Documentation Library

Web Spooled File Manager

Administrator Guide

Contents summary

WELCOME TO SPOOLED FILE MANAGER FOR ADMINISTRATORS 8

ROAD MAP 8

SECTION 1 - GETTING USERS STARTED 9

WHAT IS WEB SPOOLED FILE MANAGER? 9
INSTALLATION FOR USERS OF WSFM 11

SECTION 2 - ADMINISTRATION 13

ARCHITECTURE 13
ADMINISTRATOR RESPONSIBILITIES 14
BEFORE YOU START 14
INSTALL SERVER COMPONENTS 15
LICENCES 15
RELATED PRODUCTS 16
REGISTER USERS 16
FONTS 18
DOCUMENTATION 21

SECTION 3 – HOUSEKEEPING AND TROUBLESHOOTING 23

LOGGING 23
TRACING 24
CERTIFICATE MANAGEMENT 25
TROUBLESHOOTING 26
BEFORE YOU CONTACT AXES SUPPORT 29

SECTION 4 — CONFIGURATION 30

THE CONFIGURATION PROCESS 30
ABOUT THE CONFIGURATION FILES 30
CONFIGURE PORTS 33
CONFIGURE JSM HTTP SERVER 34
CONFIGURE SERVICES 44
REFERENCE GUIDE: JSM HTTP SERVER CONFIGURATION 49

APPENDICES 57

GLOSSARY 57
REFERENCED DOCUMENTS AND SOURCES 58
ASSUMED AND PREREQUISITE KNOWLEDGE 58
BROWSER BEHAVIOUR DIFFERENCES 59
WORKSTATION REQUIREMENTS 59
RUNNING WSFM AND DE SIDE BY SIDE 59
IBM I PRINTING REFERENCE 62

Content © LANSA Group
All Rights Reserved

Contents

WELCOME TO SPOOLED FILE MANAGER FOR ADMINISTRATORS 8

ROAD MAP 8

SECTION 1 - GETTING USERS STARTED 9

WHAT IS WEB SPOOLED FILE MANAGER? 9
INSTALLATION FOR USERS OF WSFM 11
Starting 11
Log on 12

SECTION 2 - ADMINISTRATION 13

ARCHITECTURE 13
Components and structure 13
WSFM database 13
ADMINISTRATOR RESPONSIBILITIES 14
BEFORE YOU START 14
Prerequisites 14
Decisions you need to make 14
Port number 14
Register users 14
Installation and configuration process 15
INSTALL SERVER COMPONENTS 15
New installations 15
Upgrades 15
LICENCES 15
RELATED PRODUCTS 16
REGISTER USERS 16
Why register users? 16
What is registration? 16
How to register users manually 16
Use SQL to register users 16
Write a program to register users 17
Register multiple users as a batch job 17
How to register users automatically 17
How to remove registered users 17
User identifications beginning with the letter Q 17
FONTS 18
Internal fonts 18
Constraints 18
Optional IBM fonts 19
Third party fonts 20
Fonts and server memory usage 20
DOCUMENTATION 21
Administrator and user guides 21
Portfolios 21

SECTION 3 – HOUSEKEEPING AND TROUBLESHOOTING 23

LOGGING 23
Log files: names and locations 23
Enable and disable logging 23
Archive log files 23
Delete log files 23
TRACING 24
Trace files: names and locations 24
Enable and disable tracing 24

Content © LANSA Group
All Rights Reserved

Clear trace files *25*
Archive trace files *25*
CERTIFICATE MANAGEMENT 25
TROUBLESHOOTING 26
Installation and configuration *26*
JSM HTTP server does not start 26
IBM Toolbox for Java not installed 26
File ownership and permissions for files in the IFS 26
WSFM database not found 26
Problems when running spool filters and queue filters *27*
Problems viewing the content of spooled files *27*
Browser response is slow or unresponsive *27*
Creating PDFs becomes slower and slower *28*
Managing errors *28*
SSL related errors 28
Browser errors 28
BEFORE YOU CONTACT AXES SUPPORT 29

