEQ is the most restrictive setting. When selecting MAINT, the user will go directly to the application sequence screen, where the sequence of the user's applications may be changed. This is the only screen that the user can see.

Master Operator

Specify YES or NO to indicate whether or not this user is a Master Operator.

You can also specify RES (restricted) to disallow the use of the special operator commands (/SHUTDOWN, /OPEN, etc.).

Terminal lock admin.

Specify YES or NO to indicate whether or not this user is allowed to use the terminal lock routine in order to unlock terminals.

Only with group code (Terminal lock admin....)

A Master Operator or a user with terminal lock administration authority can be restricted to one or more groups of users. For example, if you specify TE (or TE*) here, this user can only perform functions for users that belong to groups beginning with the letters TE.

Can change password

Specify YES or NO to specify whether or not this user is to be able to change the password. If set to NO and the user's password is expired, he will be unable to sign on to InterSession.

Note that this also applies to users in External Security (RACF etc.).

This setting can be useful if the user profile is used by more than one individual. You can then specify NO to prevent one individual from changing the password and thus locking out the other individuals using this profile.

Update info screens

Specify YES or NO to indicate whether or not this user is to be authorized to update information screens. (Users who are designated as Master Operators have this authority automatically.)

Use ad-hoc sessions

Specify YES or NO to indicate whether or not this user is to be authorized to start ad-hoc sessions with the Start command on the menu screen.

Access

For a User, this field indicates whether user access is "Enabled" or "Revoked". To change the user access, type an E or R in this field. To enable a revoked user, you may also type Resume in this field. If the user is defined to External Security, this field will contain "External" and can not be changed.

To convert this profile to a Model, type "model" in this field. When you press enter, this User Profile will be converted to a Model and you will go back to the main selection screen or the User listing.

Last access date

This is a read-only field displaying the date when this user last used InterSession.

Revoke date

If user access is revoked, this field contains the date when the revoke status was set. If user access is enabled, you may enter a future date here to specify when the user's access will be revoked automatically. (This can be useful if you have personnel working for your company on a temporary basis.)

Two-level Menu

Specify NO, YES or DEF (default). If you specify DEF the Screen Layout will decide if a one- or two-level menu will be used. NO will result in a one level menu.

Max application sessions

For a single session user, specify 01. For a multiple session user, specify the maximum number of concurrent sessions the user is allowed to have at one time.

Max terminal sessions

By default this value is 01, which means that you are only allowed to use this user id on one terminal at a time. If you want to use this user id on more than one terminal, specify the limit here. When you reach this limit, the sessions from the terminal with the oldest sign on will be transferred to the current terminal. If you specify 99, there will be no limit to the number of concurrent terminals that can be logged on with this user id. This setting is important if you use more than one Entrance, see below.

Terminal idle timeout

Specify the number of minutes that a terminal can be left unattended after which the sign-on screen will be displayed.

DEF indicates the system default value should be used.
999 indicates that the timeout feature is not used.

See the chapter “The Timeout Functions” for details.

Standby at timeout

If you want the standby screen to be displayed when a terminal timeout occurs, specify YES. If you want the sign on screen to be displayed, specify NO. To use the system default value, specify DEF.

Note: If a user has signed on to InterSession with a PassTicket or with an MFA product, the Standby Screen will not be sent to the terminal. Instead, the Sign On Screen will be sent.

Standby idle timeout

Specify the number of minutes, starting from the time the standby screen has been displayed on the terminal, after which the sign on screen will be displayed.

DEF indicates the system default value should be used.
999 indicates that the timeout feature is not used.

See the chapter “The Timeout Functions” for details.

Widow session timeout

After a terminal timeout where the sign on screen is displayed, any active application sessions are considered to be “widow” sessions. These sessions will be terminated after the time interval in minutes specified in this field.

DEF indicates the system default value should be used.
999 indicates that any widow sessions should never be terminated.

See the chapter “The Timeout Functions” for details.
This setting is important if you use more than one Entrance, see below.

Application session timeout

On an individual Application Profile you may specify that the User Profile value for application idle timeout is to be used, by setting “Application session timeout” in the Application Profile to “USR”. This value will then be used.

DEF indicates the system default value should be used.
999 indicates that the timeout feature is not used.

See the chapter “The Timeout Functions” for details.

Mailbox open

Specify YES or NO. If you do not want any mail or messages to be sent to this user, specify NO.

Show immediate messages

Specify YES or NO. If you do not want any immediate messages to be shown for this user (and possibly disturb the user), specify NO. Any immediate messages sent to this user will then be saved in the user’s mailbox.

Use multiple entrances

If you use more than one entrance, specify YES. This will keep all applications started in one instance together. If you have multiple terminal sessions, each to a separate entrance and then disconnects two or more terminal sessions, the applications is grouped together on their instances. When you reconnect, the application sessions will reappear in their original entrances.

When using multiple entrances, **Widow session timeout** should not be zero, and **Max terminal sessions** must be greater than one.

Background update action

What action to be taken when a background session is updated.

NO No action to be taken.
ALARM The terminal alarm will sound when the user press the Enter key.
SWITCH Automatically switch to the session which has been updated.
MENU Automatically switch to the menu screen.

Print receiver profile

The Mail/Message System is capable of sending mail directly to a printer instead of a user’s mailbox. To do this, a User Profile must exist with a printer specified and with this option set to YES. When sending mail to this user id it will be printed on the specified printer. Note that such a User Profile can NOT be used for normal processing; i.e. it is not possible to log on to InterSession with such a user id. All normal User Profiles MUST have this option set to NO.

New Password

This is not used if the user is defined in External Security; the field is then protected.

The following applies only to users not defined in External Security.

A new user is not assigned a password unless you enter one into this field. This means that the user can get into InterSession the very first time without a password and would provide the first password at that time. The password is never displayed, but an administrator may assign a new password here (for example if the old password is forgotten).

In the System Options, you may have defined an “expired password value” (any eight-character string). If you assign the new password this value, the password is immediately expired, and the user is forced to enter a new password at next sign on.

'Delete' for removal

To delete this User Profile, enter the word 'delete' in this field.

As mentioned earlier, the basic data of the User Profile is displayed on three screens. To see the second screen, press PF8. A screen like the following will be displayed:

```
InterSession ----- Maintenance, User Profile -----
User Id ADCDMST          Basic Data 2/3
Page => █ Models 01-10   Names from RACF   02 models assigned
====> SAMPMDL1 =====> SAMPMDL2 =====> =====>
====> =====> =====> =====> =====>

Attn key functionality ==> DEF Top line menu initial command ==> S
  Attention key ==> Attn      Printer id ==>
    Jump key ==> PA1        Print header ==> DEF
      Command key ==> ENT    Form feed after header ==> DEF
        Command prefix ==> ..
Autostart applications ==> =====> =====> =====>
      =====> =====> =====> =====>
    Data field %D1 ==>
    Data field %D2 ==>
    Data field %D3 ==>
    Data field %D4 ==>
    Data field %D5 ==>
    Data field %D6 ==>
    Data field %D7 ==>
    Data field %D8 ==>
F1-help  F2-applications  F3-return  F7/8-bwd/fwd
```

(You can use PF7 and PF8 to move between the three screens of basic data.)

An explanation of the fields follows:

Models nn-nn

If you leave these fields blank, you can use the application access screen for this user. The application access screen is used to authorize the user for individual applications (unless you are using External Security for this purpose).

If you don't want to authorize each user for application access individually, you can create one or more Models, each with the required set of authorized applications, for different groups of users. You can specify up to 200 Model names, and the user will get application access as the combination of the Models specified.

You have twenty screen pages where each page holds ten Models.

The first page is shown by default. To go to another page, type the page number 1-20 in the **Page** field.

Attn key functionality

Specify what action the attention key should result in.

TLM	The attention key produces the Top Line Menu.
TV	The attention key mimics the CA-Teleview session manager behaviour.
SS	The attention key mimics the CL/Supersession session manager behaviour.
TPX	The attention key mimics the CA/TPX session manager behaviour.
DEF	The action will be taken from this setting in the Screen Layout.

Attention key

Jump key

Command key

Command Prefix

These fields are used to provide the "Attention Key" to activate the top line menu and to provide defaults for the user's session keys. (See "Screen Layout 3/19".) Unless you have protected the "Session key" fields on the menu, each user will be able to change these values.

Autostart applications

Specify up to eight name(s) of the Application Profiles which should be automatically started at Sign On. Refer to the section on "Autostart Application After Sign On" for more information.

Data fields %D1-%D8

These fields can be used to specify user specific data that can be passed to different applications (for example, accounting codes, etc.) Each field can be up to 32 bytes long.

Data fields can be typed in mixed case by enclosing them in single quotes, like this: 'Data in MIXED case'.

Data fields can be specified in hexadecimal, like this: X'nn..nn'

These fields can be marked as hidden and/or protected. See "Screen Layout 10/13".

Top Line Menu initial command

Specify a command character from the top line menu to be automatically executed when the attention key is pressed.

Printer id

Specify the name of the VTAM printer to be used as the destination for "hardcopy" screen prints, and MMS messages that are printed.

Print header

Specify YES or NO to indicate whether or not you want InterSession to print a heading page prior to each "hardcopy screen print" or MMS message printed.

Form feed after header

Specify YES or NO to indicate whether or not you want InterSession to print the heading page on a separate page, or on the same page as the screen print or message.

To see the third screen, press PF8. A screen like the following will be displayed:

```
InterSession ----- Maintenance, User Profile -----
User Id ADCDMST          Basic Data 3/3

Hot keys:
PF1 ==> > PF9 ==> > PF17 ==> >
PF2 ==> > PF10 ==> > PF18 ==> >
PF3 ==> > PF11 ==> > PF19 ==> >
PF4 ==> > PF12 ==> > PF20 ==> >
PF5 ==> > PF13 ==> > PF21 ==> >
PF6 ==> > PF14 ==> > PF22 ==> >
PF7 ==> > PF15 ==> > PF23 ==> >
PF8 ==> > PF16 ==> > PF24 ==> >

Hot keys active:
  On menu screen ==> DEF      In Top Line Menu ==> DEF
  In applications ==> DEF - only with Cmd Prefix ==> DEF

Misc settings:
  Virtual terminal id ==>

Web interface:
  Show configuration link ==> YES

F1-help  F2-applications  F3-return  F7/8-bwd/fwd
```

On this screen you may change the user's Hot keys and web parameters. You can use the Hot Keys in two ways:

a) Type an application name (Application Profile id) in the PF key field. When the user presses this PF key, a session switch to this session will occur, or if the session is not active it will be started. You may also type an R in the second field associated with the PF key. When the new session is terminated, return will then not be made to the menu screen but to the session that was active when the Hot Key was hit.

b) Type a session command in the PF key field, complete with the Command Prefix. Accepted commands are N, P, M, T and H. For instance, ..H in the PF24 field means that a screen hardcopy will be taken when the PF24 key is pressed.

Hot keys active:

These settings do only affect Hot Keys connected to an Application Profile.

There are three settings: NO, YES or DEF (DEF = the default setting in the System Options). The default value is DEF.

On menu screen

If YES, the Hot Keys are active on the application menu screen.

In Top Line Menu

If YES, the Hot Keys are active in the Top Line Menu, Sessions window.

In applications

If YES, the Hot Keys are active in all application screens. To be able to use the Hot keys as regular PF keys in the application, you should set the next parameter to YES:

-only with Cmd Prefix

If YES, the Hot Keys will only be intercepted if the user has typed the Command Prefix in the first input field of the application screen.

Virtual terminal id

If specified, this VTAM ACB / APPLid name will be used when starting application sessions. All POOL and UNIQUE specifications on the Application Profiles will be ignored for this user.

If the name contains asterisks, these will be replaced by the corresponding positions of the terminal id the user is signed on to.

The name may also be globally altered before use by the Startup Parameter VTERMMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. Any characters in the mask will replace the corresponding positions of this name. See "Defining the Startup Parameters" in the chapter "Sysplex Functionality".

CICS security profile

If the InterSession/CICS programs are installed in CICS, you may want to use this field. Specify the name of another User Profile where the CICS security tables are to be fetched from during CICS sign on.

Show configuration link

YES or NO. If set to NO the user will not see the configuration link on the web menu screen, and can therefore not make any changes to the personal configuration.

User Application Access and Personal Application Profiles

To view the applications screen for a user, press PF2 while one of the three basic data screens is on display. (If you have specified an application access profile, the application access screen will not be shown.) A screen like the following will be displayed:

```

InterSession ----- Maintenance, User Profile -----
User Id ANNA          Shared Application Access, Personal Appl Profiles
Enter +/- and name of Shared Application ==> | (or in table below)
Enter name of new Personal Appl ==>

INTAPPL  Internal  MYAPP  My applica
+PROF    Your user
+MMS     Message/m
+STBY    Standby s
+OFF     Logoff In
INFO     Informati
+OPEN    Open hour
EXTAPPL  External
-CICS    A CICS sy
+IMS     An IMS sy
+CMS     VM/CMS
+TSO     TSO/ISPF
+NVIEW   Network c
+T3270   Mainframe
+START   Window to
Personal Systems
F1-help  F2-application sequence  F3-return  F7/8-bwd/fwd

```

This screen is used to assign shared application access and to maintain the personal Application Profiles for a user.

If you have more applications than will fit on one screen, you can scroll backward and forward, using PF7 and PF8. To view the sequence of the shared applications, press PF2. To return to the basic data, use PF3.

Shared Application Access

All shared applications defined at your installation are shown, with a plus sign (+) if the user is authorized for the application, and a minus sign (-) if the user is not authorized for the application. To change the authorization status for this User Profile, you simply position the cursor and set plus and minus signs for the individual applications.

You can optionally change the authorization for specified shared applications by entering a + or - and the application name in the first field on the screen, for example "+nview".

If you have User Profile authority with restricted update, you will only see the applications you are authorized for.

Note: If you are using an External Security Manager such as RACF or TopSecret, you may not be able to change the application access here, depending on the settings in External Security.

Personal Application Profiles

Below the heading "Personal Applications" you will find a list of all personal Application Profiles defined for this user. To maintain any of these, position the cursor and press ENTER.

To add a new personal Application Profile, enter the new name in the second field of the screen and press ENTER.

In each case you will switch to Application Profile Maintenance, see below. When you have finished updating the Application Profile, you will return to this screen.

User Application Sequence

To view the application sequence for a user, press PF2 on the previous screen. A screen like the following will be displayed:

```

InterSession ----- Maintenance, User Profile -----
User Id ANNA          Systems Sequence          (In standard sequence)
Pos Application      Pos Application          Pos Application
H01 INTAPPL Internal ap 014 START window to s
001 MAINT InterSessio 015 MYAPP My applicat
002 STAT InterSessio
003 TLOCK Terminal lo
004 PROF Your user p
005 MMS Message/mai
006 STBY Standby scr
007 OFF Logoff Inte
H02 INFO Information
008 OPEN Open hours
H03 EXTAPPL External ap
009 IMS An IMS syst
010 CMS VM/CMS
011 TSO TSO/ISPF
012 NVIEW Network con
013 T3270 Mainframe T
Move Start:  End: After: Command ==>
F1-help F3-return F7/8-bwd/fwd

```

This screen is used to change the order of the applications on the menu screen.

If you have more applications than will fit on one screen, you can scroll backward and forward, using PF7 and PF8. To return to the application access screen, use PF3.

You can arrange the applications in any order. If the sequence is not changed, the applications on the menu screen will be displayed in the order they are listed in the Shared Applications Listing (see section below on Application Profile maintenance), followed by the personal applications.

The applications are numbered from 1 and upwards. The Header applications are not part of this sequence but are numbered separately as Hnn. They are however in correct sequence as they appear on the menu screen.

In the heading line, the text "**In standard sequence**" appears if the sequence is unaltered, i.e. the same as the Shared Applications Listing.

To alter the sequence, use the **Move** fields. For example, if you want to move the applications starting with IMS and ending with TSO to the end of the list, enter the command:

Move Start: 11 End: 13 After: 17

The screen will be rearranged. To move applications to the beginning of the list, specify '0' in the 'After' field. To move a header application, prefix the header number with H as listed, for example **H02**.

If you have a user-defined sequence and remove an application from the authorization list (by using the **minus sign** on the application access screen), it will be removed from the sequence list and replaced by an empty gap. The sequence numbers will not be changed. When you add an application to the authoriza-

tion list (by using the **plus sign** on the application access screen), it will be added to the end of the sequence list.

Commands

You may enter the following commands:

STDSEQ Sets the applications in the same order as they are listed on the shared applications listing.

REVERT After a STDSEQ command, restore the application sequence to the state it was before the STDSEQ command was issued.

COMPRESS remove all "gaps" in the list.

DEL nnn delete gap number nnn.

INS nnn insert a gap after number nnn.

Note! For all commands, the sequence numbers will be rearranged!

User Profile Listing

If you want to select a User Profile from a list, enter L under "User Profiles" on the maintenance selection screen. A screen like the following will be displayed:

User Id	Name	Group	Sysadm	Upd.user	Mastop	Access
ANNA	Anna Hagman		YES	YES	YES	Enabled
CAL	Cal Aström		YES	YES	YES	Enabled
GUEST	Guest		NO	NO	NO	Enabled
HAI	Hans Ivarsson		NO	NO	NO	Enabled
MATTEUS	Matteus Sjögren		NO	NO	NO	Enabled
TOSV	Torbjörn Svensson		NO	NO	NO	Enabled

F1-help F3-return F7/8-bwd/fwd

To select a User Profile from this screen, position the cursor to a user ID and press ENTER. When you press PF3 on the User Profile screen, this screen will be redisplayed.

If you have more users than will fit on one screen, you can scroll backward and forward using PF7 and PF8.

Model Maintenance

Model maintenance is much the same as User maintenance.

Models contains a subset of User data, but also based on three types of information:

- Basic data contained on three screens
- Shared application access
- Application sequence as seen on the user's menu screen.

Model Basic Data

If you want to maintain a Model, enter the Model id in the "Model" field on the maintenance selection screen. This is the three screens with basic data:

```

InterSession ----- Maintenance, Model Profile -----
Model Id SAMPMDL1          Basic Data 1/3

  Model description ==> Sample Model 1
    Group ==>
    Screen Layout ==>
    Two-level menu ==> DEF
  System administrator ==> NO
  Update user profiles ==> NO
    Only with group ==>
  Maintain own profile ==> NO
    Master Operator ==> NO
  Terminal lock admin. ==> NO
    Can change password ==> YES
    Update info screens ==> NO
    Use ad-hoc sessions ==> NO
    Max application sessions ==> 010
    Max terminal sessions ==> 001
    Terminal idle timeout ==> DEF
    Standby at timeout ==> DEF
    Standby idle timeout ==> DEF
    Widow session timeout ==> DEF
    Application session timeout ==> DEF
    Use multiple entrances ==> DEF
    Background update action ==> ALARM
    Mailbox open ==> YES
    Show immediate messages ==> YES

  'Delete' for removal ==>

F1-help  F2-applications  F3-return  F7/8-bwd/fwd

```

```

InterSession ----- Maintenance, Model Profile -----
Model Id SAMPMDL1          Basic Data 2/3

  Attn key functionality ==> DEF Top line menu initial command ==> S
    Attention key ==> Attn
    Jump key ==> PA1
    Command key ==> ENT
    Command prefix ==> ..
    Printer id ==>
    Print header ==> DEF
    Form feed after header ==> DEF
  Autostart applications ==>
    ==>
    ==>
    ==>
    Data field %D1 ==>
    Data field %D2 ==>
    Data field %D3 ==>
    Data field %D4 ==>
    Data field %D5 ==>
    Data field %D6 ==>
    Data field %D7 ==>
    Data field %D8 ==>

F1-help  F2-applications  F3-return  F7/8-bwd/fwd

```

```
InterSession ----- Maintenance, Model Profile -----
Model Id SAMPMDL1          Basic Data 3/3
Hot keys:
PF1 ==> > PF9 ==> > PF17 ==> >
PF2 ==> > PF10 ==> > PF18 ==> >
PF3 ==> > PF11 ==> > PF19 ==> >
PF4 ==> > PF12 ==> > PF20 ==> >
PF5 ==> > PF13 ==> > PF21 ==> >
PF6 ==> > PF14 ==> > PF22 ==> >
PF7 ==> > PF15 ==> > PF23 ==> >
PF8 ==> > PF16 ==> > PF24 ==> >
Hot keys active:
  On menu screen ==> DEF      In Top Line Menu ==> DEF
  In applications ==> DEF - only with Cmd Prefix ==> DEF
Misc settings:
  Virtual terminal id ==>
Web interface:
  Show configuration link ==> YES
F1-help  F2-applications  F3-return  F7/8-bwd/fwd
```

Application access in Models

To define which Applications a Model should represent, follow the same procedure as with User Profile:

PF2 on one of the Basic Screens will take you to the Application access screen.

PF2 on the Application access screen will take you to the Application sequence screen.

Application Profile Maintenance

Application Profile maintenance is used for both shared and personal Application Profiles. The profile type is indicated on the screen. Application Profile maintenance consists of the following:

- Creating a new Application Profile using the new Application Profile screen
- Maintaining an existing Application Profile, using the Application Profile screens
- Rearranging the order of the applications, using the Application Profile listing screen (shared Application Profiles only).

New Application Profile

If you want to create a new Shared Application Profile, enter N (new) in the "Shared Application Profiles New/List" field of the maintenance selection screen.

A screen like the following will be displayed:

```
InterSession ----- Maintenance, New Shared Application Profile -----
Application id DEVPRO
      Application type ==> 
      Insert after id ==>          (Position on the menu screen)

Valid application type codes:
Vtam..... A VTAM 3270 application
TN3270... A Telnet 3270 application

MAint.... Maintenance routines
STAT.... Status/statistic routines
TLock.... Terminal lock maintenance
Uprof.... User profile routine
Msgsys... Message/mailbox application
STBy.... Standby feature
Header... A heading line on the menu screen
INfo.... To create an information screen
Scrip... Selection script / Popup screen
Logoff... To logoff from the application

F1-help  F3-return
```

Application Types

Application types fall into three groups:

- For external applications
 - For internal applications
 - For miscellaneous use
-

Application Types for External Applications

Vtam	Is used for all VTAM 3270 applications, like TSO, CICS or CMS. Requires that the VTAM interface is activated.
TN3270	Represents the built-in TN3270 client. Is used for all applications with a TN3270 server (such as another mainframe system) or other 3270 applications accessible over the Internet. Requires that a TCPIP interface is activated.

Application Types for Internal Applications

Maint	Maintenance routines
STAt	Status/statistic routines
Tlock	Terminal lock routine
Uprof	User Profile maintenance
Msgsys	Message/mailbox application
STBy	Standby routine

Application Types for Miscellaneous Use

Script Represents an internal routine that must be used together with a script (Session Script). This type of application can be used to create a popup menu to select among specific actions, to start multiple applications with a single keystroke etc. See below for an example.

Header Represents a header. A header is used to group applications on the menu. It is displayed as a heading line on a one-level menu, or as a first-level application on a two-level menu. For a header, only the "Application type" field and the "Application text" fields can be entered.

Info Used to create an item on the menu to display information screens (with the information screen facility).

Logoff Will create an item on the menu that, when selected, will sign the user off from InterSession.

Main Menu Position

An application's position on the menu is established when you create the Application Profile. This is done by specifying an existing Application Profile name in the "Insert After ID field". If no name is entered, the new Application Profile will be added as the last profile. However, you can rearrange existing Application Profiles using the Application Profile listing screen (shared Application Profiles only). For more information on this, refer to "Application Profile List" later in this section. You can also rearrange the application sequence for each user. If a user has its own sequence defined, a new application will be added at the end of the list, regardless of the default position specified here.

Application Profile Screen 1/2, type VTAM

If you want to define or redefine an Application Profile that you have created, enter an Application Profile ID in the "Application ID" field on the maintenance selection screen. A screen like the following will be displayed. (The fields that actually appear on the screen will vary depending on the type of the Application Profile. The internal applications and the application types for miscellaneous use will have very few of the following fields. For example, for a header, most of the input fields are not applicable and not shown.)

This is an example of a VTAM application:

```

InterSession ----- Maintenance, Shared Application Profile 1/2 -----
Application id TSO                                Change application id ==>
  Application type ==> vtam                        Application start key ==>
    Menu level ==> 2                             Read terminal buffer ==> NO
    Hide application ==> NO                       3270 data compression ==> NO
    Authorization check ==> YES                   Appl will pass session ==> NO
    VTAM (netid.)applid ==> A06TSO
    Session applid type ==> POOL                  Lock pool applid to user ==> NO
    Session applid/Pool no ==> 1                  Appl sends first screen ==> YES
    Session start script ==> TSOON                Session portability ==> YES
    Session end script ==> TSOOFF                 Application idle timeout ==> DEF
    Codepage ==> DEF                             Web language code ==>
    Inquire appl status ==> YES                   Model terminal support ==> NO
    Data to pass to appl ==>
Application text, language codes 1-6:
1> TSO/ISPF                                     2>
3>                                                4>
5>                                                6>
'Delete' for removal ==>
F1-help  F3-return  F7/8-bwd/fwd

```

An explanation of the fields follows:

Change application ID

You can change the name of an Application Profile by entering a new name in this field.

Application type

You can change the type of the Application Profile by entering a new value in this field. If you do, however, the defaults may not be as described in this manual.

Menu level

Enter 1 or 2 depending on whether you want this application to appear on the first- or second-level menu (provided that a two-level menu has been requested, either in the Screen Layout or in the User Profile).

Hide application

Enter YES if you do not want the application to show on the menu screen. Default is NO.

Authorization check

Enter YES, EXT or NO to indicate whether the user's authorization should be checked.

- YES** The User Profile's application authorization data will be used to determine if the user is authorized to use the application.
- EXT** Your External Security Manager will be used for user authorization. (If no External Security Manager is active, EXT is equivalent to YES.)
- NO** Bypass all access control. The application will be available to all users.

Depending on the settings in the System Options, External Security, the setting YES can be equivalent to EXT.

VTAM (netid.)applid

Enter the VTAM netid (optional) and the VTAM APPLid of this application.

Session APPLid type

Enter: POOL, GROUP, UNIQUE or NONE.

- POOL** An unused application ID (ACB) will be selected from the pool specified in the APPLPOOL definitions.
- GROUP** This VTAM host subsystem can handle several sessions (a group of sessions) using the same ACB. This is true for applications like TSO.
- UNIQUE** The VTAM application ID is constructed by expanding the information in the "Session applid/Pool no" field.
- NONE** This application will only be used in pass mode, even if it is selected by a multiple-session user. NONE cannot be used if a Session Script is specified.

Session applid/Pool no [VTAM]

If "Session APPLid type" is POOL, this is the APPLpool number to be used when selecting application IDs.

If "Session APPLid type" is GROUP, specify the name of the VTAM application ID to be used.

If "Session APPLid type" is UNIQUE, specify a combination of 1) any System Variable, 2) any character(s) and 3) asterisks (representing the corresponding positions of the terminal netname).

Refer to the section on "Application Sessions" for more information.

Session start script

Session end script

Specify which scripts are to be executed when starting and ending the session. See the section on "Session Script Maintenance" for a description of scripts.

Codepage

If you are using different codepages (national character sets) for your applications and terminals, specify the applicable codepage number for this application. If it differs from the terminal codepage, automatic translation between the codepages will be made.

See also the section “National Characters and Codepage Support” for more information.

Inquire about appl status

Specify YES or NO.

If YES is specified, VTAM is queried for the status of the application.

If NO is specified, the application will always be shown as active on the menu. For cross-domain applications, you might want to set this value to NO.

Note: A change of this parameter will also affect all other Application Profiles with the same VTAM application ID.

Data to pass to application

For VTAM applications, you can enter logon data to be passed by VTAM to the application in the session bind process. The following types of data can be entered in this field in any combination:

Text	All characters and digits.
	Mixed case can be entered by enclosing it in single quotes: 'Data in MIXED case'
	Hexadecimal data may be entered as: X'nn..nn'
Variable	Any variable as listed under “System Variables” earlier in this manual.

Application start key

Specify a PF key or blank..

If a PF key is specified, the application can be started when pressing this key from the menu screen.

This is true for all users.

Read terminal buffer

Specify YES or NO.

If YES is specified, terminal image of a session will not be saved in virtual storage, until a session switch is requested. A Read Terminal Buffer command will then be issued to save the entire terminal buffer.

If NO is specified, the incoming 3270 data from the application and the terminal will be continuously merged together, and a Read Terminal Buffer will never be issued.

Refer to the section on "Application Sessions" for more information.

3270 data compression

To invoke the data compression feature, specify YES. Refer to the section on "3270 Data Compression".

Appl will pass session

Specify YES or NO.

If the application system issues CLSDST PASS after data has been exchanged on the session, code YES in this field.

Refer to the section on "Application Sessions" for more information.

Lock pool APPLid to user

Specify YES or NO.

Certain application systems, like IMS, will require this field to be set to YES. It means that once a new application ID from the pool is selected for a user, that application ID will be assigned solely to that user. The "lock" is released at midnight.

Refer to the section on "Application Sessions" for more information.

Appl sends first screen

Specify YES or NO.

Normally, the application system will send the first data to the terminal. However, if the terminal is to send the first data, specify NO in this field.

Refer to the section on "Application Sessions" for more information.

Session portability

Specify YES or NO.

YES means that an application session may be transferred from one terminal to another.

If you specify NO, the session will be canceled if you try to move it to another terminal.

Refer to the section on "Application Sessions" for more information.

Application idle timeout

Specify the value in minutes before an application session which have had no activity will be terminated. 999 indicates that the session will not be terminated due to inactivity. USR indicates that the idle timeout value should be taken from the User Profile. DEF indicates system default.

Web language code

This is the default language code used by the web browser, according to the ISO 639-1 standard. Note that InterSession does not check the validity.

Model terminal support

YES or NO. If YES, then InterSession will include a VTAM MTS vector in the application session start request. The Model name in the MTS vector will be set to the logmode entry name that InterSession has selected for the session. See the Customization section, Model Terminal Support, for more information.

Application text, language codes 1-6

This is the explaining text that is shown on the menu screen. If you are using more than one language, you can specify the text in up to six languages. The “Language number” in the Screen Layouts is used as an index in this text table.

'Delete' for removal

To remove the Application Profile, type the word 'delete' in this field.

There is a second Application Profile screen. To move between the first and second screen, use PF7 and PF8. For CICS options, use PF2.

Application Profile Screen 1/2, type TN3270

This is an example of a TN3270 application:

```
InterSession ----- Maintenance, Shared Application Profile 1/2 -----
Application id TN3270                      Change application id ==>
  Application type ==> TN3270              Application start key ==>
    Interface name ==> TCPIP                Read terminal buffer ==> YES
      Menu level ==> 2                     3270 data compression ==> NO
    Hide application ==> NO
    Authorization check ==> YES
      IP address(:port) ==> 127.0.0.1
        Device/LU name ==>
    Session start script ==>              Appl sends first screen ==> YES
    Session end script ==>                Session portability ==> YES
      Codepage ==> DEF                     web language code ==>
    Appl idle timeout ==> DEF

Application text, language codes 1-6:
1> Mainframe TN3270 server                2>
3> TCP/IP Interface must be active         4>
5>                                         6>

F1-help  F3-return  F7/8-bwd/fwd
```

Most fields are the same as for a VTAM type application.

An explanation of the fields specific to the TN3270 application type follows:

Interface name

Specify the name of the InterSession TCPIP interface profile.

IP address(:port)

Enter the IP address and the port (optional) of this application.

Device/LUname

If you want InterSession to send a device / LU name to the.TN3270E server, enter the name here.

The name can be in plain text, one or more System Variables (for example %UI, %TI, %D3) or a combination. For variables you may use substrings. The name can be up to 20 characters.

Examples:

TEST3592

%UI (1,4)WORK (If the user id is JERTHOM1 the resulting name will be JERTWORK)

%TI (2,6)%D3 (2,2) (If the terminal id is ISB35011 and Data field 3 of the User Profile contains TOMATOES the resulting name will be B35011MA).

Application Profile Screen 2/2

For applications of type VTAM or TN3270 there is a second Application Profile screen. To move between the first and second screen, use PF7 and PF8. For CICS options, use PF2.

Note that most of these fields are not applicable to TN3270 applications.

```
InterSession ----- Maintenance, Shared Application Profile 2/2 -----
Application id TSO
    Signoff at session end ==> NO
    3270 data trans. table ==>
    Passticket external security id ==>
    Perform background update action ==> YES
    Background update script ==>
    Bracket protocol conversion ==> YES
    Append %TD to 'data to pass...' ==> YES
    Propagate menu screen info ==> NO
VTAM Logmodes for Pass Mode (from terminal logmode table):
    SNA Logmode name ==>
    Non-SNA Logmode name ==>
VTAM Logmodes for Relay Mode (from INTSMTAB):
    SNA Logmode name ==>
    Non-SNA Logmode name ==>
    COS name ==>
CICS appl with I/S support ==> NO
F1-help F3-return F7/8-bwd/fwd
```

An explanation of the fields follows:

Signoff at session end

If YES is specified, when an application session created by this Application Profile ends, the sign-on screen will appear instead of the menu. (All active sessions will remain active.)

This option can be useful if you have dial-up connections. This prevents a dial-up caller from being able to use an existing sign on from a previously terminated call.

3270 data trans. table

The InterSession translate tables are primarily used to support National Character sets. With this option, you can specify a translate table to be used with this Application Profile. Refer to the section on "3270 Data Translation" for more information.

PassTicket External Security id

If you are using one of the %PT, %PTU or %PTT variables in the “Data to pass to application” field or in an associated Session Script, in order to send a PassTicket to the application instead of the user’s password, you may need to specify the PassTicket id from the External Security definitions for this application. For example, the TSO application controlled by RACF requires a PassTicket id of TSOxxxx, where xxxx is the SMF system id.

Perform background update action

Specify YES or NO. If YES is specified, the action selected by the user when a background session is updated will take place. If NO is specified, no action will take place, regardless of the user’s setting. This may be valuable for applications which update the screen frequently, for example status monitoring applications with regular screen updates.

Background update script

If you want InterSession to monitor screen updates in a background session (not currently on the user’s screen), you should define the name of an monitoring script here. The script will be executed each time the application sends data.

Such a script can for example be used with a mail application to detect new incoming messages, and can be coded to send a message box to the screen with an informative message. See the MSGBOX command in the section “Session Scripts”.

The following fields are only applicable to application type VTAM. They will not show for a TN3270 application.

Bracket protocol conversion

Specify YES or NO. By specifying YES, change direction protocol will always be used against the terminal. Application requests with End Bracket will be converted to Change Direction.

With applications frequently updating the screen with End Bracket, the scroll speed may be slowed down. Also, the input inhibited indicator may cause problems to type data in the screen fields. In such a case, it is recommended to set this option to NO, which will cause the bracket indicators to be sent unchanged to the terminal.

Append %TD to 'data to pass...'

Specify YES or NO. If set to YES, any data written after the application code on the menu (substituted with the %TD variable) will be appended to the data in the “Data to pass to application” field. If set to NO, the %TD data will not be appended.

Propagate Menu Scrn info

Specify YES or NO. If YES is specified, anything entered into the "INFO" field of the menu for this application will be propagated to all other applications with the same VTAM application ID. Refer to the *User’s Guide* for more information.

VTAM Logmodes for Pass Mode (from terminal logmode table):

When a session is started in pass mode, the terminal is disconnected from InterSession, and connected to the application system. If no logmode is specified for pass mode, the default terminal logmode (DLOGMOD parameter on the terminal definition in VTAM) will be used.

Specifying a logmode name for pass mode is equivalent to specifying a logmode on the VTAM USS screen.

VTAM Logmodes for Relay Mode (from INTSMTAB):

When a session is started in relay mode, the terminal session remains active. InterSession starts a second session between itself and the application system using an APPL statement as a virtual terminal.

A logmode for this session will be selected from the INTSMTAB logmode table. If the relay mode logmode is not specified, InterSession will try to match on the PSERVIC parameter, comparing the terminal logmode and the logmode table entries.. If no match is found, the last entry in INTSMTAB, named DE-FAULT, will be used.

If a relay mode logmode is specified, the name must exist in the logmode table.

You can either specify a particular logmode name, or you can specify a logmode mask (for example, "*****N1"). A logmode will then be selected as follows:

1. First the logmode table is scanned, searching for a logmode entry with a matching PSERVIC parameter.
2. Then, the asterisks in the mask will be replaced with the characters from the name of the matching logmode entry.
3. Finally, the logmode table is searched a second time with the new name from step two.

In the example above, if the matching logmode in step one was "S2480E2", the logmode used would be "S2480N1". This allows logmodes to vary depending on terminal screen sizes.

COS name

If you need to use different classes of service (COS), you must code the required logmode entries in INTSMTAB. InterSession will then locate the entry that matches both the terminal PSERVIC parameter and the COS name specified in the Application Profile.

Note: You cannot specify both a relay mode logmode and a COS name in the same Application Profile.

CICS appl with I/S support

If this profile represents a CICS system where the InterSession support programs have been installed, specify YES, otherwise NO. If you specify YES, you will be able to use the PF2 key to get to the CICS specific options of the Application Profile.

Note: A change of this parameter will also affect all other Application Profiles with the same VTAM application ID.

