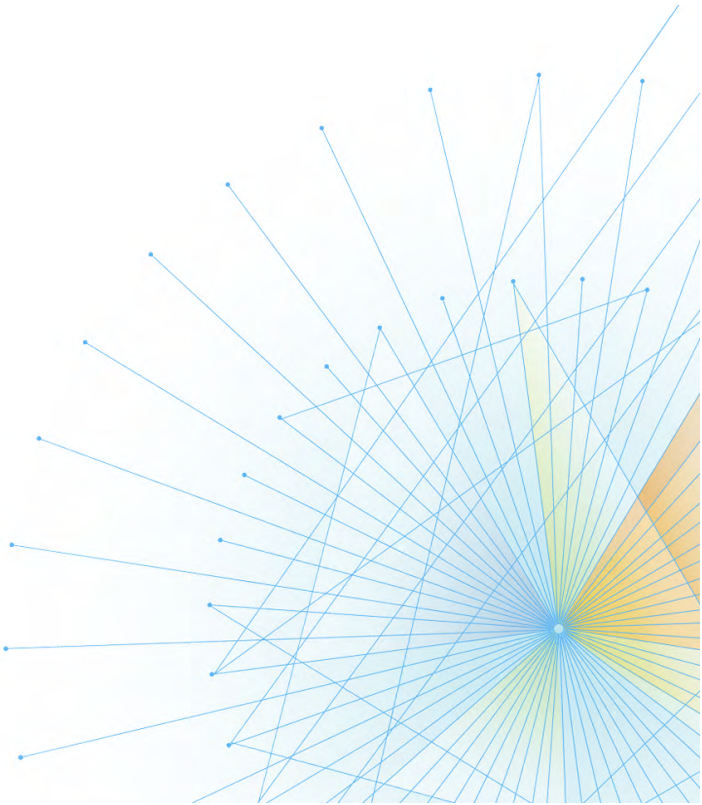
Compuware | The Mainframe Software Partner For The Next 50 Years

ISPW
Remote Server Guide

Release 18.02



Please direct questions about ISPW
or comments on this document to:

Compuware Support Center

https://go.compuware.com/

Doc. APR2019
March 22, 2019

Contents

Introduction

This manual documents the ISPW Remote Server, and contains the following chapters:

- Overview
- Remote Server Basics
- Security (Authentication).

Related Publications

- *ISPW Release Notes:* Overview of release features and any new ISPW information.
- *ISPW Installation and Configuration Guide*: Gives step-by-step instructions for the system programmer to configure, customize, and maintain ISPW. Refer to it when installing ISPW according to the *Compuware Installer Mainframe Products SMP/E Installation Guide*.
- *ISPW Deploy Reference*: Introduces ISPW users to the new ISPW Deploy product. It gives details of the concepts and facilities from both an end-user and technical perspective.
- *ISPW Interfaces Guide*: Describes ISPW's external call interface, stand alone load modules, and use with DB2 programs, plans, packages, and generated DECLARE statements. Interfaces with Telon, QMF, and Natural are also documented.
- *ISPW Planning Guide*: Provides information for use in the early stages of an ISPW implementation. It contains only what is necessary for planning and initial installation.
- *ISPW Messages and Codes*: Documents the messages and codes for ISPW, including started task errors, abend codes, return codes, allocation errors, and ISPW CM errors.
- *ISPW Technical Reference*: Provides detailed information on ISPW's structure, terms and concepts, maintenance functions, processing, security, and other technical content.
- *ISPW User Guide*: Provides an overview for Applications and other Information Systems staff to use ISPW effectively.
- *ISPW Upgrade Guide, Release 4.4 to 17.02*: Describes the major differences between ISPW 4.4 and ISPW 17.02 and serves as a guide for the upgrade process between these versions.
- *ISPW Web Interface Installation and Configuration Guide*: Provides instructions on how to install the ISPW Web Interface. ISPW Web is an Internet-based application designed to be used on workstations or smartphones. The ISPW Web Interface uses a Web browser that enables you to remotely approve or reject ISPW actions as well as deploy software to mainframe environments.

