z/OS Interactive System Productivity Facility

Use of the ISPF Workstation Agent

Version 2 Release 2

Note:
Links to related publications are from original documents and might not work. The links to publications are included for reference purposes only.

Contents

Chapter 1. ISPF Planning and Customizing

Customizing DM

Customizing DM describes procedures you can use to customize the DM component of ISPF to suit the particular needs of your installation:

- "Prohibiting connections to the ISPF Workstation Agent"
- Changing the default name for the ISPF Client/Server component download data set
- Set up ISPF GUI for TSO Line Mode support
- SMF command accounting
- Preallocation of List/Log data sets to SYSOUT
- Specifying the maximum number of split screens
- Setting ISPF site-wide defaults
- Customizing command tables
- Creating ISPF terminal translation tables
- Creating ISPF code page translation tables
- Displaying square brackets used in C programs
- ISPEXEC processing
- ISPF-to-APL2 terminal type mappings
- Load APL2® workspace
- Tailoring ISPF defaults
- Customizing the ISPF TSO command table (ISPTCM)
- Alternate option 7.1 panels
- ISPF multicultural support

See also ISPF installation-wide exits.

Prohibiting connections to the ISPF Workstation Agent

The communication between ISPF and the ISPF Workstation Agent is not secure. Therefore, avoid using the ISPF Workstation Agent. z/OS V2R4 is planned to be the last release to support the ISPF Workstation Agent.

System Authorization Facility (SAF) resource ISPF.WSA, in the FACILITY class, can be used to prohibit users from initiating a connection from ISPF to the ISPF Workstation Agent.