SECTION 4 — CONFIGURATION 30

THE CONFIGURATION PROCESS 30
ABOUT THE CONFIGURATION FILES 30
File locations *30*
Manager.properties file *31*
Httpd configuration file *31*
Axinfo configuration file *33*
CONFIGURE PORTS 33
CONFIGURE JSM HTTP SERVER 34
Server instance configuration *34*
Controlling access to the server instance *36*
MIME types for the server instance *37*
Virtual host configuration *38*
Virtual host access 39
Virtual host protect 40
Virtual host script 42
Virtual host MIME types 43
CONFIGURE SERVICES 44
JSM HTTP file service configuration *44*
Allow and deny user access to services *45*
User registration *47*
REFERENCE GUIDE: JSM HTTP SERVER CONFIGURATION 49
Configuration item reference *49*
MIME types *52*
Access allow and deny directives *53*
Sample configurations *54*
Default configuration for WSFM 54

APPENDICES 57

GLOSSARY 57
REFERENCED DOCUMENTS AND SOURCES 58
ASSUMED AND PREREQUISITE KNOWLEDGE 58
BROWSER BEHAVIOUR DIFFERENCES 59
WORKSTATION REQUIREMENTS 59
Hardware *59*
Software *59*
Connectivity *59*
RUNNING WSFM AND DE SIDE BY SIDE 59
Configuration options *60*
User registration when operating both WSFM and DE *61*

Content © LANSA Group
All Rights Reserved

Configuration files *61*
axinfo.json 61
IBM I PRINTING REFERENCE 62
Definitions *62*
Host print transform 62
Stream files and SCS 62
Host Print Transform: limitations and constraints *62*

List of Figures

Figure 1: WSFM Screen Components and Layout 9
Figure 2: Options for Displaying the Content of Spooled Files 10
Figure 3: Display Spooled File Content as HTML 10
Figure 4: Access Logon Page 12
Figure 5: Web Spooled File Manager Architecture and Components 13
Figure 6: WSFM and DE on a single instance and virtual host 60
Figure 7: WSFM and DE on a single instance and two virtual hosts 60
Figure 8: WSFM and DE on two instances and two virtual hosts 61

List of Tables

Table 1: WSFM Database - SQL Tables 13
Table 2: Internal Fonts 18
Table 3: Font Constraints in WSFM 18
Table 4: Optional IBM font products 19
Table 5: IBM iSeries Font Products 20
Table 6: Microsoft Fonts 20
Table 7: Documentation: Administrator and User Guides 21
Table 8: Documentation: Administrator Portfolio 21
Table 9: Documentation: User Portfolio 22
Table 10: Information to Send to Support 29
Table 11: Configuration File Locations 30
Table 12: Explanation of manager.properties 31
Table 13: Example of an Updated manager.properties File 31
Table 14: Structure of the httpd Configuration File 31
Table 15: Mandatory and Optional Changes to Configuration Items and Parameters 32
Table 16: axinfo.json Configuration File for WSFM 33
Table 17: Configuration Items in axinfo.json 33
Table 18: Default Ports 33
Table 19: Configure Server Instance 34
Table 20: What to Configure for the Server Instance 35
Table 21: Control Access to the Server Instance 36
Table 22: What to Configure for Server Instance Access 36
Table 23: MIME Types for the Server Instance 37
Table 24: What to Configure for the Server Instance MIME Types 38
Table 25: Virtual Host Configuration 38
Table 26: What to Configure for One Virtual Host 38
Table 27: Virtual Host Access Directives 39
Table 28: What to Configure for Virtual Host Access 40
Table 29: Virtual Host Protect Configuration 41
Table 30: Configuring Virtual Host Protect 41
Table 31: Virtual Host Script Configuration 42
Table 32: Virtual Host MIME Type Configuration 43
Table 33: What to Configure for Virtual Host MIME Types 44
Table 34: Configure JSM HTTP File Service 44
Table 35: What to Configure for JSM HTTP File Service 45
Table 36: User Identification/Profile service.user Allow and Deny Parameter Syntax 45
Table 37: Example Configuration for service.user Allow and Deny Parameters 46
Table 38: Controlling Access to Services – service.user Allow and Deny Examples 47
Table 39: Autoregister Parameter for the Service sfmservice.jsp 47
Table 40: Autoregister Parameter for Automated or Manual User Registration 48