Virtual terminal id

If specified, this VTAM ACB / APPLid name will be used when starting an application session. POOL and UNIQUE specifications on the Application Profile will be ignored.

If the name contains asterisks, these will be replaced by the corresponding positions of the terminal id the user is signed on to.

The name may also be globally altered before use by the Startup Parameter VTERMMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. Any characters in the mask will replace the corresponding positions of this name. See "Defining the Startup Parameters" in the chapter "Sysplex Functionality".

Note: This parameter can only be used and is only shown on a Personal Application Profile.

Application Profile Screen, type SScript

If you have selected the application type as **SScript**, you will see the following screen:

```

InterSession ----- Maintenance, Shared Application Profile -----
Application id START                                Change application id ==>

  Application type ==> SScript
  Hide application ==> NO
  Authorization check ==> YES
  Script ==> STARTAPP

Application text, language codes 1-6:
1> window to start multiple apps      2>
3>                                     4>
5>                                     6>

F1-help  F3-return

```

Hide application

Enter YES if you do not want the application to show on the menu screen. Default is NO.

Authorization check

Enter YES, EXT or NO to indicate whether the user's authorization should be checked. See above for a detailed explanation.

Script

Enter the name of a Session Script where you should code statements to be executed when the application is started.

An example of such a Session Script named START follows. This script will create a popup screen for the user to make a selection and start a set of applications. For detailed information on the script language, see the section Session Script Maintenance below.

```

A1  SET %IFA1=3
    MSGBOX BEGIN
    MSGBOX ;Type a selection number and press ENTER.
    MSGBOX ;
    MSGBOX &%IFA1;1. start PROD applications
    MSGBOX ;      2. Start TEST applications
    MSGBOX ;      3. Cancel this menu
    MSGBOX ;
    MSGBOX END,KEYS=CANCEL
    IF %IFA1=1
        START APPL=CICS
        START APPL=TSO

```

```

        TERM Prod applications started
    ENDIF
    IF %IFA1=2
        START APPL=CICST
        START APPL=TSOT
        TERM Test applications(s) started
    IF %IFA1=3
        TERM
    GOTO A1

```

When this application is selected from the menu screen, the script STARTAPP will be executed and produce the following screen:

```

InterSession ----- M E N U ----- Sat Nov 28, 2015 13:45

APPLICATION          INFO COM  APPLICATION          INFO COM
-----Internal applications----- ! NVIEW Network control  ??
MAINT InterSession maint ! T3270 Mainframe TN3270 serv ??
STAT. InterSession status ! START window to start multi
TLOCK Terminal 1
PROF. Your user
MMS.. Message/ma
STBY.. Standby sc
OFF.. Logoff Int
-----Informat
OPEN.. Open hours
-----External
CICS.. A CICS sys
IMS.. An IMS sys
CMS.. VM/CMS
TSO.. TSO/ISPF      ??      !

Type a selection number and press ENTER.
1. start PROD systems
2. Start TEST systems
3. Cancel this menu
F12-cancel

===== Session status =====
Attention key Attn  Jump key PA1  Command key ENT  Prefix ..

Application ==>
F1-help  F3-sign off  F7/8-bwd/fwd  ENT-system select  CAL
SC0TCP06

```

Application Profile Screen, type Logoff

If you have selected the Application type as **Logoff**, you will see the following screen:

```

InterSession ----- Maintenance, Shared Application Profile -----
Application id OFF                                Change application id ==>

  Application type ==> Logoff
    Menu level ==> 2
  Hide application ==> NO
  Authorization check ==> NO
  Cancel all sessions ==> NO
  Disconnect terminal ==> YES
  Remove VTAM LOGAPPL ==> NO

Application text, language codes 1-6:
1> Logoff InterSession      2>
3>                          4>
5>                          6>

'Delete' for removal ==>
F1-help  F3-return

```

Hide application

Enter YES if you do not want the application to show on the menu screen. Default is NO.

Authorization check

Enter YES, EXT or NO to indicate whether the user's authorization should be checked. See above for a detailed explanation.

Cancel appl sessions

Enter YES or NO to cancel / not cancel any existing application sessions.

Disconnect terminal

Enter YES or NO. YES disconnects the terminal from InterSession. NO means that InterSession's Sign On screen will be shown.

Remove VTAM LOGAPPL

Enter YES or NO. YES remove any VTAM LOGAPPL on the terminal, and the terminal will not automatically connect to InterSession. Valid for VTAM terminals only.

Shared Application Profiles Listing

If you want a listing of the Shared Application Profiles (either to select one for maintenance or to change the order in which they will appear on the menu), type L in the "New/List" field under "Shared Application Profiles" on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Shared Application Profiles -----
Pos Application      Pos Application      Pos Application
001 INTAPPL Internal ap
002 MAINT InterSessio
003 STAT InterSessio
004 TLOCK Terminal lo
005 PROF Your user p
006 MMS Message/mai
007 STBY Standby scr
008 OFF Logoff Inte
009 INFO Information
010 OPEN Open hours
011 EXTAPPL External ap
012 CICS A CICS syst
013 IMS An IMS syst
014 CMS VM/CMS
015 TSO TSO/ISPF
016 NVIEW Network con
017 T3270 Mainframe T
018 START window to s
Move Start:      End:      After:
F1-help  F3-return  F7/8-bwd/fwd
```

To view / change an individual Application Profile, position the cursor on the line and press ENTER. The Application Profile screen will then be displayed. When you press PF3 on the Application Profile screen, this screen will be redisplayed.

You can rearrange the applications on the menu by using the "Move " fields on the last line of this screen. For example, if you want to move the applications starting with IMS and ending with NVIEW) to to the end of the list, enter the command:

Move Start: 14 End: 17 After: 18

The screen will be rearranged. To move applications to the beginning of the list, specify '0' in the 'After' field.

Compressing the Application Security Keys

Each time you add a new Application Profile, it will receive a unique internal application security key ID between 1 and 1018. This value will be increased by 1 for every new Application Profile.

When 1018 additions have been made, no more Application Profiles may be created, even if the current number of Application Profiles is less than 1018.

The COMPRESS command of the INTSUTIL program will reformat the application security codes, which are also part of the User Profile records. After the compress function has been completed, new Application Profiles may again be added.

Refer to the section "The Batch Routines" for more information.

Session Script Maintenance

Script Residence

Your scripts may reside either in the InterSession INTSFLE VSAM file, or in a separate PDS dedicated for your scripts.

Scripts in the INTSFLE file

This is the default and need no setup.
All functions of the Script Editor are available. See below for details.

Scripts in a separate PDS

The PDS must be defined as fixed blocked with a record length of 80.
To enable this function you must add a DD card to the InterSession startup JCL:

```
//SCRIPTS DD DSN=file name,DISP=SHR
```

Set the option below, located in the System Options, Scripting, and restart InterSession,

```
InterSession ----- Maintenance, Scripting -----
Scripts reside in a PDS ==> YES
```

You must edit the scripts in the PDS with ISPF. The InterSession Script Editor can only be used for view-ing.

Also, on the MAINT selection screen the functionality is limited. You can not add or delete scripts via MAINT..

Instead, the **R** (refresh) command should be used when you have added, updated or deleted a script in the PDS: InterSession will then update its copy of the script from the PDS.

```
InterSession ----- Maintenance, Selection ----- Version 8.1.23
Users:
  New/List ==> █ User or Group ==> Copy ==>
Models:
  New/List ==> Model ==> Copy ==>
Shared Applications:
  New/List ==> Application ==> Copy ==>
Session Scripts:
  Refresh/List ==> Script ==>
```

Script Editing

To edit a script, enter the script name in the "Script" field on the maintenance selection screen. A screen like the following will be displayed if your scripts reside in INTSFLE. If they reside in a PDS you can only view the script here.

```
InterSession ----- Maintenance, Session Script -----
Script TS00N
Command ==> Descr. ==> Logon to TSO
Line Statement
<001> TYPE %UI Type user id
<002> ENTER Press ENTER key
<003> IFSTR IKJ56420 User not defined?
<004> TERM '%UI not a TSO user'
<005> TYPE %PW Type password
<006> HOME Tab to last
<007> TABB 2 Tab to reconnect fld
<008> TYPE S Select reconnect
<009> ENTER Press ENTER key
<010> IFSTR IKJ56421 Invalid password?
<011> TERM 'Invalid TSO password' Yes, terminate
<012> IFSTR IKJ56425 Already logged on?
<013> TERM 'You are already logged on to TSO' Yes, terminate
<014> CLEAR No, press CLEAR
<015> TYPE ISPF Type ISPF
<016> ENTER Press enter
<017> END Successful logon
<018>
F1-help F3-return F7/8-bwd/fwd
```

A script may consist of up to 390 statements. Use PF7 and PF8 to scroll through the script.

The Script Commands

if the scripts reside in INTSFLE, the valid commands are **SAVE**, **CANCEL**, **CHECK** and **DELETE**.

If the scripts reside in a PDS, the valid commands are **CHECK** and **REFRESH**.

SAVE saves any changes made and leaves the script editor.

CAN[CEL] discharges any changes made since the last **SAVE** and leaves the script editor.

CHECK runs a rudimentary syntax check and outlines any errors. Note that the error messages will update the script, to the rightmost part of the line. To get rid of these messages you have to issue the **CANCEL** command.

DELETE removes the script from the system.

REF[RESH] reads the script from the PDS and updates or the inline script copy. If the script has been deleted from the PDS the inline script copy is removed.

The Script Statements

The statements in a Session Script are entered in free format, with the following layout:

[label] command [operands] [comment]

A character string (operand) with more than one word must be enclosed in single quotes. For certain commands, to distinguish the operands from a comment, you may have to start the comment with a semi-colon (;). The statements are treated as is, with no uppercase translation. The command codes are recognized in both upper and lower case.

The following **line commands** can be entered in the statement number column:

In	Insert n blank lines after this line
Dn	Delete n lines, starting with this line
Rn	Repeat this line n times
Cn	Copy n lines, starting with this line
Mn	Move n lines, starting with this line
A	Insert the lines to be copied or moved after this line
B	Insert the lines being copied or moved before this line

The n value can be in the range 1-99. If it is not specified, one line is assumed.

Script Commands

The following commands can be used in a Session Script:

Note that a variable must be prefixed by either an "and" sign (&) or a percent sign (%).

If more than one variable are defined in succession, they must be separated by a period (.) .

TYPE KEY	Simulates keyboard input. KEY is an alias for TYPE.
EEOF EOF	Simulates the "Erase end of field" key. EOF is an alias for EEOF.
UP DOWN LEFT RIGHT	Moves the cursor on the screen, simulating the arrow keys.
TAB TABF BTAB TABB TABL NEWL NL HOME	Simulates the tabulating keys. TABF is an alias for TAB. TABB is an alias for BTAB. TABL tabulates to the last input field of the screen. NL is an alias for NEWL.

ENTER CLEAR PFn PF n PAn PA n	Simulates an ENTER, CLEAR, PF, or PA key.
IFSTR	Scans the application screen for a character string.
IF	Compares a variable against a character string or another variable.
ENDIF	Delimits the IF or IFSTR sequence.
GOTO	Goes to another part of the script.
SRCH SEARCH	Scans the application screen for a character string and sets the condition code and the %LOC variable. SEARCH is an alias for SRCH.
SEARCHF	Continues to search for the character string in previous SEARCH. The search starts in the position after the %LOC value.
CMP COMPARE	Compares a variable against a character string or another variable and sets the condition code. COMPARE is an alias for CMP.
BR BRANCH	Goes to another part of the script depending on the condition code. BRANCH is an alias for BR.
OUTPUT	Displays a string on the screen. Syntax is OUTPUT string [position]. "position" can be specified as a screen position or as (row,col)
DISPLAY	Displays an ISPF-type panel screen, required parameter is the pnel name.
INPUT	Waits until the user has sent data from the terminal to the application / script. Used after a DISPLAY or INPUT command.
WINP	Waits for the application to send the next screen, i.e. until the keyboard is unlocked.
WSTR WAITSTR	Waits until a specified character string appears on the screen. WAITSTR is an alias for WSTR.
MSGBOX	Sends a message box (popup window) to the terminal.
WAIT	Halts the execution of the script for a specified time interval.
RESET	Simulates the terminal RESET key.

TERM TERMSESS	Terminates the session. TERMSESS is an alias for TERM.
MENU	Returns to the menu screen.
UPDACT	Is used in a background update script to update the active session.
LET SET	Sets a variable to a mix of other variables and character data. Defines the variable if it does not exist.
UDEFINE VDEFINE	Explicitly defines a variable. Deletes a variable.
UDELETE VDELETE	
ADD	Adds a number or an arithmetic variable to an arithmetic variable.
SUB SUBTRACT	Subtracts a number or an arithmetic variable from an arithmetic variable. SUBTRACT is an alias for SUB.
SHOW SHOW ALL	Displays the current application screen. SHOW ALL displays all application screens.
START	Starts another application. Control is kept in the current script.
WTO MSG	Writes a message to the system log. MSG is an alias for WTO.
CALL XCTL ACLPGM	Calls or transfers control to another script. ACLPGM is an alias for CALL..
NOOP	No Operation, label placeholder.
END RETURN STOP	Ends the script. STOP and RETURN are aliases for END.
*comment	Comment line.

Notes on Variables

A variable can be either

- A previously defined variable by the LET/SET/VDEFINE/UDEFINE commands
 - A variable defined in the System Options, populated by user data from External Security, see System Options, Scripting.
 - A System Variable as listed in the section “The System Variables” in this manual.
-

If a variable is to be concatenated with another variable or a text string, the variables and the string must be separated with a period. For instance, if the variable %D1 contains **CE**, the string %D1.**MT** will be expanded to **CEMT**. The string %D1**MT** will however not be expanded, since the variable is not recognized.

The contents of a variable may be selected by a substring. The substring is defined with start position and length. For example, if the variable &MYVAR contains **Knockout of the blue**, the definition &MYVAR(6,25) will result in the string **out of the blue**.

A description of each of the script commands follows.

The TYPE (KEY) Command

The TYPE command types data in a field of the application screen at the current screen position. If the string starts with the screen position variable, %(rr,cc), the cursor will first be set to that screen position.

(label) TYPE text/variables

The following can be entered in the operand field, in any combination:

Text Any combination of characters and digits. If the text string contains spaces, it must be enclosed in single quotes, like '**a text string**'. Hexadecimal data may be entered in quotes preceded by an X, like this: X'010AFFFF'.

Variables Any variables.

Special notes for the screen position variable:
%(nnnn) or %(rr,cc)

Enter the absolute screen position (four digits 0001-3670) or row and column (two + two or three digits 01-43.01-132). This variable will be expanded to a 3270 SBA sequence.

The line number may be preceded by a – to indicate that the line number is relative to the bottom of the screen. For example, %(-02,nn) refers to line 22 on a twenty-four line screen and to line 30 on a thirty-two line screen. %(-00,nn) refers to the last line of the screen.

The EEOF (EOF) Command

The EEOF command simulates the 3270 key "Erase end of field". It will clear the contents of the current unprotected field, starting from the current cursor position and ending at the end of the field. If the cursor points at a protected field, no action is taken.

(label) EEOF

The Arrow Key Commands

These commands simulate the keyboard arrow keys.

```
[label]  UP      n
         DOWN   n
         LEFT   n
         RIGHT  n
```

The cursor will be moved the specified number of lines. If no number is given, one line is assumed.

The Tabulating Key Commands

These commands simulate the keyboard tabulating keys.

```
[label]  TAB      n
         BTAB     n
         TABL     n
         NEWL     n
         HOME
```

The cursor will be tabulated the specified number of times. If no number is given, one time is assumed.

The Terminal Key Command

The terminal key command simulates an ENTER, CLEAR, PF, or PA key. For the ENTER and PF keys, all data previously specified by the TYPE commands will be sent to the application. The script will then wait for data to be sent from the application.

```
[label]  ENTER
         CLEAR
         PFn
         PF n
         PAn
         PA n
```

The IFSTR Command

The IFSTR command is used to examine the current application screen for the presence of a specific character string.

```
[label]  IFSTR  text string
```

In the operand field, code the text string that you want to search for. The string is coded and tested as-is, respecting case. The most recent screen sent by the application is scanned for the presence of the string.

If the string is found, processing continues with the statement immediately following the IFSTR statement.

If the string is not found, the entire IFSTR sequence is bypassed. The IFSTR sequence is terminated by:

- an ENDIF command
-

- a GOTO command
- end of script (END, TERM, CALL or XCTL command or a blank line)

Nested IFSTR sequences are allowed.

The IF Command

The IF command is used to test the contents of a variable against a specific character or numeric string or against the contents of another variable.

```
[label] IF expression
```

In the operand field, code an expression with the following format::

```
operand1 comparator operand2
```

Operand1 must be a variable, and substrings can be used. Comparator can be any of the less than, greater than or equal signs (< > =). Used as. Operand2 can be a variable or a character string. A character string may be enclosed in single quotes. Example:

```
IF %TD=START
```

To test for a null variable, use two single quotes. Example:

```
IF %D1>' '
```

If the expression is satisfied (true), processing continues with the statement immediately following the IF statement.

If the expression is not satisfied (false), the entire IF sequence is bypassed. The IF sequence is terminated by:

- an ENDIF command
- a GOTO command
- end of script (END, TERM, CALL or XCTL command or a blank line)

Nested IF sequences are allowed.

The ENDIF Command

This command is used to terminate an IF or IFSTR sequence.

```
[label] ENDIF
```

The GOTO Command

The GOTO command is used to transfer processing to the script statement with the 'label' given in the "Operand" field.

```
[label] GOTO label
```

The SRCH Command

The SRCH command is used to examine the current application screen for the presence of a specific character string. It will set the condition code to be tested by a subsequent BR command.

If the string is found, the EQ condition code is set. If not found, the NE condition code is set.

```
[label]  SRCH  text string
```

In the operand field, code the text string that you want to search for. The string is coded and tested as-is, respecting case.

The CMP Command

The CMP command is used to test the contents of a variable against a specific character string or against the contents of another variable.

```
[label]  CMP  operand1,operand2
```

Operand1 must be a variable. Operand2 can be a variable or a character string. Example:

```
CMP  %TD,START
```

The condition code is set to be tested by a subsequent BR command.

The BR Command

The BR command is used to transfer processing to the script statement with the 'label' given in the "Operand" field, depending on the condition code set by a previous SRCH or CMP command.

```
[label]  BR   EQ,label
          NE
          LT
          LE
          GT
          GE
          ANY
```

Example:

```
BR   NE,CONT10
```

Goes to label CONT10 if the condition code is "not equal".

```
BR   ANY,CONT20
```

Goes unconditionally to label CONT20.

The WINP Command

The WINP command suspends the script processing until the application has sent the next screen, i.e. unlocked the keyboard.

```
[label] WINP
```

Note1: After the script has sent data to the application with any of the terminal key commands, processing will be suspended until the keyboard is unlocked by the application. Therefore, you should normally not use this command after a terminal key command.

Note2: You should normally not code this command at the beginning of a script. A script will not be started until the application has sent its first screen. However, if the setting "Application sends first screen" in the Application Profile is set to NO, the script will be started immediately.

The WSTR Command

The WSTR command suspends the script processing until the application has sent a screen containing the specified character string.

```
[label] WSTR text string
```

The WSTR command is used when the application sends parts of the screen in succession, and the script wants to wait for a specific string to appear on the screen. The string is coded and tested as-is, respecting case.

The MSGBOX Command

The MSGBOX command is used to display a message on the user's screen in the form of a message box. The command may appear anywhere in a Session Script, and you may code one to twelve lines of text in a message box.

When the MSGBOX command is executed, script execution is halted until the user closes the message box. This is done by pressing one of the keys specified in the MSGBOX END statement, or with the ENTER key if the IFUn / IFAn variables are used.

Normally, you create a MSGBOX by coding at least three lines, the first with the BEGIN operand and the last with the END operand. However, you may also create a message box by coding a single "MSGBOX text..." command.

MSGBOX may also be used to input user data to the script, using the %IFUn / %IFAn variables, see below.

```
[label] MSGBOX BEGIN
MSGBOX text
MSGBOX END [ ,KEYS={GOTO|GOTOALT|TERMINATE|CANCEL}]
```

"text" may be preceded in the first position by a plus (+) or minus (-) sign for high or normal intensity.

These characters will not occupy a position on the screen.

"text" may include any variables, and any of the Screen Tags that you have defined in the Screen Layout. These screen tags occupies one screen position.

Note that the "BEGIN" and "END" words must be in either upper or lower case to be recognized; they can not be in mixed case. If they are, the MSGBOX command is treated as a single line command.

Input fields, the %IFUn / %IFAn variables

The variables %IFU1, %IFU2, %IFU3, %IFU4 and %IFA1, %IFA2, %IFA3, %IFA4 may be coded in a MSGBOX text. They will create an input field in the message box, where the user can enter any desired data to be processed by the script.

The data in the IFUn variables will be translated to upper case, whereas the data in the IFAn variables will be kept as typed on the screen.

The ENTER key must be used to fill the IFxn variable(s) with the screen data.

When you create such an input field, make sure that you delimit the field by a screen tag. See sample 2 below.

Note that to use the IFxn variables, the “MSGBOX text” command(s) must be enclosed in MSGBOX BEGIN and MSGBOX END commands.

The END statement

In the END statement you may specify one to three keys that will be displayed in the last line of the message box. The texts associated with the keys are specified in the Screen Layout 17/21, Top Line Menu / Message Box.

The associated terminal keys are taken from the System Options, Terminal Keys Defaults.

GOTO	Closes the message box, switches to the session executing the script. The PF key used for this purpose is the “Various use key 1” as specified in the System Options.
GOTOALT	As GOTO, but the PF key used for this purpose is the “Various use key 1, Alternate” as specified in the System Options. Note that this is the only terminal key that can be specified in the System Options as ENTER.
TERMINATE	Closes the message box, terminates the session executing the script. The PF key used for this purpose is the “Various use key 2” as specified in the System Options.
CANCEL	Closes the message box, current session is still active (the default). The PF key used for this purpose is the “Window cancel key” as specified in the System Options.

If no keys are specified, the CANCEL key will be displayed.

For a single line message, only the CANCEL key will be in effect.

Sample 1:

```
MSGBOX BEGIN
MSGBOX Line 1 of the message box (normal)
MSGBOX +Line 2 of the message box (high)
MSGBOX -Line 3 of the message box (normal)
MSGBOX Line 4 of the message box (normal)
MSGBOX END,KEYS=(GOTO,TERMINATE,CANCEL)
```

Sample 2:

In this sample the user is requested for a new password, which is stored in Data Field 1 of the User Profile. Note the “ and ; screen tag characters.

```
MSGBOX BEGIN
MSGBOX Your current password is"%D1.
MSGBOX Enter a new password below.
MSGBOX New password:"%IFU1 ;
MSGBOX END,KEYS=(TERMINATE,CANCEL)
IF %IFU1>' '
    SET %D1=%IFU1
ENDIF
```

The WAIT Command

The WAIT command can be used to suspend the script processing for a specified time interval. The time interval is specified in seconds or in seconds and tenths of a second.

```
[label] WAIT n
          n.n
```

This command may be required in certain cases if the Session Script is "too quick" for the application. Some applications might respond with the same screen over and over again, if the terminal response comes too quickly. A WAIT of one second between the interactions will usually cure the problem.

The RESET Command

The RESET command can be used to simulate pressing the RESET key on the terminal.

```
[label] RESET
```

This command may be required in certain cases where a terminal user is required to press the RESET key after pressing a "send" key.

This command, if specified, must appear immediately after a terminal-key command (ENTER, PF1, etc.).

The TERM Command

The TERM command is used to terminate the current session and redisplay the menu.

```
[label] TERM [message text]
[label] TERM [APPLICATION=name|APPL=name|SYSTEM=name]
```

If a message is coded in the "Operand" field, it will be displayed on the menu.

If the APPLICATION parameter is coded, the specified application will be started instead of returning to the menu. If the application is already started, control will be passed to the active session.

The MENU Command

The MENU command will terminate the script and return to the Main Menu. The session is still active.

```
[label] MENU
```

The XCTL Command

The XCTL command transfers control to another script. Return will not be made to the calling script.

```
[label] XCTL scriptname
```

The CALL Command

The CALL command will transfer control to another script. Return will be made to the calling script to the statement following CALL.

```
[label] CALL scriptname
```

The RETURN Command

The RETURN command will transfer control back to the script that called the current script. If the current script was not called, RETURN is equivalent to END.

```
[label] RETURN
```

The UPDACT Command

The UPDACT command is used in a background update script to indicate to the active session (or the menu) that the background session has been updated.

```
[label] UPDACT
```

The UDEFINE/VDEFINE Commands

The UDEFINE and VDEFINE commands are used to define a variable. The difference between them is that the variables defined by VDEFINE are deleted when the script ends, whereas the UDEFINE variables are not deleted until the user signs off from InterSession.

```
[label] VDEFINE variable [TYPE=CHAR|UPCHAR|NUM]
```

You may specify the type of data the variable will contain. The default is CHAR.

The UDELETE/VDELETE Commands

The UDELETE and VDELETE commands are used to delete a variable. You can delete variables created by the LET/SET commands as well.

The LET (SET) Command

The LET command is used to:

- Optionally define and put data into a variable or into a field in the User Profile.
- Override default loop detection and wait limits.

```
[label] LET variable=fromdata
[label] LET LOOPCNT=nnn
[label] LET MAXWAIT=nnn
```

“variable” can be any of the following:

- A previously defined variable (defined by another LET or xDEFINE command)
- A new variable
- User name %UN
- User Group %UG
- Printer Id %PI
- Data fields 1-8 %D1 - %D8

“fromdata” can be any combination of variables, character or numeric strings.

Concatenated items must be separated with a period.

Character strings containing blanks must be enclosed in single quotes.

The LOOPCNT parameter is used to override the loop detection limit. By default, a maximum of 100 script statements can be executed before the script is considered to be in an endless loop. With this command you can set the loop limit to any value between 1 and 999.

The MAXWAIT parameter is used to override the wait limit. By default, the script will wait 30 seconds for the application to respond to a WINP or terminal key command. When this time interval has elapsed, the menu screen will display with an error message.

The ADD Command

The ADD command is used to add an integer or an arithmetic variable to an arithmetic variable. Note that the variables do not wrap around, if you add to a variable containing 999999, the result will still be 999999.

```
[label] ADD variable,[integer|variable]
```

The SUB Command

The SUB command is used to subtract an integer or an arithmetic variable from an arithmetic variable. Only the variables %A1-%A4 may be used. Note that the variables do not wrap around or become negative, if you subtract from a variable containing 0, the result will still be 0.

```
[label] SUB variable,[integer|variable]
```

The START Command

The START command is used to start another application. If the user is not authorized for the application, script execution is halted with an error message. If the application is not active, the START request is ignored. Control remains in the current application / script.

```
DISPLAY INPUT OUTPUT ovh PANELS abc123
```

```
[label] START [APPLICATION=name|APPL=name|SYSTEM=name]
```

The WTO Command

The WTO command is used to write a message to the log.

```
[label] WTO message text
```

The SHOW Command

The SHOW command is normally only used for debugging purposes. It will show either the current screen or all script interactions on the user's terminal.

```
[label] SHOW [ALL]
```

If the ALL parameter is not specified, only the current screen will be shown.

The NOP Command

The NOP command does nothing, it is merely used as a placeholder.

```
[label] NOP
```

The END (TERM) Command

The END command delimits the script. It is optional, but must be used if you want to GOTO the end of a script.

```
[label] END [APPLICATION=name|APPL=name|SYSTEM=name]
```

If the APPLICATION parameter is coded, the specified application will be started instead of showing the current screen of the application. If the application is already started, control will be passed to the active session.

The Comment Line

You can add comment lines to your scripts by coding an asterisk in position 1 of the line.

```
* comment text
```

Example

The following is an example of an end script used to log off from TSO from any ISPF screen:

```
START  IFSTR 'IKJ56700A ENTER USERID'
      GOTO END
LOOP   IFSTR 'Disposition of Log Data Set'
      GOTO CONT
      IFSTR READY
      GOTO LOGOFF
      PF3
      GOTO LOOP
CONT   TYPE 2
      ENTER
LOGOFF TYPE logoff
      ENTER
END
```

Error messages

If an error is found during script execution, the menu screen will be displayed with an appropriate error message.

Just as any other error messages, these messages can be customized for your installation using Screen Layout maintenance.

ISPF Panel Support

InterSession has built-in limited support for use of ISPF Panels.

The Panels must reside in a PDS, see **System Options, Scripting**.
They are invoked by the **DISPLAY** script command.

What is currently implemented

The)ATTR and)BODY sections are fully supported.

In the)INIT section, only the .ZVARS and .HELP functions are supported.

With the .HELP functionality the PF1 key must be used to display a help panel ,and PF3 must be used to return from the help screen.

Working Example:

```
)ATTR
$ TYPE(OUTPUT) INTENSE(HIGH) SKIP(ON) COLOR(GREEN)
% TYPE(OUTPUT) SKIP(ON) COLOR(YELLOW)
? TYPE(INPUT) INTENSE(LOW) MDT(ON) COLOR(RED)
+ TYPE(TEXT) SKIP(ON) COLOR(WHITE)
< TYPE(TEXT) SKIP(ON) INTENSE(HI) COLOR(BLUE)
_ TYPE(TEXT) SKIP(ON) COLOR(YELLOW)
" TYPE(TEXT) SKIP(ON) COLOR(RED) INTENSE(HIGH)
)BODY TYPE=BREAKIN ALARM=NO
_*----- DEMOPANL ----- %ZDATE      %ZTIME
+
+This is a small ACL script to change some of a user's data.
+It uses the PROF application and screen scraping.

"*-----
<
<
+          User name ==>?Z          "
<
+          Printer ==>?Z          "
<
+General purpose field ==>?DATAFLD          "
<
+    Attn key function ==>?Z          "
<
<
<
<
<
<
<
"*-----
%MESSAGE
)INIT
. ZVARS (NAME PRINTID ATN)
. HELP= (HELPPANL)
)END
```

Session Script Listing

If you want to display a list of Session Scripts, from which you can select one to maintain, enter L under "Session Scripts" on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Session Scripts -----
```

Script	Description	Chg date	Chg time	Chg by
CMS0N	Logon to z/VM CMS			
SELF0N	Log on to I/S	11/17/24	21:39:39	ADCDMST
TS00FF	Logoff from TSO			
TS00N	Logon to TSO	11/10/24	19:15:15	ADCDMST
TS00N2	** COPY OF TS00N **	10/21/24	11:43:43	ADCDMST

```
F1-help  F3-return  F7/8-bwd/fwd
```

If the listing contains more than one screen of scripts, use the PF7 and PF8 keys to scroll backward and forward through the listing.

To view or edit an existing script, position the cursor on a script ID and press ENTER. When you press PF3 on the script screen, this screen will reappear.

Session Script Recording

To simplify the task of creating Session Scripts, a session recording feature is available that will create scripts by monitoring your terminal interactions. This facility is only available to System Administrators.

The session recording script makes use of the /REC command, which is given on the menu screen with the following format:

```
/REC name[,REP]
```

name The name of the script to be created or replaced.

REP REP (replace) indicates that the script already exists and is to be replaced by the script being recorded.

The procedure is as follows:

1. In the "Application" or "Command" field on the menu, enter the /REC command specifying the name of the script (and whether it is to replace an existing script).
-

Press the ENTER key. InterSession will confirm that script recording has started.

2. Start the session to be recorded (or, in case of a logoff script, enter your existing session).

Note: An existing session start script specified in the Application Profile will be ignored during script recording.

Log on to the application manually, until you have reached the desired position in the application.

3. Press the jump key to return to the menu. If a logoff script is being recorded, you will return to the menu when the session is terminated. InterSession will confirm that script recording has ended.

Note: The jump key is the only key that will function during script recording.

4. You can now use the script maintenance routines to make any further changes to the script. Things you normally may want to do are:

- Substituting variables for user ID, password, and the like (%UI, %PW, etc.)
- Adding IFSTR statements to test for error messages, etc.

5. Enter the script name in the Application Profile.

Screen Layout Maintenance

In the Screen Layouts you can alter all panels that are available to a regular end user.

The default set of Screen Layouts is named DEFAULT. Included are also Screen Layouts that are coded in other languages or that resembles other session manager products.

To make your own Screen Layouts, copy an existing layout to a new name and do the appropriate changes in the new layout.

Note: Do not customize the DEFAULT layout for your own use, since it will normally be replaced when upgrading to a new version of InterSession.

Each set of Screen Layouts is maintained on a set of screens.

Screen Variables

A number of variables can be coded on any panel. These are substituted with the corresponding value when the screen image is created. See the section "System Variables" for a listing of available variables. Each variable must be prefixed by the percent sign (%).

Panel text attribute tags

To visually enhance the InterSession panels, up to 10 user-defined attribute tags may be used on any panel. Each tag can be assigned extended attributes, such as color and reverse video. The standard message tags can also be user-tailored. See the section "Panel Tags" below for further explanation.

Screen Layout, Selection

To view and optionally change a set of Screen Layouts, enter the name of Screen Layouts in the "Screen Layout ID" field of the maintenance selection panel. The Screen Layout selection screen is displayed.

```
InterSession ----- Maintenance, Screen Layout -----
Screen Layout DEFAULT      Description Default screen layout
      select ==> █
      1 Usage/Commands
      2 Language/Heading
      3 Sign On Screen
      4 Main Menu Screen
      5 Messages
      6 Terminal Lock Screen
      7 Message System Screens
      8 User Profile Screens
      9 Standby Screen
      A Top Line Menu / Message Box
      B Printer Header Page Text
      C Panel Tags
      D Web Layout Settings

      'Delete' for removal ==>
      F1-help  F3-return  F7/8-bwd/fwd
```

To select an item, type the appropriate code 1-9, A-D and press Enter.

You can also browse through the screens by using PF7 and PF8.

'Delete' for removal

Enter the word **delete** if you want to remove this entire Screen Layout.

To return to the maintenance selection screen, use PF3

```
InterSession ----- Maintenance, Screen Layout 1/23 -----
Screen Layout LIKEPRD1      Usage/Commands
Default layout ==> YES      Description Resembles CA-TPX
Entrances:
> > > > > >
Terminals (group or single terminal id):
> > > > > >
> > > > > >
> > > > > >
> > > > > >
> > > > > >
Session commands:
      Next J      Previous B      Menu W
      Start A      S/relay      S/pass
      S/noscript G      Terminate I      Standby L
Top line menu      Hardcopy P      Remove D
      Sign off F      Logoff K      <- Need 'Logoff' applprof w/same name
      Disable X      Enable Y
Always use alternate screen size ==> NO
F1-help  F3-return  F7/8-bwd/fwd
```

Screen Layout, Usage/Commands

he

Default layout

If this is the default layout (which will be used for all terminals not specified in the Terminal list), specify YES, otherwise NO.

Note: Changing the default layout (or a layout for a user) will not take effect until a user signs on to InterSession again.

Entrances

If you are using more than one entrance to InterSession, you can specify here which entrance(s) that should use this Screen Layout.

Terminal list

Here you can enter terminal IDs (VTAM netnames) for which this Screen Layout is used. These fields cannot be specified if "Default layout" is specified as YES. You can either specify a single terminal ID or a group of terminals, in the form ABC*, i.e. all terminals starting with the characters ABC.

Session commands

In these fields you can change or remove the character strings used for the session commands (1-8 characters). You should use a character string that is unique for each command. If a command code is not specified, the corresponding function is disabled.

The possible commands are:

Next	Go to next active session
Previous	Go to previous session
Menu	Go to the application menu
Start	Start a session. The command must be immediately followed by the application name.
S/relay	As Start but the session is always started in relay mode.
S/pass	As Start but the session is always started in pass mode.
S/noscript	As Start but any start script is not executed..
Terminate	Terminate the session you give the code in.
Standby	Go to the Standby (lock) screen.
Top Line Menu	Start the Top Line Menu.
Hardcopy	Take a screen hardcopy.
Remove	Removes an ad-hoc session from the menu screen.
Signoff	Sign off (see below).
Logoff	Log off (see below).
Disable	Disables all special keys (jump key, command key) and all commands except Enable.
Enable	Enables all keys and commands after a Disable.

Signoff / Logoff considerations

For any of these two commands you must define an application profile with type Logoff.

Example:

Signoff is set to F.

Define a Logoff application profile with the name F and type Logoff:

```

InterSession ----- Maintenance, Shared Application Profile -----
Application id F                               Change application id ==>
    Application type ==> Logoff                 Application start key ==>
    Menu level ==> 2
    Hide application ==> YES
    Authorization required ==> NO
    Cancel all sessions ==> YES
    Disconnect terminal ==> NO
    Remove VTAM LOGAPPL ==> NO

Application text, language codes 1-6:
1> For the "F" command           2>
3>                               4>
5>                               6>

'Delete' for removal ==>
F1-help  F3-return

```

Set "Hide application = YES" and "Authentication required = NO" so all users can use the command.

Specify what actions should be taken, cancel sessions, disconnect terminals etc for this command.

Always use alternate screen size

YES or **NO**. Controls how the sign on and menu screens should use the alternate screen size as set in the 3270 client. **NO** (the default) = do not use alternate screen size if number of columns is greater than 80. **YES** = always use alternate screen size.