Use the following commands to define the resource ISPF.WSA in the FACILITY class with a universal access (UACC) of NONE. This will prohibit all users from initiating a connection to the ISPF Workstation Agent.

```
RDEFINE FACILITY ISPF.WSA UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

A sample job to issue the commands is supplied in member ISPRACF in the ISPF samples data set ISP.SISPSAMP.

Chapter 2. ISPF User's Guide Volume II

Initiate the workstation connection

If you select "Workstation connection" and your Workstation Agent code matches the latest level available, the Initiate Workstation Connection panel appears, as shown in Figure 1.

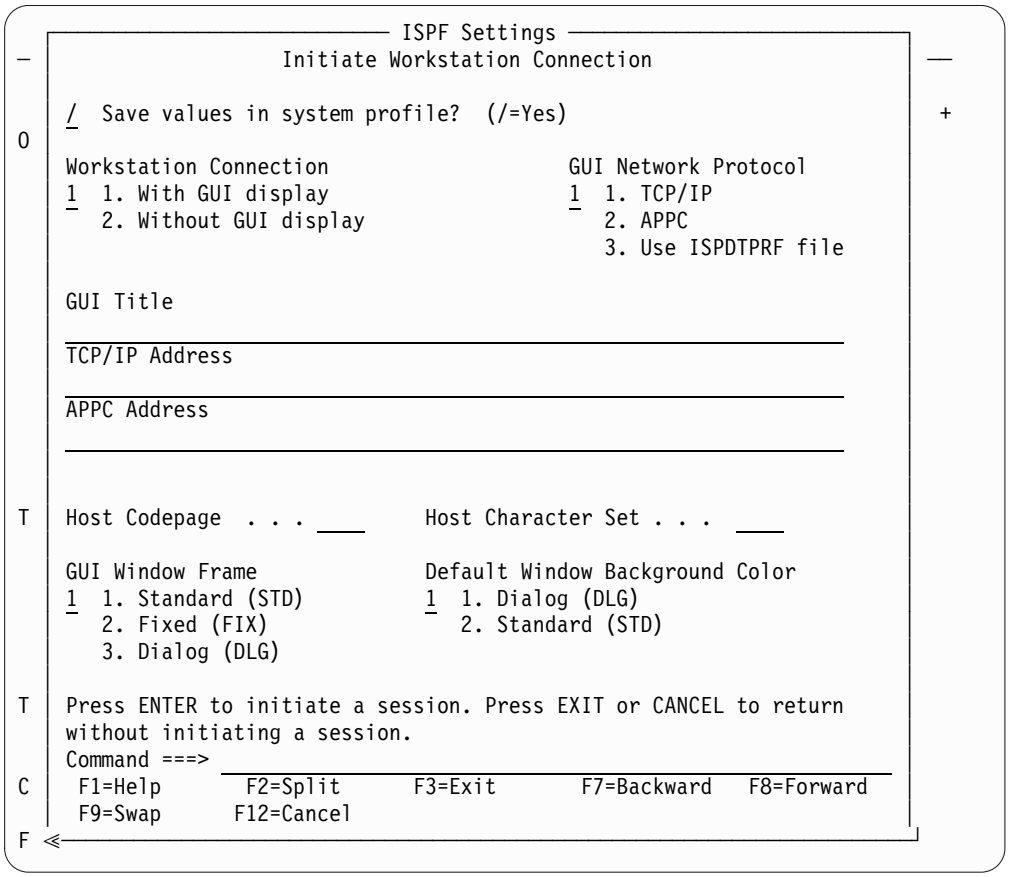

Figure 1. Initiate Workstation Connection panel (ISPISMGI)

Note: If your WSA is not running, this panel will appear but you will not be able to establish a connection.

Note: If the SAF resource ISPF.WSA is defined in the FACILITY class and you are not permitted access to that resource, this panel will appear, but you will not be able to establish a connection.

The Initiate Workstation Session panel allows you to specify that you want to start a GUI session. Starting a GUI session from this panel if you are in split screen mode or 3290 partition mode is not supported. If you select Workstation connection, you must specify the information in these fields, as appropriate:

Save values in system profile?
The default for this setting is YES. Any changes to this field are saved in the user's system profile.

Workstation connection
Allows you to specify one of these types of connections for your workstation session:

With GUI display
A GUI interface is provided for this session.

Without GUI display
A standard ISPF type of interface is provided for this session.

GUI Network Protocol
The type of network you use to connect the workstation to the host: TCP/IP or APPC.

You can also select the third option "Use ISPDTPRF file", to specify that ISPF get your network address from the file allocated to DD ISPDTPRF. The file can be sequential or a member of a PDS, and it can be fixed blocked (FB) or variable blocked (VB). Each line of the file should be formatted as follows: `userid WORKSTAT protocol_id:network_address`, where:

`userid`
user's TSO userid

`protocol_id`
network protocol identifier, either **ip** for TCP/IP or **lu** for APPC.

`network_address`
workstation address

For example, KEENE WORKSTAT ip:9.45.202.69.

GUI Title
The title you want displayed in the window frame of your GUI session. This value will be used if dialog variable ZWINTTL or ZAPPTTL is not found.

TCP/IP Address
The workstation's IP address. Required if you specified TCP/IP in the GUI Network Protocol field. The TCP/IP Address prompt is point-and-shoot text. If selected, a pop-up window is displayed containing the last five addresses saved in the system profile.

A TCP/IP address can be in dotted decimal format or in domain name format. Dotted decimal format is a sequence of decimal numbers separated by periods, for example, **9.87.654.321**.

A TCP/IP address in domain name format consists of one or more domain qualifiers separated by periods. The minimum specification for addresses within the same domain is a TCP/IP host name, for example, **jsmith**. The fully-qualified domain name for *jsmith* is formed by appending the appropriate subdomain name and root domain name to *jsmith*, such as **jsmith.raleigh.ibm.com**. To use domain naming, a domain name server must be active and providing domain name resolution for domain names within your TCP/IP network. The domain name server address is determined by the value of the **NSINTERADDR** statement in the TCP/IP configuration data set. ISPF must be able to locate the TCP/IP configuration data set as described in the section on configuring TCP/IP connections in the *z/OS ISPF User's Guide Vol I*.

If an asterisk (*) is specified, the TCP/IP address is obtained automatically from the value of the system variable ZIPADDR.

APPC Address

The workstation's APPC network name. Required if you specified APPC in the GUI Network Protocol field. The APPC Address prompt is point-and-shoot text. If selected, a pop-up window is displayed containing the last five addresses saved in the system profile.

An APPC address can be in fully-qualified LU name format or in symbolic destination name format. A fully-qualified LU name format consists of a network identifier and an LU name, separated by a period. For example, **USIBMNR.NRI98X00** is a fully-qualified LU name.

An APPC address in symbolic destination name format consists of a 1- to 8-character name such as **JSMITH**. The symbolic destination name must be defined as a *DESTNAME* and the corresponding fully-qualified LU name must be defined as the associated *PARTNER_LU* in the APPC/MVS side information.

Host Codepage

The host code page value used in translating data from the host to the workstation. This value **must** be specified with a Host Character Set value if it is to be used. If only one, or neither, of these values is specified, the values from the terminal query are used. If your terminal or emulator does not support code pages, the CODEPAGE and CHARSET parameter values on the ISPSTART command are used. If the ISPSTART values are not specified, the default code page and character set is ENGLISH.

Host Character Set

The host character set value used in translating data from the host to the workstation. This value **must** be specified with a Host Codepage value if it is to be used. If only one, or neither, of these values is specified, the values from the terminal query are used. If your terminal or emulator does not support code pages, the CODEPAGE and CHARSET parameter values on the ISPSTART command are used. If the ISPSTART values are not specified, the default code page and character set is ENGLISH.

GUI Window Frame

Allows you to specify one of these types of window frames for your GUI session:

1 **Standard (STD)**. A GUI window frame that can be resized and that has max/min buttons.

2 **Fixed (FIX)**. A GUI window frame that has a min button but cannot be resized.

3 **Dialog (DLG)**. A GUI window frame that cannot be resized and that does not have max/min buttons.

Note: Pop-up panels will always be displayed in dialog window frames.

Default window background color

Select the background color:

Dialog (DLG)

Standard (STD)

When you complete the fields shown in Figure 1 on page 3 and press Enter, the WSA connection panel is displayed in a separate window (unless your system has been set up to bypass it - see the topic about the System Register panel in "Installing the Client/Server component", in the *z/OS ISPF User's Guide Vol I* for

details).

Figure 2. WSA connection panel

This panel indicates the requestor and the type of connection requested. Click on **Yes** to accept the connection as described, or **No** to reject the connection.

If you accept the connection, the ISPF Settings panel is displayed. This will be in standard or GUI mode, depending on the option selected in the With GUI display field.

Chapter 3. ISPF Software Configuration and Library Manager (SCLM) Guide and Reference

SCLM support for workstation builds

You can store the source for workstation applications in SCLM. You can then use the configuration functions to build and promote the application. The build function transfers the source to an ISPF connected workstation, runs the compiler or other workstation tool, and then stores the results back into SCLM.

Storing workstation applications in SCLM provides several benefits:

- You can use SCLM as a single point of access for the workstation code.
- You can protect and back up the application source, executables, and outputs using the host.
- Host applications and workstation applications can share source.
- You can use SCLM's configuration management to ensure that the application is current.
- You can use the library management and versioning capabilities to track the application parts through the hierarchy and to retain backup versions.

Note: If the SAF resource ISPF.WSA is defined in the FACILITY class and you are not permitted access to that resource, you will not be able to establish a connection to the workstation.

Chapter 4. ISPF Messages and Codes

ISPI011 **ISPI011 Invalid environment, ISPF version 4 requires TSO/E 2.1 or later**

Explanation: The NOREXX keyword is required for this release of TSO.

User response: Correct your clist or exec.

ISPI012 **ISPI012 Invalid IP address**

Explanation: IPV6 is not supported.

User response: The message is issued by WSCON service. Either do not use WSCON in your environment, or logon to a system that still uses IPV4.

ISPI013 **Invalid environment for a workstation connection.**

Explanation: Connecting to a workstation is not supported when ISPF is invoked from a client.

System programmer response: If you require a workstation connection then start an ISPF session from a 3270 type screen.

ISPI014 **SAF check failed - The System Authorization Facility (SAF) has denied the request to initiate a workstation connection. The resource ISPF.WSA defined in the FACILITY class is defined with UACC(NONE) or the user is not permitted access. 'SAF RC=*aaaa*, RRET=*bbbb*, RREA=*cccccccc*'**

Explanation: An attempt to initiate a workstation connection was denied by the System Authorization Facility (SAF). The SAF resource ISPF.WSA is defined in the FACILITY class and the user who attempted to initiate the workstation connection is not permitted access to the resource.

System programmer response: If the user should be allowed to initiate a workstation connection, modify the SAF configuration to permit the user access to the ISPF.WSA resource in the FACILITY class.

User response: Contact your system programmer.

ISPI021 **ISPI021 Unrecoverable error in initialization of**

Explanation: A problem exists with the initialization of the function listed with this message.

System programmer response: Possible bad data set in the allocations shown in the message. If initialization continues to fail, contact IBM® for assistance.

User response: Contact your system programmer.

ISPI022 **ISPI022 ISPF cannot continue. ISPF abending.**

Explanation: A severe error occurred when ISPF was initializing. This message follows ISPI021 and can be eliminated when the problem described by the first message is corrected.

System programmer response: Correct the problem described by ISPI021.

User response: Contact your system programmer.

ISPI023 **ISPI023 ENVIRON TERMTRAC definition OFF, buffer could not be obtained**

Explanation: Storage was not available for creating the buffer and thus ENVIRON TERMTRAC is not available.

System programmer response: Determine why storage is not available.

User response: Contact your system programmer.

ISPI024 ISPI024 TSO module IRXECUSP could not be loaded

Explanation: REXX could not be initialized.

System programmer response: Determine if IRXECUSP exists and why the load fails. Contact IBM support for further assistance.

User response: Contact your system programmer.

ISPI025 ISPI025 TSO routine IRXINIT severe error - REXX environment could not be initialized.

Explanation: A severe error occurred while initializing the REXX environment.

System programmer response: Determine why the REXX environment can not be initialized. Contact IBM support for further assistance.

User response: Contact your system programmer.

Chapter 5. SNA Messages

ISTH035I The ISPF Workstation Agent is not in use on this system

Explanation: The check ISPF_WSA ran successfully and found no exceptions. The check determined that the ISPF Workstation Agent (WSA) has not been used on this system during this IPL.

The communication between ISPF and the ISPF Workstation Agent is not secure. Therefore, avoid using the ISPF Workstation Agent on your system. z/OS V2R4 is planned to be the last release to support the ISPF Workstation Agent.

System action: The system continues processing.

Operator response: Not applicable.

System programmer response: Not applicable.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server Health Checker

Module: ISTHCCK2

Routing code: Not applicable.

Descriptor code: Not applicable.

Automation: Not applicable.

Example:

```
ISTH035I The ISPF Workstation Agent is not in use on this system
```

ISTH036E The ISPF Workstation Agent is in use on this system

Explanation: The check ISPF_WSA determined that the ISPF Workstation Agent (WSA) has been used on this system during this IPL.

The communication between ISPF and the ISPF Workstation Agent is not secure. Therefore, avoid using the ISPF Workstation Agent on your system. z/OS V2R4 is planned to be the last release to support the ISPF Workstation Agent.

System action: The system continues processing.

Operator response: Not applicable.

System programmer response: System Authorization Facility (SAF) resource ISPF.WSA, in the FACILITY class, can be used to prohibit users from initiating a connection from ISPF to the ISPF Workstation Agent.

See the information about *Prohibiting connections to the ISPF Workstation Agent* in z/OS ISPF Planning and Customizing for more information.

When the check ISPF_WSA determines that the ISPF Workstation Agent is in use on this system, it will continue to be reported for the duration of this IPL, or as long as this Migration Health Check is active. Message ISTH036E is followed by message ISTH900I, which indicates the date and time that the ISPF Workstation Agent was last started. You can use message ISTH900I to determine whether a new use of the ISPF Workstation Agent has been detected or this report is related to an earlier use of the ISPF Workstation Agent.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server Health Checker

Module: ISTHCCK2

Routing code: Not applicable.

ISTH900I

Descriptor code: Not applicable.

Automation: Not applicable.

Example:

```
ISTH036E The ISPF Workstation Agent is in use on this system
```

ISTH900I **Function:** *mhc_function* **last** *mhc_usage* **on** *mhc_date* **at** *mhc_time*.

Explanation: A preceding exception message of type ISTH*xxx*E was generated. See those messages for more information.

In the message text:

mhc_function
The name of the function that was being checked.

mhc_usage
Possible values are:

started
This value is displayed when checking applications.

used
This value is displayed when checking configuration statements or functions.

mhc_date
The date that the function was last started or used.

mhc_time
The time that the function was last started or used.

System action: The system continues processing.

Operator response: Not applicable.

System programmer response: Not applicable.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS® Communications Server Health Checker

Module: ISTHCCK2

Routing code: Not applicable.

Descriptor code: Not applicable.

Automation: Not applicable.

Example: Not applicable.

Chapter 6. IBM Health Checker for z/OS User's Guide

ISPF checks (IBMISPF)

ISPF_WSA

Description:

Checks whether the ISPF Workstation Agent is in use on this system.

If this check determines that the ISPF Workstation Agent is in use on this system, it will continue to be reported for the duration of this IPL, or as long as this Migration Health Check is active. When this exception condition is detected, message ISTH036E is issued and is followed by message ISTH900I, which indicates the date and time that the ISPF Workstation Agent was last started. You can use message ISTH900I to determine whether a new use of the ISPF Workstation Agent has been detected or the exception condition is related to an earlier use of the ISPF Workstation Agent.

Reason for check:

The communication between ISPF and the ISPF Workstation Agent is not secure. Therefore, avoid using the ISPF Workstation Agent on your system. z/OS V2R4 is planned to be the last release to support the ISPF Workstation Agent.

z/OS releases the check applies to:

- z/OS V2R2 and V2R3 with the PTFs for APARs OA56980 and OA56984 applied.
- z/OS V2R4 and later.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line (ADDREPLACE POLICY) and use the UPDATE statement on a **MODIFY hzsproc** command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)] [STATEMENT(name)]
UPDATE
CHECK(IBMISPF,ISPF_WSA)
DATE('date of the change')
REASON('Your reason for making the update')
INACTIVE
SEVERITY(LOW)
INTERVAL(24:00)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:
See the information about *Prohibiting connections to the ISPF Workstation Agent* in *z/OS ISPF Planning and Customizing*.

Messages:
This check issues the following messages:

- *ISTH035I*
- *ISTH036E*
- *ISTH900I*

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:
SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

Printed in USA