Online Documentation

The ISPW product installation package does not include the product documentation. Access the ISPW documentation from the Compuware Support Center website at **https://go.compuware.com** in the following electronic formats:

- Release Notes in HTML format
- Product manuals in PDF format
- Product manuals in HTML format.

The product documentation is available for viewing or downloading:

- View PDF files with the free Adobe Reader, available at **http://www.adobe.com**.
- View HTML files with any standard web browser.

Customer Solutions

Visit the Compuware Support Center, **https://go.compuware.com**, to find product documentation, knowledge articles, and other technical resources. You can open a case with the Customer Solutions team, order products, and much more.

Contact Customer Solutions by phone:

- USA and Canada: 1-800-538-7822 or 1-313-227-5444.
- All other countries: Contact your local Compuware office. Contact information is available at **https://go.compuware.com**.

Visit Compuware on the web at **http://www.compuware.com** for additional product information.

Overview

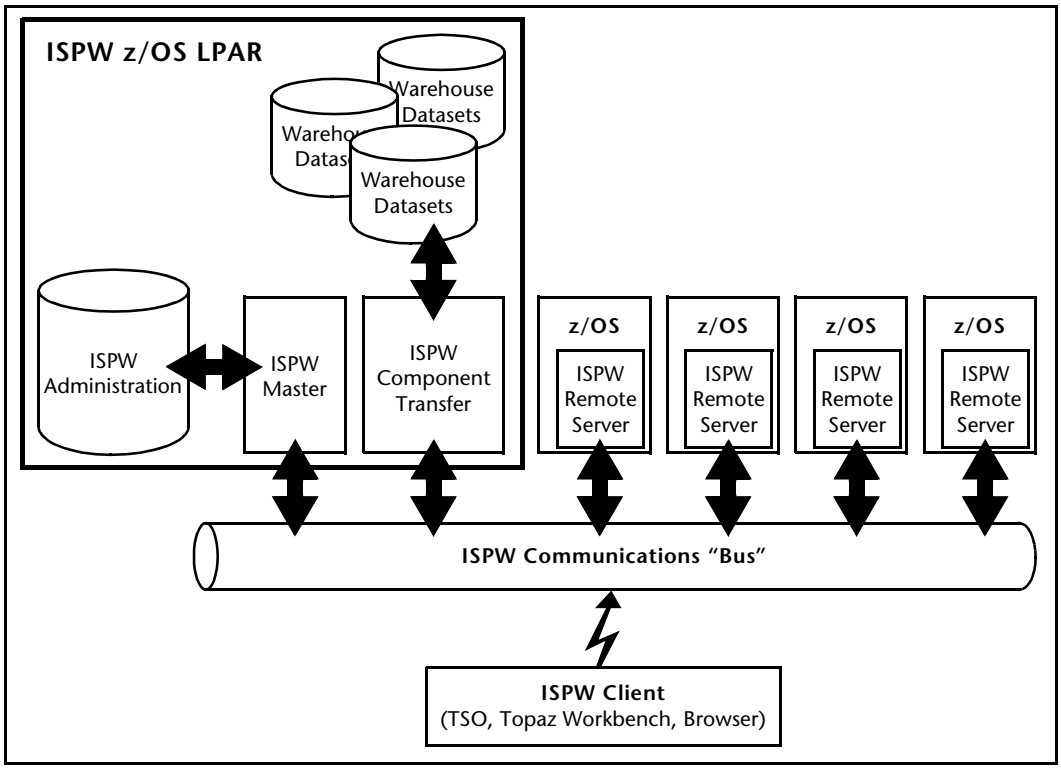
This manual describes the ISPW Remote Server. Remote Servers are ISPW Started Tasks running on the same or separate LPARs from the main ISPW Administration Server. ISPW Remote Servers are in constant communication with the ISPW Administration Server and are capable of:

- Receiving components to be stored in a local warehouse
- Accepting requests from the ISPW Master Server to initiate a deploy process
- Accepting Component Transport requests to receive a file from the requester and store it in the ISPW Warehouse or other location.

Architecture

Figure 1 illustrates the ISPW Architecture and where the Remote Servers fit in.

Figure 1. ISPW Architecture



Remote Server Basics

This chapter explains the fundamental concepts that apply to z/OS ISPW Remote Servers.