Screen Layout, Language/Heading

```

InterSession ----- Maintenance, Screen Layout 2/22 -----
Screen Layout DEFAULT      Language/Heading
Language number ==> 1      Codepage ==> 00000
Help screens ==> DEFAULT  Date format ==> MDY

'YES' ==> YES      'NO' ==> NO      'DEF' ==> DEF
'ALARM' ==> ALARM  'SWITCH' ==> SWITCH  'MENU' ==> MENU
'Today' ==> Today  'Now' ==> Now      'ALL' ==> ALL
'Available' ==> Available  'Not available' ==> Not available
'Active' ==> Active      'Output pending' ==> Output pending
'Last seen' ==>          'Session end' ==>
'More BW' ==>
'More FW' ==>

Month names ==> Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Day names ==> Mon Tue Wed Thu Fri Sat Sun
Heading line:
"InterSession -----%TC----- %DN %MN %D, %C%Y %TIME

F1-help  F3-return  F7/8-bwd/fwd

```

Language number

Up to six different languages are supported. In this field, enter the language number, from 1 to 6, for this Screen Layout. The language number will be used as an index in the application description text table in the Application Profiles.

Codepage

If different National Character Sets are used among the terminals, you may need to specify a codepage number here. This value is used when the codepage can not be determined from the terminal query.

Help screens

Enter the name of the help screens to be associated with this Screen Layout.

Date format

Enter the date format, using the codes Y, M and D. This format will be displayed on the menu and the message status screen.

YES / NO / DEF / ALARM / SWITCH / MENU / Today / Now

Enter the character representations for these values.

Available / Not available / Active / Output pending / Last seen / Session end

These texts are used to expand the %SS screen variable (system status). The **Last seen** text is shown on the last used active session. The **Session end** text is shown on a newly terminated session. These two texts are optional.

More BW / More FW

The text you enter in these fields will be placed at the beginning and end of the menu list, to indicate that more pages exist. If you are on the second and subsequent page of the menu list, the 'More BW' text will be placed at the beginning of the menu list. If you are not on the last page of the menu list, the 'More FW' text will be placed at the end of the menu list. If these fields are blank, no text for this purpose is placed in the menu list. If you enter a text, the first position must be a Panel Tag.

Example of a 'More BW' text: **▣Press PF7 for more applications**

Month names

Day names

In these tables, you can alter the month names and day names that are used on the various InterSession screens.

Heading line

Specify the format of the very first line of the Main Menu. The first character must be a plus or minus (high or normal intensity). Within the line, you may enter one or more of the screen variables (see above)

Screen Layout, Sign On Screens

```

InterSession ----- Maintenance, Screen Layout 3/23 -----
Screen Layout DEFAULT          Sign On Screen 1/2

      Heading text ==> Sign On
      Terminal keys: Help ==> DEF   Logoff ==>
      User/Timeout signoff application profiles ==>
      Hide MFA and PT fields ==> NO

Lines 1-13 (line command I/R/D):
%HDLINE
:
:
: $IIII;          $tt;          #Applid:<<%APPLID
: $II;$nn$nnn;$tttt; $eeee;$rr$rr; #Terminal:<%TI
: $II;$nnn;$nn;$tt; $ee;$ee$rr; #Logmode:<<%LM
: $II;$nn; $nn;$tt;$tt$eeee;$rr; #Version:<%VER
: $II;$nn; $nn;$tt;$tt$ee; $rr; #IP-Addr:<%IP
: $IIII$nn; $nn; $tttt; $eeee;$rr; #Julian:<<%Y.%JD
:
:
: [SSSS;[EEEEEE;[SSSS;[SSS;[IIII;[0000;[NNN;[NNN;
: [SSS[SSS[EEE;/[E[SSS[SSS[SSS[SSS;[III;[000[000[NNNN[NNN;
: [SSS;[[[EEE; [[[SSS;[[[SSS;[[[III;[000[000[NNN[NNNN;
F1-help F3-return F7/8-bwd/fwd

```

[illegible]

On these two screens, you can enter the format of the sign-on screen. An explanation of the fields on this screen follows:

Heading text

Enter the panel identification text. The System Variables %TS and %TC will be substituted with this string. (By default, these variables are used in the heading line on Screen Layout 1). Percent signs in the text will be treated as blanks.

Terminal keys: Help

If a terminal key is specified here, the use of it will display the help screen. DEF means the system default key as specified in the System Options. An empty field means that the function is disabled.

Terminal keys: Logoff

If a terminal key is specified here, the use of it on the sign on screen will logoff the user from InterSession. An empty field means that the function is disabled.

User signoff Application Profile

If you want the user to logoff from InterSession instead of going to the sign on screen when the user press the sign off key, you should specify an Application Profile name here. This Application Profile type must either be Logoff or SScript, if not the sign on screen is shown. The settings in the Logoff Application Profile have full relevance, for example if you have requested that all active application sessions shall be canceled.

Timeout signoff Application Profile

If you want the user to logoff from InterSession instead of going to the sign on screen when the user terminal session times out, you should specify an Application Profile name here. This Application Profile type must be Logoff, if not the sign on screen is shown. The settings in the Logoff Application Profile have full relevance, for example if you have requested that all active application sessions shall be canceled.

Hide MFA and PT fields

If you are using MFA or Pass Tickets for logon to InterSession, you can choose if the contents of these fields should be visible or not.

Line start column 80/01/02

Normally the 3270 line attribute is put into column 80. You can also set the line to start in position 01 or 02, in which case you can enter any character in the first position, not just an attribute (panel tag).

Lines 1-13, Lines 8-24

In these lines, you can code text and variables to be shown on the sign-on screen, including at least the three variables for the input fields User id, Password and New Password (variables %UI or %UU, %PW and %NP).

Use the panel tags (defined on the last page of the Screen Layout) as a 3270 attribute to define the characteristics for a field. The characteristics for a specified tag will be valid for all following text, until the next tag.

Every line must start with a panel tag in the first position, unless the above setting "Line start column" is 01 or 02, in which case the first position can contain any character. A question mark (?) in the first position of a line means that the line will not be displayed.

You may also use any applicable System Variable anywhere on the screen.

Line editing commands can be used in the first position:

I	insert a new line after this line
R	repeat this line
D	delete this line

Notes: The two System Variables %UI (user id, can also be %UU) and %PW or %PP (password, passphrase) must both exist somewhere on the screen in order for the user to be able to enter his credentials.

The System Variables %NP, %VNP (new password, verify new password) and/or %NPP, %VNPP (new passphrase, verify new passphrase) and the MFA fields %MFA1 - %MFA5 may also exist in order for the user to change password / passphrase or to enter MFA Pass Tokens.

The System Variable %RG (RACF user group) may also exist somewhere on the screen in order for the user to select a RACF group.

These variables will not show any contents on the sign on screen but rather as unprotected (input) dark fields.

Screen Layout, Main Menu Screens

```
InterSession ----- Maintenance, Screen Layout 5/23 -----
Screen Layout DEFAULT      Main Menu Screen 1/2

    Heading text ==> M E N U%
    Two-level menu ==> NO      Appl list columns (1/2/A) ==> A
    Column delimiter char ==> !      Highlight field panel tag ==> #
    Info column characters ==> ??    Highlight application ==> UNAVAIL
    Terminal keys: Help ==> DEF      Sign off => DEF      Bwd => DEF      Fwd => DEF
    Cursor at appl list line cmd ==> NO      Active sessions first ==> NO
    Header lines (line cmd I/R/D):      Line start column 80/01/02 ==> 80
%HDLINE
:
?
?
?
?
?
?
?
Hdr/model lines:      Appl number counts: Notauth apps => NO      Hidden apps => YES
APPLICATION          INFO *
&%AN.....;%AD      &%AI  Ä%AX;
F1-help      F3-return      F7/8-bwd/fwd
```

```
InterSession ----- Maintenance, Screen Layout 6/22 -----
Screen Layout DEFAULT      Main Menu Screen 2/2

Application list group header line:
#-----%ADC-----
Active sessions header lines:
:
:
Ä===== Session status =====
Active sessions model line:
&%AN..;%AD          %AA
Active sessions footer line:
ÄAttention key&%AK  ÄJump key&%JK  ÄCommand key&%CK  ÄPrefix&%CC  ;
Footer lines (line command I/R/D):
?
?
?
?
?
?
:
ÄApplication ==>&%APN          ;          %UI
%IMSG                          %TI
F1-help      F3-return      F7/8-bwd/fwd
```

On these two screens, the format of the menu screen is specified.

The InterSession menu screen is built up with four parts:

The header lines. This part forms the top of the screen. This part is optional.

The application list. This part forms a list of all authorized applications for the user. This part is mandatory. The application list may be defined with one or two columns.

The active session list. This part forms a list of all active sessions for the user. This part is optional. The active session list uses one or two columns, as specified for the application list.

The footer lines. This part forms the bottom of the screen. This part is optional.

Note: If an active OPER interface does not exist in the system, then somewhere in the header or footer lines the System Variable %APN (application name / system command) must be coded. This is to ascertain that a System Administrator is able to enter InterSession commands.

An explanation of the fields on this screen follows:

Heading text

Enter the panel identification text. The System Variables %TS and %TC will be substituted with this string.

Two level Menu

Specify YES or NO. If NO, only one-level menus will be generated with both headers and applications. If YES, the first menu level will display all header Application Profiles and the second level will display all application Application Profiles under a header.

Application list columns

Specify if you want one or two columns of applications. An 'A', for "automatic centering", means two columns, but if the number of applications only require one column to display, the column will be centered on the screen.

Column delimiter char

For a two column menu, this is the character that will be used to separate the columns.

Highlight field panel tag

When InterSession needs to highlight a field on the menu screen, for instance when an application has become inactive, this panel tag is used by InterSession.

Info column characters

first field	If an application is inactive and no return time is set by the Master Operator, the two characters specified here will be displayed in the INFO field (%SI variable). Default is ??.
second field	When a background session is updated by the application, or if you have mailbox messages you have not read, these two characters will be displayed in the INFO field (%SI variable). Default is !!.

Highlight application

If set to UNAVAIL, the application name variable AN will be highlighted if the system is not available. If set to ACTIVE, the AN variable will be highlighted if the user has an active session with the system. If set to NEVER, the AN variable will never be highlighted.

Menu keys: Help, Sign on, Bwd, Fwd

If you want to use other terminal keys on the menu screen than the system default, you can specify PF1-24, PA1-3, CLR, DEF or the field can be empty. DEF means the system default key as specified in the System Options. An empty field means that the function is disabled.

Cursor at appl list line command

YES, TOP or NO. If YES, the cursor will be positioned in the last used %AC/AU/U command field in the application list. If TOP, the cursor will be positioned in the first %AC/AU/U command field in application list. If NO, the cursor will be positioned in the %APN command field (the default).

Active sessions first

Specify YES or NO. Normally you do not want to change the order of the applications on the menu screen, depending on if they are active or not. However, if you want to move the applications with active sessions to the beginning of the list, specify YES. Default is NO.

Line start column 80/01/02

Normally the 3270 line attribute is put into column 80. You can also set the line to start in position 01 or 02, in which case you can enter any character in the first position, not just an attribute (panel tag).

Header Lines

You can use up to nine header lines on the menu screen. They can be used to pass urgent information to the users, to show an explanation of the menu, to display a logo, etc.

The first position contains an attribute (panel tag) or a question mark, unless the above setting "Line start column" is 01 or 02, in which case the first position can contain any character. A question mark indicates that no further lines will be displayed.

Attribute tags as well as screen variables may be coded anywhere in these lines.

You may also use the line editing commands I, R and D in the first position.

Application list header and Model lines

These two fields define the appearance of the application list.

Enter the text of the application list header.

Define the appearance of an application list line with a combination of the following System Variables, together with appropriate attribute tags:

AC Application line command, AU and U – underscore field
AU AC/AU takes up three screen chars, U takes up two
U

AN Application name

ADC Application description centered

AD Application description

AH Application hot key

ASK Application start PF key number (**SP** is an alias). See options below.

ASN	Application start sequence number (SR is an alias). For numbers 1-24 the corresponding PF key can be used. See options below.
AS	Application status
AI	Application info
AX	Application comment

Appl number counts: Notauth apps

YES or NO.

When set to YES, the **ASK/SP/ASN/SR** variables counts all applications. If a user does not have access to all applications, this will result in a broken sequence, for example 1, 2, 7, 8, 11 etc.

When set to NO (the default) the variables counts only applications for which the user is authorized. This will result in an unbroken sequence, for example 1, 2, 3, 4, 5 etc.

Appl number counts: Hidden apps

YES or NO.

When set to YES (the default), the **ASK/SP/ASN/SR** variables counts applications that are hidden. If some of your applications are hidden, this will result in a broken sequence, for example 1, 2, 7, 8, 11 etc.

When set to NO, the variables does not count hidden applications. This will result in an unbroken sequence, for example 1, 2, 3, 4, 5 etc.

Application list group header line

When creating the application list, the information from a header application (group header) will use this Model line.

Active sessions header lines

If you want a list of the active sessions to show beneath the application list, specify this and the two next fields. In this field you can code up to two lines of heading information.

If you do not want such a list, code a question mark (?) in the first position of all related fields.

The active session list, if specified, is shown to multiple session users only.

Active sessions Model line

Define the appearance of an active session list line with a combination of the same System Variables used for the application list Model line, together with appropriate attribute tags. In addition, the following variable may be used:

%AA Session applid/ipaddr

Active sessions footer line

Any appropriate information connected with active sessions or a multiple session user.

Footer lines

You can use up to nine footer lines. They can be used to display the application name / system command variable **APN**, pass urgent information to the users, to show an explanation of the menu, to display a logo, etc.

The first position contains an attribute tag or a question mark. A question mark indicates that no further lines will be displayed.

Attribute tags as well as screen variables may be coded anywhere in these lines.

You may also use the line editing commands I, R and D in the first position.

Screen Layout, Messages

```
InterSession ----- Maintenance, Screen Layout 7/22 -----
Screen Layout DEFAULT      Messages 1/6

Sign on ?HL-help    ENT-sign on with user id and password
Menu ?HL-help      %RT-sign off %BW/FW-bwd/fwd  ENT-system select
Menu ?HL-help      %RT-level 1 %BW/FW-bwd/fwd  ENT-system select
Info ?RT-menu      %BW/FW-bwd/fwd
Info ?HL-help      %V1-update mode %RT-menu %BW/FW-bwd/fwd
Info ?HL-help      %V1-non-update mode %RT-menu %BW/FW-bwd/fwd
Stat ?HL-help      %V1-shift %RT-return %BW/FW-bwd/fwd
Trm lock Contact your System Administrator to unlock the terminal
Msg stat ?HL-help  %RT-return %V2-distr.lists %BW/FW-bwd/fwd
Msg text ?HL-help  %V1-send %RT-return %V2-receivers %BW/FW-bwd/fwd
Msg rec. ?HL-help  %RT-return %V2-select receivers %BW/FW-bwd/fwd
Msg rec. ?HL-help  %RT-return %V2-select all %BW/FW-bwd/fwd
Msg imm. %V1-save in mailbox %RT-continue %BW/FW-bwd/fwd
Misc scr ?HL-help  %RT-return %BW/FW-bwd/fwd
Misc scr ?HL-help  %RT-return
Mai User ?HL-help  %V1-applications %RT-return %BW/FW-bwd/fwd
Mai User ?HL-help  %V1-application sequence %RT-return %BW/FW-bwd/fwd
Help ?RT-return   %BW/FW-bwd/fwd
Help ?HL-variables %RT-return %BW/FW-bwd/fwd
F1-help  F3-return F7/8-bwd/fwd
```

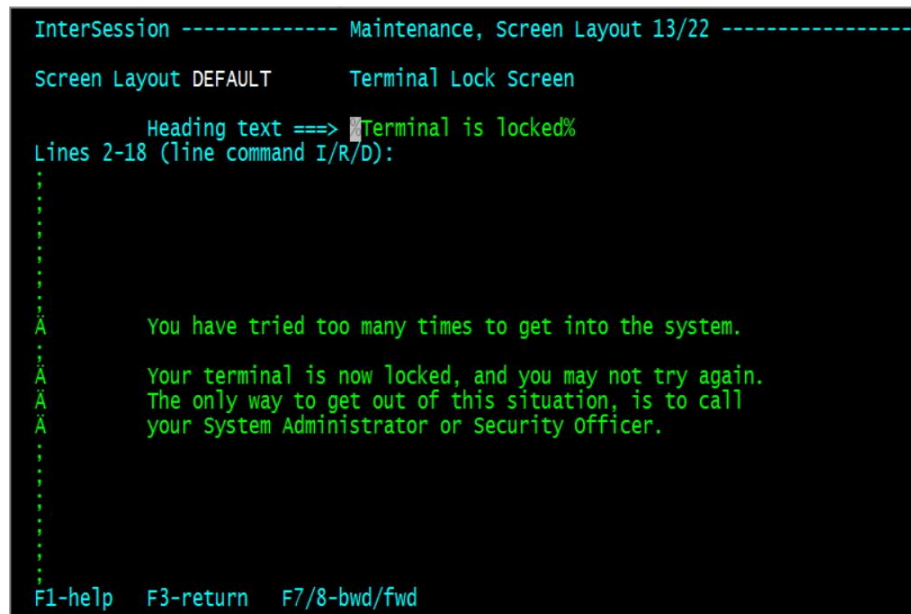
You can use this screen to alter all messages displayed by InterSession. There are five screens with instruction and error messages.

Any System Variable in these messages will be expanded.

Any x's in the messages will be replaced by an appropriate ID or number. The x's can be entered in either upper or lower case.

Note that the extended RACF messages for new password errors are located at the last (sixth) message screen.

Screen Layout, Terminal Lock Screen



This screen can be used to customize the text that is sent to a terminal when too many sign on attempts have been made. An explanation of the fields on this screen follows:

Heading text

The text that will be shown on the first line, if %TC or %TS is used in the "Heading line" field for screen 1.

Lines 2-18

These lines contain the text that will be displayed at the terminal.

The first position contains an attribute tag or a question mark. A question mark indicates that no further lines will be displayed.

Attribute tags and screen variables can be used anywhere in the text.

You may also use the line editing commands I, R and D in the first position.

Screen Layout, Message System Screens

```
InterSession ----- Maintenance, Screen Layout 14/22 -----
Screen Layout DEFAULT Message System Screens 1/2

----- Message status -----
%Message status%
New message title ==>
Commands: S-select, D<n>-delete, C-copy, P-print
Cmd_Title_____Created/sent by_____Status_____Date/time
Created          Altered          Sent to xx/xx      Sent/system
Sent/sign on     Will be sent      Received           Received/read
Commands - Select: S Delete: D Copy: C Print: P
----- Message text/send -----
%Message text/send%
Message title:          Created/sent by:
M(ail) / I(mm) / B(reak) ==> At date ==> At time ==>
To user id(s) ==>      To terminal id(s) ==>
To users in system ==> To users in VTAM APPL ==>
At sign on time ==>    To users selecting system ==>
----- Page
Send Mail: M Immediate: I Break: B Line Insert: I Delete: D Repeat: R
----- Immediate message -----
Message from:          Page      Subject:          Sent:
F1-help F3-return F7/8-bwd/fwd
```

There are two screens where you can change the text that will appear on the Message System screens.

You can also change the command codes used by the Message System.

Screen Layout, User Profile Screens

```

InterSession ----- Maintenance, Screen Layout 16/22 -----

Screen Layout DEFAULT      User Profile Screens

User id ==>                User group code ==>
User name ==>              Screen layout ==>
Two level Menu ==>         Autostart application ==>
Attn key function ==>      Initial command ==>
Printer id ==>             Print header ==>
Newpage after header ==>   Mailbox open ==>
Standby at timeout ==>    Background update action ==>
Data field 1 ==>          Field attribute ==> UNPROT
Data field 2 ==>          -:- -:- ==> UNPROT
Data field 3 ==>          -:- -:- ==> UNPROT
Data field 4 ==>          -:- -:- ==> UNPROT
Data field 5 ==>          -:- -:- ==> UNPROT
Data field 6 ==>          -:- -:- ==> UNPROT
Data field 7 ==>          -:- -:- ==> UNPROT
Data field 8 ==>          -:- -:- ==> UNPROT
Jump key ==>              Attention key ==>      Command key ==>
Command prefix ==>        New password ==>      Verify new password ==>
Hot keys: Enter application code (+ an "R" for return to calling session)
Hot keys in Top Line Menu ==> Hot keys with Cmd Prefix ==>
F1-help  F3-return  F7/8-bwd/fwd

```

You can use this screen to change all text that will appear on the User Profile screens.

If you are using certain Data fields for a specific purpose, for example a User ID or Password for a specific application, you may want to change the field descriptions, and/or prevent users from updating the fields themselves.

The following field attributes can be specified:

UNPROT	The field can be entered by each user.
PROT	The field will be visible, but cannot be changed.
DARK	The field will not be visible and cannot be changed.

```
InterSession ----- Maintenance, Screen Layout 17/22 -----  
Screen Layout DEFAULT      Standby Screen  
  
Lines 1-18 (line command I/R/D):  
HDLINE  
. . . . .  
Ä SSSSSS TTTTTTTT AA NN NN DDDDDD BBBBBB YY YY  
Ä SSS TT AAAA NNN NN DD DD BB BB YY YY  
Ä SSSS TT AA AA NN NN NN DD DD BBBB YYYY  
Ä SSS TT AAAAAAAA NN NNNN DD DD BB BB YY  
Ä SSSS TT AA AA NN NN DDDDD BBBBBB YY  
. . . . .  
UserÄUI ;has set this terminal in standby status atÄTIME  
  
Type your password ==> %PW ;  
  
F1-help F3-return F7/8-bwd/fwd
```

You use this screen to change the text that is displayed on the standby screen.

The first position contains an attribute tag or a question mark. A question mark indicates that no further lines will be displayed.

Standard and user-defined attribute tags as well as screen variables may be coded anywhere in these lines.

You may also use line editing commands I, R and D in the first position.

Screen Layout, Top Line Menu / Message Box

```

InterSession ----- Maintenance, Screen Layout 18/22 -----
Screen Layout DEFAULT      Top Line Menu / Message Box

Attn key functionality ==> LM
Selection texts (one unique character capitalized in each):
Sessions      hardCopy      Edit      Give      shaRe
giveBack      Attn          Help      exit
Printer text: Printer:      Current session char: *
User text: User id:         Input/error char: ?
PF key texts: %BW-bwd       %FW-fwd   %CA-end
Edit texts: Cut             Paste
Cut help: Position cursor and press ENTER
Message Box: Goto %V1-goto   Term %V2-terminate  Canc %CA-cancel
----- Enhanced color ----- ----- 4-color -----
Border: BLue               Border: WHItE
First line: GREen          First line: GREen
Capitalized chars: RED      PF keys: BLue
PF keys: GREen             Session names: WHItE
Session names: PINK         Input fields: RED
Input fields: RED           Help text: BLue
Help text: YELlow           Intense help text: WHItE
Intense help text: TURquoise
F1-help  F3-return  F7/8-bwd/fwd

```

You use this screen to change the text and colors used to display the top line menu and the message box.

Attn key functionality

Specify what action the attention key should result in. Note that this is the default value and can be overridden in the User Profile.

TLM	The attention key produces the Top Line Menu.
TV	The attention key mimics the CA-Teleview session manager behaviour.
SS	The attention key mimics the CL/Supersession session manager behaviour.
TPX	The attention key mimics the CA/TPX session manager behaviour.
NO	The attention key will be sent to the application.

The command **Selection texts** can each be up to 12 characters in length. Each command must contain one capitalized letter that is unique to all of the command texts. This capitalized letter becomes the command character that can be selected from the terminal keyboard.

The top line menu will be displayed in color if the terminal supports it. You can define two sets of colors:

- One set for terminals that support enhanced colors. Available colors are BLue, WHItE, RED, GREen, YELlow, PINK and TURquoise.
- One set for terminals that support the basic four colors. Available colors are BLue, WHItE, RED and GREen.

You only have to enter the first three characters (capitalized in the lists above) of the color name.

Screen Layout, Print Header Page Text

```
InterSession ----- Maintenance, Screen Layout 19/22 -----
Screen Layout DEFAULT      Print Header Page Text
* * * * * InterSession Print Request * * * * *
Distribute to: %UI / %UN
Identification: %PX
      Terminal: %TI      Printer: %PI
      Date: %M/%D/%Y      Time: %H.%M

F1-help  F3-return  F7/8-bwd/fwd
```

On this screen you can change the text that is used when printing header pages for hardcopy screen prints and printed messages.

You can specify in each User Profile whether or not header pages are to be printed.

Screen Layout, Panel Tags

To visually enhance the appearance of the panels, you may alter the default attribute tags and define your own tags.

```
InterSession ----- Maintenance, Screen Layout 20/22 -----
Screen Layout DEFAULT      Panel Tags

Tag  Attribute  Color  Highlighting  Attribute  Colors
|    NORMa|  TURquoise
A    HIGH     WHItE
€    HIGH     RED
§    NORMa|  BLUe      REVerse
[    HIGH     WHItE      REVerse
"    HIGH     YELlow    REVerse
<    HIGH     PINK
&    NORMa|  GREEN

                                Highlighting
                                -----
                                DEFault
                                BLInk
                                REVerse
                                UNDerline

InfoMessage NORMa|  YELlow  REVerse
ErrorMessage HIGH    RED      REVerse

F1-help  F3-return  F7/8-bwd/fwd
```

ou may define up to 12 attribute tags. The last two lines represent the attributes for information messages and error messages.

Each tag is a special character, such as "&" which can be assigned both standard and extended attributes, for example reverse video. These special characters are then used on the various panels to indicate the beginning of a field with these attributes.

Note that if the question mark "?" is defined as an attribute tag, you can not use it in the first position of a line.

Screen Layout, Web Layout Settings 1/2

From the Screen Layout you may alter some aspects of the web layout. On the first web customization screen you can define and alter the html file variables. The html files that may contain these variables are **signon.html**, **menu.html**, **sessend.html** and **logoff.html**.

Note that in addition to the variables defined on this screen, these HTML files may contain any of the System Variables. For a complete list see the section "The System Variables".

```

InterSession ----- Maintenance, Screen Layout 22/23 -----
Screen Layout DEFMFA      Web Layout Settings 1/2

  Language code ==> 
  Signon title %STITLE ==> InterSession: Signon
  Menu title %MTITLE ==> InterSession: Menu
  Sessend title %ETITLE ==> InterSession: Session ended
    Text %TEXT1 ==> InterSession signon
    Text %TEXT2 ==> Select application
    Text %TEXT3 ==> Session ended
    Text %TEXT4 ==> Close window
    Text %TEXT5 ==> User logged off
  Userid text %TXUI ==> User id:
  Password text %TXPW ==> Password/phrase:
  New pw text %TXNPW ==> New password/phrase:
  Verify pw text %TXVPW ==> Verify new:
MFA factor1 text %TXMFA1 ==>
MFA factor2 text %TXMFA2 ==>
MFA factor3 text %TXMFA3 ==>
MFA factor4 text %TXMFA4 ==>
MFA factor5 text %TXMFA5 ==>
  Pass ticket text %TXPT ==>
F13-help  F3-return  F7/8-bwd/fwd

```

Language code

This is the default language code used by the web browser, according to the ISO 639-1 standard. Note that InterSession does not check the validity. If nothing is specified, **en** for English is used. It can also be overridden in the Application Profiles.

The **%xTITLE** variables are used as the web window titles for the signon, menu and sessend html files.

The **%TEXT1** - **%TEXT5** are used in various html files.

The variables **%TXUI**, **%TXPW**, **%TXNPW**, **%TXVPW**, **%TXMFA_n** and **%TXPT** are used in the **signon.html** document.

For each variable where you enter a text, one more line where you can enter this credential is produced on the sign on screen. Both the text and corresponding input field are added.

For example, if you want to enter a pass ticket to sign on, just type an appropriate text in the **Pass ticket text %TXPT** field.

Screen Layout, Web Layout Settings 2/2

```
InterSession ----- Maintenance, Screen Layout 23/23 -----
Screen Layout DEFAULT      Web Layout Settings 2/2

Image name %IMAGE1 ==> LOGOPNG.PNG      %IMAGE2 ==>
Image name %IMAGE3 ==>                  %IMAGE4 ==>

Menu HTML document name ==> MENU.HTML
Expand menu listing ==> YES
Menu config header text ==> Configuration
Config expand menu text ==> Expand menu:
Config screen size text ==> Screen size:
Config 3270 style text ==> 3270 style:
Config 3270 key area ==> 3270 key area:
Web user guide text ==> Web User Guide
Terminate window text 1 ==> TERMINATE Application
Terminate window text 2 ==> Are you sure?
Logoff redirect URL ==>

3270 style names (.css) ==> PCOMMX ==> INTRSESS ==> INFO3290
                  (.css) ==> PCOMM ==> ==>
                  (.css) ==> ==> ==>
Keys Above/Below/Hide ==> Above ==> Below ==> Hide
F1-help F3-return F7/8-bwd/fwd
```

Image name

The **%IMAGE_n** variables can be used anywhere in the html files and represent images that are stored in the z/OS HTMLBIN library or the z/VSE InterSession install sublibrary. By default, the **%IMAGE1** is used in the **signon.html** file. Images 2,3 and 4 are unused.

Menu HTML document name

By default, the menu html document is named **menu.html**. If you have created your own version of this html document, specify its name here.

Expand menu listing

If you want the menu listing to be expanded, with one application per line and with the application description included, specify YES, otherwise NO.

Menu config header text

This text will form the link below the menu listing that will open up the configuration section of the menu. If you leave this field blank, the configuration section will be disabled on the menu.

Config expand menu text / screen size text / 3270 style text

These three texts represents the three options in the configuration section of the menu. If you leave any of these texts blank, the corresponding option will be disabled in the configuration section.

Terminate window text 1-2

These texts are used in the **sessend.html** and **logoff.html** files.

Logoff redirect URL

When the user selects an application with application type LOGOFF (default Application Profile name OFF), a box with the message "User logged off" will be shown by default. However, if you rather want to redirect the user to another location in your intranet, you should specify its URL here, for example **//www.acme.com**

3270 style names (.css)

InterSession comes with six sets of Cascading Style Sheets (css).

They are **INTRSESS**, **PCSWIN**, **INFO3290** and **COOL**. If enabled by the "3270 style text" above, the user will have the option to select between these styles in the configuration section of the menu.

You can disable any of these styles by removing them from the list. You can also create your own css file. If so, specify its name here (see also the section "The Web Gateway" below). The first entry will be the default style.

Keys Above Below Hide

The text in the selection box, controlling the placement of the on-screen keyboard.

Screen Layout Listing

If you want to select a set of Screen Layouts from a list, enter L under "Screen Layouts" on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Screen Layouts -----
Screen Layout  Language Default Description
DEFLPW        1      NO      As DEFAULT with long passwords/phrases
DEFPWPP       1      NO      As DEFAULT with RACF pass phrases
DEUTSCH       1      NO      In German
ESPAÑOL       1      NO      In Spanish
LIKEPRD1      1      NO      Resembles CA-TPX
LIKEPRD2      1      NO      Resembles CA-Televue
LIKEPRD3      1      NO      Resembles CA-Solve:Access MAI
LIKEPRD4      1      NO      Resembles CA-Solve:Access EASINET
LIKEPRD5      1      NO      Resembles CL-Supersession
LIKEPRD6      1      NO      Resembles Netview Access Services
SVENSKA       1      NO      In Swedish

F1-help  F3-return  F7/8-bwd/fwd
```

To select a set of Screen Layouts from this screen, position the cursor on a layout ID and press ENTER.

When you press PF3 on the Screen Layout maintenance screen, this screen will be redisplayed.

If you have more Screen Layouts than will fit on one screen, you can scroll backward and forward, using PF7 and PF8.

Screen Layout Examples

Due to the flexible design of the Screen Layouts, the appearance of the screens may be highly customized.

This section shows the sign on and menu screens for two system defined Screen Layouts, the DEFAULT and the LIKEPRD1 layouts.

```

InterSession ----- Sign On ----- Sat Nov 28, 2015 14:43

      IIII      tt      eeee  rr  rrr
      II  nn  nnn  tttt  ee  ee  rrr
      II  nn  nn  tt  tt  eeee  rr
      II  nn  nn  tt  tt  eeee  rr
      IIII  nn  nn  tttt  eeee  rr

      SSSS  EEEEEEE  SSSS  SSS  IIIII  00000  NNN  NNN
      SSS  SSS  EEE  /  E  SSS  SSS  SSS  SSS  III  000 000  NNNN  NNN
      SSS  ///  EEE  /  SSS  ///  SSS  ///  III  000 000  NNN  NNNN
      /  SSSS  EEEEE  /  SSSS  /  SSSS  /  III  000 000  NNN  NNN
      ///  SSS  EEE  /  ///  SSS  ///  SSS  III  000 000  NNN  NNN
      SSS  SSS  EEE  E  SSS  SSS  SSS  SSS  III  000 000  NNN  NNN
      /  SSSS  EEEEEEE  SSSS  /  SSSS  IIIII  00000  NNN  NNN
      /  SSSS  EEEEEEE  SSSS  /  SSSS  IIIII  00000  NNN  NNN

User id ==> Password ==> New password ==>
F1-help  ENT-sign on with user id and password SC0TCP07
  
```

```

      IIII      tt      eeee  rr  rrr
      II  nn  nnn  tttt  ee  ee  rrr
      II  nn  nn  tt  tt  eeee  rr
      II  nn  nn  tt  tt  eeee  rr
      IIII  nn  nn  tttt  eeee  rr

      SSSS  EEEEEEE  SSSS  SSS  IIIII  00000  NNN  NNN
      SSS  SSS  EEE  /  E  SSS  SSS  SSS  SSS  III  000 000  NNNN  NNN
      SSS  ///  EEE  /  SSS  ///  SSS  ///  III  000 000  NNN  NNNN
      /  SSSS  EEEEE  /  SSSS  /  SSSS  /  III  000 000  NNN  NNN
      ///  SSS  EEE  /  ///  SSS  ///  SSS  III  000 000  NNN  NNN
      SSS  SSS  EEE  E  SSS  SSS  SSS  SSS  III  000 000  NNN  NNN
      /  SSSS  EEEEEEE  SSSS  /  SSSS  IIIII  00000  NNN  NNN

Copyright 2015 Astrom Software AB Version 7.2

Userid: Password: New Password:
14:41.23 11/28/15 SC0TCP07 IBM3278-2E

InterSession - the smart alternative

F1-help  ENT-sign on with user id and password
  
```

```

InterSession ----- M E N U ----- Mon Jan 03, 2022 11:01

APPLICATION          INFO *      APPLICATION          INFO *
-----Internal applications----- ! T3270... Mainframe TN3270 se ??
MAINT... InterSession maint      ! START... Window to start mul
STAT...  InterSession status      !
TLOCK... Terminal lock list      !
PROF...   Your user profile       !
MMS..... Message/mailbox sys     !
STBY....  Standby screen          !
OFF.....  Logoff InterSession    !
-----Information screens----- !
SUPPORT.  Contact information     !
-----External applications----- !
CICSP...  Production CICS        ??
CICSD...  Development CICS       ??
Z/VM....  VM/CMS                 ??
TSO.....  TSO/ISPF               !

===== Session status =====
Attention key Attn  Jump key PA1  Command key ENT  Prefix ..

Application ==> 
F1-help  F3-sign off  F7/8-bwd/fwd  ENT-system select  CAL  ISB00002

```

```

InterSession Main Menu for CAL

Attention key Attn  Jump key PA1
Command key ENT    Cmdchar ..

Terminal SC0TCP07
Model    IBM3278-2E
Logmode  SNX32702
System   INTSTEST

Cmd  Sessid  Sesskey  Session Description  Status
MAINT  InterSession maint
STAT   InterSession status
TLOCK  Terminal lock list
PROF   Your user profile
MMS    Message/mailbox system
STBY   Standby screen
OFF    Logoff InterSession
OPEN   Open hours
CICS   A CICS system          N/A
IMS    An IMS system          N/A
CMS    VM/CMS                 N/A

Command ==> 
F1-help  F3-sign off  F7/8-bwd/fwd  ENT-system select

```

Printer Maintenance

Printer maintenance consists of the following:

- Creating profiles on how to format print output for screen hardcopies and MMS messages (printer type HARDCOPY)
- Creating profiles for printing VTAM output to TCPIP printers (printer types TN3270E, LPD, RAW and PJI)
- Creating profiles for printing VTAM output to the spool system (JES, POWER, RSCS)

New Printer

If you want to create a new Printer profile, enter N (new) in the "Printer New/List" field of the maintenance selection screen.

A screen like the following will be displayed:

```
InterSession ----- Maintenance, New Printer -----
Printer Id SP00L
      Printer type ==> 
Valid printer type codes:
HARDCOPY.. Hardcopy/messages to VTAM printer
TN3270E... VTAM gateway to TN3270 printer
LPD..... VTAM gateway to LPD daemon
RAW..... VTAM gateway to LAN printer
PJI..... VTAM gateway to HP LAN printer
SP00L..... VTAM gateway to OS spool system

F1-help  F3-return
```

Define what type of printer profile you want to define and press ENTER.

Printer type HARDCOPY

For HARDCOPY, one printer options profile is supplied. It is named DEFAULT. This profile will be used for any VTAM printer that does not have a printer options profile specifically defined for it.

Modify the DEFAULT profile to match the majority of your VTAM printers, and then define specific profiles for all VTAM printers that do not match the DEFAULT. Note that the InterSession printer name does not have to be the same as the VTAM netname for the printer.

To maintain a printer, enter the name of the printer in the "Printer" field on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Printer -----
Printer Id DEFAULT

Printer type ==> ARDCOPY          Started ==> YES
VTAM Netname ==>
Forms length lines ==> 064
Line width columns ==> 000

Form feed supported ==> YES
Overprint supported ==> YES
NL after full line ==> YES

Top margin lines ==> 00
Bottom margin lines ==> 06
Left margin columns ==> 00 (Message)
Left margin columns ==> 00 (Hardcopy)
Form feed before print ==> NO
Form feed after print ==> YES
Print header ==> YES
Form feed after header ==> YES

'Delete' for removal ==>
F1-help F3-return
```

An explanation of the fields on this screen follows:

Started

YES or NO.