TABLE 41: SERVER REFERENCE: CONFIGURATION ITEM REFERENCE 49
TABLE 42: JSM HTTP SERVER REFERENCE: MIME TYPE EXAMPLES 52
TABLE 43: SERVER REFERENCE: ACCESS ALLOW AND DENY ADDRESSES 53
TABLE 44: SERVER REFERENCE: ACCESS ALLOW AND DENY CONTENT LENGTH 53
TABLE 45: SERVER REFERENCE: ACCESS ALLOW AND DENY USER AGENTS 53
TABLE 46: SERVER REFERENCE: SAMPLE LIST OF USER AGENTS 54
TABLE 47: SERVER REFERENCE: DEFAULT HTTPD CONFIGURATION FOR WSFM 54
TABLE 48: GLOSSARY OF ABBREVIATIONS AND TERMS 57
TABLE 49: REFERENCED DOCUMENTS AND INFORMATION SOURCES 58
TABLE 50: ASSUMED AND PREREQUISITE KNOWLEDGE 58
TABLE 51: BROWSER BEHAVIOUR DIFFERENCES 59
TABLE 52: AXINFO.JSON CONFIGURATION FILE FOR BOTH DE AND WS 61

Content © LANSA Group
All Rights Reserved

Welcome to Spooled File Manager for administrators

aXes Web Spooled File Manager (referred to as WSFM) helps you manage IBM i (System i, iSeries or AS/400) output queues and spooled files via the Internet from a browser. Typical tasks are:

- Search for spooled files
- Search output queues for spooled files
- Save the search criteria in folders and use them again
- Print spooled files
- Convert spooled files to HTML, PDF and/or text
- Download spooled files to your computer or mobile device

Once you have downloaded spooled files, you can include information from the spooled files into business applications like Microsoft Excel and Word.

This guide describes how to manage Web Spooled File Manager and the configuration options available to administrators.

Road Map

Use the road map to find information about Web Spooled File Manager.

If you want to...	Refer to...
Get started quickly	Section 1 - Getting users started with WSFM User installation, starting WSFM and log on instructions.
Understand operational concepts, install WSFM and manage users	Section 2 - Administration This section explains operational concepts and administrator responsibilities.
Housekeeping and troubleshooting	Section 3 – Housekeeping and troubleshooting This section describes housekeeping tasks, such as clearing log files, and explains how to track down problems.
Set values for configuration items and parameters	Section 4 - Configuration This section explains how to configure WSFM by setting values for the configuration items and parameters. The section includes a reference guide for the JSM HTTP server.
Read reference information	Appendices

For information about using Web Spooled File Manager to manage spooled files refer to the Web Spooled File Manager User Guide and the Pocket Guide.

Content © LANSA Group
All Rights Reserved

Section 1 - Getting users started

Getting users started provides an overview of WSFM including an explanation of the page content, layout and what WSFM can do to help users work with spooled files.

This section describes how to install, start and log on to WSFM from your computer or mobile device.

What is Web Spooled File Manager?

WSFM is a Web application that you use to manage spooled files and output queues on an IBM i server. The WSFM page consists of two panes. The left hand pane is the search filter and folder navigation pane. It contains filters and folders where you save the filters used to search for spooled files and output queues. The right hand pane consists of one or more tabs. The tabs contain search criteria, search results, forms for editing filters and setting options.