Execution Environment

The Server runs as an MVS Started Task.

Installation

See the *ISPW Installation and Configuration Guide* for details, and follow the instructions for the setup of a CT Started Task.

Entry in CMSC PARMLIB Member

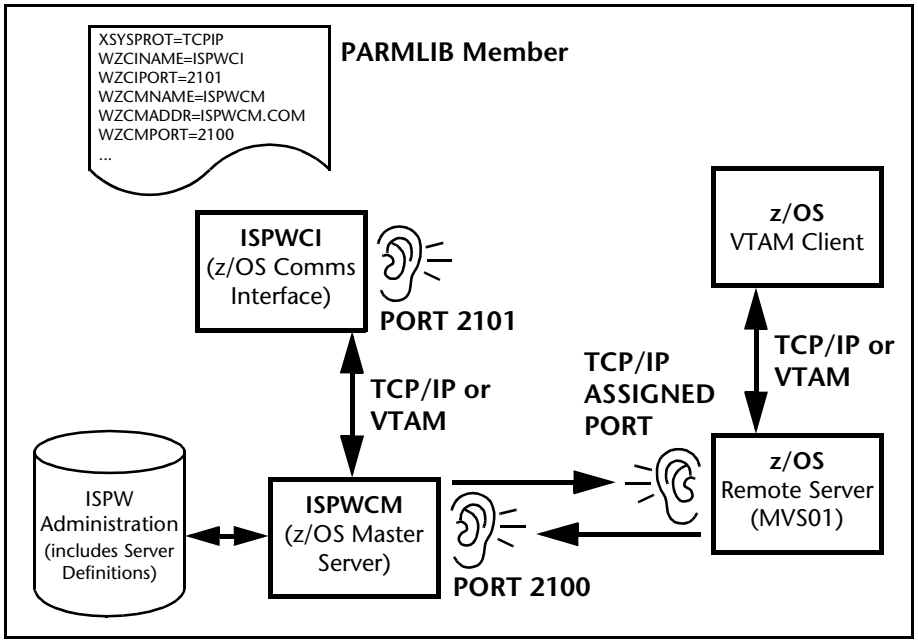
Every z/OS Remote Server must be reflected by a PARMLIB member entry for the Compuware Mainframe Services Controller (CMSC). For a discussion of PARMLIB configuration, see “Compuware PARMLIB Information” in the chapter entitled “ISPW Overview” in the *ISPW Installation and Configuration Guide*. For installation details, see “Task 8.6 Generate Started Task PARMLIB Members” in the same manual.

Method of Communication

Remote Servers establish a direct connection with the ISPW Master Server ISPWCM. Remote Servers also accept requests directly from ISPW Clients.

Figure 2 depicts the various Remote Server connections.

Figure 2. Remote Server Communication



Remote Server Startup Process

When a Remote Server starts, the processing described in Table 1 takes place.

Table 1. Remote Server Startup

Sequence	Description
1	Read the applicable PARMLIB member.
2	Establish a connection and log onto ISPW using the values in the PARMLIB member. This connection will remain open for requests that originate from the ISPW Master Server (ISPWCM).
3	Server definition parms (defined in M.SV) are returned, which include the port number to listen on for requests coming directly from other ISPW processes, including ISPW CT and Remote Servers.
4	Listen on port defined in M.SV for remote requests.

Local Warehouse

Each Remote Server has the capability of storing components in a local warehouse. ISPW's Deploy feature uses the warehouse to stage components prior to them being implemented. The z/OS warehouse is a PDS/E implementation.

Spawning Processes

Remote Servers have the ability to spawn processes for Deploy Operations. These processes run independently of the Remote Server and communicate back to CM the status of the implementation or activation. The mechanisms by which the processes are spawned is a z/OS Started Task. The Remote Server issues the MVS START command. The task will run under the authority of the UserID associated with the Started Task.

M.SV Entry

The ISPW Maintenance option M.SV is used to define Remote Servers, and all Remote Servers must be defined here. The M.SV entry screen is shown in Figure 3.