VTAM netname

The VTAM netname of the printer must be specified, except for the DEFAULT profile, where this field must be blank.

Forms length lines

Specify the maximum number of lines per page for the paper being used in this printer. This field is required if NO is specified for field "Form feed supported".

Line width columns

If the printer line width is less than 132 and the printer wraps lines that are too long onto the next line, you must specify the maximum width here.

Form feed supported

Specify YES or NO to indicate whether this printer supports the form-feed command (x'0C'). If you specify NO, you must specify a forms length in the "Forms length lines" field.

Overprint supported

Specify YES or NO to indicate whether this printer supports the "Print-and-space-0" command (x'0D'). If you specify YES, highlighted fields will be printed twice to appear bold. NO indicates that highlighted areas will not show on the printout.

NL after full line

Some printers skip to next line when all print columns are filled, which results in a blank line due to the New Line (NL) control character inserted after each line. To avoid this, code NO in this field, which indicates not to insert a NL character when all print columns are filled. This is related to the Line width columns above.

Top margin lines

Specify the number of lines to be left blank at the top of each page.

Bottom margin lines

Specify the number of lines to be left blank at the bottom of each page.

Left margin columns (Messages)**Left margin columns (Hardcopy)**

Specify the number of columns to be left blank at the beginning of each line. Separate values can get provided for MMS messages, and hardcopy screen prints.

Form feed before print

Specify YES if you want InterSession to advance to a new form before printing each request. Specify NO if the printer is at "Top-of-Form".

Form feed after print

Specify YES if you want InterSession to advance to a new form after printing each request. Specify NO if the printer should be positioned at the end of the printed output.

Print header

Specify YES or NO to indicate whether or not you want to print a heading page prior to each "hardcopy screen print" or MMS message printed.

This option can be overridden by each user using the PROF application.

Form feed after header

Specify YES or NO to indicate whether or not you want to print the heading page on a separate page, or on the same page as the screen print or message. This option can be overridden by each user using the PROF application.

Blank lines after header

Specify how many blank lines you want (0-9) between the heading page and the print data. Note that this field is only shown if "Form feed after header = NO".

'Delete' for removal

To delete this printer option profile, enter the word 'delete' in this field. You cannot delete the profile for the DEFAULT printer options.

Printer type TN3270E

You use this printer type to print to a "personal" IP printer in the network. To do this, you need a TN3270 emulating program on your workstation that supports TN3270 print.

```
InterSession ----- Maintenance, Printer -----
Printer Id TN3270E

Printer type ==> TN3270E          Started ==> NO
VTAM APPLId ==> TN3270E
Interface name ==> TCPIP
EOJ timeout ==> 010
Auth network address ==> 0.0.0.0
Auth network mask ==> 0.0.0.0
Message level 0/1 ==> 1

'Delete' for removal ==>
F1-help  F3-return
```

An explanation of the fields on this screen follows:

Started

YES or NO.

VTAM APPLId

The VTAM APPLId of the associated virtual printer, to be specified in your TN3270 emulating program. Note that this name may be globally altered by using the Startup Parameter VPRINTMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. See "Defining the Startup Parameters" in the chapter "Sysplex Functionality".

Interface name

The name of a defined TCPIP interface profile.

EOJ timeout

To determine end-of-print, specify the number of seconds of no-incoming-print-data-from-VTAM after which the list is considered complete.

Auth network address

To limit the use of this TN3270E printer to a certain range of IP addresses. For instance: 192.168.5.0

Auth network mask

Used with previous parameter. For instance: 255.255.255.0

Message level 0/1

If set to 0, the printing messages IS1706I and IS2004I will not be issued.

'Delete' for removal

To delete this printer, enter the word 'delete' in this field.

Printer type LPD

You use this printer type to print data to an LPD daemon, for instance to the spool queue of a Unix system.

```
InterSession ----- Maintenance, Printer -----
Printer Id UNIX

Printer type ==> PD           Started ==> NO
VTAM APPLid ==> VP02
Interface name ==> TCPIP
IP address ==> 192.168.1.11

Print overlay name ==>
Ascii translate table ==>
VTAM EOI timeout ==> 010
IP response timeout ==> 010
IP err retry interval ==> 060
Low range client port ==> 00721
High range client port ==> 00731
Cntrl file first/last ==> LAST
LPD print queue ==> lp

Message level 0/1 ==> 1

'Delete' for removal ==>
F1-help F3-return
```

An explanation of the fields on this screen follows:

Started

YES or NO.

VTAM APPLid

The VTAM APPLid of the associated virtual printer.

Note that this name may be globally altered by using the Startup Parameter VPRINTMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. See "Defining the Startup Parameters" in the chapter "Sysplex Functionality".

Interface name

The name of a defined TCPIP interface profile.

IP address

The IP address of the LPD daemon.

Print overlay name

Specify the name of a load module in a load library accessible by InterSession, in which a print overlay has been generated. A print overlay module contains printer control statements and contains two parts, to be sent to the printer before and after the print data. See the source library members PCLLAND and PCLPORT for examples of print overlays.

VTAM EOJ timeout

To determine end-of-print, specify the number of seconds of no-incoming-print-data-from-VTAM after which the list is considered complete.

IP response timeout

Specify the number of seconds InterSession should wait for acknowledgement from the printer. After this interval, InterSession disconnects the session and will retry after another time interval:

IP err retry interval

This is the number of seconds InterSession will wait before retrying after a timeout has occurred.

Low range client port / High range client port

Specify the range of the client port numbers. Default port range is 721-731.

Cntrl file first/last

The LPD daemon requires a control file to be sent either before or after the print data. Default is LAST, but certain LPD daemons need to have the control file sent first.

LPD print queue

Specify the name of the LPD daemon's print queue. Default is 'lp'.

Message level 0/1

If set to 0, the printing messages IS1706I and IS2004I will not be issued.

'Delete' for removal

To delete this printer, enter the word 'delete' in this field.

Printer type RAW or PJL

You use this printer type to print data to an IP printer directly connected to the network.

```

InterSession ----- Maintenance, Printer -----
Printer Id HP4550

Printer type ==> PJL          Started ==> NO
VTAM APPLid ==> VP01
Interface name ==> TCPIP
IP address ==> 192.168.1.55

Print overlay name ==>
Ascii translate table ==>
VTAM EOI timeout ==> 010
IP response timeout ==> 010
IP err retry interval ==> 060

Message level 0/1 ==> 1

'Delete' for removal ==>
F1-help F3-return

```

An explanation of the fields on this screen follows:

Printer type

PJL or RAW. Specify PJL if the IP printer supports the HP Printer Job Language, otherwise RAW.

Started

YES or NO.

VTAM APPLid

The VTAM APPLid of the associated virtual printer.

Note that this name may be globally altered by using the Startup Parameter VPRINTMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. See “Defining the Startup Parameters” in the chapter “Sysplex Functionality”.

Interface name

The name of a defined TCPIP interface profile.

IP address

The IP address of the printer.

Print overlay name

Specify the name of a load module in a load library accessible by InterSession, in which a print overlay has been generated. A print overlay module contains printer control statements and contains two parts, to be sent to the printer before and after the print data. See the source library members PCLLAND and PCLPORT for examples of print overlays.

ASCII translate table

Specifies the name of a module containing an EBCDIC-ASCII translate table (a load module in the InterSession library). See the assembler example members SWE850 and SWE88591 (Swedish codepages 850 and 88591) in the source library for how such a module should be created. The source members should be assembled and link edited to InterSession's load library. If no translate table is defined, a translation between EBCDIC codepage 37 and ASCII is performed.

VTAM EOJ timeout

To determine end-of-print, specify the number of seconds of no-incoming-print-data-from-VTAM after which the list is considered complete.

IP response timeout

Specify the number of seconds InterSession should wait for acknowledgement from the printer. After this interval, InterSession disconnects the session and will retry after another time interval:

IP err retry interval

This is the number of seconds InterSession will wait before retrying after a timeout has occurred.

Message level 0/1

If set to 0, the printing messages IS1706I and IS2004I will not be issued.

'Delete' for removal

To delete this printer, enter the word 'delete' in this field.

Printer type SPOOL

You use this printer type to write print data to the system's spool queue.

```

InterSession ----- Maintenance, Printer -----
Printer Id JES2

Printer type ==> SPOOL           Started ==> NO
VTAM APPLid ==> INTSVPO1
EOJ timeout ==> 010

Class ==> S
Forms id ==> IS72
Destination node ==>
Destination user ==>
External writer ==>
FCB name ==>
UCS name ==>
Flash value ==>

Break string ==>
Break column ==> 000
Break flunk pages ==> 0
Insert form feed ==> YES
Message level 0/1 ==> 1
'Delete' for removal ==>
F1-help F3-return

```

An explanation of the fields on this screen follows:

Started

YES or NO.

VTAM APPLid

The VTAM APPLid of the associated virtual printer.

Note that this name may be globally altered by using the Startup Parameter VPRINTMASK. This is a parameter normally used in a sysplex environment, but can be used for a stand-alone InterSession system also. See “Defining the Startup Parameters” in the chapter “Sysplex Functionality”.

EOJ timeout

To determine end-of-print, specify the number of seconds of no-incoming-print-data-from-VTAM after which the list is considered complete.

Class / Forms id / Destination / External writer / FCB name / UCS name / Flash value / Job name

Specify the characteristics of how the spool queue entry should be created.

Break string

When InterSession finds this text string in the print data, it will cause a report break, i.e. a new spool file.

Break column

Defines the column where the string defined in "Break string" should start. The first printable column is 001. Setting the value to "000" disables the break function.

Break flunk pages

Number of pages to be flunked when "Break string" is found. Set to 0 to include the page where the string was found in the new report, set to 1 to ignore one page (starting with the page the string was found on) etc.

Insert form feed

YES or NO. Specify YES if InterSession shall insert a form feed character at the beginning of the report.

Message level 0/1

If set to 0, the printing messages IS1706I and IS2004I will not be issued.

'Delete' for removal

To delete this printer, enter the word 'delete' in this field.

Printer Listing

If you want to display a list of all printers, from which you can select one to maintain, enter L in the "New/List" field under "Printer" on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Printers -----
Printer Id  Type      Netname   Started
DEFAULT    HARDCOPY
HP4550      PJI         VP01      NO
UNIX        LPD         VP02      NO

F1-help  F3-return  F7/8-bwd/fwd
```

To select a printer from this screen, position the cursor on a screen ID and press ENTER. When you press PF3 on the Printer Options screen, this screen will be redisplayed. If you have more printers than will fit on one screen, you can scroll backward and forward, using PF7 and PF8.

Interfaces Maintenance

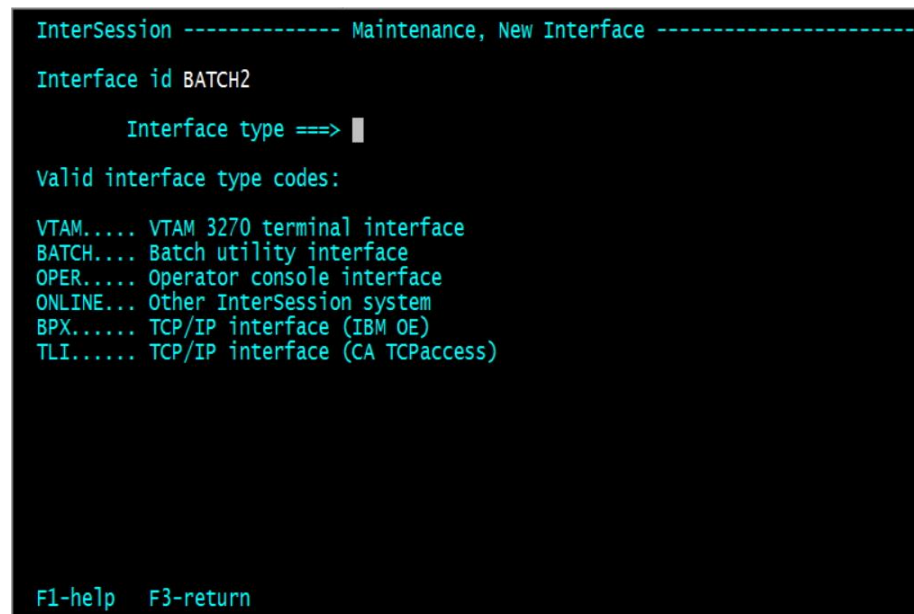
InterSession need to have one or more interfaces to the outer world. They are used for terminal, application and printer connections and for service functions like the console operator or batch connections.

If all interfaces are disabled or deleted, preventing you from establishing a session with InterSession, they can be activated at startup by using **INTERFACE** startup parameters. See the "Startup Parameters" section earlier in this manual.

New Interface

If you want to create a new Interface, enter N (new) in the "Interface New/List" field of the maintenance selection screen.

A screen like the following will be displayed:



```
InterSession ----- Maintenance, New Interface -----
Interface id BATCH2
      Interface type ==> 
Valid interface type codes:
VTAM.... VTAM 3270 terminal interface
BATCH.... Batch utility interface
OPER.... Operator console interface
ONLINE... Other InterSession system
BPX..... TCP/IP interface (IBM OE)
TLI..... TCP/IP interface (CA TCPaccess)

F1-help  F3-return
```

A description of the interface codes follows:

OPER

The OPER interface must be active in order for InterSession to accept commands from the operator console.

VTAM

The VTAM interface is used for incoming VTAM 3270 terminal connections and for the batch and online interfaces. It need not be active for to use application sessions of type VTAM.

BATCH

The BATCH interface is needed if you want to use the batch utility INTSUTIL functions that establishes a VTAM session

ONLINE

If you have more than one InterSession system and need to use the functions for sending MMS mail and messages between the systems, you must define an ONLINE interface for each other system you want to send to.

BPX

This is the TCPIP interface for IBM's TCPIP stack (z/OS).

Interface Type VTAM

```
InterSession ----- Maintenance, Interface -----
Interface id VTAM                                Change interface id ==>
      Interface type ==> VTAM
      VTAM applid ==> INTSTEST
      LOGAPPL applid ==>
      Active ==> YES

F1-help  F3-return
```

Change interface id

If you want to rename the interface, enter the new name here.

VTAM applid

The main APPLid used by VTAM 3270 terminals. This is mandatory. If the interface is active, you can not alter the APPLid.

LOGAPPL applid

The logon APPLid used by VTAM 3270 terminals. This is optional and, if used, causes InterSession to become the VTAM logon application for the terminal.

Active

YES or NO.

'Delete' for removal

Enter the word 'delete' to delete the interface. The interface must be inactive for this field to appear.

Interface Type BPX

```

InterSession ----- Maintenance, Interface -----
Interface id TCPIP                                Change interface id ==>

    Interface type ==> BPX
    TCP/IP ident ==> 
    Termid 1st char ==> T
    Active ==> NO

'Delete' for removal ==>
F1-help  F3-return

```

Interface type BPX (z/OS)

This also known as IBM Open Edition (OE), Open Extensions or Unix Services.

TCP/IP ident

This is the name of the STC/job name of the TCPIP stack. If you have only one stack, you should leave it blank.

Termid 1st char

The first character in the generated pseudo LU-name.

Notes

- Your z/OS system must have at least version 2.5 of the Unix Services.
- The z/OS user id who submits the InterSession job must have an OMVS segment defined in RACF with a GID value.

If the user has no OMVS segment defined, you can locate a RACF group with an OMVS segment and with a GID defined. Then use the RACF command **ALTUSER userid DFLTGRP(group)**.

There are other ways to accomplish t

his, please see the appropriate IBM documentation.

Interface Type BATCH

```
InterSession ----- Maintenance, Interface -----
Interface id BATCH                                Change interface id ==>
    Interface type ==> BATCH
    VTAM applid ==> INTSUTIL
    Active ==> YES

'Delete' for removal ==>
F1-help  F3-return
```

A BATCH interface is needed if you want to perform certain functions in the batch program INTSUTIL, such as the MAINT function.

VTAM applid

This is the VTAM APPLid used by the INTSUTIL program (see the APPLID= card).

Active

YES or NO.

Interface Type ONLINE

```

InterSession ----- Maintenance, Interface -----
Interface id INTSESS2          Change interface id ==>

  Interface type ==> ONLINE
    VTAM applid ==> INTSESS2
    Site id ==> INTS2

    Active ==> YES

'Delete' for removal ==>
F1-help  F3-return

```

The ONLINE interface is needed if you have more than one InterSession system and want to send MMS mail / messages between the systems.

VTAM applid

This is the VTAM APPLid used by the other InterSession system.

Site id

To send to the other system you need to prefix the user id with this unique id, for example INTS2.MIKECH. This site id must be defined in the other InterSession system, using MAINT, System Options and APPLpools, Other System Options, field "System site id".

Active

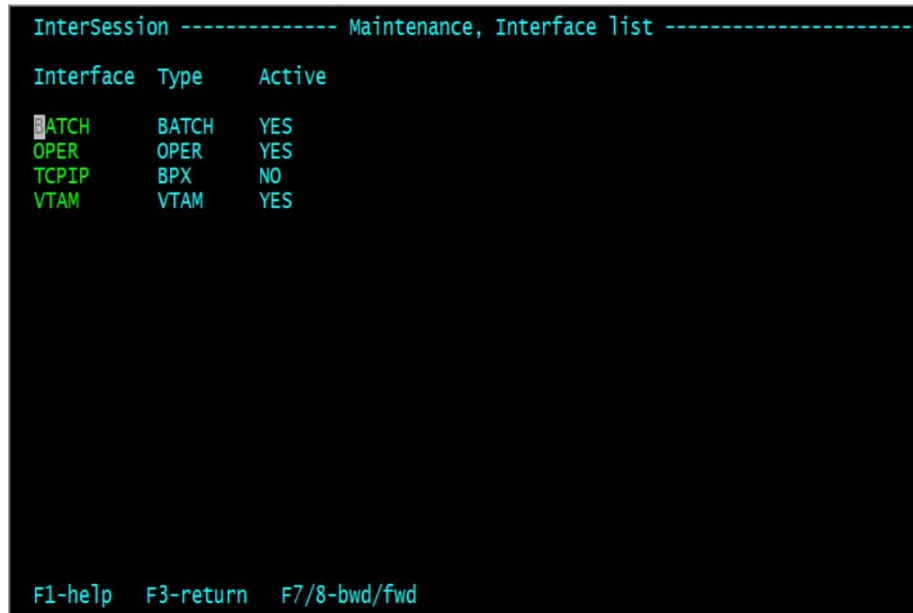
YES or NO.

Notes

- For each other InterSession system, you will need to define an ONLINE interface. For example, if you have three systems you should define systems 2 and 3 in system 1, systems 1 and 3 in system 2 and systems 1 and 2 in system 3.
 - InterSession will automatically establish a VTAM session to each other system defined by an ONLINE interface.
 - When there is a change in the session status you will see any of the IS0801I, IS0802I and IS0803I messages on the system console.
-

Interface Listing

If you want to display a list of all interfaces, from which you can select one to maintain, enter L in the "New/List" field under "Interfaces" on the maintenance selection screen. A screen like the following will be displayed:



InterSession ----- Maintenance, Interface list -----		
Interface	Type	Active
BATCH	BATCH	YES
OPER	OPER	YES
TCPIP	BPX	NO
VTAM	VTAM	YES
F1-help F3-return F7/8-bwd/fwd		

To select an interface from this screen, position the cursor on a screen ID and press ENTER. When you press PF3 on the Interface screen, this screen will be redisplayed. If you have more interfaces than will fit on one screen, you can scroll backward and forward, using PF7 and PF8.

Services Maintenance

A service must be defined in the following cases:

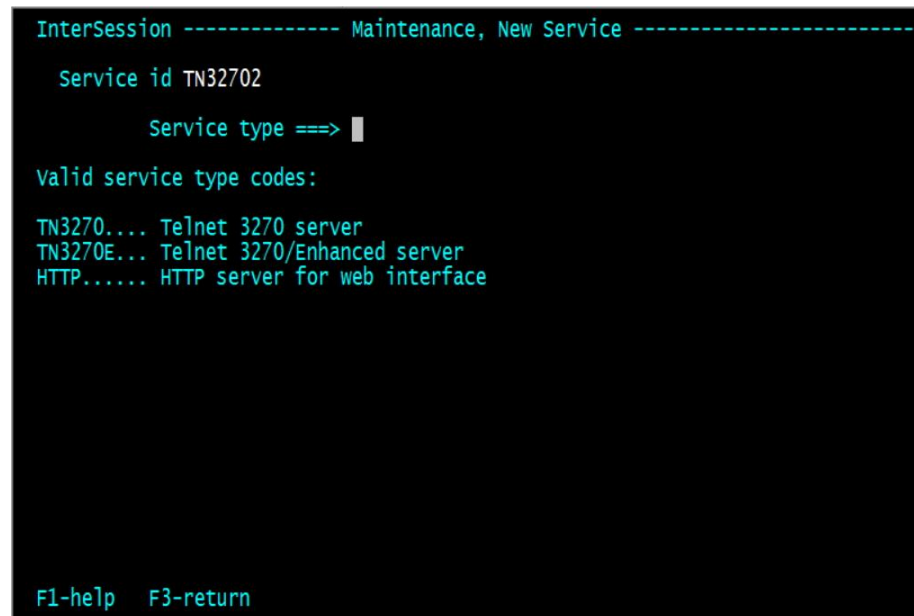
If you want to connect to InterSession from a TN3270 client program

If you want to connect to InterSession from a web browser.

New Service

If you want to create a new service, enter N (new) in the "Service New/List" field of the maintenance selection screen.

A screen like the following will be displayed:



```
InterSession ----- Maintenance, New Service -----
Service id TN32702
      Service type ==> 
Valid service type codes:
TN3270.... Telnet 3270 server
TN3270E... Telnet 3270/Enhanced server
HTTP..... HTTP server for web interface

F1-help  F3-return
```

Service type

Specify TN3270 or TN3270E (Enhanced) if you want InterSession to start a new TN3270 server.

Specify HTTP if you want InterSession to start a new HTTP server for the Web Gateway.

Service Types TN3270 and TN3270E

```

InterSession ----- Maintenance, Service -----
  Service id TN3270                      Change Service id ==>

    Service type ==> TN3270E
      Interface ==> TCPIP
        Port ==> 02323
  Multi-homed IP address ==> 0.0.0.0

    Queue length ==> 005
      Active ==> NO

  'Delete' for removal ==>
F1-help  F3-return

```

Interface

The name of the TCPIP interface you want to use for this service (normally, you only have one TCPIP interface defined).

Port

The port number on which the service will appear.

Multi-homed IP address

If you have more than one IP address defined in your TCP/IP stack and you want InterSession to use only one of them, specify here which address InterSession should use.

Queue length

The length of the listen queue, usually in the range 5-20.

Active

YES or NO.

Notes

- "Service Type" can be TN3270E or TN3270. If TN3270E is specified, InterSession will try to negotiate a TN3270E connection. If that fails, a normal TN3270 session will be established. Certain older clients may fail to negotiate a TN3270 connection from a TN3270E service. If so, create a TN3270 service on another port, or change the Service Type to TN3270.
 - The TN3270E service implements "Basic TN3270E" described in RFC2355 (Obsoletes RFC1647).
-

- “Port” must be coordinated with other services on your machine. Suggested numbers are 1023, 2023, 3023. You may have to do configuration changes in your TCP/IP stack (see *TCP/IP Interfaces*). If you want to use port 23 you need to disable that port in your TCP/IP stack.
- “Queue Length” is the number of unprocessed connections InterSession can handle. The connect process normally takes a fraction of a second. “5” means that a connection rate of more than 5 new connections/second can be handled. Do not increase this number unless you experience problems. 5 is suitable for “small” sites (less than hundred users). A higher number than necessary may cause overhead in the TCP/IP stack.
- See *Appendix D* for recognized terminal types.

Service Type HTTP – The Web Gateway

```

InterSession ----- Maintenance, Service -----
Service id HTTP                                Change Service id ==>
Service type ==> HTTP
Interface ==> TCPIP
Port ==> 08080
Multi-homed IP address ==> 0.0.0.0
Queue length ==> 005
Identification text ==>
Root folder name ==>
Use HTTPLOG ==> NO
Active ==> NO

'Delete' for removal ==>
F1-help  F3-return

```

Interface

The name of the TCPIP interface you want to use for this service (normally, you only have one TCPIP interface defined).

Port

The port number on which the service will appear.

Multi-homed IP address

If you have more than one IP address defined in your TCP/IP stack and you want InterSession to use only one of them, specify here which address InterSession should use.

Identification text

This text will appear in the browser's user identification window.

Root folder name

If you need a common top level folder name for all web traffic on this service, specify the folder name here. It must be specified as a simple name, without any leading, embedded or trailing slashes.

Queue length

The length of the listen queue, usually in the range 5-20.

Use HTTPLOG

YES, VSAM or NO.

YES: InterSession will create a sequential HTTP log file. You must have a sequential file with the name HTTPLOG defined in the InterSession startup JCL.

VSAM: InterSession will create a VSAM wrap-around HTTP log file. You must create the HTTPLOG VSAM file and have it defined in the InterSession startup JCL. The VSAM file will also be viewable in the STAT application.

For more information, see the section "The Web Gateway" later in this manual.

Active

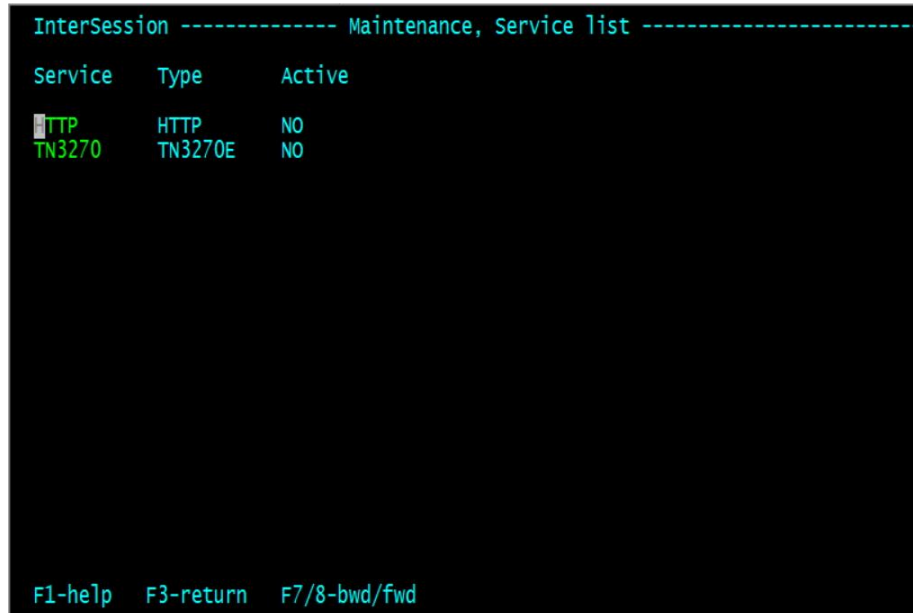
YES or NO.

Notes

- "Port" must be coordinated with other services on your machine. You may have to do configuration changes in your TCP/IP stack (see *TCP/IP Interfaces*). If you want use port 80 you need to disable that port in your TCP/IP stack.
 - "Queue Length" is the number of unprocessed connections InterSession can handle. The connect process normally takes a fraction of a second. "5" means that a connection rate of more than 5 new connections/second can be handled. Do not increase this number unless you experience problems. 5 is suitable for "small" sites (less than hundred users). A higher number than necessary may cause overhead in the TCP/IP stack.
-

Service Listing

If you want to display a list of all services, from which you can select one to maintain, enter L in the "New/List" field under "Services" on the maintenance selection screen. A screen like the following will be displayed:



Service	Type	Active
HTTP	HTTP	NO
TN3270	TN3270E	NO

F1-help F3-return F7/8-bwd/fwd

To select a service from this screen, position the cursor on a screen ID and press ENTER. When you press PF3 on the Service screen, this screen will be redisplayed. If you have more services than will fit on one screen, you can scroll backward and forward, using PF7 and PF8.

Help Screen Maintenance

If you want to maintain a set of help screens, enter the name of the help screens in the "Help Screen ID" field on the maintenance selection screen.

A screen like the following will be displayed:

```
InterSession ----- Maintenance, Help screen selection -----
Help screen id DEFAULT
      Select help item ==> █      'Delete' for removal ==>
01 - Sign on screen              08 - Message receiver list
02 - Menu screen                 09 - Message list of DL-s
03 - Info screen                 10 - Message list of one DL
04 - User profile screen 1/2     11 - Message receiver selection
05 - User profile screen 2/2     12 - Message receiver sel. users
06 - Message status screen       13 - Message receiver sel. DL-s
07 - Message text screen         14 - Top Line Menu
More item numbers on next page

F1-help  F3-return  F7/8-bwd/fwd
```

These help screens are available for all Help screen sets.

Help items over 14 are only available for screen set DEFAULT and are used for help texts related to screens available only to users with special privileges, such as System Administrators or Master Operators. To view these help items, use the PF8 key.

The help text for item 14 (Top Line Menu) can only be 40 characters per line because the text is displayed within a help window.

To delete an entire set of help screens, enter 'Delete' in the "'Delete' for removal" field and press ENTER.

Select the desired help item and press ENTER.

Depending on the item selected, a screen like the following will be displayed:

```

InterSession ----- Maintenance, Help screen text -----
Help screen id DEFAULT  Header: Help - User Profile Screen 1/2      Page 1
Copy from id:
- All fields shown except the user id and user group may be altered.
-
- +Autostart+Application: One or more systems can be automatically started
- after a successful sign on, which means that the user will go directly from
- the sign on screen to the application(s) coded here.
- If you have started more than one application, or if it is unavailable,
- or if you are not authorized for the system, the Menu Screen will appear.
- +Screen+Layout: There may be more than one screen layout available, in
- different style or language etc. Ask your System Administrator for the names.
- +Two+level+Menu: The Menu Screen may be shown in one or two levels.
- +Attn+key+function: How the Attention Key is used:
-   +TLM = Top Line Menu.
-   +TV  = Televue behaviour.
-   +SS  = Supersession behaviour.
-   +BRK = Menu screen.
-   +NO  = Attention key sent to application.
-   +DEF = system default.
- +Initial+command: Here you may code a character representing a Top Line Menu
- command (one of the capitalized characters). This will be executed directly.
F1-help  F3-return  F7/8-bwd/fwd

```

You can use this screen to modify the text of the help screens, up to three pages of text per help item.

You may also use the "Copy from id" field to replace all text for this screen with the text from another set of Help Screens. Type the name of the other Help Screen id and press ENTER.

An entire line may be highlighted by typing a + (plus) sign in the first position. A plus sign in front of a word will highlight that word only (if the first position of the line is a -).

You may also use line editing commands in the first position:

- I Insert a new line after this line
- R Repeat this line
- D Delete this line

Help Screen Listing

If you want to display a list of sets of help screens, from which you can select one to maintain, enter L under "Help Screens" on the maintenance selection screen. A screen like the following will be displayed:

```
InterSession ----- Maintenance, Help screens -----
Help screen id
█ DEFAULT
DEUTSCH
ESPANOL
LIKEPRD1
LIKEPRD2
LIKEPRD3
LIKEPRD4
LIKEPRD5
LIKEPRD6
SVENSKA

F1-help  F3-return
```

To select a set of help screens from this screen, position the cursor on a help screen ID and press ENTER. When you press PF3 on the help maintenance screen, this screen will be redisplayed. If you have more sets of help screens than will fit on one screen, you can scroll backward and forward, using PF7 and PF8.

System Options and APPLpools Maintenance

On the MAINT selection screen the System Options entry will only be visible to System Administrators:

```

New/List ==>      Help Screen Set ==>      Copy ==>
System Options and APPLpools:
Password ==>

F1-help  F3-return

```

To enter the System Options maintenance, type your current password or pass phrase in this field.

If you have signed on to InterSession using MFA credentials or a PassTicket, you will instead be prompted to type an "S" to select the System Options maintenance.

The following screen will appear.

System Options Selection

```

InterSession ----- Maintenance, System Options -----

      Select ==>  New APPLid Pool number ==>

1 Internal Security
2 External Security 1/3
3 External Security 2/3
4 External Security 3/3
5 Scripting
6 User/Application Defaults
7 Terminal Keys Defaults
8 Other System Options
9 User Exits

A APPLid Pools for application sessions
N New APPLid Pool

F1-help  F3-return  F7/8-bwd/fwd

```

To view/change any of the System Options, type a digit from 1 to 9 in the "Select" field.

To get a listing of your APPLid Pools, type an A. From this listing you can then select one of the pools for further updates.

To create a new APPLid Pool, type an N plus the new pool number in the "New APPLid Pool number" field.

System Options, Internal Security

```
InterSession ----- Maintenance, Internal Security Options -----
Password options:
  Min password length ==> 1
  Max password/phrase length ==> 008
  Min no. of upper case letters ==> 00
  Min no. of lower case letters ==> 00
  Min no. of numeric characters ==> 00
  Min no. of special characters ==> 00
  Passwords are case sensitive ==> YES
  Phrases are case sensitive ==> YES
  Embedded blanks allowed ==> NO
  Compare no. of old passwords ==> 08
  Pw expiration warn msg (days) ==> 05
  Expired password value ==>
Other internal security options:
  Signon attempts before lock ==> 10
  -- within number of minutes ==> 010
  Inactive days before revoke ==> 030
  Signon attempts before revoke ==> 05
  Signon attempts standby screen ==> 03
  Terminal id logon supported ==> NO
F1-help  F3-return  F7/8-bwd/fwd
```

These are the system-wide options used if no External Security Manager like RACF is installed, or for users not defined to External Security.

An explanation of the fields on this screen follows:

Minimum password length
Maximum password length
Min no. of upper case letters
Min no. of lower case letters
Min no. of numeric characters
Min no. of special characters
Passwords are case sensitive
Embedded blanks allowed

With these parameters you control the appearance of user passwords / passphrases. Note that if you use passphrases the option “**Embedded blanks allowed**” must be set to **YES**.

Compare no. of old passwords

This operand is used to check old passwords whenever a user alters his or her password. This prevents a user from reusing an old password for the number of password changes specified here.

You can specify from 1 to 64. The default value is 8.

Password expiration warn message (days)

A warning message may be issued to the user after a successful sign on, which indicates in how many days the current password will expire. Specify here how many days in advance this message is to be shown. A value of zero disables this message.

Expired password value

When this character string is entered by an administrator as a user's new password, it will immediately be expired. This is useful when a user has forgotten his current password. When this password is set for the user, he is forced to enter a new personal password at first signon.

Signon attempts before lock
- within number of minutes

These operands can be used to lock a terminal's keyboard if the specified number of invalid sign on attempts occurs within the specified time interval. When the terminal is "locked", the lock screen is displayed and an informative message of the violation will be written to the system log.

Specify the number of invalid sign on attempts. If 99 is specified, the terminal will never be locked.

Specify the time interval within which the invalid sign on attempts must occur. If 0 is specified, the number of attempts can occur over any time interval.

The default values are 10. Each time a successful sign on is completed, these values are reset.

Inactive days before revoke

Specify the number of days of user inactivity at which point you want a user's access to be automatically revoked. If 999 is specified, the user's access will never be revoked due to inactivity.

System Administrator Profiles will never be revoked via this operand.

The default value is 30.

Signon attempts before revoke

Specify the number of unsuccessful sign on attempts at which point you want to automatically revoke the user's access. If 99 is specified, the user's access will never be revoked due to too many sign on attempts.

The default value is 5.

Signon attempts standby screen

Specify the number of allowed logon attempts on the standby screen at which point the sign-on screen will be automatically redisplayed.

The default value is 5.

Terminal id logon supported

If set to YES, a pseudo-automatic sign on may be used. If a user hits the Enter key on the Sign On screen without entering a user id or password, the terminal id will be used to search the User Profiles. If a User Profile with user id equal to the terminal id is found and no password is set in the User Profile, the sign on is accepted.

This means that the administrator must have created a User Profile with this id and with blanks typed in the password field. It is also recommended to set "Can change password" to NO in these profiles.

System Options, External Security

There are three screens where you define the options for External Security. Some of the options on these screens will not have immediate effect but requires a system restart. Such parameters are marked with x) on the screen.

Refer to the section on "External Security" for more information.

General settings

```
InterSession ----- Maintenance, External Security Options 1/3 -----
General:
  Security manager x) ==> RACF
  Number of subtasks x) ==> 002