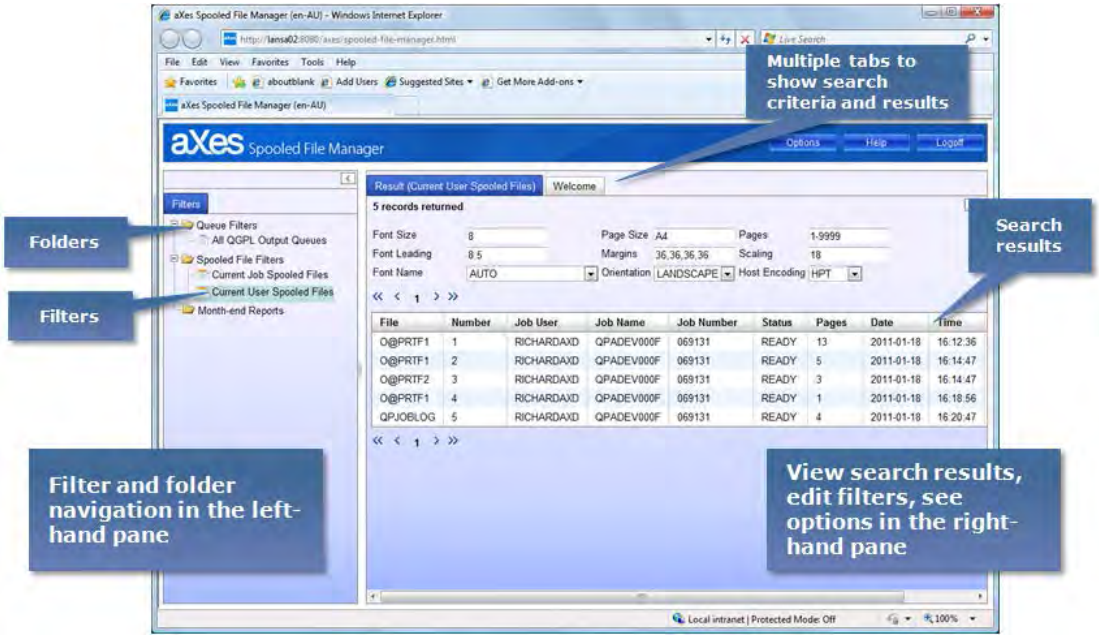

Figure 1: WSFM Screen Components and Layout

Figure 1 (page 9) shows two tabs in the right hand pane. The visible tab presents a list of spooled files for the person currently logged on and shows the search results from running the Current User filter. The second tab (out of view) is the Welcome page.

Figure 2 (page 10) shows a floating menu with options for working with spooled files. The options are opening to view as PDF, PDF image, text or HTML, holding, releasing and deleting a spooled file.

Clicking the left mouse button on a row in the list of spooled files selects the spooled file you want to work with (selected rows have a coloured background).

Clicking the right mouse button opens the floating menu (Figure 2, page 10) showing options for displaying spooled files (as PDF, PDF image, HTML or text) and actions for holding, releasing or deleting the selected spooled file. The properties option displays the attributes (or metadata) associated with the selected spooled file.