Figure 3. M.SV Entry Screen

```
ISPW               ADD SERVER TABLE DETAIL (W3M)
Command ===>

Enter required details:

 Server Name (KEY) ==>
 System Type       ==>           (MVS/WIN/AIX/LINX/SUN/HPUX)
 Server Type       ==>           (CT/CI/RS/CM)
 Address           ==>                                          (CT/RS Only)
 Socket            ==>           (CT/RS Only. Restart CT/RS if changed)
 CSS Socket        ==>           (CT Only. Restart CT if changed)
 Deploy            ==>           (Y/N CT/RS Only)
 Description       ==>



Press ENTER to complete the change or END to terminate
Note: To add a new entry the Key must be unique
```

See the *ISPW Technical Reference Guide* for a description of the input fields. The Address and Socket should be specified for z/OS Remote Servers.

Security (Authentication)

This chapter describes how Remote Servers are authenticated to ISPW.

Overview

Authentication is the process by which a Remote Server establishes its credentials with the ISPW Master Server (ISPWCM) whereby the Master Server confirms that the Remote Server really is who it says it is.

If the authentication process were to be compromised, it would be possible for unauthorized Remote Servers to establish contact with the Master Server and participate in component transport functions.

Centralized Authentication

All Remote Servers are authenticated centrally by the ISPW Master Server (ISPWCM). This is achieved by the combination of the security checks listed in Table 2.

Table 2. Centralized Authentication

Check	Security
1	A SAF UserID of the same name as the Server Name is defined in the security product (for example, RACF, ACF2, or TOP SECRET).
2	The UserID has authority to the ISPW Security rule SERVER LOGON.
3	The UserID has authority to the ISPW Security rule SERVER CTIDENT.
4	An entry exists in the ISPW Server Table (M.SV) for the server name.
5	The use of Security Tokens.

See the *ISPW Technical Reference* for a description of the various Security Rule definitions.

No Exposure to Passwords

The primary objective is to have a secure setup with no exposure to passwords being stored locally and being sent to the ISPW Master Server (ISPWCM). This is achieved via the use of Security Tokens that change on a regular basis.

Connecting the First Time

When a Server connects for the first time, and passes security checks one to four in Table 2, it receives a Security Token that is used in conjunction with subsequent authentication requests. This Token is stored in a registry file that is in the working directory.

It is recommended that the Remote Server be started as soon as possible after it has been defined, so that it can initiate the Token process. This will prevent any rogue processes connecting to ISPW with that definition and authority.

Security Token

The Security Token is randomly generated and changed periodically. It is stored in the ISPW database by the CM Task on z/OS.

Using the Token

Every time the Remote Server makes a request to ISPW, it sends its Security Token. As well as verifying the UserID, ISPWCM will check that the Token matches the one it issued. If it does not match, ISPWCM will reject the request.

Storing the Token

The Token is required to be securely stored on both the remote platform and within ISPWCM. Table 3 describes where it is stored and the security requirements required.

Table 3. Storing the Token

ISPW Server	Security Considerations
z/OS Master Server (ISPWCM)	Tokens for all Servers are stored in the DB2 Repository. It is recommended that the DB2 repository be protected and not able to be viewed.
z/OS Remote Server	Authentication on z/OS is guaranteed in that it is not possible for another UserID to "spoof" the CT Address space.

Refreshing the Token

The Security Token is changed at each server logon.

Reset Tokens

It may be possible that the Security Token needs to be reset because it is out of sync with the ISPW CM Task. This could happen, for example, if the Remote Server was moved to a different machine. There is a mechanism in M.SV to reset the Tokens for a server. The effect of this is as though the Remote Server is connecting for the very first time.

It is recommended that the Remote Server be started as soon as possible after the Reset Token has been done, so that it can initiate the Token process. This will prevent any rogue processes connecting to ISPW with that definition and authority.

Internal Tickets

For requests made directly between Remote Servers, ISPWCM will ensure that only authorized requests are made via the use of an internal ticket. If one Remote Server needs to connect to another Remote Server, ISPWCM will authorize the request and send an internal ticket to both servers so that they can verify that the request is valid.

Encryption

The signon string that is sent from the Remote Server across the network is encrypted. All other message data and file data is not encrypted.