  Passwords are case sensitive ==> YES
  Phrases are case sensitive ==> YES
  Accept password in phrase field ==> YES

  Extract to user profile Y/N: Name> N Group> N CICS opid> N

  Store extsec users in data base ==> YES

  Show security manager messages ==> NO

  Get better invalid pw messages ==>
  To get InterSession messages, enter your RACF passwd rules below:
  Minimum length ==> Maximum length ==> Mask ==>
  Blank/N clears rules Mask legend A C c V v W N L m x s
  Special chars allowed ==>

  x) Changes to these fields will not take effect until next startup
  F1-help F3-return F7/8-bwd/fwd
```

Security manager

If you do not use an Security Manager, leave this field blank. Otherwise, specify the name of the Security Manager, that is RACF, ACF2 or TSS.

Number of extsec subtasks (z/OS only)

This parameter controls the "Multithreaded signon" facility, see the External Security chapter.

All External Security processing takes place within one or more subtasks. A system with several thousands of users may see performance degradation in the sign on processing. You can then specify a higher number of subtasks (threads), in the range from 2 to 255.

If you are using an MFA product for user authentication, the number should probably be increased, since in most cases a remote server is involved.

The default is 2.

Passwords are case sensitive

Phrases are case sensitive

If set to NO, InterSession will always convert a password / phrase entered on the sign on screen to upper case. If the passwords / phrases are case sensitive, specify YES.

Accept password in phrase field

If you have phrase fields on the sign on screen (using the %PP, %NPP and %VNPP variables) and do not want the users to enter passwords in these fields, specify NO. This is useful if you do not have any password fields on the sign on screen and want to force the use of pass phrases.

If set to YES, the users can enter both passwords and phrases in the %PP, %NPP and %VNPP fields.

Extract to User Profile Y/N

Specify Y or N for the three fields Name, Group and CICS Opid. Any of the three fields set to Y will cause InterSession to extract this information from the External Security Manager at sign on time and update the corresponding User Profile field.

Store extsec users in data base

YES or NO. If set to YES, a new User Profile will be added to the InterSession data base when a user signs on that does not exist in InterSession, but exist in the External Security Manager. If set to NO, a User Profile will only be created in storage but not added to the data base.

Show security manager messages

YES or NO. If YES, all relevant messages from the security manager is shown to the user, either on the sign on screen or on the menu screen, depending on if the signon failed.

Get better invalid pw messages (RACF only)

If you specify your current RACF password rules in the following fields, InterSession will do the same password contents checks as RACF. InterSession will then be able to give the end user a detailed error message when an error in a new password is detected. If you specify nothing, a generic error will be issued, simply saying that the new password is in error.

Minimum length

Give the minimum length of a password 1-8. To clear all password rules fields, enter a blank or the character "N".

Maximum length

Give the maximum length of a password 1-8.

Mask

Valid mask characters are shown on the screen. For detailed information on these codes, see the appropriate IBM RACF documentation. The mask must be exactly as long as the "Maximum length". If you are not using a RACF mask, type asterisks "*" in this field.

Special chars allowed

Type YES or NO..

Note that the option above "Passwords are case sensitive" is also used to perform the password checks.

Press PF8 to see the second screen on External Security,

Application Access:

```
InterSession ----- Maintenance, External Security Options 2/3 -----
Application access:
Obtain application access from ==> MODELS    MODELS, APPLNAMES or -blank-
      Select model names from ==> XSGROUP    XSGROUP, XSDEFGRP, XSPROFILE,
      Security manager class ==>             INSTDATA or model name
      Access required ==>                   READ/UPDATE
      'XSGROUP' group name prefix ==>
      'INSTDATA' model prefix string ==>
      'INSTDATA' stop character ==>
      Copy model attributes ==> YES         YES/NO/EXT
      Copy at every signon ==> NO          YES/NO
      Copy from first model only ==> NO     YES/NO

F1-help  F3-return  F7/8-bwd/fwd
```

Obtain application access from

Set to **MODELS**, **APPLNAMES** or leave it blank.

MODELS if you use Models to give the user access to applications. See next option.

APPLNAMES means that every Application is checked with the security manager to see what applications the user should see.

Select model names from

This field can be set to **XSGROUP**, **XSDEFGRP**, **XSPROFILE**, **INSTDATA** or the name of a specific Model.

See the section **Controlling Application Access** in the External Security chapter for information.

Security manager class

This must be specified if the previous field is set to **XSPROFILE**.

For RACF, it can be any system- or user-defined class.

For TopSecret, this can be **XLCFCMD**, **ABSTRACT** or any other user-defined class.

For ACF2, this should be the name of an ACF2 resource type, such as **CKC** (CICS transactions) or any user-defined resource type.

You can only specify a single class or resource type, which means that all InterSession resources must belong to this class or have this resource type.

Access required

If you have set the Security manager class field, you must define here if the user will need **READ** or **UPDATE** access to the Security manager's **PROFILES**.

"XSGROUP" group prefix

You can set a group name prefix here from one to eight characters. InterSession will match the security manager group names against this prefix to determine what group names to use as Model names.

Default is blank, meaning all group names.

“INSTDATA” model prefix string

If the Model name does not start in the first position of the INSTDATA field, specify a string to search for in order to find the model name in INSTDATA. Default is first position of INSTDATA. Example **TELEVIEW(**

“INSTDATA” stop char

If the Model name is delimited by a special character, specify this character here, for instance “)”. By default there is no stop character and eight characters are picked up by InterSession

Copy Model attributes

This parameter refers to the “External Security user Model”, see above. When set to YES or EXT, certain information from the Model profile(s) will be copied to the user’s profile. See the section **User Model Application Access** in the External Security chapter for more information.

The effect of adjusting this parameter can be monitored with the STAT application.

Copy at every signon

This parameter refers to the “External Security user Model”, see above. When set to NO (the default) the Model will only be applied if the user does not exist in InterSession. When set to YES, the Model will be applied to the User Profile every time the user signs on to InterSession. This can be useful if you want to add or remove applications from the Model and have these changes propagated to the User Profiles.

Note 1: When set to YES, any sign on exit will be called with a type “2” call every time a user signs on.

Copy from first model only

Specify whether InterSession should copy information from all Models or from the first Model only.

MFA options

```
InterSession ----- Maintenance, External Security Options 3/3 -----
MFA options:
  Message number prefix ==> 
  Msg number error suffix ==> 
  Msg number info suffix ==> 

  Compound In-Band factors ==> 

  Show MFA messages to user ==> YES
  Show waiting msg after nn secs ==> 00 00 - no msg

F1-help  F3-return  F7/8-bwd/fwd
```

Message number prefix
Msg number error suffix
Msg number info suffix

See the section **Identifying MFA messages** for information.

Compound In-Band factors

See the section **IBM MFA compound In-Band support** for information.

Show MFA messages to users

YES or NO. If YES, all relevant messages from the MFA system is shown to the user, either on the sign on screen or on the menu screen, depending on if the signon failed.

Show waiting message after nn secs

If you are using an MFA product for user authentication and are experiencing long response times when signing on to InterSession, you may want to show an explaining message to the user who waits for the sign on to complete.

Setting this to 00 disables the function. The message text is found in the Screen Layout, Messages 7/7.

See also the section on Multi-Factor Authentication.

System Options, Scripting

```

InterSession ----- Maintenance, Scripting -----
Scripts reside in a PDS ==> x)  YES
Using Panel PDS ==> x)  YES

User related variables populated from extsec data:
Variable      Extsec      Extsec      Extsec      Length   Type
name          class       segment     field name  1-99     CUNPX

==> NAME       ==> USER    ==> BASE     ==> PGMNAME ==> 24    ==> C
==> DEFGRP     ==> USER    ==> BASE     ==> DFLTGRP ==> 08    ==> C
==> INSTDATA   ==> USER    ==> BASE     ==> INSTDATA ==> 60    ==> C
==>           ==>         ==>         ==>         ==>         ==>
==>           ==>         ==>         ==>         ==>         ==>
==>           ==>         ==>         ==>         ==>         ==>
==>           ==>         ==>         ==>         ==>         ==>
==>           ==>         ==>         ==>         ==>         ==>
==>           ==>         ==>         ==>         ==>         ==>

x) Changes to these fields need a restart
F1-help  F3-return  F7/8-bwd/fwd

```

On this screen you can change the system-wide options related to scripts.

Scripts reside in a PDS

By default, the scripts reside in the INTSFLE VSAM file.
If your scripts reside in a PDS, set this option to YES.

Using Panel PDS

If you are using Panels (for example by the DISPLAY command in TPX ACLs) you can give InterSession access to them by setting this option to YES.
The Panels must be written following the IBM ISPF structure.

Note that the PDSs must be defined as fixed blocked with a record length of 80.
You must also put DD cards in the InterSession startup JCL:

```
//SCRIPTS DD DSN=the.scripts.pds,DISP=SHR
//PANELS  DD DSN=the.panels.pds,DISP=SHR
```

User related variables populated from extsec data

You can define up to ten system-wide read-only variables that can be used in scripts or on the menu screen. These variables contain user-specific data obtained from External Security.

For each variable you should define

- The variable name
- The External Security field name, the Extsec class name and if applicable the segment name. See the appropriate publication from the External Security vendor. For example, a list of RACF field and segment names are listed in the IBM manual *z/OS Security Server RACF Macros and Interfaces, Appendix D, User template for the RACF database*.
- The field type and length. Type represent the form the data is stored and can be C[har], U[ppercase], N[um], P[acked] or X[hexadecimal]. InterSession will convert types P and X to numeric or hexadeci-

mal readable characters. Length must be the field length specified in the RACF/TSS/ACF2 field description.

TSS has also a programming interface, TSSAI, which can give you access to more variables and is supported by InterSession. With TSS, the screen above has an extra field ('X' to use TSSAI) which you must set to X, indicating that TSSAI should be used for this variable. To obtain information on TSSAI please consult the appropriate TSS documentation.

System Options, User/Application Profile Defaults

```

InterSession ----- Maintenance, User/Application Profile Defaults ----
User Profile Defaults:
    Terminal idle timeout ==> 20      Standby at timeout ==> NO
    Widow session timeout ==> 060    Standby idle timeout ==> 020
    Connect all widow sessions ==> NO
    Hot keys on menu screen ==> YES
    Hot keys in Top Line Menu ==> NO
    Hot keys in applications ==> NO
    - only with Command Prefix ==> NO
    Hot keys from Syst.acc. profile x) ==> NO
        Attn key ==> Attn
        Jump key ==> PA1
        Command key ==> ENT
        Command prefix ==> ..
        Number of sessions ==> 15      Repl. Attn key for LU0 ==>
        Number of terminals ==> 01     User info in upper case ==> NO
        Password duration days ==> 365
Application Profile Defaults:
    Application idle timeout ==> 999
    Codepage ==> 00000
    Ad hoc model profile ==>
x) Any changes to these fields will not take effect until next startup
F1-help  F3-return  F7/8-bwd/fwd

```

On this screen you can specify default values for certain parameters on the User and Application Profiles. These values will be used when adding a new profile.

An explanation of the fields on this screen follows:

Terminal idle timeout

This specifies how many minutes a terminal can be left unattended before the sign-on or standby screen will be automatically redisplayed. All application sessions will be maintained. This value can be overridden on the individual User Profile.

The default value is 20. Specify 999 if you do not want this feature to be activated.

Standby at timeout

Specify YES or NO. YES indicates that the standby screen will be displayed when a terminal timeout occurs. If you specify NO the sign-on screen will be displayed. This value can be overridden on the individual User Profile.

Note: If a user has signed on to InterSession with a PassTicket or with an MFA product, the Standby Screen will not be sent to the terminal. Instead, the Sign On Screen will be sent.

Standby idle timeout

This specifies the number of minutes that the standby screen will remain displayed before the sign-on screen is automatically redisplayed.

The default value is 120.

Widow session timeout

When a user has left a terminal unattended, and the sign-on screen has been redisplayed, any active sessions at the time (widow sessions) will be automatically terminated after the time interval specified here has elapsed. This value can be overridden on the individual User Profile.

The default value is 20 (minutes). The maximum is 720 (12 hours). Specify 999 if you do not want this feature to be activated.

Connect all widow sessions

When a user signs on, widow sessions originally started by this user will be connected to this terminal. If NO is specified, only widow sessions started at this particular terminal will be connected. If YES is specified, all widow sessions at all terminals for this user will be connected. This value can be overridden on the individual User Profile.

Hot keys on menu screen

Hot keys in Top Line Menu

Hot keys in applications

only with Command Prefix

These settings are the default values for where the Hot Keys should be active. They do only affect Hot Keys connected to an Application Profile. They can be set to YES or NO.

See the corresponding settings in the User Profile.

Hot keys from Appl.acc profile

If "Application access" profiles are used, this setting controls if the Hot Keys from the Application access profiles will be used rather than individual Hot Key settings. The default is YES.

Attention key

This is used as the attention key to activate the top line menu. Valid specifications are PA1-PA3, PF1-PF24 or Attn. Your users can change these keys anytime on the menu or PROF screens.

Jump key

This is used to specify the default Jump Key for multiple session users. When the Jump Key is pressed, a scroll to the next application session will be done. When the last session is displayed, pressing the Jump Key will cause the menu screen to be displayed.

Your users can change this key anytime they want on the menu or PROF screens. Valid specifications are PF1-PF24, PA1-PA3, ENTER or ENT.

Command key

This is used to specify the default command key. This is used along with a command code to direct InterSession to perform specific actions. Your users can change this key anytime they want on the menu or PROF screens. Valid specifications are PF1-PF24, ENTER or ENT.

Command prefix

This is used to specify the default command prefix character(s), which will be used to prefix a session command from within an application screen. These characters are used to distinguish the session command from ordinary terminal input. You can specify from one to five characters.

Session commands can only be used in relay mode. Your users can change this character string anytime on the menu or PROF screens.

Number of sessions

This is used to specify the default maximum number of concurrent sessions the user is allowed to have at any one time.

Number of terminals

This is used to specify the default maximum number of terminals a user is allowed to be logged on to at any one time.

Replacement Attn key for LU0

You may specify a PA or PF key, or you can leave this field empty. If a user has assigned the 3270 Attn key as his Attention key, and signs on to an LU0 terminal, InterSession will replace the Attn key with this key, if specified. When the user signs on to an LU2 terminal, the Attn key will be restored.

User info in upper case

Specify YES or NO. If YES, the user name and the eight user data fields will be translated to upper case when the information is updated in MAINT. Default is NO.

User can maint own prof

Specify YES, NO, RES, or SEQ. This value is used when the User Profile setting is DRF.

Password duration days

Note that this parameter is only active for users that are not defined to External Security. If you have such users defined, specify the number of days before these users' password will expire.

You can specify up to 999 days. If you specify 0, the passwords will never expire. This value can be overridden on the individual User Profile.

The default value is 30. Specify 999 if you do not want this feature to be activated.

Application idle timeout

Specify the default value in minutes before an application session which has had no activity will be terminated. 999 indicates that the session will never be terminated due to inactivity. This value may be overridden on the individual Application Profile.

Codepage

If you are using different codepages (national character sets) for your applications and terminals, you should specify the application's codepage here and/or in the Application Profiles. If the terminal codepage is not the same as the application codepage, automatic translation between the codepages will be made.

This codepage number will be used for Application Profiles that do not have any codepage specified.

See also the section "National Characters and Codepage Support" for more information.

Ad hoc Model profile

Specify the name of a predefined Application Profile that will be used as a Model when a user starts an ad hoc session. If left blank the system default Application Profile will be used as a Model.

This allows you to specify system-wide default characteristics in the named Application Profile, to be used for ad hoc sessions.

System Options, PF Keys Defaults



```
InterSession ----- Maintenance, Terminal Keys Defaults -----
                                     Help key ==> F1      Alternate ==>
    Various use key 1 / MSGBOX GOTO ==> PF2    Alt / GOTOALT ==>
                                     Return key ==> PF3    Alternate ==>
    Various use key 2 / MSGBOX TERMINATE ==> PF4    Alternate ==>
                                     Scroll backward key ==> PF7    Alternate ==>
                                     Scroll forward key ==> PF8    Alternate ==>
    Window cancel key / MSGBOX CANCEL ==> PF12
                                     F1-help  F3-return  F7/8-bwd/fwd
```

On this screen you can change the terminal keys InterSession will use. Note that if you change any of these, the corresponding texts in your Screen Layouts will be automatically altered, provided the screen variables for the keys are used in these texts.

All keys can be set to any PF key in the range PF1-PF24, and each may also have an alternative (alias) key set, except for the Window cancel key, where only one key can be assigned, and where the range must be between PF10-PF24. The alternative “Various use key 1”, the “Alt / GOTOALT” key, may also be set to ENT or ENTER.

“Various use key 1” and “Various use key 2” are used for some special functions, such as sending a message in the MMS application.

They are also used in the Session Script MSGBOX END statement, in the KEYS= operand.

System Options, Other

```

InterSession ----- Maintenance, Other System Options -----
      System site id ==> 
      Logmode table name x) ==> INTSMTAB
      Accounting x) ==> SMF
      Account record layout x) ==> INTX   Account record SMF no. ==> 128
      Interval record interval ==> 000
      Use wrap-around log file x) ==> NO
      Use spin-off log files x) ==> NO
      Use JES2 log file ==> NO
      Force WTO message numbers ==>      ==>      ==>
      ==>      ==>      ==>
      Static input buffers x) ==> 020   Static output buffers x) ==> 020
      Dynamic output buffers ==> 080
      Appl. status check interval ==> 02
      Close inactive VTAM ACBs ==> YES
      Session start timeout (sec) ==> 030
      Signoff after last session ==> NO
      Use pass mode ==> NO   Use SIMLOGON w pass mode ==> NO
      Delete oldest if mailbox full ==> NO
      No. of subpools fixed areas ==> 04   Subpools dynamic areas ==> 08
      Minimum free storage Below ==> 0256   Above ==> 0512
x) Any changes to these fields will not take effect until next startup
F1-help  F3-return  F7/8-bwd/fwd

```

Some of the parameters on this screen will not have immediate effect but requires a system restart. Such parameters are marked with x) on the screen.

An explanation of the fields on this screen follows:

System site id

Specify a one- to eight-character unique name. This name can be referred to by the %SITE variable. It is also used by the InterSession messaging facility (MMS) to refer to this system when sending MMS messages from another InterSession system.

Logmode table name

If you want InterSession to use another logmode table than the system default INTSMTAB, specify the name of the logmode table here. Note that the load module of this logmode table must be available to InterSession.

Accounting

Specify YES, NO or SMF. NO means that no accounting records will be generated. YES means that accounting records will be written to a VSAM ESDS file. SMF means that accounting records will be written to SMF.

For more information, refer to the section on "The Accounting Routines."

Account record layout

The accounting records can be written using one of two different layouts, INTS, INTX, TV or TVX. INTS and INTSX refers to the InterSession account record layouts you can view in the installation source library members ACNTREC and ACNTRECX. TV and TVX refers to a layout that resembles the account record layout used by the CA-Television session manager. See Appendix A for a description of the account record layouts.

Account record SMF no

If you set accounting to SMF, you must specify the SMF user record number in the range 129-255. This record number must not be used by any other software in your installation.

Interval record interval

Normally, session account records will only be written when a session is ended. With this parameter you may specify a time interval in minutes. At the end of each time interval, session account records are written, equal to the session end record but containing only data related to the latest interval. Such a record is written for every active session in the system. This function can be of use when analysing the variation of application response times over the day. A value of 000 disables this function.

This record has a record type of X'38'. See Appendix B in this manual for a description of the session end record.

Note: This parameter must be handled with great care and should not be used on a daily basis since it significantly increases the number of account records written. A value of zero disables the function.

Use wrap-around log file

Specify YES or NO. If you want InterSession to write all system log messages to the wrap-around log file, specify YES.. Refer to the section on "The Wrap-Around Message Log File" for more information.

Use spin-off log files

Specify YES or NO. If you want InterSession to write all system log messages to the spin-off log files, specify YES.. Refer to the section on "The Spin-Off Message Log File" for more information.

Use JES2 log file

Specify YES or NO. If you want InterSession to write all system log messages to JES2 spool, specify YES.. Refer to the section on "The JES2 Message Log File" for more information.

Force WTO message numbers

Many InterSession messages are only written to the Log file, if any. If you want certain messages to be written to the system console, specify up to ten message numbers here, for instance 1201 or 1205 (user sign on / sign off).

Static input buffers / Static output buffers

InterSession has a static buffer pool that is used for all communication to VTAM. This is not used to maintain specific session data.

Each buffer is 5120 bytes long, and as a default, 10 static input buffers and 10 static output buffers are used. This value should be sufficient for most installations.

The usage of the static buffers is displayed on the System Status screen.

Dynamic output buffers

At times when the static output buffers are not sufficient, dynamic output buffers will be acquired and released as required. The value given here is the maximum number of dynamic output buffers that may be acquired at any given time.

The usage of the dynamic output buffers is displayed on the System Status screen.

Appl. status check interval

The status of all VTAM applications will be checked for availability at the interval specified here. The interval is specified in minutes.

The larger the number of different VTAM applications specified, the longer a VTAM application could become active or inactive before the change in status is reflected on the menu screen.

Close inactive VTAM ACBs

If you specify YES, any VTAM ACB that is not being used for a session will be closed. This can save virtual storage.

If you specify NO, all VTAM ACB's will remain open at all times.

Session start timeout

When InterSession tries to establish an application session, it will wait up to the interval specified here for a BIND to be sent by the application. While the default interval of 30 seconds is almost always sufficient, it is possible to increase it.

Signoff after last session

If you want the sign on screen to be shown instead of the menu screen when a user ends his last session, specify YES, otherwise NO.

Note: A combination of YES and a Logoff Application Profile name in "User signoff Application Profile" in the Screen Layout causes the user to be completely logged off from InterSession when the user ends his last session.

Use pass mode

YES or NO. YES means that InterSession can use the VTAM CLDST/PASS instruction to pass the terminal directly to the application when a user starts a VTAM application session. However, this can only be done if the user is a single session user (number of sessions = 01) and if the associated Application Profile does not contain a start script.

If set to NO, InterSession will never pass a terminal to an application, but always use relay mode sessions. This is also the default.

Use SIMLOGON w pass mode

YES or NO. YES means that InterSession uses the VTAM SIMLOGON instruction to regain control of the terminal after a pass mode session. NO means that InterSession issues the VARY NET,LOGON command to set InterSession as the logon application for the terminal, i.e. VTAM starts a session with InterSession when no other application session is active for the terminal.

Delete oldest if mailbox full

YES or NO. If set to YES, InterSession will automatically delete the oldest MMS message from the receiver's mailbox when receiving a message and the mailbox is full (the maximum number of messages in a mailbox is 255). Default is NO.

No. of subpools fixed areas

No. of subpools dynamic areas (z/OS only)

From two up to 126 storage subpools can be used.

For systems with a small workload the performance improvement by using many subpools will be minor, but for systems with a high load the performance improvement may be very high. In general, the higher the system workload, the higher the number of subpools that should be specified.

There are two separate values, representing two groups of storage areas; one range of subpools that is used for long-lived or "fixed" storage areas and another range of subpools that is used for short-lived or "dynamic" areas.

For a specific workload there will be an optimum number of subpools where the improvement is highest. Specifying a larger number of subpools will cause the performance to decrease again. The optimum point is depending on the system workload and the z/OS release, and can only be found by a "trial and error" method. A value calculated as "CPU seconds per transaction" should be used; that is, the CPU usage should be monitored over a longer period of time (such as a working day). It should then be divided by the number of transactions from the STAT screen. By changing the number of subpools daily and comparing the CPU per transaction values the optimum point can then be found.

The default values are 4 (four) subpools for fixed areas and 8 (eight) subpools for dynamic areas. Each group can have from one up to 63 subpools.

The value for dynamic areas will be by far the most critical factor; only for systems with many Pass Mode users will a change to the value for fixed areas have more than a noticeable effect.

When changing the values, the system need not be recycled; the new values will take effect immediately. Note however that it will take a longer time for the system to adjust to a change to the fixed areas value than to a change to the dynamic areas value.

Minimum free storage

Specify the minimum of region/partition free storage in kB below and above 16MB. When the amount of free storage falls below these values, a warning message is issued to the system log.

The amount of free storage can be monitored on the System Status screen.

System Options, User Exits

```

InterSession ----- Maintenance, User Exits -----

    Sign on exit name x) ==>
    Session start exit name x) ==>
    Session switch exit name x) ==>
    Top Line Menu exit name x) ==>
    Telnet LU-name exit name x) ==>

                                Current:

Term. data stream exit name x) ==>
- XLATE termid mask 1 ==>      XLATE table 1 ==>
  XLATE termid mask 2 ==>      XLATE table 2 ==>
  XLATE termid mask 3 ==>      XLATE table 3 ==>
  XLATE termid mask 4 ==>      XLATE table 4 ==>
  XLATE termid mask 5 ==>      XLATE table 5 ==>
  XLATE termid mask 6 ==>      XLATE table 6 ==>
  XLATE termid mask 7 ==>      XLATE table 7 ==>
  XLATE termid mask 8 ==>      XLATE table 8 ==>

Menu screen field exit name x) ==>
- screen field length x) ==>  - save area length x) ==>
  Maint. security exit name x) ==>
  IP host table name x) ==>
x) changes to these fields can take effect by using the LOAD command
F1-help  F3-return  F7/8-bwd/fwd

```

This screen is used to define the names of any user exits. Most of the parameters on this screen will not have immediate effect but requires a system restart. Such parameters are marked with x) on the screen.

An explanation of the fields on this screen follows:

Sign on exit name

Session start exit name

Session switch exit name

Top Line Menu exit name

Telnet LU-name exit name

These are used to specify the names of your own various exits.

Refer to the section on "The Sign On Exit", "The Session Start Exit", "The Session Switch Exit", "The Top Line Menu Exit" and "The Telnet LU-name Exit" for more information.

Term. data stream exit name

This is used to activate the 3270 Data Translation Facility, or your own data stream exit.

If you want to use the system-supplied terminal data stream exit, specify XLATE. If you have written your own terminal data exit, give the name of the exit. Refer to the section on "3270 Data Translation" and "User Written Routines" for more information.

XLATE termid mask n / XLATE table n

If XLATE is specified in "Term. data stream exit name", you can use these fields to connect certain terminals to certain translate tables. Refer to the section on "User Written Routines" for more information.

Menu screen field exit name

screen field length

save area length

These operands are used for your own Menu Screen Field Exit .

Specify is the name of your exit program, the length of the user data, and optionally, the length of the save area.

Refer to the section on "Menu Screen Field Exit Facility" for more information.

Maint. security exit name

This operand is used to specify the name of your own maintenance security exit.

Refer to the section on "The Maintenance Security Exit " for more information on this exit.

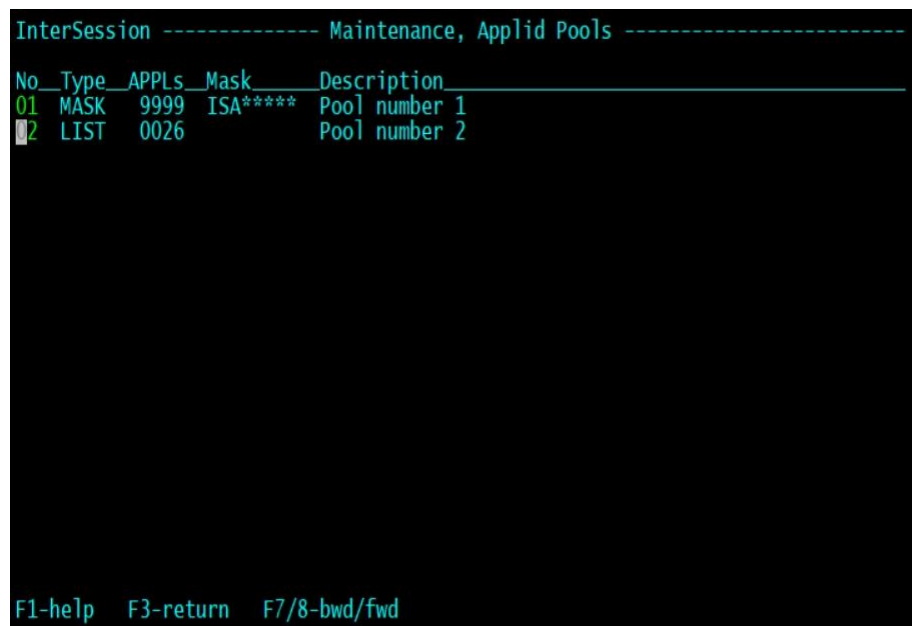
APPLid Pool List

The APPLid Pools are used for application sessions to VTAM applications.

The Pool Number is set in the Application Profiles.

Here you describe the number and format of the VTAM APPLids in each pool

If you type an A in the Select field of the System Options selection screen and press Enter, you will see a list of all your current APPLid pools.



The screenshot shows a terminal window titled "InterSession Maintenance, Applid Pools". It displays a table with the following columns: No, Type, APPLs, Mask, and Description. The table contains two entries: 01 MASK 9999 ISA***** Pool number 1, and 02 LIST 0026 Pool number 2. The cursor is positioned on the second line. At the bottom, there are function key instructions: F1-help, F3-return, and F7/8-bwd/fwd.

No	Type	APPLs	Mask	Description
01	MASK	9999	ISA*****	Pool number 1
02	LIST	0026		Pool number 2

F1-help F3-return F7/8-bwd/fwd

To select an APPLid pool, position the cursor to the line and press Enter. If you have more pools than will fit on one screen you can browse through them with PF7 and PF8.

You may have up to 99 pools in your system.

There are two types of pools, MASK and LIST.

APPLid Pool With a Mask

```
InterSession ----- Maintenance, Applid Pool -----
Pool number 01   Description Pool number 1
    Pool type MASK/LIST ==> MASK      'Delete' for removal ==>
    Number of APPLid-s ==> 9999
Use APPLid-s round-robin ==> NO
    APPLid mask ==> ISA*****

F1-help  F3-return  F7/8-bwd/fwd
```

An explanation of the fields on this screen follows:

Pool number

This number corresponds to the “Session applid/Pool no” field in the Application Profiles.

Description

This is a text for documentation purposes only.

Pool type MASK/LIST

In this case, the pool type is MASK.

'Delete' for removal ==>

To remove the APPLid pool, type the word 'delete' in this field.

Number of APPLid-s

APPLid mask

Defines the names you use for the VTAM APPL statements in this pool.

Setting “Number of APPLid-s” to 9999 means that there is “no limit”; the maximum number is then determined by the number of asterisks in the mask (up to five, meaning an absolute limit of 99999).

The “APPLid mask” is a string of characters followed by a string of one to five asterisks. The asterisks will be replaced with a number from 1 and upwards, to the number set in “Number of APPLid-s”.

In this example, the pool consists of an unlimited number of APPLid-s, in the range of ISA00001 to ISA99999. These APPLid -s must be defined to VTAM as described in the section on "VTAM APPL Statements".

Use APPLid-s round-robin

YES or NO. YES - next APPLid is selected from the previous used entry in the list. NO (the default) - next APPLid is selected from the beginning of the list.

APPLid Pool With a List of APPLids

```
InterSession ----- Maintenance, Applid Pool -----
Pool number 02   Description Pool number 2
Pool type MASK/LIST ==> LIST   'Delete' for removal ==>
Number of APPLid-s ==> 0010
Use APPLid-s round-robin ==> NO

001> BA01    002> BB01    003> BC01    004> BD01    005> BE01
006> BF01    007> BG01    008> BH01    009> BI01    010> BJ01
011>         012>         013>         014>         015>
016>         017>         018>         019>         020>
021>         022>         023>         024>         025>
026>         027>         028>         029>         030>
031>         032>         033>         034>         035>
036>         037>         038>         039>         040>
041>         042>         043>         044>         045>
046>         047>         048>         049>         050>
051>         052>         053>         054>         055>
056>         057>         058>         059>         060>
061>         062>         063>         064>         065>
066>         067>         068>         069>         070>
F1-help  F3-return  F7/8-bwd/fwd
```

An explanation of the fields on this screen follows:

Pool number

This number corresponds to the "Session applid/Pool no" field in the Application Profiles.

Description

This is a text for documentation purposes only.

Pool type MASK/LIST

In this case, the pool type is LIST.

'Delete' for removal ==>

To remove the APPLid pool, type the word 'delete' in this field.

Number of APPLid-s

For pool type LIST, you cannot type anything in this field. It is an automatic counter of all the APPLid-s you have specified in the list.

nnn>

Defines the names you use for the VTAM APPL statements in this pool.
Each APPLid in the pool must be explicitly defined. You may define up to 500 APPLid-s.

To delete an APPLid, use the Erase Eof key and press Enter. The list will close.

To insert an APPLid between two existing id-s, type /I in the field and press Enter. The list will open with an empty field.

Each of the APPLid-s specified must be defined to VTAM as described in the section on "VTAM APPL Statements".

System Options that will Take Effect First After Next Startup

Changes to some of the System Options will not immediately take effect, but need a system restart. Examples of such options are all user exit specifications and the External Security specifications. They are all marked with an X).

Problems with Exits etc. Causing System to Abend at Startup

If, for instance, a user exit option is changed, which will cause an abend at next system startup due to errors in the exit, you will not have a chance to correct the System Options. In the startup parameters, you should then insert the following statement:

FAILSAFE=USEREXIT

No user exits will then be loaded, thereby enabling the system to start up successfully.

The Web Gateway

The Web Gateway makes it possible to access the InterSession-defined applications from a web browser, without any need for a 3270 emulator to be installed in the workstation.

It runs completely within the mainframe and there is no middleware involved.

The Web Gateway handles all static objects needed, such as CSS files, JavaScript files and images. The layout can be modified using standard CSS files.

The Web Gateway consists of three parts:

- A web server
- A web application menu generator
- A 3270-to-web converter.

To the end user, the access and usage of the applications via the Web Gateway is very similar to using InterSession with a 3270 emulator; the menu listing contain the same applications, and Session Scripts etc. functions the same way.

However, 3270-terminal-specific functionality like the Top Line Menu and the Jump, Command and Hot keys are not available in the web environment.

The Web Server

The web server works as a normal web server, with the following important exceptions:

- All static files are kept in one (for z/OS two) libraries.
- In z/OS, file extensions are not used; files are stored according to their nature, binary or text.
- There is no directory structure.

Defining and Starting the Web Server

The web server is defined and started by creating a HTTP service:

```

InterSession ----- Maintenance, Service -----
Service id HTTP                               Change Service id ==>
    Service type ==> HTTP
    Interface ==> TCPIP
    Port ==> 08080
Multi-homed IP address ==> 0.0.0.0
    Queue length ==> 005
    Identification text ==> InterSession mainframe applications
    Root folder name ==>
    Use HTTPLOG ==> NO
    Active ==> YES

```

Enter a port number and set Active to YES. Optionally, set "Use HTTPLOG" to YES or VSAM if you want InterSession to create a HTTP log file (see below).

The "Identification text" will be displayed in the web browser authentication window.

Note that a TCPIP interface must be defined and active.

If more than one server (HTTP service) is started, then all servers share the file system. They can however have different root folder names (see below).

The File System

Folder names

InterSession will use the following folder names:

/signon/ for the internal sign on window

/menu/ for the menu listing

/appl/ for the application session windows

/html/ for other, static files.

Access to "/" will result in a redirection to "/signon/index.html".

In the HTTP service, you may specify a root folder name. If so, this folder will prefix the above folder names. In this way, you will get a common top level folder name for all web traffic on this HTTP service.

There are two kinds of files: **text files** and **binary files**.

Text Files

Text files are stored in EBCDIC and can be modified from the mainframe host using normal host editors. The text files are parsed for SSI commands and then translated to ASCII before being sent to the web browser. The ASCII translation is done using the code page specified in the InterSession Screen Layout.

Binary Files

Binary files are stored as-is and are sent to the web browser without any modification. They are typically images, sounds or ASCII files (like Java scripts) that requires no processing on the host.

How the Files Are Kept

On **z/OS** the files are kept in PDS files, one for text files (**DD:HTMLTXT**) and one for binary files (**DD:HTMLBIN**). When the web server receives a request for a file, it first searches the text files (ignoring any extension), and if the file was not found there, it searches the binary files.

The file properties for both files are:

RECFM(VB) LRECL(256) BLKSIZE(4096)

In **z/VM**, the files are stored as CMS files on the A disk. The file types are used to distinguish between text and binary files.

In **z/VSE** the files are kept in a sublibrary (by default, the installation sublibrary). The file extensions are used to distinguish between text and binary files.

Special Files

A few files with a special purpose must exist. They are stored in EBCDIC and can be customized using a host editor:

error401.html	Error page when user auth has failed
error404.html	Error page for <i>page not found</i> errors
menu.html	The template for the application menu
intrsess.css	Default css file
sessend.html	Info page for <i>Session ended</i>
logoff.html	Info page for <i>User logged off</i>
signon.html	Sign on page

Note: If you are creating your own version of the application menu template, you may use another name than **menu.html** (see below).

The File Cache

InterSession will cache all files from the web file system in a storage cache.

If you have changed any of the files, you must refresh the cache. This is done by using the REFRESH FORCE command. See the manual “User Guide for 3270 Users” for information on the REFRESH FORCE command.

The Application Menu

The application menu interface uses the special file **menu.html** in the file system (must be a text file). This file is a template for the menu listing page. This file must contain one line with the **%MENU** variable in column 1. This variable will be substituted with the menu listing. Any other data on that line will be ignored.

The application menu uses InterSession’s normal access rules and will display a list of applications similar to that of a 3270 terminal.

The URL for the application menu is `/sess/`. The applications can be regarded as files in the `/sess/` directory. Access to a non-existent application will result in the application menu.

Accessing the Application Menu from Another Web Page

To access the application menu, simply link to the `/sess/` directory in your html code. In this example the port 9980 is defined in the HTTP service:

```
<LI><A HREF=http://mf.acme.com:9980/sess/ target="_self">
Mainframe applications</A></LI>
```

Accessing a Particular Application from Another Web Page

To access a particular application, link to the `/sess/application` directory in your html code, where *application* is the Application Profile name in 16 EBCDIC hexadecimal characters. In this example we are accessing an Application Profile with a name of TSO, hexadecimal E3E2D6:

```
<LI><A HREF=http://mf.acme.com:9980/sess/E3E2D64040404040 target="_self">
TSO/ISPF </A></LI>
```

If the user is not signed on to InterSession at the time, the sign on web page will be shown before InterSession starts the application.

Redirect from InterSession Logoff to Another Web Page

When a user logs off from InterSession by selecting an Application Profile with type LOGOFF (default Application Profile name OFF), either the **signon.html** or the **logoff.html** web page is shown, depending on the LOGOFF Application Profile setting "Disconnect terminal" is NO or YES . If you rather want the user to return to a specific web page in your intranet structure, you can define its URL in the Screen Layout, Web Layout Settings 2/2, field "**Logoff redirect URL**". The URL specified must be complete, like **http://www.acme.com** or **//www.acme.com**

The HTTP Log File

Accesses to the Web Gateway can be logged to the HTTPLOG file.

The log records are written in the *Combined Log Format*, a common format used by most other web servers and which can be used by many log analysers.

The use of the HTTPLOG file is specified in the HTTP Service. You can define YES, VSAM or NO.

YES (z/OS and z/VM only) means that InterSession uses a sequential file. This type of file must be defined with RECFM=VB, LRECL=512, BLKSIZE=*any*. The file must be defined with the name HTTPLOG in the InterSession startup JCL.

When this type of file becomes full, InterSession stops writing web log records. You can then copy the contents to another file and reopen it manually.

VSAM means that InterSession uses a wrap-around VSAM file, which never reaches a “full” condition. When all allocated space is used up, old records are overwritten.

You must define the file to VSAM, using the JCL HTTPLOG from the installation source library. The file must be defined with the name HTTPLOG in the InterSession startup JCL. At first time use, you will see the VSAM messages IEC161I 080-053 and IEC070I 203-204 in the InterSession job log. This is normal and should be ignored.

This type of file can be viewed in the same manner as the standard InterSession log file, in the STAT internal application.

Since it is a wrap-around type of file, the records are not in date/time order. There is a “break” in the file where the last record was written. The file can therefore be copied in batch with INTSUTIL, using the COPY HTTPLOG command (see the section “Batch Routines” later in this manual). The output records will then be in ascending date/time sequence. It should be noted that on the VSAM file, the data is prefixed by 23 bytes of date/time/site id fields. These fields are removed with COPY HTTPLOG.

Both types of log file can be closed and opened with either a command on the menu screen, an operator command or via a batch job. See the manual “User’s Guide for 3270 users” and the section “Batch Routines” later in this manual.

Changing the HTTPLOG file from YES to VSAM

When changing from a sequential file to VSAM, you should follow this procedure:

- Define the VSAM HTTPLOG file with the HTTPLOG JCL.
- Change the parameter **Use HTTPLOG** in MAINT, Service from YES to VSAM. You can also change this parameter using the SERVICE parameter card in the startup.
- Change the InterSession JCL to point the HTTPLOG file to the newly created VSAM file.
- Restart InterSession. You will see the messages IEC161I 080-053 and IEC070I 203-204 in the InterSession job log. These should be ignored.

Customization

Simple Customization

The Screen Layouts are used to perform simple customization, such as changing texts, images etc. See the section “Screen Layout, Web Layout Settings” for more information.

The selection of which Screen Layout to use is based on:

The Screen Layout name in the User Profiles

The Screen Layout DEFAULT setting

Replacing images

By default, one image is used in the web windows, **LOGOPNG.PNG**.

If you want to replace this image, do as follows:

Select a proper image, around 400 pixels wide. It must be in PNG format.
FTP the image file binary to the InterSession library (for z/OS, the HTMLBIN PDS).

Specify its name in the Screen Layout, Web Layout Settings, in the %IMAGE1 field.

To see the result immediately, issue the REFRESH FORCE command.

Language Support

By default, InterSession will use the web language code **en** for English. This can be changed in the Screen Layout Web settings. If you have an application in another language than the default, you can set the language code in the Application Profile. The language codes are not checked for validity by InterSession, but must conform to the ISO639-1 standard.

Advanced Customization

Making Changes in the .html Files

All **.html** files can be modified as you wish. They are stored in EBCDIC and can therefore be changed by any host editor. The **.html** files are:

signon.html, **menu.html**, **sessend.html**, **logoff.html**, **error401.html** and **error404.html**.

If you make changes to the **menu.html** file, make sure that one line contains the **%MENU** variable in position 1, see below.

You can also make use of the unused variables %IMAGE2-4.

Server Side Includes (SSI) Variables

The web server supports SSI variables. They can be specified in any of the **.html** files and includes the standard InterSession System Variables. For a complete list see the section "The System Variables". There are also specific variables for the web server that are specified in the Screen Layout (see the section "Screen Layout, Web Layout Settings"). These variables are:

%STITLE	Signon window title
%MTITLE	Menu window title
%ETITLE	Session end window title
%TEXT1-5	Various texts
%IMAGE1-4	Various images
%TXUI	User id text (signon.html file only)
%TXPW	Password text (signon.html file only)
%TXNPW	New password text (signon.html file only)
%TXVPW	Verify password text (signon.html file only)

For the **signon.html** file only, the following specific variables must be used:

%LOGUSR **User id field**

%LOGPWD **Password field**

%ERRMSG **Error message**

The following two variables have special purposes:

%CP **Code page number, must be specified in column 1**

%MENU **The menu listing, must be specified in column 1**

To use a variable, simply include the variable name in the html code:

```
<table>
  <tr><td>Time:           </td><td>%TIME </td></tr>
  <tr><td>IP address: </td><td>%IP   </td></tr>
</table>
```

The **%CP** variable can be assigned a value (a code page number). The code page controls how the EBCDIC to ASCII translation is done. To specify a special translation, insert "%CP=value" as the first line in the document:

```
%CP=278
<html>
<head>
  <title>Hello, world!</title>
...
```

Note: The **%CP=** must be the only text on the line.

Replacing the “menu.html” File

If you want to make changes to the menu.html file, it is recommended that you make a new file with another name. The name of the new file must then be specified in the Screen Layout, Web Layout Settings 2/2.

The CSS Files

The CSS (Cascading Style Sheet) files are used to control the layout of the application windows.

The web user can, via the configuration section of the menu window, select which style (CSS file) he wants to use. The system comes with a number of CSS files. These files are named in the Screen Layout, Web Layout Settings 2/2. The first file defined in this list will be the default CSS file. The files are:

INTRSESS.CSS The default CSS file. Must never be changed.

PCOMM.CSS Resembles IBM Personal Communications

PCOMMX.CSS As **PCOMM** but with visible input fields.

INFO3290.CSS Resembles the 3290 Information Panel.

If you want to make changes to the Style Sheets, you should not change any of the system defined CSS files. Instead, create a new CSS file by using one of the existing files as a template.

When you have created the new CSS file you must specify its name in the Screen Layout, Web Layout Settings 2/2, in order for the new file to be selectable by the web user.

The Entrances feature

The Entrances feature allows a single InterSession system to act as a multiple of separate Instances.

This may be useful for users that need to have several instances of an application running simultaneously. This can be done without Entrances, but there is a risk that the different applications will be mixed up after a client disconnect and reconnect.

An Entrance can be a VTAM APPLid, where the default VTAM interface is one entrance. To define more VTAM entrances you need to start a tiny InterSession program for every other instance, that runs in parallel with the InterSession system. They are only active during user connections. See below.

Other types of Entrances are TN3270 Services and HTTP Services.
You can define as many of each type as you need.

User Profile settings

There are three User Profile settings that are important when using Entrances:

Max number of terminals, must be a value greater than 1.

Widow session timeout, should be set to a rather high value to avoid application session cancellation after a terminal disconnect.

Use multiple entrances, must be set to YES.

The last two settings can be defined as User Profile default values in the System Options.

Setting up more VTAM entrances

For each additional VTAM entrance, you should start a copy of the InterSession program INTSEINTR, either as a job or as a started task. INTSEINTR listens on a specific VTAM APPLid, where this APPLid will also be the Entrance Name, and when a user connects to this APPLid, control will be passed to the main InterSession system, with the Entrance id as a parameter.

This APPLid must be defined to VTAM with the same parameters as the INTSAPPL id.

You will find a sample JCL, INTSEINTR, in the installation source library:

```
//INTSESSB JOB NNNN,MSGCLASS=X,CLASS=A,TIME=1440
//INTS      EXEC PGM=INTSEINTR,REGION=0M
//STEPLIB DD DSN=INTS.VER810.INSTALL.LOADLIB,DISP=SHR
//SYSABEND DD SYSOUT=*
//SYSIN DD *
ENTRANCE=INTSESSB
INTSAPPL=INTSESS
/*
```

The INTSESSB APPLid should be defined to VTAM as

```
INTSESSB APPL AUTH=(ACQ,PASS),PARSESS=YES,LOSTERM=IMMED
```

When you start the INTSEINTR program, you will see the following messages:

```
IE06I  Accepting logons on Entrance appl=INTSESSB
IE07I  Will transfer sessions to InterSession appl=INTSESS
```

Setting up TN3270 and HTTP entrances

Every TN3270 Service and HTTP Service that is active will automatically become an Entrance, with the Service Id will be the Entrance id.

You may start as many Services that are needed,

Showing the Entrance id to the user

You can use the variable %ENTR in the Screen Layout to show the Entrance id to the user.

You can for example put this variable in the first line of the Sign on and Menu screens:

```
InterSession ----- Maintenance, Screen Layout 2/23 -----
Screen Layout DEFAULT      Language/Heading
Language number ==>      Codepage ==> 00000
Help screens ==> DEFAULT Date format ==> MDY

'YES' ==> YES      'NO' ==> NO      'DEF' ==> DEF
'ALARM' ==> ALARM  'SWITCH' ==> SWITCH 'MENU' ==> MENU
'Today' ==> Today  'Now' ==> Now     'ALL' ==> ALL
'Available' ==> Available 'Not available' ==> Not available
'Active' ==> Active  'Output pending' ==> Output pending
'Last seen' ==>      'Session end' ==>
'More BW' ==>
'More FW' ==>

Month names ==> Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Day names ==> Mon Tue Wed Thu Fri Sat Sun
Heading line:
"InterSession ----- Entrance %ENTR ----- %DN %MN %D, %C%Y %TIME

F1-help  F3-return  F7/8-bwd/fwd
```

The Entrance id is now shown in the Sign On and Menu screens:

```
InterSession ----- Entrance INTSF0RM ----- Sun Jun 09, 2024 20:08
APPLICATION          INFO *  APPLICATION          INFO *
-----Internal applications----- ! T3270... Mainframe TN3270 se
MAINT... InterSession maint      ! START... Window to start mul
STAT... InterSession status      !
TLOCK... Terminal lock list      !
PROF... Your user profile         !
MMS.... Message/mailbox sys      !
STBY... Standby screen           !
OFF.... Logoff InterSession      !
-----Information screens----- !
SUPPORT. Contact information      !
-----External applications----- !
CICSP... Production CICS        ?? !
CICSD... Development CICS       ?? !
Z/VM.... VM/CMS                 !
TSO..... TSO/ISPF               !

===== Session status =====
Attention key Attn  Jump key PA1  Command key ENT  Prefix ..

Application ==>      ADCDMST
F1-help  F3-sign off  F7/8-bwd/fwd  ENT-system select  TCP00003
```

Sysplex Functionality

Two or more (up to eight) InterSession instances can work together in a z/OS sysplex environment. The InterSession sysplex functions allows you to:

- Share your User Profiles, Application Profiles, Session Scripts, Screen Layouts and Printer Options between the InterSession instances, using VSAM Record Level Sharing
- Load balance and backup for your VTAM terminal sessions, using VTAM Generic Resources.

This manual does not describe how to set up the z/OS sysplex environment, it describes only how to use InterSession in a sysplex.

To implement InterSession sysplex functionality, you should follow the guidelines in the implementation steps below. These steps are:

- Setting up the VSAM files
- Defining the SYSIN parameters.
- Starting the InterSession instances
- Other considerations.

Prerequisites

To run InterSession in a sysplex environment, the following criterias must be met :

- Two or more z/OS systems running in a sysplex with a CF (coupling facility)
 - Each z/OS system must be running the SMSVSAM server, which in turn requires that:
 - The sharing control data sets (SHCDS) exists
 - The CF structure IGWLOCK00 exists
 - A CF cache structure exists, which is defined to a cache set.
 - SMS must have a storage class pointing to the cache set.
 - The INTSFLE VSAM file must reside in SMS-managed storage and have the above storage class assigned to it.
 - For VTAM generic resources, the CF structure ISTGENERIC must exist. You may have given it another name in the VTAM start option STRGR.
-

Setting Up the VSAM Files

With a stand-alone InterSession system, the INTSFLE VSAM file contains all the configuration data (as can be viewed from the MAINT selection screen).

With more than one InterSession system in a sysplex, most of this data can be shared between the InterSession instances, but some of the data must be unique to each instance.

These unique (local) specifications must therefore reside in a second VSAM file, INTSLCL.

Each InterSession instance will therefore point out both the shared INTSFLE and the local INTSLCL files with normal DD cards.

The INTSFLE VSAM File

This file is shared among all InterSession instances. It must therefore reside on a disk accessible to all instances.

If you already have a stand-alone InterSession system running (which is most likely) you should use your existing INTSFLE. You need not to change any of the VSAM file parameters but will be able to use it as is. If you are starting from scratch, please see the Installation chapter for instructions.

InterSession will share the following data from INTSFLE:

- User Profiles
- Application Profiles
- Session Scripts
- Screen Layouts
- Printer Options
- Help Screens.

InterSession keeps all this information in internal memory. When one InterSession instance updates any of the above information, InterSession uses the messaging feature of the sysplex to inform the other InterSession instances (sysplex members) of the update. The other members then refreshes the internal memory copy from INTSFLE.

The INTSLCL VSAM File

This file holds all information unique to each InterSession instance. This information consists of the following types:

- Interfaces
- Services
- System Options
- VTAM APPLPOOLS

Defining the INTSLCL file

For each InterSession instance you will need to define an INTSLCL file. You should use the **VSAMLOCL** job contained in the installation source library:

```
//INTSLOCL JOB 1,CLASS=A,MSGCLASS=X,REGION=2M <---- ACCOUNT & CLASS
//IDCAMS1 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
DELETE INTS.VER720.LOCAL1 CL /* <---- I/S FILE */
SET MAXCC=0
DEFINE CLUSTER
  (NAME (INTS.VER720.LOCAL1) /* <---- I/S FILE */ -
  VOL (NNNNNN) /* <---- DISK VOLID */ -
  KEY (10 0) -
  REC (100 100) -
  SHR (2 3) -
  RECSZ (4088 4088) -
  CISZ (4096) )
/*
//FORMAT EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER720.LOADLIB,DISP=SHR <---- I/S LOADLIB
//INTSLCL DD DSN=INTS.VER720.LOCAL1,DISP=SHR <---- I/S FILE
//SYSIN DD *
FORMAT LOCAL
/*
```

As you can see, this file can be kept very small.

Note that when starting your InterSession instances for the first time, all your settings related to the information types listed above (such as Interfaces and System Options), are reset to their default values (because of the FORMAT LOCAL function).

You will therefore need to enter this information again. Remember to keep them unique to each instance. Also, you will need to enter the VTAM APPLid of the InterSession instance in the SYSIN parameters to be able to log on to the system (see startup example below).

Defining the Startup Parameters

All InterSession sysplex parameters are to be defined as Startup Parameters in the SYSIN file. These are:

SYSPLEXGROUP=group name

Specify a sysplex group name that is to be shared among all InterSession instances. This parameter is mandatory and can be up to 8 bytes long.

SYSPLEXMEMBER=member name

Specify a sysplex group member name that is to be unique for this InterSession instance. This parameter is mandatory and can be up to 16 bytes long.

The **SYSPLEXGROUP** and **SYSPLEXMEMBER** parameters together define the InterSession instance uniquely to the sysplex and activates the InterSession sysplex routines.

VSAMRLS=YES/NO

To be able to share the INTSFLE VSAM file you must specify **VSAMRLS=YES**. The INTSFLE will then be opened with VSAM Record Level Sharing. For testing purposes, for example with a single instance of InterSession and VSAM/RLS not installed, you can set this parameter to NO.

Using the VTAM Interface

To use the InterSession VTAM Interface in a Sysplex, you should use the z/OS feature VTAM Generic Resources.

Specify the following parameter:

VTAMGNAME=generic resource name

If you want VTAM load balancing and backup between the InterSession instances, specify a VTAM Generic Resource name in this parameter. This name must be the same in all InterSession instances.

When this name is used to VTAM connect to InterSession, VTAM selects among the active InterSession instances the one with the lowest load (smallest number of connected LUs). This parameter is optional.

VTERMMASK=mask

This parameter is optional. **It is needed only if you use the User Profile option “Virtual terminal id”.**

This mask is used to form the VTAM APPLid to be used for a particular user. The characters entered in this mask will replace the corresponding position(s) in the “Virtual terminal id” before use. If there are leading characters in the “Virtual terminal id” that is not to be replaced, enter an asterisk in these positions of the mask. The character replacement is done internally and can not be seen in the User Profile.

For example, if “**VTERMMASK=**YZ1**” and “**Virtual terminal id = ABCD0020**” the resulting name will be “**ABYZ1020**”.

With this parameter you can set different prefixes for the InterSession instances, to give unique VTAM APPLids for each instance.

VPRINTMASK=mask

This parameter is optional. **It is needed only if you use InterSession VTAM printing** and is used together with the parameter “VTAM APPLid” of the Printer Options Profiles. It has the same function as the VTERMMASK parameter, except that it is used for printers.

Using the TCP/IP Services

To use the InterSession TN3270 and Web servers in a sysplex environment, you should use the z/OS feature **TCPIP Sysplex Distributor**, with VIPA (Virtual IP Addressing) or DVIPA (Dynamic VIPA),

TCPIP Sysplex Distributor is application transparent and need no definitions in InterSession.

The TCPIP workload will be distributed among the InterSession instances and assist in case of an instance failure.

For installations with limited experience of this feature we recommend the IBM Redbook **Communications Server TCP/IP Implementation: Volume 3 High Availability, Scalability, and Performance**.

Starting the InterSession Instances

Make sure the InterSession load library is APF authorized.

Use copies of the **STARTPLX** JCL from the installation source library to startup the InterSession instances:

```
//INTSPLX1 JOB NNNN,MSGCLASS=X,CLASS=A,TIME=1440 <---- ACCOUNT & CLASS
//INTS EXEC PGM=INTSESS,REGION=0M
//STEPLIB DD DSN=INTS.VER720.LOADLIB,DISP=SHR <---- I/S LOADLIB
//INTSFLE DD DSN=INTS.VER720.FILE,DISP=SHR <---- I/S FILE
//INTSLCL DD DSN=INTS.VER720.LOCAL1,DISP=SHR <---- I/S LOCAL FILE
//LPRQFLE DD DSN=INTS.VER720.LPRQ1,DISP=SHR <---- LPRQ FILE
//HTMLBIN DD DSN=INTS.VER720.HTMLBIN,DISP=SHR <---- HTML BIN FILE
//HTMLTXT DD DSN=INTS.VER720.HTMLTXT,DISP=SHR <---- HTML TXT FILE
//SYSABEND DD SYSOUT=*
//SYSIN DD *
LICENSEKEY=XXXXXXXXXXXXXXXXXXXXXXXXXXXX
APPLID=INTSPLX1
SYSPLEXGROUP=INTSESS
SYSPLEXMEMBER=INTSESS1
VTAMGNAME=INTSESS
VSAMRLS=YES
```

Notes:

- The sysplex group is INTSESS and the sysplex member is INTSESS1.
- The VTAM APPLid is INTSPLX1 and the VTAM generic resource name is INTSESS. Using INTSPLX1 to VTAM log on takes you to this specific instance. Using INTSESS takes you to any of the active InterSession instances.
- Since we are using VSAM Record Level Sharing, we have defined an INTSLCL file and specified it here.
- The LPRQFILE must be unique to each instance. You need therefore to create one such file for each instance, using the LPRQFILE JCL.

Other Considerations

You should be aware of the following facts and restrictions:

- If one of the InterSession instances becomes unavailable, the application sessions that were started in that instance will be lost. There is no automatic takeover of the application sessions.
 - For VTAM sessions, affinity for an LU is removed when the LU disconnects from InterSession. The next time this LU is used to log on to InterSession, VTAM can select another instance.
 - For VTAM sessions, if one of the InterSession instances becomes unavailable, the LUs that were connected to that instance will not be automatically connected to another instance. The user has to log on to the generic resource name again to be connected to another instance.
-

The IOS/Android Tablet App

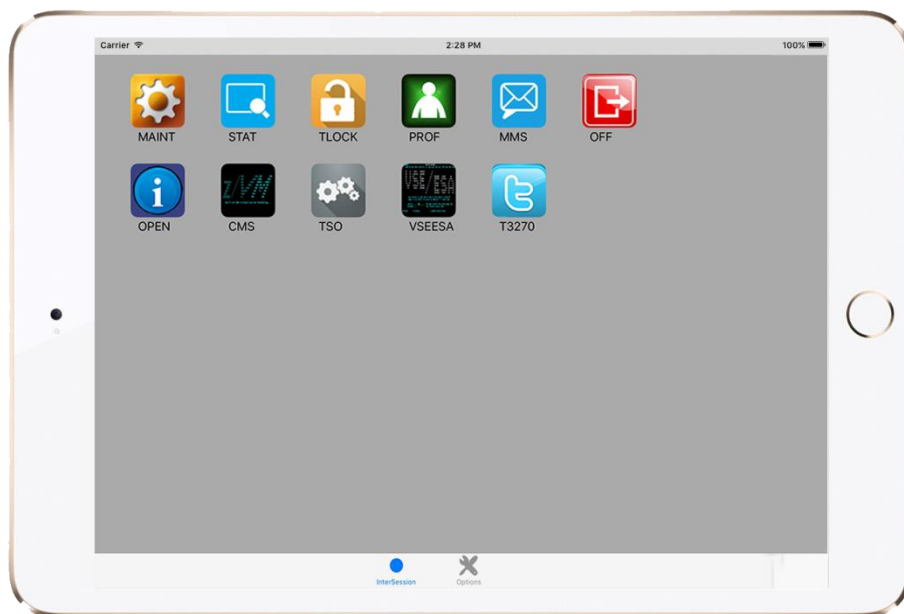
With the free InterSession app you will get easy access to your mainframe applications from an iPad or an Android tablet.

It will give you a modern and comfortable way to run your 3270 applications.
The app can be found on the App Store or Google Play.

To use the app, the InterSession Web Gateway must be active in the mainframe.

Adding New Icon Files

After logging on to the InterSession mainframe server, your applications will be shown as icons:



The icon files are stored as PNG files in the InterSession mainframe library (for z/OS, the HTMLBIN file).

Applications that do not have any icon file in the library will be shown as a standard blue icon with the first character from the application name.

If you want any of your own applications to be shown as a specific icon, you must create such an icon file and add it to the InterSession mainframe library.

The icon file should be 75 x 75 pixels in size, be in PNG format and have the same name as the InterSession Application Profile

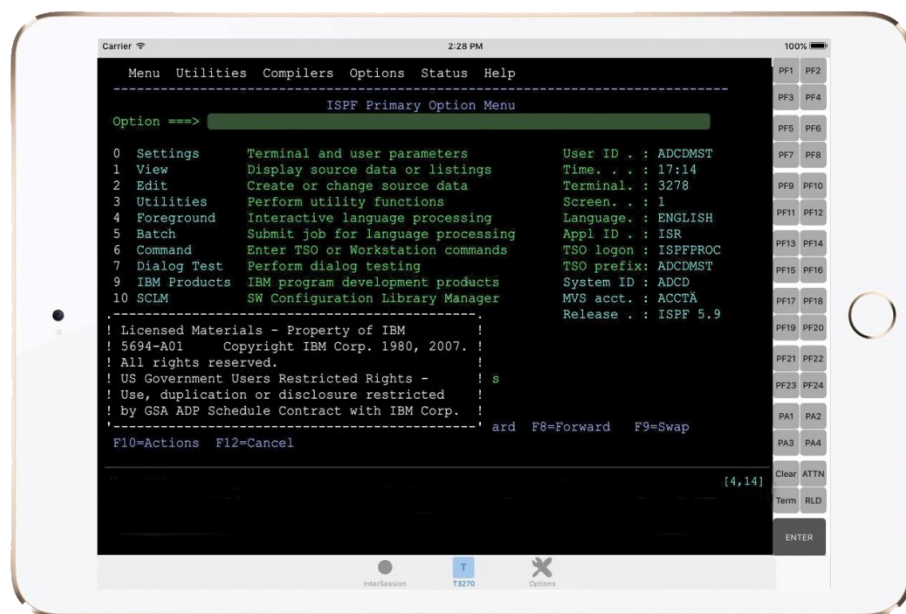
FTP the icon file binary to the mainframe as follows:

- For z/OS, to the HTMLBIN PDS (no PNG suffix of course)
- For z/VM, to the A disk as **name PNG A**

- For z/VSE, to the VSE InterSession sublib as **name.PNG**

Changing the Application Window Style

When selecting an application, a 3270 session tab will be shown, with the 3270 keys to the right:



In the “Options” tab the user can select which 3270 style to use. The style names are names of .css files (Cascading Style Sheets) as they are listed in the Screen Layout. They are the same as those used in the Web Gateway.

If you want to create new styles, see the section “**The CSS files**” in “**The Web Gateway**” chapter above.

Installation-Written Exit Routines

The Sign On Exit

This exit is called up to three times during the sign on process, and once at terminal sign off time.

The first type of call will always be made.

The second and third types of calls are made only if External Security has been defined in the System Options.

The exit can be written in any language. For Assembler, normal linkage conventions apply. For COBOL, the "PROCEDURE DIVISION USING..." technique should be used. The exit is invoked in 31 bits addressing mode.

System Option Specification

In the System Options, specify the name of the exit module in the field "Sign on exit name". The exit will be loaded at system initialization time.

Calls To The Interface

Sign On Screen Data Validation Call

This call is made each time a user presses ENTER on the Sign On screen, before any checks have been made to the screen fields.

The exit is passed eight parameters:

- TYPECALL one byte = "1"
- RETCODE one byte
 - "0" ==> OK, accept sign on
 - "1" ==> OK, but display the MESSAGE warning text
 - "9" ==> Reject sign on, display MESSAGE text
- TERMID eight bytes
- USERID eight bytes
- PASSWORD 100 bytes
- NEWPASSWORD 100 bytes
- USERFIELDS 304 bytes, see below
- MESSAGE 70 bytes.

The TYPECALL field indicates that this is a Sign On screen data call.

The exit must supply a value in RETCODE, see above.

If the user id has no match among the InterSession User Profiles, the USERFIELDS field will be low-value.

The exit may alter the data in any of the USERID, PASSWORD, NEWPASSWORD or USERFIELDS fields.

If a message is to be displayed, the exit must supply the text in the MESSAGE field.
 For RETCODE=9, MESSAGE is displayed on the Sign On Screen.
 For RETCODE=1, MESSAGE is displayed on the Main Menu Screen.

External Security Model Call

This call is made when a user is defined to External Security but no InterSession User Profile exists.

Note: if the System Option “Apply Model at every signon” is set to YES, the exit will be called every time a user signs on, even if the User Profile exists.

The purpose of this call is to supply InterSession with a User Profile Model to be used when creating the new User Profile.

The exit is passed nine parameters:

- TYPECALL one byte = "2"
- RETCODE one byte, not used in this call
- TERMID eight bytes
- USERID eight bytes
- USERMODEL eight bytes
- XSBLOCK, ACEE or mini-UCB
- ACF2LID, logon id record (ACF2 only)
- EXTRACTINFO 39 bytes, see below
- SYSTACCPROF application access profile, eight bytes

Upon entry to the exit, the USERMODEL field contains the Model name that was specified in the System Options parameter XSMODEL. The exit may change this to another Model name.

XSBLOCK is the appropriate External Security control block; the ACEE for RACF and TopSecret and the mini-UCB for ACF2. ACF2LID is mapped by the ACF2 macro LIDREC. For RACF and TopSecret, the address to this parameter is zero.

In addition to setting the USERMODEL field, the exit may also set the id of an application access profile (i.e. the id of another User Profile which will supply access to the Application Profiles).

Update User Profile Call

This call is made after an external sign on has completed successfully.

The purpose of this call is to update some of the InterSession User Profile fields with data from the user control blocks of the External Security Manager, and/or to change the application authorization for the user.

The exit is passed nine parameters:

- TYPECALL one byte = "3"
- RETCODE one byte
 - "0" ==> APPLICATIONLIST information not changed by exit
 - "1" ==> APPLICATIONLIST information changed, see below
- TERMID eight bytes
- USERID eight bytes
- COMMAREA 200 bytes; is used to communicate data between this exit and the Installation-Written External Security Interface (see below).
- XSBLOCK, ACEE or mini-UCB
- USERFIELDS 304 bytes, see below
- EXTRACTINFO 39 bytes, see below
- APPLICATIONLIST 9216 bytes, see below

XSBLOCK is the appropriate External Security control block; the ACEE for RACF and TopSecret and the mini-UCB for ACF2.

With the APPLICATIONLIST information the exit may change the application authorization for the user, see below.

Sign Off Call

This call is made whenever a user signs off the system, either by hitting the PF3 key on the menu screen or by using any of the Logoff System Profiles.

The purpose of this call is for the exit to get information of the changed status for the user.

The exit is passed four parameters:

- TYPECALL one byte = "4"
- RETCODE one byte, not used in this call
- TERMID eight bytes
- USERID eight bytes

Contents of the UserFields Area

- User name, 24 bytes
- User group, 8 bytes
- User data field 1, 32 bytes
- User data field 2, 32 bytes
-
- User data field 8, 32 bytes
- Date of latest sign on, 6 bytes YYMMDD
- Time of latest sign on, 6 bytes HHMMSS
- Number of days before current password will expire, 3 bytes
- Today's day of week, one byte 1-7; 1=Monday, 2=Tuesday etc.

Note that you cannot alter the date, time and number of days fields; they are of a read-only nature. Any changes to these fields will be ignored.

The number of days before password expiration will contain 999 if the user is not allowed to alter the password. It will contain 000 if the password is already expired.

Contents of the ExtractInfo Area

This area contains information that was extracted from the External Security Manager. If a field does not have a valid value, it contains high-values (X'FF').

- User group, 8 bytes
- User name, 24 bytes
- User CICS operator id, 3 bytes
- Date for last password change, 3 bytes packed value
- Password change interval, 1 byte hexadecimal value

The ApplicationList Information

This area contains information about the application access for the user. Only Application Profiles with "Authorization check = YES" are contained in this list. Each entry contains:

- Code for access, 1 byte containing a plus (+) or minus (-) sign.
- Application id, 8 bytes.

The list is terminated with a high-value (X'FF') in the code field.

The exit may alter the codes to change access to the applications. However, the list must not be changed in any other way.

If the exit is building the access list from scratch, the code in all entries must be set by the exit.

To indicate to InterSession that the application access has been changed, the return code must be set to "1".

Note that if an application access profile is defined for the user, any alterations to the access list will be ignored.

Sample Sign On Exit

In the source library you will find the sample exit SIGNEXIT.

This exit handles the Sign On screen data call only.

The exit does the following:

- The first seven bytes of Data Field 8 of the User Profile is searched for a match on today's weekday number.
 - If a match is found, the sign on is rejected with a message indicating "You are not allowed to sign on today". For example, if the digits "67" are put into Data Field 8, the user is not permitted access on Saturdays or Sundays.
 - If the number of days before current password expiration is less than 10, a message is displayed on the Main Menu Screen indicating the number of remaining days.
 - Otherwise, a message is displayed on the Main Menu Screen indicating the date and time of the previous sign on.
-

The Terminal Data Stream Exit

The purpose of the terminal data exit is to give you the ability to inspect and alter the contents of the 3270 data stream being sent to and received from a terminal. Control will be given to the exit for all screens, menus, internal application screens, and application screens.

Pass mode sessions are not connected to InterSession when working inside an application, and therefore the exit will not get control. However, for relay mode, the exit will be active.

Before writing an exit, study the system-supplied exit INTSXLAT, which is delivered in source format. In many cases, this exit, together with a translation table, may provide the required functionality.

Writing the Exit

The terminal data exit must be compiled and link-edited to a library which is available to InterSession. The exit module will be loaded during system startup.

When the exit is called, standard IBM register conventions are used.

The following parameters is passed to the terminal data exit:

1. Address of a ten-byte field with the following contents:

1	"S" or "R" indicating send to or receive from the terminal
2	"M" or "A" indicating menu or application screen. Internal applications are indicated as "A".
3-10	The application (Application Profile) name or two bytes menu number: 01 Sign-on screen 02 Menu 06 Terminal lock screen The top line menu will appear as an application screen with a name of "99999999".

2. The address of the 3270 data stream.
3. The address of a halfword containing the data stream length.
4. The address of an eight-byte field containing the VTAM terminal netname.
5. The address of a table inside InterSession. This table is created by the XLATETB parameter of the System Option generation (see below). The table consists of a maximum of eight entries, where each entry has the following format:
 - Eight-byte field with the terminal ID mask
 - Eight-byte field with the translation table name
 - Fullword containing the address of the translation table
6. The address of an Application Profile-specified translation table, or 0 if no table is used.

Other Exit Considerations

You can manipulate the data stream. You can also shorten the length by placing a smaller value in the length field, but you may not increase the length of the data stream (increasing the length value).

If you are doing file manipulation within the exit, this may impact performance of the system.

Activating the Exit

To activate the terminal data exit, specify the name of the exit in the field "Term. Data stream exit name" of the System Options.

The System-Supplied Exit

If you want only to use the terminal data exit to translate characters in the 3270 data stream, the system-supplied exit can be used. Two steps must be performed:

1. Create translation tables
2. Set System Option parameters

Step 1: Create Translate Tables

An Assembler macro, IXLATE, is provided in the installation source library. This macro is used to generate translation tables. You can have up to eight different system-wide translation tables, where each table is given a unique name. In addition, you can have one or more tables for use with individual Application Profiles. Each table consists of one or more IXLATE statements, which must be assembled and link-edited with a suitable module name. The format of the IXLATE macro is:

$\text{IXLATE} \quad \left\{ \begin{array}{c} \text{IN} \\ \text{OUT} \end{array} \right\} , \text{ fromchar, tochar}$
--

Specify IN if the translation is to be made when data is received from the terminal. Specify OUT if the translation is to be made when data is sent to the terminal.

Fromchar	The terminal representation of the character on input, the internal representation on output.
Tochar	The internal representation of the character on input, the terminal representation on output.

The fromchar and tochar must be in the form C'x' or X'nn', where x is the EBCDIC character and nn the hexadecimal representation.

Example