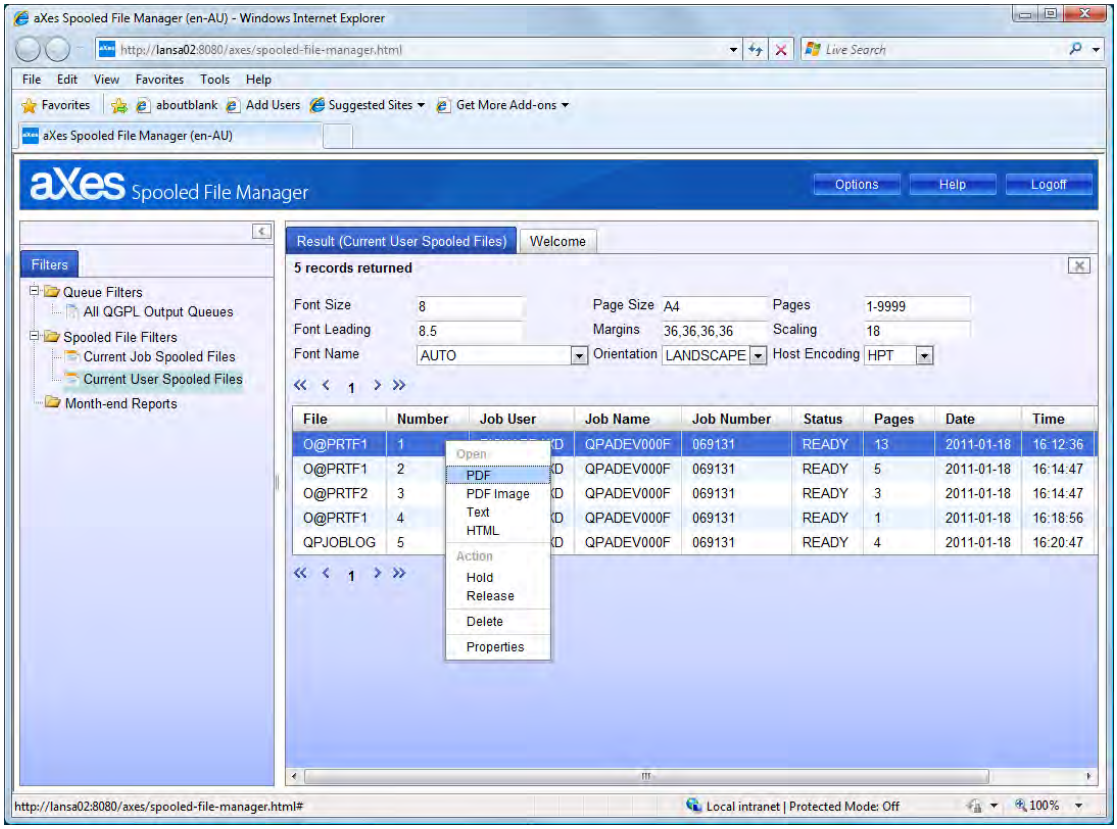

Figure 2: Options for Displaying the Content of Spooled Files

Clicking the HTML item from the floating menu opens a new window to reveal the content of the selected spooled file displayed as HTML.

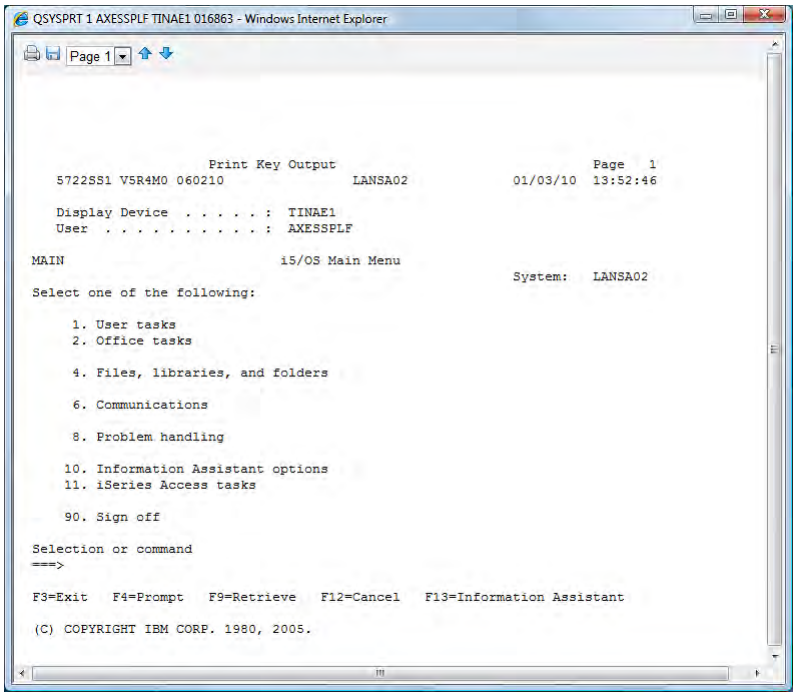

Figure 3: Display Spooled File Content as HTML

Figure 3 shows a spooled file displayed as HTML in its own window.

Installation for users of WSFM

Users do not need to install any software on their computer or mobile device to use WSFM.

The prerequisites for WSFM are:

- A supported browser - Chrome, Firefox, Internet Explorer and Safari
- A network connection to the Internet and/or corporate network (fixed line or wireless)
- The address (URL) for WSFM at your site

Administrators will provide the address (URL) for WSFM or place an icon on the desktop.

Starting

From your browser

To start WSFM from your browser:

1.	Open the browser.
2.	Type the address (URL) into the location bar and press the Enter key or the Go icon.
3.	Wait for WSFM to display the Access log on page and then follow the log on instructions.