```

IXLATE IN,X'C0',C'_'
IXLATE IN,X'D0',C'_'
IXLATE IN,X'6A',C'_'
END

```

In this example, if the specified terminal characters x'C0', x'D0' and x'6A' are received from a terminal, they will be converted to underscore characters.

The END statement delimits the input to the Assembler.

Step 2: Set System Option Parameters

First, specify XLATE in the field "Term. data stream exit name" of the System Options.

Second, specify the terminal ID pattern (termidmask) and the name of the translation table (tabname) in the fields "XLATE table n" and "XLATE termid mask n" of the System Options, where:

termidmask	Terminal ID or terminal ID pattern for which the translation table that follows is to be used. The terminal ID can include letters, digits, and asterisks, which are wildcards considered to match any character. In determining a match, trailing asterisks in the pattern are ignored. (For example, ACC***** is considered to match ACCT.)
tabname	The translation table associated with the preceding terminal ID or terminal ID pattern.

You may specify up to eight pairs of termidmask and tabname

Note: You can also specify the use of an individual translation table for a particular application on the Application Profile maintenance screen. If specified, such a table always takes precedence over any terminal-related table.

The Menu Screen Field Exit

The purpose of the Menu Screen Field Exit is to give you the ability to generate a data field that is unique to the specific terminal user. The data generated in this data field can be displayed on the various InterSession screens, or passed to individual applications via the %UD variable. The terminal user can also be permitted to modify the data field.

Writing the Exit

Two sample user data exits have been provided in the installation source library, UDEXITA in Assembler, and UDEXITC in COBOL.

The user data exit must be compiled and link-edited to a library which is available to InterSession. The exit module will be loaded during start-up.

To activate the exit, you must specify the System Options fields "Menu screen field exit name", "- screen field length" and, optionally, "- save area length".

When the exit is called, standard IBM register conventions are used if you are using Assembler. If the exit is written in COBOL, the "PROCEDURE DIVISION USING ..." technique should be used.

Six (6) parameters will be passed to the user data exit, as follows:

1. A one-byte field containing a numeric code:
 - 1 The exit is being called before the menu is written to the terminal. The length of the output screen field (see parameter 4 below) that may be used by the exit is dependent on the format of the last line of the menu (see the appropriate Screen Layout)
 - 2 Input from the screen has been received. The input screen field, if any (see parameter 4), is eight bytes long.
2. A 70-byte area where the exit may place an error message to be displayed on the message line of the terminal. If no error is found by the exit, do not move anything into this field.
3. The saved user data field (unique for each terminal). The length of this field is determined by the generation parameter UDLEN. Optionally, this field may be followed by a work area, which also is unique for the terminal. The presence of such a work area is controlled by the generation parameter UD-SAVE.
4. The screen field. For screen output, this field can be modified by the exit to provide information to the user; it can also be an input field or a combination. The first two bytes of this field must contain the length (in binary) of the data that follows. The exit data is placed on the next to the last line (to the right of the Application field). In this field, the exit may place 3270 control characters (SBA strings, SF, etc.) for the proper display of the screen field.

For screen input, the field is eight bytes long (without any two-byte length field), which means that this is the maximum length for an unprotected screen field. InterSession will place the first eight bytes from the Application select field immediately after this field.

5. The VTAM Terminal ID (eight bytes)
6. The User ID (eight bytes)

The Security Maintenance Exit

The purpose of the security maintenance exit is to give you the ability to use your own security techniques for the maintenance routines.

To activate the exit, the name of the exit must be entered in the System Options field "Maint. security exit name".

When the exit is called, standard IBM register conventions are used if you are using Assembler. If the exit is written in COBOL, the "PROCEDURE DIVISION USING ..." technique should be used.

Four or five parameters are passed to the security maintenance exit, as follows:

1. The address of a one-byte field containing a numeric code:
 - 1 The exit is being called before the menu is written to the terminal. The length of the output screen field (see parameter 4 below) that may be used by the exit is dependent on the format of the last line of the menu (see the appropriate Screen Layout)
 - 2 The exit is being called when the user has entered input on the Maintenance Selection screen. The fifth parameter points to a screen image area as specified below.
 - 3 The exit is being called when a User Profile record has been read and is about to be displayed.
 - 4 The exit is being called when an Application Profile record has been read and is about to be displayed.
 - 5 The exit is being called when a Screen Layout record has been read and is about to be displayed.
 - 6 The exit is being called when a Session Script record has been read and is about to be displayed.
 - 7 The exit is being called when a printer options record has been read and is about to be displayed.
 - 8 The exit is being called when a set of help screen records has been read and is about to be displayed.
2. The address of a 70-byte area where the user may place an error message to be displayed on the message line of the terminal. If no error is found by the exit, do not enter anything into this field.
3. The address of an area containing data about the user currently using the maintenance routines:

Location	Length	Description
1-8	8	User ID

9-32	24	User's name
33-40	8	User's Group ID
41-48	8	User's password
49-51	3	YES or NO (System Administrator)
52-54	3	YES, NO, or RES (update User Profile authority)
55-70	16	8 two-byte binary fields (COBOL S9(4) COMP) containing the length of each user data field
71-326	256	User data fields (the eight user data fields)

4. The address of an eight-byte field containing the terminal name (VTAM netname).

5. The address of a field, the contents of which depend on the code returned in the first parameter:

For code = 1, this field is not present.

For code = 2, the field is a screen image area with the following layout:

Location	Length	Description
1	1	User Profile type
2-9	8	User Profile ID
10-17	8	User Profile copy ID
18	1	Application Profile type
19-26	8	Application Profile ID
27-34	8	Application Profile copy ID
35	1	Application Profile type
36-43	8	Application Profile ID
44-51	8	Application Profile copy ID
52	1	Screen Layout type
53-60	8	Screen Layout ID
61-68	8	Screen Layout copy ID
69	1	Printer options type
70-77	8	Printer options ID
78-85	8	Printer options copy ID
86	1	Help screens set type
87-94	8	Help screens set ID
95-102	8	Help screens set copy ID

For code = 3-8, this field is an eight-byte field containing the record ID for the record which is about to be displayed.

External Security Exit

This exit allows an installation to provide its own External Security processing routine.

The exit is called at the following points:

- System initialization
- Security refreshing
- Start of user verification (userid/password verification)
- User/Application Profile authorization check
- End of user verification

InterSession will save all relevant information about the user, so there is no need for the exit to retain data.

If the exit reports that a user is defined to External Security, the exit will be responsible for the following actions for that user:

- Number of allowed sign-on attempts
- Revoking user access
- Password expiration
- Layout of new password

The exit can be written in either Assembler Language or COBOL. For Assembler Language, normal linkage conventions apply. For COBOL, the "PROCEDURE DIVISION USING..." technique should be used. The exit is invoked in 24 bits addressing mode.

System Option Specification

In the System Options:

Specify "USER" in the field "External Security Manager" of the Security Options screen.

Specify the name of the exit module in the field "USER module name".

Calls to the Exit

System Initialization

This call is made within the system initiation process. The interface is passed three parameters:

TYPECALL	"1"
RETCODE	one byte
MESSAGE	70 bytes

The TYPECALL field indicates that this is an initialization call. If the exit's processing is successful, RETCODE should be set to 0. If not, the RETCODE should be any other value. If a message is put into the MESSAGE field, it will be displayed on the log.

Start of User Verification

This call is the first of three types of calls that are made each time a user signs on. The exit is passed the following parameters:

TYPECALL	"2"	
RETCODE	one byte	
	"0"	OK, normal sign on accepted; no new password was given
	"1"	User not defined to External Security; InterSession will look for the user among the User Profiles
	"2"	OK, the new password is accepted
	"3"	OK, the new password is accepted, but a warning message is placed in MESSAGE
	"4"	OK, normal sign on accepted; no new password was given, but a warning message is placed in MESSAGE
	"9"	Sign on was not accepted; an error message is placed in MESSAGE
MESSAGE	70 bytes	
USERID	8 bytes	
PASSWORD	8 bytes	
NEWPSWD	8 bytes; will be low-values if no new password has been entered.	
TERMINID	8 bytes terminal id	
COMMAREA	200 bytes; is used to communicate data between this exit and the Sign on exit (see above).	

If the user supplies a new password, note that the exit will be called twice:

1. Start/end of user verification calls without the new password to verify the current password
2. All three calls with the new password.

User/Application Profile Authorization Check

This call is the second of three types of calls which are made each time a user signs on. The exit will be called once for each Application Profile defined with "Authorization check == EXT" specified.

The exit is passed the following parameters:

TYPECALL	"3"	
RETCODE	one byte	
	"0"	the user is granted access to this application
	"9"	the user is not allowed access to this application
MESSAGE	70 bytes (not used in this call)	
USERID	8 bytes	
NEWPSWD	8 bytes; the name of the Application Profile	

This call will only be made if the start of user verification call was accepted.

End of User Verification

This call is the last of the three calls which are made each time a user signs on.

The exit is passed the following parameters:

TYPECALL	"4"
RETCODE	one byte (not used in this call)
MESSAGE	70 bytes (not used in this call)
USERID	8 bytes

This call is only made if the start of user verification call was accepted.

Security Refreshing

This call is made every 30 minutes and every time a /REFRESH command is issued. The purpose of this call is to allow the exit to check for any security rules that is kept in memory by the exit and which may have been updated.

Only one parameter is passed:

TYPECALL	"5"
----------	-----

Top Line Menu Exit

With this optional exit, the installation may control many of the features of the Top Line Menu (TLM). The exit is called at the following points of the TLM processing:

- Before the selection line is written to the terminal.
- Before the "hardCopy" pull-down menu is written to the terminal, and after input on the "hardCopy" pull-down menu.
- After input on the "Give" pull-down menu.
- After input on the "shaRe" pull-down menu.

The exit program can be written in Assembler language using standard linkage conventions, or in COBOL using the `PROCEDURE DIVISION USING` technique. The exit program will be called in `AMODE=24` and `RMODE=24`.

The name of the exit program is defined in the System Options in the field "Top Line Menu exit name".

The exit program will be passed the following seven parameters:

- `Call_code` 1 byte (character)
- `Return_code` 1 byte (character)
- `Terminal_id` 8 bytes
- `User_id` 8bytes
- `User_data_fields` 8 x 32 bytes
One or more of the user data fields can be used as input to the exit to control its execution.
- `Call_specific_data_1` 8 bytes (see below for usage)
- `call_specific_data_2` 8 bytes (see below for usage)

The Initial TLM Call

The exit is called before the TLM selection line is written to the terminal. The purpose of this call is to disable one, more, or all functions of the TLM.

`Call_code` contains "1".

`Call_specific_data_1` contains an 8-byte string where each byte contains an "N" or a "Y" to enable/disable a certain function:

Byte 1: Sessions

Byte 2: hardCopy

Byte 3: Give

Byte 4: shaRe

Byte 5: giveBack

Byte 6: Attn

Byte 7: help

Byte 8: eXit

The exit may set each of these bytes to "N" or "Y" respectively.

Return_code should be set to "1" if changes are made. To disable the TLM entirely, set Return_code to "2".

The "hardCopy" Call

The exit is called before the "hardCopy" pull-down menu is written, and also after input on the pull-down menu. The purpose of this call is to check and possibly alter the printer name.

Call_code contains "2".

Call_specific_data1 contains the printer name and may be changed by the exit.

Return_code should be set to "1" if the printer name is changed. To reject the given printer name (no changes made by the exit), set Return_code to "2".

The "Give" Call

The exit is called after input on the "Give" pull-down menu. The purpose of this call is to check the User ID of the receiver and the Session ID that is about to be given away.

Call_code contains "3".

Call_specific_data1 contains the User ID of the receiver.

Call_specific_data2 contains the Session ID of the session to be given.

Return_code should be set to "2" if the given attempt is to be rejected.

The "shaRe" Call

The exit is called after input on the "shaRe" pull-down menu. The purpose of this call is to check the User ID of the receiver and the Session ID that is about to be shared.

Call_code contains "4".

Call_specific_data1 contains the User ID of the receiver.

Call_specific_data2 contains the Session ID of the session to be shared.

Return_code should be set to "2" if the share attempt is to be rejected.

Session Start Exit

With this exit the user may alter many of the fields of an Application Profile dynamically at session startup time.

The exit is called each time a session is about to be started.

The exit program can be written in Assembler language with normal linkage conventions, or in COBOL using the PROCEDURE DIVISION USING technique.

The exit program will be called in AMODE=24 and RMODE=24.

The name of the exit program is to be defined in the System Options in the field "Session start exit name".

The exit program will be passed the following five parameters:

- Terminal id, 8 bytes.
- User id, 8 bytes.
- Application Profile id, 8 bytes.
- Application Profile attributes:
 - Application APPLid, 8 bytes
 - Session APPLid type, 6 bytes
 - Pool number/group name/UNIQUE mask, 8 bytes
 - Logmode name, pass mode SNA, 8 bytes
 - Logmode name, pass mode non-SNA, 8 bytes
 - Logmode name, relay mode SNA, 8 bytes
 - Logmode name, relay mode non-SNA, 8 bytes
 - COS name, 8 bytes
 - Data to pass to application, 64 bytes
 - CICS transaction id, 4 bytes.
- Any terminal data (the %TD variable), 20 bytes.

The exit program may alter the Application Profile attributes and/or the terminal data.

Note that the in-core Application Profile will be directly updated by these changes; the next time the exit is called for the same Application Profile, it will contain the latest changes.

The disk version of the Application Profile will **not** be changed; when you update the Application Profile in MAINT, or at the next system startup, the original values will be restored.

The "Session APPLid type" and "Pool number/group name/UNIQUE mask" will be checked for validity in the same way they are checked in MAINT.

Note that if these fields are invalid, the changes are not accepted (the Application Profile will not be updated), but no error message will be given.

Note that for an outbound TN3270 Application Profile, the fields which are only relevant for VTAM Application Profiles will contain irrelevant information, and any changes made to these fields will be ignored.

In the installation source library you will find a sample exit called SSTEXIT. You may use this sample as a source for your own exit.

Session Switch Exit

This exit allows InterSession to support the NETSPY product or other similar products.

These types of products collect statistics based on what is written to the terminal. Among other things, these products reports how many I/O-s a certain application has written to a terminal.

With a session manager working in Relay Mode, this means that all terminal I/O is reported to the session manager instead of the user applications.

With this exit, a specific character string is written to the terminal each time a session switch occurs. This string contains among other things the name of the user application and is intercepted by the statistics product.

The string is created by the exit.

The name of the exit program is to be defined in the System Options in the field "Session switch exit name".

NETSPY Exit

A system-supplied exit for NETSPY support is delivered, both in source and executable format.

To implement NETSPY support, specify the name NETSPY in the System Options field "Session switch exit name".

This will cause InterSession to load and call the system-supplied session switch exit (the name of the exit is NETSPY).

For further details, please review the source member NETSPY in the source library.

User Written Session Switch Exit

If you have another session-statistics product than NETSPY, you can write your own exit to satisfy the needs of your product.

All you must do is to create the string that should be written to the terminal; InterSession will do the necessary terminal I/O.

The exit is called with standard linkage conventions and is presented the following seven parameters:

- TERMID eight bytes (terminal id)
- APPLid eight bytes (application VTAM APPLid)
- APPLICATION eight bytes (Application Profile name)
- LUNAME eight bytes (APPLid from an APPLPOOL)
- VTAMADR eight bytes (VTAM Net Address, CID, in EBCDIC)
- STRINGLEN two bytes binary (length of STRING, created by the exit)
- STRING max 1024 bytes (created by the exit)

If a switch is to occur to a user application screen, the APPLID, APPLICATION, LUNAME and VTAMADR parameters represents the application session.

If a switch is to occur to an InterSession internal application screen, APPLid contains the InterSession APPLid, APPLICATION contains the Application Profile name, LUNAME is blank and VTAMADR represents the terminal session.

If a switch is to occur to any of the Sign On, Main Menu or Terminal Lock screens, APPLid contains the InterSession APPLid, APPLICATION and LUNAME is blank and VTAMADR represents the terminal session.

The exit should create the terminal string, including the 3270 Write Command and Write Control Character, in the STRING field. The length of the string is to be placed in STRINGLEN field. If STRINGLEN is less than 2 or greater than 1024, no data is written to the terminal.

Please also review the source member NETSPY, which may serve as a Model for your exit.

The Telnet LU-name Exit

The virtual LU names are constructed for and they are unique within the InterSession system. VTAM will never see these names. In order to make these names more meaningful there is an exit, the Telnet LU-name Exit, which can be tailored to meet your requirements.

The default LU-names

The default names are constructed as follows:

TCPaccess:

XEEEEEEE

Where X is the prefix character from the Host Application Profile and EEEEEEE is the EPID in hex from the TLI connection.

IUCV (z/VM)

XPPPSSSS

Where X is the prefix character from the Host Application Profile, PPP is the IUCV path number and SSSS is the socket number.

BPX (z/OS)

XSSSSSSS

Where X is the prefix character from the Host Application Profile and SSSSSSS is the socket number.

TCP/IP for z/VSE

XDDDDDDD

Where X is the prefix character from the Host Application Profile and DDDDDDD is the connection descriptor in hex.

The Exit

The exit is called when a connection is accepted, but before the TN3270 negotiation has started. The exit should not do anything that causes WAITs to be issued. Doing so will degrade performance. There is a sample exit, TELNEXIT, supplied on the source library. The exit should be written in assembler language.

To activate the exit, specify its name in the System Options field "Telnet LU-name exit name".

Entry parameters

The exit is called with respect to its AMODE and in PROBLEM state and uses standard linkage, R15 points to entry point, R14 contains the return address and R13 points to a save area.

On entry R1 points to a parameter area:

Field	Size	Description
ECODE	H	Entry code
LUNAME	CL8	The current LU-name. On the first call it is the constructed LU-name
IPADDR	XL4	The IP address of the client.
PORT	H	The Port number of the client.
APPLICATION	CL8	The name of the Host Application Profile
SYSTYPE	CL8	The type of the <i>Host Application Profile</i> , currently always "TN3270"
INTFACE	CL8	The name of the Interface Application Profile.

The ECODE is defined as follows:

ECODE	Meaning
0	First call on a new connection
4	The supplied LU name was not unique.

Return parameters

The exit should update the LU-name parameter.

On return R15 should be set to the desired return code.

R15	Meaning
0	Accept the supplied LU-name without any change
4	The LU-name has been changed.
8	Reject the connection.

When R15=8, R0 can be used to pass a reason code that will appear in the reject message.

The Batch Routines

The InterSession batch program provides the following functionality:

Functionality	Command	Session*
Retrieving User and Application Profiles, copying the log files.	COPY	NO
Maintaining User and Application Profiles.	MAINT	YES
Creating reports on User and Application Profiles	LIST	NO
Sending MMS messages from batch.	SEND	YES
Closing and opening system files.	CLOSE, OPEN	YES
Create update records to MAINT based on search fields c0ntwnreeee data in a field--	UPDATE	NO
Deleting old MMS messages.	DELMSG	YES
Printing the INTSLOG log file.	PRINTLOG	NO
Inactivating/activating Application Profiles	INACT/ACT	YES
Compressing internal security keys.	COMPRESS	NO
Issuing a VTAM command.	vtamcmd	NO
Initializing the VSAM file.	FORMAT	NO
Upgrading the VSAM file to a new InterSession version.	UPGRADE	NO

*Specifies if the function requires a VTAM session between INTSUTIL and the online system (interface type BATCH).

Setting Up the VTAM Session

1. If it does not exist, create the following Interface:

```
Interface type ==> BATCH
  VTAM APPLid ==> utilappl
    Active ==> YES
```

2. For "utilappl", specify a unique VTAM APPLid to be used by the INTSUTIL program. This VTAM APPLid must be specified with the parameter AUTH=ACQ.

If you need to run INTSUTIL from two or more VTAM hosts, you will need a unique VTAM APPLid and Interface for each VTAM host.

3. Use the following parameter cards in the INTSUTIL execution:

```
APPLID=utilappl
CONNECT APPLID=intsappl[USER=userid PASSWORD=passw]
```

In the APPLid card, specify the same VTAM APPLid specified in steps 1 and 2.

In the CONNECT card, the APPLid name is equivalent to the VTAM APPLid defined in the SYSIN startup parameters or in the InterSession VTAM Interface.

The “userid” must exist as a User Profile in InterSession. Most functions require the user to be a System Administrator or Master Operator. In these cases, you must specify the current password for the user.

Note: If the job is submitted from an environment controlled by an External Security Manager (such as TSO under RACF), the USER and PASSWORD should not be specified. In such a case, the userid which submitted the job will be used.

Retrieving User and Application Profiles—COPY

The COPY command copies the User Profiles, Application Profiles or Screen Layouts to INTSREC, a sequential file with variable length records, by reading the INTSFLE VSAM file. See Appendix B for the record layouts. The records are copied based on a selection criteria specified in the parameter card. The sequential file may then be input to a report generator or any other user-written program.

The INTSREC records may also be used as input to the MAINT function.

In the batch job JCL, you must supply INTSFLE and INTSREC DD/DLBL cards.

Only one COPY card can be used for each time you execute INTSUTIL. Use the following parameter card:

```
COPY {USER|USERS|APPLICATION|APPL|LAYOUTS [WITH field <=> value]}
```

The WITH operand

field can be any of the field names listed in the record layouts in Appendix B. **value** can be generic, i.e. **SYSP*** as in the following examples. Only one WITH operand can be coded. Only those profiles that fits the selection criteria will be listed in the report.

z/OS Example:

```
//INTSCOPY JOB xxxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//INTSFLE DD DSN=INTS.VER72.FILE,DISP=SHR
//INTSREC DD DSN=INTS.COPY.PROF,DISP=(NEW,CATLG),
//          SPACE=space,UNIT=unit,DCB=(RECFM=VB,BLKSIZE=8192)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COPY USERS WITH GROUP=SYSP*
/*
```

COPY command examples:

COPY USERS WITH SADM=YES	Copies all System Administrators.
COPY USERS WITH NSESS>1	Copies all Multiple Session Users.
COPY USERS WITH APPAC=TSO	Copies all users with access to Application TSO.

COPY APPLICATIONS

Copies all Application Profiles.

COPY APPL WITH ID=TSO

Copies the Application Profile TSO.

COPY LAYOUTS

Copies all Screen Layouts.

Creating Update Records for User and Application Profiles— UPDATE

The UPDATE command creates update records in order to change the contents of the fields in User and Application profiles. UPDATE selects records from the INTSFLE VSAM file in the same manner as COPY by using the WITH parameter. See Appendix B for the names of the INTSFLE record fields. When a profile record has been selected from INTSFLE, UPDATE reads information on what fields and what the fields should contain. This information is defined in one or more cards in the SYSIN file. For each field a card is defined, containing the field name and the new field contents. You may have up to 20 field cards. The update records are written to the INTSREC variable blocked file, which later should become input to the MAINT function, where the actual update takes place.

In the batch job JCL, you must supply INTSFLE and INTSREC DD cards

Only one UPDATE card can be used for each time you execute INTSUTIL. Use the following syntax:

UPDATE {USER|USERS|APPLICATION|APPL|LAYOUTS [WITH field <=> value]

The WITH operand

field can be any of the field names listed in the record layouts in Appendix B. **value** can be generic, i.e. **SYSP*** as in the following examples. Only one WITH operand can be coded. Only those profiles that matches the selection criteria will be processed further.

The field and field contents card(s)

These cards must immediately follow the UPDATE card and contain a six bytes field name, immediately followed by the field contents which must be of the same type and length as described in Appendix B (numeric, upper case etc.)

Example:

```
//INTSCOPY JOB xxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER81.LOADLIB,DISP=SHR
//INTSFLE DD DSN=INTS.VER81.FILE,DISP=SHR
//INTSREC DD DSN=INTS.COPY.PROF,DISP=(NEW,CATLG),
//          SPACE=space,UNIT=unit,DCB=(RECFM=VB,BLKSIZE=8192)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
UPDATE USERS WITH GROUP=SYSP*
NSESS 999
MASTOPYES

/*
```

Copying the log files—COPY LOG / COPY HTTPLOG

This COPY command copies either the INTSLOG or HTTPLOG wrap-around file to LOGOUT, a sequential file with variable length records, with a maximum record length of 512.

In the batch job JCL, you must supply INTSLOG/HTTPLOG and LOGOUT DD/DLBL cards.

COPY LOG

The output records on LOGOUT will be written in ascending date/time sequence. The records have the following layout:

- 8 bytes date CCYYMMDD
- 7 bytes time HMMSSST
- 8 bytes site id
- 72 bytes log message

z/OS Example:

```
//INTSCOPY JOB xxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//INTSLOG DD DSN=INTS.VER72.LOGFILE,DISP=SHR
//LOGOUT DD DSN=INTS.COPY.INTSLOG,DISP=(NEW,CATLG),
//          SPACE=space,UNIT=unit,DCB=(RECFM=VB,BLKSIZE=8192)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COPY LOG
/*
```

z/VSE Example:

```
// JOB INTSCOPY
// LIBDEF PHASE,SEARCH=ints.library
// DLBL INTSLOG,'INTS.VER72.LOGFILE',,VSAM
// DLBL LOGOUT,'INTS.COPY.INTSLOG'
// EXTENT SYSnnn,volser,,,start,alloc
// ASSGN SYSnnn,DISK,VOL=volser,SHR
// EXEC INTSUTIL
COPY LOG
/*
```

COPY HTTPLOG

The output records on LOGOUT will be written in ascending date/time sequence. The records consist of the log message in Combined Log Format only, the date/time/site id fields from the VSAM file is stripped off.

z/OS Example:

```
//INTSCOPY JOB xxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//HTTPLOG DD DSN=INTS.VER72.HTTPLOG,DISP=SHR
//LOGOUT DD DSN=INTS.COPY.HTTPLOG,DISP=(NEW,CATLG),
//          SPACE=space,UNIT=unit,DCB=(RECFM=VB,BLKSIZE=8192)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COPY HTTPLOG
/*
```

z/VSE Example:

```
// JOB INTSCOPY
// LIBDEF PHASE,SEARCH=ints.library
// DLBL HTTPLOG,'INTS.VER72.HTTPLOG',,VSAM
// DLBL LOGOUT,'INTS.COPY.HTTPLOG'
// EXTENT SYSnnn,volser,,,start,alloc
// ASSGN SYSnnn,DISK,VOL=volser,SHR
// EXEC INTSUTIL
COPY HTTPLOG
/*
```

Maintaining User and Application Profiles—MAINT

The MAINT command creates, updates, and deletes User Profiles and Application Profiles. MAINT can also update the usage fields of a Screen Layout and entire Screen Layouts that have been created by the COPY function.

The INTSFLE VSAM file can not be directly updated from a batch program, since the file is open for update in the on-line system. The APPLid and CONNECT cards must therefore be used to establish a VTAM session with the online system. This session is then used to transfer the data to the online system. Use the following parameter cards:

```
APPLID=utilapp]
CONNECT APPLID=intsapp] [USER=.. PASSWORD=..]
MAINT [INPUT=[CARDS|FILE]] [DLM=d1m]
[maint record]
[maint record]
[.....]
```

A System Administrator user ID must be used.

The default is INPUT=FILE, which means that you must have created a sequential, variable blocked file which contains the maintenance records. The name of the file is INTSMNT.

If you specify INPUT=CARDS, the maintenance records must immediately follow the MAINT card. In this way you can only submit maintenance records that fit on a single card - continuation cards are not allowed. You may also specify a delimiter string with the DLM parameter in which case MAINT reads the card file until the DLM string is found at the beginning of a card.

The results of the update operations are returned to the batch program, where a control list is created.

This technique allows you to perform remote updates over the network.

Maintenance Records

The following types of records can be used:

1. An entire User or Application Profile as described in Appendix B.

Note that the record you create must follow the record layout exactly, with each field in the correct format. If the profile does not exist, it will be added to the InterSession file. If it exists, it will be updated by the new record. If the word "DELETE" is specified in the DELET field, the profile will be deleted.

Note also, that this gives you the ability to perform mass-changes to the InterSession profiles:

Read the profiles to a sequential file with the COPY command.

Update the profiles on the sequential file with your own-written batch program.

Return the resulting output records from this program to the InterSession System with the MAINT command.

For this purpose, use the record layouts IUPROFC/IAPROFC for COBOL and IUPROFA/IAPROFA for Assembler. These copy books can be found in the installation source library. If you create the profile records from scratch (without using COPY), note that the fields marked "RESERVED" should contain hexadecimal zeroes (low-values) to ensure compatibility with future releases of InterSession.

2. To add a new User Profile or a shared Application Profile, create a record with the following appearance:

2 bytes = "UN" or "AN" (U – User Profile, A – Application Profile).

8 bytes = User ID or Shared Application ID.

8 bytes = Spaces or the ID of an existing User or Shared Application Profile to be used as a base for the new profile.

3. To add a new personal Application Profile, create a record with the following appearance:

2 bytes = "PN".

8 bytes = User ID.

8 bytes = Personal Application ID.

8 bytes = Spaces or the ID of an existing Shared Application Profile to be used as a base for the new profile.

Note: If the "User ID" field is left blank, the record will be handled as a shared Application Profile according to 2) above.

4. To update a single field in a User Profile or a shared Application Profile, create a record with the following appearance:

2 bytes = "UF" or "AF" (U - User, A - Application Profile).

8 bytes = User ID or Shared Application ID.

8 bytes = Field name, see Appendix B.

n bytes = Field data, in the format described in Appendix B.

5. To update a single field in a personal Application Profile, create a record with the following appearance:

2 bytes = "PF".

8 bytes = User ID.

8 bytes = Personal Application ID.

8 bytes = Field name, see Appendix B.

n bytes = Field data, in the format described in Appendix B.

Note: If the "User ID" field is left blank, the record will be handled as a shared Application Profile according to 4) above.

6. To alter the shared Application Profile authorization for a user, create a record with the following appearance:
 - 2 bytes = "UA".
 - 8 bytes = User ID.
 - 1 byte = "+" or "-" to turn on and off authorization.
 - 8 bytes = Shared Application Profile ID.

7. To alter the shared application sequence for a user, create a record with the following appearance:
 - 2 bytes = "US".
 - 8 bytes = User ID.
 - 8 bytes = Shared Application Profile ID.
 - 3 bytes = The position on the menu screen, three digits.

8. To compress the shared application sequence for a user (equivalent to the online COMPRESS command), create a record with the following appearance:
 - 2 bytes = "UC".
 - 8 bytes = User ID.

9. To alter the usage fields of a Screen Layout, create a record with the following appearance:
 - 2 bytes = "SL".
 - 8 bytes = Screen Layout ID.
 - 8 bytes = Field name, see Appendix B.
 - n bytes = Field data, in the format described in Appendix B.

z/OS Example:

```
//INTSUPD EXEC PGM=INTSUTIL
//INTSMNT DD DSN=name,DISP=OLD
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=SYST PASSWORD=ADMIN
MAINT INPUT=FILE
```

z/VSE Example:

```
// DLBL INTSMNT,'name'
// EXTENT SYS000,volser
// ASSGN SYS000,DISK,VOL=volser,SHR
// EXEC INTSUTIL
```

```

APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=SYST PASSWORD=ADMIN
MAINT INPUT=FILE
/*

```

Creating Reports on User and Application Profiles—LIST

The LIST command creates a report on User and Application Profiles by reading the INTSFLE VSAM file. The profiles can be listed based on a selection criteria specified in the parameter card.

In the batch job JCL, you must supply an INTSFLE DD/DLBL card.

Use the following parameter card:

```

LIST {USER|USERS|APPLICATION|APPLICATIONS}
    [WITH field <=> value]
    [FIELDS=field,field,field...]
    [SEQ=STD|ID]
    [LINECT=nn]

```

You may use one or two continuation cards. If you do, type data up to column 72, type any character in column 72 and continue in any column on the next card.

The WITH operand

field can be any of the field names listed in the record layouts in Appendix B. **value** can be generic, i.e. **TSO*** as in the following examples. Only one WITH operand can be coded. Only those profiles that fits the selection criteria will be listed in the report.

The FIELDS operand

By default the following profile fields are listed:

For User Profiles:

```

ID , NAME , GROUP , SADM , UPDUP , UGRP , MAST , MGRP , TLOCK , ADATE , RDATE
SACP , NSESS , NTERM , NAPP , APPAC

```

For Application Profiles:

```

ID , TEXT1 , TYPE , AQUAL , HIDE , AUTCK , SATYP , SAPPL , SSCRIP , ESCRIP ,
DATAP , CMPR , CICS , SPORT , IDLE

```

If you need to see other fields, you may use this operand to tailor the appearance of the report. **field** can be any of the field names listed in the record layouts in Appendix B.

If you just want to replace a few fields, you can use a + and – sign in front of the field name. For example, to see the Data Field 1 of a User Profile instead of the user's name, you can code **FIELDS=-NAME , +DATA1**

If you need to create a completely different report, you have to specify all fields you want to see, for example **FIELDS=ID , NAME , DATA1 , DATA2 , DATA3 , NSESS**

The SEQ operand

This is used for the Application Profile listing only. **SEQ=STD** lists the profiles in the standard application sequence as they appear on the menu screen. **SEQ=ID** lists the profiles in application name alphabetic order.

The LINECT operand

This is used to set the number of lines to be printed on each page. Specify a two-digit value from 01 to 99. The default value is 56.

If you specify **LINECT=00**, only one header will be written at the beginning of the list (for field identification) and no page breaks will exist in the listing.

The DATA_n and TEXT_n fields

The DATA1-8 fields of the User Profile and the TEXT1-6 fields of the Application Profile are not displayed in their full length (32 characters), in order to save space on the print line and make room for more fields.

However, if you need to see these fields in their full length, suffix the field name with the letter L, i.e. **FIELDS=DATA4L** or **FIELDS=TEXT1L**.

The APPAC field on the User Profile has a special meaning. It will list the entire system access list with one line for each system the user is authorized to use, i.e. the user's menu listing. For each system the following information is listed: Menu sequence number, Name, Description and VTAM APPLid.

If you do not want to see the system access list, specify **FIELDS=-APPAC**

If you use APPAC in the WITH operand, only those users who have access to the specified system will be listed, for example **WITH APPAC=TSO**

z/OS Example:

```
//INTSLIST JOB xxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//INTSFLE DD DSN=INTS.VER72.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
LIST USERS WITH GROUP=SYSP* FIELDS=-APPAC
/*
```

z/VSE Example:

```
// JOB INTSCOPY
// LIBDEF PHASE,SEARCH=ints.library
// DLBL INTSFLE,'INTS.VER72.FILE',,VSAM
// EXEC INTSUTIL
LIST USERS WITH GROUP=SYSP* FIELDS=-APPAC
/*
```

LIST command examples:

LIST USERS WITH ADM=YES	Lists all System Administrators.
LIST USERS WITH NSESS>1	Lists all Multiple Session Users.
LIST USERS WITH APPAC=TSO	Lists all users with access to Application Profile TSO.
LIST APPLICATIONS SEQ=ID	Lists all Application Profiles in alphabetic order.
LIST APPLICATION WITH ID=TSO	Lists the Application Profile TSO.

Copying / moving application access list—COPYACC / MOVEACC

The COPYACC and MOVEACC commands transfers the application access list from one application to another. These functions reads the INTSFLE VSAM file, selects all users who have access to the SOURCE application. It then writes one, two or three INTSUTIL MAINT records for each user to a sequential file. These records are:

- One UA record that sets application access to the TARGET application (always created) for this user
- One UA record that removes application access from the SOURCE application for this user (only for the MOVEACC command)
- One US record that sets the application sequence number for the TARGET application (only for the MOVEACC command and if there is a user-specific application sequence. If this is not required, use the KEEPSEQ=NO option, see below).

The MAINT records thus created must be input to the MAINT function in a second job step (see example below).

In the batch job JCL, you must supply an INTSFLE DD/DLBL card.

Use the following parameter card:

COPYACC|MOVEACC SOURCE=appname TARGET=appname
[KEEPSEQ=YES|NO]

COPYACC copies the application access list for the SOURCE application to the TARGET application. After the MAINT operation, all users that had access to the SOURCE application will also have access to the TARGET application.

MOVEACC moves the application access list for the SOURCE application to the TARGET application. After the MAINT operation, all users that had access to the SOURCE application will instead have access to the TARGET application. If KEEPSEQ=YES (the default) the TARGET application will appear in the same position as the SOURCE application did in the user application sequence, if any.

The SOURCE operand

This is mandatory and specifies the name of the source application. If the name contains embedded blanks, enter the name within single quotes.

The TARGET operand

This is mandatory and specifies the name of the target application. If the name contains embedded blanks, enter the name within single quotes.

The KEEPSEQ operand

This is optional and only used with the MOVEACC command. If set to YES, the target application will appear in the same position as the SOURCE application did. Users without a user specific application sequence will not be affected by this option. The default is YES.

z/OS Example:

```
//INTSMACC JOB xxxx,CLASS=x,MSGCLASS=x
//MOVEACC EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//INTSFLE DD DSN=INTS.VER72.FILE,DISP=SHR
//INTSMNT DD DSN=INTS.VER72.MAINTREC,DISP=(,CATLG,DELETE),
```

```
//          RECFM=VB,BLKSIZE=8192,SPACE=(CYL,(5,5))
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
MOVEACC SOURCE=TSOX TARGET='TSO PROD'
/*
//MAINT     EXEC PGM=INTSUTIL
//STEPLIB  DD DSN=INTS.VER720.LOADLIB,DISP=SHR
//INTSMNT  DD DSN=INTS.VER720.MAINTREC,
//          DISP=(OLD,DELETE,DELETE)
//SYSPRINT DD SYSOUT=*
//SYSABEND DD SYSOUT=*
//DEBUG    DD SYSOUT=*
//SYSIN    DD *
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=userid PASSWORD=password
MAINT INPUT=FILE
/*
```

NOTE that if you have more than one InterSession system, the INTSFLE file in the first step must represent the same system as indicated by the APPLid in the second step!

Sending MMS Messages—SEND

The SEND command sends MMS messages from batch to one or more users. Use the following parameter cards:

```
APPLID=utilapp]
CONNECT APPLID=intsapp][USER=sender PASSWORD=password]
SEND [IMM|MAIL|BREAK] [TO] [[USER=userid[,userid..]
    [[GROUP=code] | [DL=distr.list]]
    [INPUT=CARDS|FILE] [DLM=d1m] [TITLE=title]
[message line]
[message line]
[.....]
```

You can send the message as an immediate or breakthrough message, or as an MMS mail message. It can be sent either to one or more user id's, to a user group or to an MMS distribution list.

The default is INPUT=CARDS. If you specify INPUT=FILE, the message lines must be located in a variable blocked file named INTSMMSG. Each card/record data should not be longer than 64 bytes. Any over-length data will be truncated.

Each card/record may have a plus or minus sign in its first position to denote a normal or high intensity line.

If you have several messages in the data stream with imbedded SEND commands, you should use the DLM parameter to delimit the messages. For example, if you specify DLM=*EOM*, the message lines for each message should be followed by a card with *EOM* in columns 1-5.

The message will be saved in the sender's mailbox as if it was created on-line. However, if sender=receiver, only the received message will be saved in the user's mailbox. Example:

```
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=STEVE
SEND MAIL TO JAN TITLE=MESSAGE FROM BATCH
+THIS IS THE FIRST LINE
THIS IS THE SECOND LINE
+THIS IS THE THIRD LINE
```

Closing and Opening System Files—CLOSE and OPEN

The CLOSE and OPEN commands close and open the account and log files. Use the following parameter cards:

```
APPLID=utilapp1
CONNECT APPLID=intsapp1 [USER=mastop] [PASSWORD=password]
{OPEN ACCOUNT|CLOSE ACCOUNT}
{OPEN LOG|CLOSE LOG}
{OPEN HTTPLOG|CLOSE HTTPLOG}
```

At least one OPEN and CLOSE command must be coded. The user "mastop" must be defined as a Master Operator.

z/OS Example:

```
//INTSOPEN JOB xxxx,CLASS=x,MSGCLASS=x
//INTSUTIL EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER72.LOADLIB,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=STEVE PASSWORD=GERANIUM
OPEN ACCOUNT
/*
```

z/VSE Example:

```
// JOB INTSOPEN
// LIBDEF PHASE,SEARCH=ints.library
// EXTENT SYSnnn,volser,,,start,alloc
// ASSGN SYSnnn,DISK,VOL=volser,SHR
// EXEC INTSUTIL
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=STEVE PASSWORD=GERANIUM
OPEN ACCOUNT
/*
```

Deleting Old MMS Messages—DELMSG

The DELMSG command deletes messages queued for users:

```
APPLID=utilapp1
CONNECT APPLID=intsapp1 [USER=sysadm] [PASSWORD=pass]
DELMSG [ALL] [USER=xxxx] [AGE=nnn]
```

The user ID in the CONNECT card must be defined as a System Administrator.

If no user ID is specified in the DELMSG card then all user accounts are scanned for old messages.

If the AGE parameter (number of days) is not specified then 30 days is assumed.

ALL means that all messages are deleted regardless of the message status, with the exception of the following:

- The message status is "Created" or "Altered".
- One or more message receivers are stored with the message.

Messages of the above type are considered to be local distribution lists.

Without ALL, only messages with status "Received/read" are affected.

With ALL and no user id specified (meaning all users), any AGE value must be 30 (days) or more. Otherwise, any AGE value, including 0, can be specified.

Note 1: To delete messages sent with the z/OS MODIFY operator command or from the z/VSE operator's console (indicated in console messages as sender = OPERATOR) you should specify the special user id ****OPER****, for example

```
DELMSG ALL USER=**OPER**
```

Note 2: Without any USER parameter, messages sent with the operator command (stored on the special user id ****OPER****) will also be deleted.

z/OS Example:

```
//DELETLG EXEC PGM=INTSUTIL
//STEPLIB DD DSN=INTS.VER720.LOADLIB,DISP=SHR
//SYSIN DD *
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=STEVE PASSWORD=GERANIUM
DELMSG ALL
/*
```

z/VSE Example:

```
// EXEC INTSUTIL
APPLID=INTSUTIL
CONNECT APPLID=INTSESS USER=STEVE PASSWORD=GERANIUM
DELMSG ALL
/*
```

Examples:

DELMSG USER=userid	Messages with status "Received/read" and older than 30 days for "userid" are deleted.
DELMSG USER=userid AGE=0	All messages with status "Received/read" for "userid" are deleted.
DELMSG ALL USER=userid	All messages older than 30 days for "userid" are deleted.
DELMSG ALL USER=userid AGE=0	All messages for "userid" are deleted.
DELMSG ALL	All messages older than 30 days for all users are deleted.

Printing the Log File—PRINTLOG

The PRINTLOG command prints the log file messages.

Note that the log file must be closed. This can be done manually with the /CLOSE command from the Main Menu Screen, or with the CLOSE LOG command.

PRINTLOG [msgno] [msgno]....

If you do not specify any message numbers, all messages will be printed. You may enter as many message numbers as can fit on a single card.

z/OS Example:

```
//PRINTLG EXEC PGM=INTSUTIL
//INTSLOG DD DSN=INTS.LOG.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
PRINTLOG IS0101 IS0103
```

z/VSE Example:

```
// DLBL INTSLOG,'INTS.LOG.FILE',,VSAM,CAT=catalog
// EXEC INTSUTIL
PRINTLOG IS0101 IS0103
/*
```

Inactivating/activating Application Profiles—INACT/ACT

The INACT/ACT commands disables or enables the use of one or more Application Profiles:

APPLID=utilappl

CONNECT APPLID=intsappl [USER=mastop] [PASSWORD=password]

INACT APPLICATION=applprof [CANCEL|FORCE] [TIME=time] [INFO=text]

ACT APPLICATION=applprof

When the INACT command is executed, the application on the menu screen will appear to the ordinary end user as not active (i.e. in red color). Additionally, an informative text and/or an estimated time of availability may be set on the menu screen application entry.

If the Application Profile parameter “Propagate menu screen info” is set to YES, then all Application Profiles with the same VTAM APPLid will be affected.

The ACT command may later be used to enable the application(s) again.

An explanation of the parameters follows:

APPLICATION=applprof

The name of the Application Profile.

CANCEL|FORCE

If specified, any active user sessions to this application will either be “soft” canceled (if any End Script is specified, it will be executed) or force terminated.

TIME=time

Specifies the estimated time of availability. It may be given in any of the formats **hhmm**, **hh:mm**, **hh.mm**, **+hhmm**, **+hh:mm** or **+hh.mm**. A plus sign indicates a time specification relative to the current time. For example, **+1.45** indicates one hour and forty-five minutes from now.

INFO=text

Specifies any text that will be used as an error message when the user tries to select the application, for example

INFO=System down for backup

Compressing Internal Security Keys—COMPRESS

The COMPRESS command reformats application security codes when no additional Application Profiles can be added. When you add a new Application Profile, it is assigned the next available application security code, a number from 1 and 1024. Security codes for deleted Application Profiles, however, are not reused. When you have added 1024 Application Profiles, you may not add any more, even if the current number of Application Profiles is less than 1024. The COMPRESS command reclaims the security codes from deleted Application Profiles. After the compression, new Application Profiles may be added again.

Note that the online system must not be active when performing this function. The COMPRESS command has no options:

COMPRESS

z/OS Example:

```
//CMPRES EXEC PGM=INTSUTIL
//INTSFLE DD DSN= INTS.VER72.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMPRESS
/*
```

z/VSE Example:

```
// DLBL INTSFLE, 'INTS.VER72.FILE',,VSAM,CAT=catalog
// EXEC INTSUTIL
COMPRESS
/*
```

Issuing VTAM Commands

INTSUTIL can issue VTAM commands. You must use the APPLid card, followed by any VTAM command:

APPLID=applid
vtam command

Other Features

Initializing the VSAM File—FORMAT

FORMAT

This command formats the InterSession VSAM file when installing the system. A number of records will be written, to ease the implementation of the system. See member FORMAT in the source library.

Note: This command can only be used on an empty file.

Upgrading to a New Version—UPGRADE

UPGRADE

This command upgrades the InterSession VSAM file when installing a new version of the system. It will read your old file, reformat the existing records and add new records to a new file. Please note that your on-line system should be inactive when upgrading to a new version. See member UPGRADE in the source library.

This command can also be used to refresh the DEFAULT Help Screens. If the DEFAULT Help Screens are changed by the InterSession support/development team without changing the version, the UPGRADE command will only upgrade the DEFAULT Help Screens and copy all other records unchanged to the new file.

Record Layouts

User Profile Record

The format of the User Profile that is used for the Maintenance functions from CICS and batch is described in Appendix B. The layout can also be found in the installation source library as copy book **IP-PROFA** for Assembler.

Application Profile Record

The format of the Application Profile that is used for the Maintenance functions from CICS and batch is described in Appendix B. The layout can also be found in the installation source library as copy book **IAPROFA** for Assembler.

Recovering from startup or sign on problems

Introduction

Situations may arise that will prevent InterSession to start, or where it is impossible for any user to sign on to InterSession.

Such situations can be caused by invalid settings in InterSession made by an administrator, or by factors outside InterSession control.

To recover from such problems you should use the InterSession Startup Parameters, especially the FAILSAFE parameter. It has the following format:

**FAILSAFE={NO,APF,EXTSEC,TCPIP,USEREXIT,NOABEXIT,AMODE24,
SYSADMIN:userid,SCRLAYOUT,YES,APPLINQ}**

NO No functions are set. This is the default.

APF The system does not test for APF authorization. z/OS only.

EXTSEC External Security support will not be activated.

TCPIP The TCPIP interface will not be activated.

USEREXIT No user exits will be activated.

NOABEXIT The InterSession abend exit will not be activated.

AMODE24 InterSession will run in 24 bits addressing mode.

SYSADMIN:userid Allows you to create a new System Administrator. The user id defined here will become a System Administrator when he/she logs on to InterSession.

SCRLAYOUT If your Screen Layout has been corrupted for some reason, preventing you from signing on to InterSession, this function will restore the contents of the DEFAULT Screen Layout to its original appearance. Also, as long as this function is in effect, all users will be forced to use the DEFAULT Screen Layout, regardless of the settings in other Screen Layouts or in the User Profiles.

YES All of the above functions are set.

APPLINQ The application status inquire mechanism of InterSession will be disabled at startup. This means that all applications will show as available, regardless of status. Note that the inquire mechanism can be enabled by the REFRESH INQ=YES operator command.

Securing TCP/IP traffic with AT-TLS

Introduction

AT-TLS (Application Transparent Transport Level Security) is a widely used component in z/OS, used to secure TCP/IP traffic.

It can be used both by IBM applications, such as the FTP and TN3270 servers, and by external vendor applications.

This chapter describes in detail how to implement AT-TLS for the InterSession TN3270 and HTTP servers.

It can be used in its entirety by non-experienced AT-TLS users or in parts by skilled users of AT-TLS (sections on server certificate creation, ring creation and policy file).

A condensed version of this chapter can also be found in the **ATTLSCFG** member of the installation source library.

In the following, all RACF commands are given via a batch job.

Use the TSO command processor IKJEFT01 with the following JCL:

```
//RACFCMD  JOB 1, 'RACF', CLASS=A, MSGCLASS=X, MSGLEVEL=(1,1)
//STEP1    EXEC PGM=IKJEFT01, DYNAMNBR=20
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
- commands -
/*
```

Also note that in the RACF commands, **USER(user id)** is the user id that is assigned to the InterSession job/stc.

If you are a skilled user of AT-TLS or if you already have a signed root certificate from an external Certificate Authority (CA), skip to Step 1B.

Otherwise, start from the beginning with Step 1A.

Step 1A. AT-TLS is not used today

Activate RACF classes and define resources

This step may already be done, but it will not harm to reissue the commands.

Issue the following RACF commands using the above JCL:

```
SETROPTS RACLIST(DIGTCERT) CLASSACT(DIGTCERT)
SETROPTS RACLIST(DIGTNMAP) CLASSACT(DIGTNMAP)
SETROPTS RACLIST(DIGTRING) CLASSACT(DIGTRING)
SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH ** UACC(ALTER) OWNER(racfadm)
RDEFINE STARTED PAGENT*. * OWNER(racfadm) +
  STDATA(USER(TCPIP) GROUP(STCGRP))
RDEFINE FACILITY IRR.DIGTCERT.LISTRING +
  UACC(NONE) OWNER(racfadm)
```

```
RDEFINE FACILITY IRR.DIGTCERT.LIST +
      UACC(NONE) OWNER(racfadm)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT +
      UACC(NONE) OWNER(racfadm)
```

Create a self-signed root certificate for testing purposes

Since you do not have a root certificate from an external CA, you can create your own root certificate. The use of such a self-signed root certificate should only be used for testing purposes and requires that you export it to your test workstation(s), see below.

Issue the following RACF commands:

```
RACDCERT CERTAUTH GENCERT +
      SUBJECTSDN(CN('InterSession CA')) +
      SIZE(1024) +
      NOTBEFORE (DATE(200-01-01)) +
      NOTAFTER (DATE(2029-12-31)) +
      WITHLABEL('INTSTLS CA') +
      KEYUSAGE(CERTSIGN) +
      ALTNAME(DOMAIN('your.domain.com'))
```

Create a server certificate signed with your test root certificate

Issue the following RACF commands:

```
RACDCERT ID(user id) GENCERT +
      SUBJECTSDN(CN('InterSession Server Certificate')) +
      SIZE(1024) +
      NOTBEFORE (DATE(2020-01-01)) +
      NOTAFTER (DATE(2029-12-31)) +
      WITHLABEL('INTSTLS Server') +
      KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN) +
      ALTNAME(DOMAIN('your.domain.com')) +
      SIGNWITH(CERTAUTH LABEL('INTSTLS CA'))
```

Export the test root certificate to a file

Issue the following RACF commands:

```
RACDCERT CERTAUTH +
      EXPORT(LABEL('INTSTLS CA')) +
      DSN('INTS.EXPORT.ROOTCERT') +
      FORMAT(CERTB64)
```

FTP the certificate file ASCII to your test client workstation(s).
Consult workstation documentation on how to install a new certificate.

Continue to Step 2.

Step 1B. AT/TLS is already in use

Since you use AT/TLS already, you have a root certificate from an external Certificate Authority installed.

Create a server certificate

Issue the following RACF command:

```
RACDCERT ID(user id) GENCERT +
  SUBJECTSDN( +
    CN('InterSession Server Certificate') +
    O('company') +
    L('location') +
    C('countrycode') ) +
  SIZE(1024) +
  NOTBEFORE(DATE(2010-01-01)) +
  NOTAFTER(DATE(2029-12-31)) +
  WITHLABEL('INTSTLS Server') +
  KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN) +
  ALTNAME( +
    DOMAIN('your.domain.com') )
```

Create a request file to send to your external CA

Issue the following RACF command:

```
RACDCERT ID(user id) GENREQ(LABEL('INTSTLS Server')) +
  DSN('hlq.SERVCERT.REQ')
```

Wait while the external CA processes your request.

When you receive the signed certificate file from the external CA:

Add the signed certificate

Issue the following RACF command:

```
RACDCERT ID(user id) +
  ADD('hlq.SERVCERT.CRT') +
  TRUST +
  WITHLABEL('INTSTLS Server')
```

Continue with Step2, Step3 and appropriate parts of Step4.

Step 2. Create a keyring for your server and connect certificates to it

Issue the following RACF commands.

Note that you should use only one of the **CONNECT** parameters, depending on if you come from Step 1A or Step 1B:

```
RACDCERT ID(user id) ADDRING(INTSRING)
```

```

RACDCERT ID(user id) +
    CONNECT(CERTAUTH LABEL('INTSTLS CA') +
        RING(INTSRING) )
RACDCERT ID(user id) +
    CONNECT(LABEL('INTSTLS Server') +
        RING(INTSRING) +
        DEFAULT)
RACDCERT ID(user id) +
    LISTRING(INTSRING)

```

Step 3. Refresh RACF classes

Issue the following RACF commands:

```

SETROPTS RACLIST(DIGTCERT) REFRESH
SETROPTS RACLIST(DIGTNMAP) REFRESH
SETROPTS RACLIST(DIGTRING) REFRESH
SETROPTS RACLIST(STARTED) REFRESH
SETROPTS GENERIC(STARTED) REFRESH

```

Step 4. Configure and start the policy agent (PAGENT)

Create a file containing the PAGENT environment variables.

Put in file `hlq.TCPPARMS (PAGENV)` :

```

PAGENT_CONFIG_FILE=/etc/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent.log

```

Create the PAGENT configuration file.

Put it in Unix System Services file `/etc/pagent.conf`.

Note stack name `TCPIP`, change if you have another name:

```

LogLevel 15
TcpImage TCPIP FLUSH PURGE
TTLSConfig //'hlq.TCPPARMS(INTSTLS)' FLUSH

```

Create the policy file for InterSession.

You can use the following example, or you can use the IBM Configuration Assistant to create your own policy file. It is available on the IBM web site.

Put in file `hlq.TCPPARMS (INTSTLS)`

Note the InterSession job name prefix `Jobname INTS*` and the InterSession ports for `TN3270` and `HTTP`, `Port 3023` and `Port 3080`.

Replace with what you have defined in InterSession.

Note also the section `TTLSCipherParms`, where you may want to use other ciphers than in this example.

```

## BeginFile
##
TTLSRule                                0~1
{
    LocalAddrSetRef                      addr1
    RemoteAddrSetRef                     addr1

```

```

LocalPortRangeRef      portR1
RemotePortRangeRef     portR2
Jobname                 INTS*
Direction               Inbound
Priority                 255
TTLSTGroupActionRef    gAct1
TTLSEnvironmentActionRef eAct1
TTLSTConnectionActionRef cAct1
}
TTLSTRule               0~2
{
  LocalAddrSetRef       addr1
  RemoteAddrSetRef      addr1
  LocalPortRangeRef     portR3
  RemotePortRangeRef    portR2
  Jobname                INTS*
  Direction              Inbound
  Priority                254
  TTLSTGroupActionRef   gAct1
  TTLSEnvironmentActionRef eAct1
  TTLSTConnectionActionRef cAct1
}
TTLSTGroupAction        gAct1
{
  TTLSEnabled           On
}
TTLSEnvironmentAction   eAct1
{
  HandshakeRole         Server
  EnvironmentUserInstance 0
  TTLSTKeyringParmsRef  keyR~INTS
}
TTLSTConnectionAction   cAct1
{
  HandshakeRole         Server
  TTLSTCipherParmsRef   cipher1~INTS
  TTLSTConnectionAdvancedParmsRef cAdv1
  CtraceClearText       Off
  Trace                  2
}
TTLSTConnectionAdvancedParms cAdv1
{
  ApplicationControlled Off
  HandshakeTimeout       10
  ResetCipherTimer       0
  SecondaryMap            Off
}
TTLSTKeyringParms       keyR~INTS
{
  Keyring                INTSRING
}
TTLSTCipherParms        cipher1~INTS
{
  V3CipherSuites         TLS_RSA_WITH_DES_CBC_SHA
  V3CipherSuites         TLS_RSA_WITH_AES_128_CBC_SHA
}

```

```

IpAddrSet          addr1
{
    Prefix          0.0.0.0/0
}
PortRange          portR1
{
    Port            3080
}
PortRange          portR2
{
    Port            1024-65535
}
PortRange          portR3
{
    Port            3023
}
##
## EndFile

```

Create the PAGENT proc.

You can use this JCL or start with the IBM sample in `hlq.TCPPARMS`.

```

//PAGENT    PROC
//PAGENT    EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//           PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/'
//STDENV    DD DSN=hlq.TCPPARMS(PAGENV),DISP=SHR
//SYSPRINT  DD SYSOUT=*
//SYSOUT    DD SYSOUT=*
//CEEDUMP   DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)

```

Step 5. Enable AT-TLS in the TCPIP stack

AT-TLS is enabled via a TCPCONFIG parameter in the `PROFILE DD` file:

```

TCPConfig
    TTLS                ; Enable AT-TLS policies

```

Step 6. Activate AT-TLS

Put a "S PAGENT" card in the system startup proc.

Re-IPL - or - restart TCPIP and start PAGENT.

NOTE that with `TCPConfigTTLS` specified, the TCPIP stack waits in the startup sequence for the PAGENT stc to be activated.

You will see the message

```
EZZ4248E TCPIP WAITING FOR PAGENT TTLS POLICY
```

When PAGENT is active the following message is displayed

EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS

Step 7. Debugging AT-TLS

If things does not work as expected, look for error messages in

- The system log
- The PAGENT log file, Unix file `/tmp/pagent.log`

Consult the appropriate IBM documentation for more information.

Appendices

Appendix A: Accounting Record Layouts

The following record layouts are used when “INTS” or “INTX” account record types are selected in the System Options, Other. These are two versions and the difference between them is that in the “INTX” records there are 36 extra bytes immediately following the record prefix, see below.

In the installation source library you will find the layout of the “INTS” and “INTX” records in the members ACNTREC and ACNTRECX.

If “TV” or “TVX” account records are selected, please see the appropriate Teleview manual. “TVX” contains some extra information.

Each accounting record is divided into two sections:

- Record prefix
- Record body

The Record Prefix

The format of the record prefix is different depending on whether you are using a VSAM file or an SMF dataset:

The SMF record prefix follows the rules for SMF records:

2 bytes	Binary record length
2 bytes	Segment descriptor
1 byte	System indicator
1 byte	Record type from System Options ACCOUNT parameter
4 bytes	Binary time of day 1/1000 sec
4 bytes	Packed date YYDDD
4 bytes	System identification

The VSAM record prefix contains the following fields:

4 bytes	Binary time of day 1/100 sec
4 bytes	Packed date YYDDD

The “INTX” extra information contains the following fields:

8 bytes	InterSession JOB/STC name
8 bytes	InterSession Site id (set in the System Options, Other)
20 bytes	Reserved for future use

InterSession will generate several types of Accounting Records. Each type begins with a 1-byte record type.

The Record Body

The Terminal Identifier

In most records the eight-byte Terminal Identifier is created. For VTAM terminals, this is the VTAM LU name of the terminal. For IP terminals (using the InterSession TN3270 server or the IBM TN3270 server) the Terminal Identifier consists of the four-byte string “IP*” followed by four bytes IP address in hexadecimal.

System Startup Record

This record is written after a successful startup.

1 byte Record type X'00'

Sign On / Sign Off Record

This record is written when a user has made a sign on or sign off-.

1 byte	Record type: X'10' – OK sign on X'11' – invalid sign on X'20' – User initiated sign off X'21' – InterSession initiated sign off
8 bytes	Terminal Identifier
8 bytes	User ID
4 bytes	Binary InterSession session ID
8 bytes	User Group Code
1 byte	External Security Indicator—Y if user is defined to an External Security Manager
2 bytes	Packed number of allowed application sessions
4 bytes	Terminal IP address, if any
12 bytes	Reserved for future use
2 bytes	Terminal port number, if any

Session Start Record

This record is written when a user has established an application or internal session:

1 byte	Record type X'30'
8 bytes	Terminal Identifier
8 bytes	User ID
4 bytes	Binary InterSession session ID
8 bytes	Application Profile name
8 bytes	VTAM APPLid of application host system (blank if internal session)
8 bytes	VTAM APPLid for the session (blank if internal session or if pass mode used)

Session Interval Record

This record is written if a time interval has been specified in the System Options field "Interval record interval". At the end of each interval, one record for every active Relay Mode session will be written. It has the same appearance as the Session End Record below, except for the record type and the last field (interval)

1 byte Record type X'38'

Session End Record

This record is written when a Relay Mode session is ended.

1 byte	Record type X'40'
8 bytes	Terminal Identifier
8 bytes	User ID
4 bytes	Binary InterSession session ID
8 bytes	Application Profile name
8 bytes	VTAM APPLid of application host system (blank if internal session)
8 bytes	VTAM APPLid being used for the session (blank if internal session)
6 bytes	Packed transaction count
8 bytes	Packed total response time in 1/1000 seconds
4 bytes	Binary total number of bytes received from the terminal
4 bytes	Binary total number of bytes sent from the application
4 bytes	Binary total number of bytes sent to the terminal (after any data compression)
5 bytes	Packed CPU time used by InterSession in 1/1000 seconds
2 bytes	Binary time interval in seconds set in System Options (only Session Interval Record)

System Shutdown or Midnight Record

This record is written when InterSession is shut down and at midnight.

1 byte	record type X'90'
8 bytes	packed total transaction count
8 bytes	packed total number of internal and application sessions
8 bytes	packed total transaction count (applications sessions only)
8 bytes	packed total InterSession response time in 1/1000 seconds
8 bytes	packed total CPU time used by InterSession in 1/1000 seconds

Appendix B: Maintenance Record Fields

The following records will be written by the INTSUTIL COPY and UPDATE commands. They can also be used as input to the INTSUTIL MAINT command.

The field names are also used in the MAINT UF / AF / AL records.

You can find these record layouts in the installation source library under the names IUPROFA and IAPROFA.

The User Profile / Model Record

Field	Length	Description	Comment
TYPE	2	Record type	"UP"
ID	8	User / Model id	
NAME	24	User name / Model description	Field name MDESC also ok
GROUP	8	Group	
STAT	8	Status	Enabled/Revoked/Model
SLID	8	Screen Layout id	
ADATE	6	Last Access date	
RDATE	6	Revoke date	
SADM	3	System Administrator	YES or NO
UPDUP	3	Update User Profiles	YES, NO or RES
UGRP	8	Update User Profile group	
MAST	3	Master Operator	YES or NO
TLOCK	3	Terminal lock admin	YES or NO
MGRP	8	Mastop/Tlock group	
UINF	3	Update info screens	YES or NO
MNTOP	3	Maintain own profile	YES, RES, SEQ, NO, DEF
ADHOC	3	Can start ad-hoc sessions	YES or NO
CHKXS	3	Check user against ESM	YES or NO
XSEC	3	User is defined to ESM	YES or NO
ALTPW	3	Can change internal password	YES or NO
PWDUR	3	Internal password duration days	
PWCD	5	Internal password change date	YYDDD
NSESS	2	Max number of sessions	
NTERM	2	Max number of terminals	
IDLE	3	Terminal idle timeout	DEF or value
IDLEA	3	Application idle timeout	DEF or value
IDLES	3	Widow session timeout	DEF or value
IDLEB	3	Standby idle timeout	DEF or value
STBY	3	Standby after terminal timeout	DEF or value
AAKEY	4	Alternate Attn key	PFnn or PAn
GSENT	3	Group sessions by entrance id	YES, NO or DEF
APUSQ	3	Applications in user-def sequence	YES or NO
AAM1	8	Appl access model name 1	

-----	776	Appl access model names 2-99	
AAM100	8	Appl access model name 100	
VTERM	8	Virtual terminal id	
SLID	8	Screen layout id	
TWOLM	3	Two-level menu	YES, NO or DEF
AAKEY	4	Attention key	PFnn or PAn
JKEY	4	Jump key	PFnn or PAn
CKEY	4	Command key	PFnn or ENT
CCHAR	5	Command prefix	
BGUPD	7	Background update action	NO, ALARM, SWITCH, MENU
MBOPE	3	Mailbox open	YES or NO
TLENA	3	Top Line Menu functionality	TLM, NO, BRK, DEF, TV, SS, TPX
TLCOM	1	Top Line Menu initial command	
HKTLM	3	Hot keys in Top Line Menu	YES, NO or DEF
HKCMP	3	Hot keys with command prefix	YES, NO or DEF
HK01	9	Hotkey 1	Shared Application + "R"
HK02	9	Hotkey 2	
HK03	9	Hotkey 3	
HK04	9	Hotkey 4	
HK05	9	Hotkey 5	
HK06	9	Hotkey 6	
HK07	9	Hotkey 7	
HK08	9	Hotkey 8	
HK09	9	Hotkey 9	
HK10	9	Hotkey 10	
HK11	9	Hotkey 11	
HK12	9	Hotkey 12	
HK13	9	Hotkey 13	
HK14	9	Hotkey 14	
HK15	9	Hotkey 15	
HK16	9	Hotkey 16	
HK17	9	Hotkey 17	
HK18	9	Hotkey 18	
HK19	9	Hotkey 19	
HK20	9	Hotkey 20	
HK21	9	Hotkey 21	
HK22	9	Hotkey 22	
HK23	9	Hotkey 23	
HK24	9	Hotkey 24	
ASAP1	8	Autostart application 1	
ASAP2	8	Autostart application 2	
ASAP3	8	Autostart application 3	
ASAP4	8	Autostart application 4	

ASAP5	8	Autostart application 5	
ASAP6	8	Autostart application 6	
ASAP7	8	Autostart application 7	
ASAP8	8	Autostart application 8	
DATA1	32	Data field 1	
DATA2	32	Data field 2	
DATA3	32	Data field 3	
DATA4	32	Data field 4	
DATA5	32	Data field 5	
DATA6	32	Data field 6	
DATA7	32	Data field 7	
DATA8	32	Data field 8	
PRTRE	3	Printer receiver profile	YES or NO
PRID	8	Printer id	
PRHDR	3	Print header	YES or NO
PRHFF	3	Form feed after header	YES or NO
WCONF	3	Web: show configuration link	YES or NO
DELET	6	"DELETE" for removal	
CHGDAT	6	Changed date YYMMDD	
CHGTIM	6	Changed time HHMMSS	
CHGUSR	8	Changed by user id	
NAPP	4	Number of authorized apps below	
APPAC	400 * 8	List of authorized shared apps	

The Shared or Personal Application Profile Record

Field	Length	Description	Comment
RECT	2	Record type	"AP" or "PP"
ID	8	Application name	
TYPE	6	Application type	VTAM/TN3270 etc
AQUAL	48	Application qualifier	[netid.]applid
TEXT1	32	Menu screen text language 1	YES/NO
XSID	8	External Security id	YES/NO/EXT
NETIF	8	Interface name	Tn3270 only
CODPG	5	Codepage	
AUTCK	3	Authorization check	YES or NO
HIDE	3	Hide application	YES or NO
STAT	1	Application status	I/A
INQAS	3	Inquire about appl status	YES/NO
PRINF	3	Propagate menu screen info	YES/NO
SATYP	6	Session APPLid type	POOL. GROUP. NONE
SAPPL	8	Session APPLid/Pool number	
LOCKA	3	Lock Pool APPLid to user	YES/NO
SSCRIP	8	Session Start Script	

ESCRIP	8	Session End Script	
USCRIP	8	Background update script	
STKEY	4	Application start key (PF key)	PF1 – PF24
DATAP	64	Data to pass to application	
APPTD	3	Append %TD to 'Data to pass..'	YES/NO
ASFS	3	Appl sends first screen	YES/NO
MODPS	8	Pass mode SNA Logmode name	
MODPN	8	Pass mode non-SNA Logmode	
MODRS	8	Relay mode SNA Logmode name	
MODRN	8	Relay mode non-SNA Logmode	
MCOS	8	Relay mode COS name	
CMPR	3	Data compression	YES/NO
TRTAB	8	3270 data translation table	
RBUF	3	Read terminal buffer	YES/NO
PASS	3	Application will pass session	YES/NO
IDLE	3	Application idle timeout	USR/DEF/value
SNOFF	3	Sign off at session end	YES/NO
SPORT	3	Session portable	YES/NO
BGUPD	3	Perform background update action	YES/NO
BCONV	3	Bracket protocol conversion	YES/NO
MTS	3	Model terminal support	YES/NO
CANS	3	Cancel session at terminal logoff	YES/NO
ENDTS	3	End terminal session at session end	YES/NO
REML	3	Remove LOGAPPL at session end	YES/NO
LEVEL	1	Menu screen level	1/2
TEXT2	32	Menu screen text language 2	
TEXT3	32	Menu screen text language 3	
TEXT4	32	Menu screen text language 4	
TEXT5	32	Menu screen text language 5	
TEXT6	32	Menu screen text language 6	
CHGDAT	6	Changed date YYMMDD	
CHGTIM	6	Changed time HHMMSS	
CHGUSR	8	Changed by user id	
INFO1	1600	Information screen 1	20 x 80
INFO2	1600	Information screen 2	20 x 80
DELET	6	"DELETE" for removal	
CHGDAT	6	Changed date	yymmdd
CHGTIM	6	Changed time	hhmmss
CHGUSR	8	User performing the change	

The Screen Layout Usage Fields

Field	Length	Description	Comment
DEF	3	Default Screen Layout	YES/NO
TIDnn	8 * 35	Terminal id TID01-TID35	Terminal id or blank

ENTRnn	8 * 7	Entrance id ENTR1-7	YES/NO
--------	-------	---------------------	--------

Appendix C: Recognized Telnet Terminal Type Strings

The following Telnet Terminal Type strings are recognized by InterSession. Other Terminal Types will be tried as **IBM-3278-2**.

IBM-327X

IBM-327X-M

IBM-327X-M-E

IBM-DYNAMIC

X is any character or digit (ignored)

M is the terminal Model (2-5)

E indicates extended datastream

Examples

IBM-3278-2 is a 24x80 terminal without extended datastream.

IBM-3279-3-E is a 32x80 terminal with extended datastream.

IBM-3277 is a 24x80 terminal without extended datastream.

Notes

"Extended datastream" is also used to determine if a terminal is "structured fields" compatible. Terminals with "extended datastream" will be queried by the system at connect.

Appendix D: The Host Table

To simplify handling and make messages more understandable there is a hostname/ip address table. Whenever a TN3270 session is started InterSession will look into this table to resolve the name or ip address. If there is a name in the host table this name appended with the port number will be used in all subsequent messages.

The host table must be assembled and should be located on a library accessible by InterSession. It can be dynamically reloaded from the console.

The host table is created using a macro, `MHOST`. The table must start with a `MHOST BEGIN` entry, and end with a `MHOST END` entry. The host entries have the following syntax:

```
MHOST ipaddr,name
```

The host names can be entered with or without the domain part. There is no practical limit to the length of the name in the table, but InterSession will only display the first 32 characters if the name with the port number appended is longer than 32 characters.

Sample HOSTS table

```
*
*      SAMPLE HOSTS TABLE
*
HOSTS  CSECT
        MHOST BEGIN
        MHOST 140.147.254.3,LOCIS.LOC.GOV
        MHOST 192.168.2.4,z/VM
        MHOST 192.168.0.102,                X
                SCOTTS.PC
        MHOST 192.168.0.103,TAPEVAULT
        MHOST END
        END
```

Appendix E: TN3270E Printing Details

TN3270E printing is a protocol used to connect TCP/IP attached printers. In the TN3270E software the remote LU-name is specified. In InterSession this is the name of the Printer Options Profile.

Supported Terminal Types

The following telnet terminal types are supported for TN3270E printing. Other types will be rejected.

IBM-3287
 IBM-3287-X
 IBM-DYNAMIC

"X" is any character or digit (ignored)

Supported Printer Modes

The TN3270E gateway supports LU1 (also referred to as SCS) and LU3 (sometimes referred to as DSC) printing. InterSession does not modify the print data in any way, and the print data is not spooled in InterSession.

IP Address and Mask

The connecting TN3270E printer's IP address is checked for validity when connecting. This is done by doing a logical AND with the IP Address Mask and then comparing the result with the IP Address in the Printer Options Profile. If the values are equal the printer may connect, otherwise the connect is rejected. In other words, for every '1' bit in the mask the corresponding bit in the printer's IP address must have the same value as the bit in the IP address in the Printer Options Profile. InterSession does not accept non-contiguous masks.

Examples

Printer IP address	Profile IP Address	Profile Mask	Result	Comment
192.168.2.102	0.0.0.0	0.0.0.0	Connect	Anyone may connect
192.168.2.102	192.168.2.102	255.255.255.255	Connect	Only this address
192.168.2.103	192.168.2.102	255.255.255.255	Reject	Only the specified address may connect
192.168.2.103	192.168.2.102	255.255.255.0	Connect	Anyone in the (class C) subnet may connect
192.168.3.1	192.168.2.102	255.255.255.0	Reject	Different subnet
10.7.3.58	10.7.3.48	255.255.255.240	Connect	Non-standard subnetting
38.14.7.22	192.168.0.0	255.255.0.0	Reject	No access from Internet
172.24.7.89	0.0.0.0	255.255.255.255	Reject	No-one can connect
-	-	255.0.255.255	ERROR	Not allowed

Appendix F: Log File Record Layout

The format of the log file record is as follows:

4 bytes	year
2 bytes	month
2 bytes	day
2 bytes	hour
2 bytes	minute
2 bytes	second
1 byte	tenth of a second
8 bytes	site id as set in the System Options
70 bytes	log message
7 bytes	not used

Appendix G: The InterSession Logon Component

It is not necessary to use this feature and it is not recommended to new InterSession customers. It is still available for back level compatibility only.

The Logon Component is only used in a situation where you have many VTAM hosts that owns old-fashioned VTAM terminals, but only runs a few InterSession systems. The Logon Component is then started in the VTAM hosts where no InterSession system is running.

The terminal users in these VTAM hosts should connect to the Logon Component by a VTAM logon to **INTSLOGN** (or whatever APPLid you have chosen).

The Logon Component will then pass the VTAM terminal to any of the InterSession systems in a round-robin fashion. The InterSession system selected by the Logon Component will then be set as the logon application for this terminal. In the following, this terminal will be automatically connected to the same InterSession system after a terminal disconnect/reconnect.

In the following examples there are three InterSession systems running in three VTAM hosts.

Defining the INTSLOGN VTAM APPLid

First, in every VTAM host where you run the Logon Component, the following VTAM APPLid must be defined:

```
INTSLOGN APPL  AUTH=(ACQ,PASS,SPO),PARSESS=YES
```

Starting the Logon Component

```
//INTSLOGN EXEC PGM=INTSLOGN,REGION=200K
//SYSIN DD *
LGAPPLID=INTSLOGN
MSAPPLID=INTSESS1
MSAPPLID=INTSESS2
MSAPPLID=INTSESS3
/*
```