From a desktop shortcut

You or your administrator can set up a shortcut to open the browser and go to the address for WSFM immediately.

To start WSFM from a shortcut:

1.	Click on the shortcut (or open the shortcut) - the browser will start and connect to WSFM.
2.	Wait for WSFM to display the Access log on page and then follow the log on instructions.

To set up the desktop shortcut for Internet Explorer, create a new shortcut, open the properties and insert the equivalent of the following as the target property:

"C:\Program Files\Internet Explorer\iexplore.exe" www.myWSFM-URL.com

To set up the desktop shortcut for Firefox, create a new shortcut, open the properties and insert the equivalent of the following as the target property:

"C:\Program Files\Mozilla Firefox\firefox.exe" www.myWSFM-URL.com

The URL http://www.myWSFM-URL.com:80/axes/spooled-file-manager.html is an example of the actual URL for WSFM at your site. This example uses port 80 and the default page for WSFM.

Content © LANSA Group
All Rights Reserved

Log on

When WSFM starts, the browser will show the Access log on page and display the Access dialogue window.

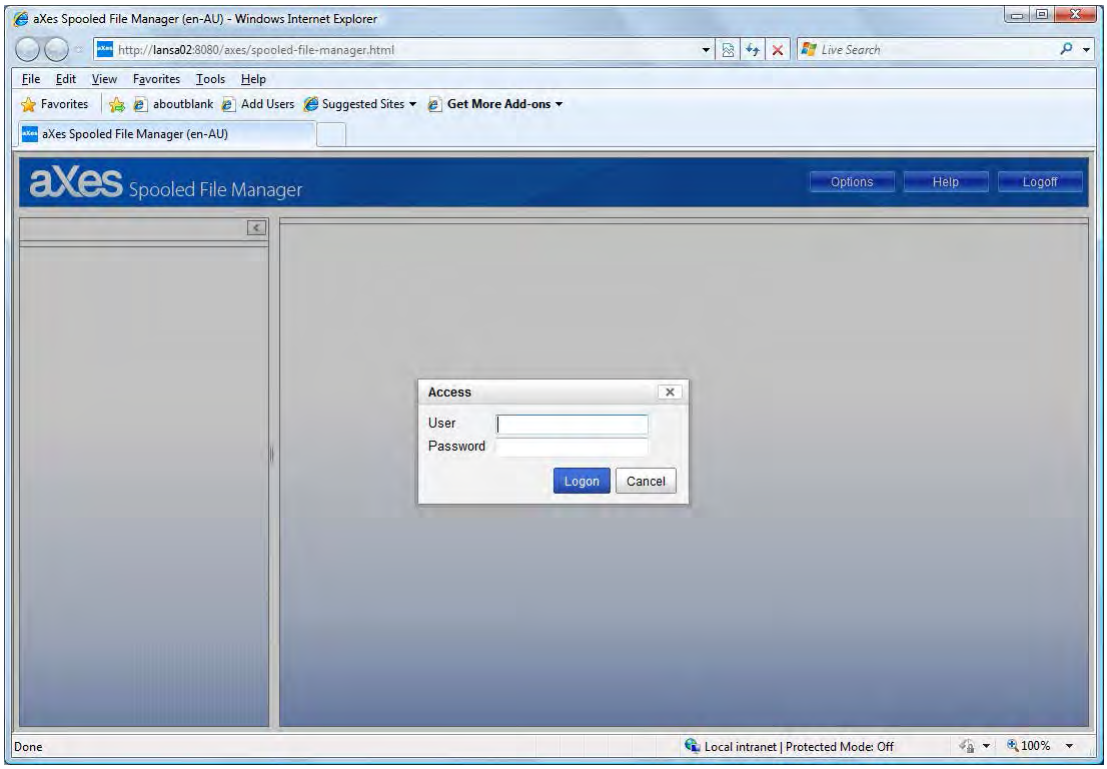

Figure 4: Access Logon Page

Your user identification and password

To log on to WSFM you must provide your user identification and password (credentials):

1.	Type your user identification.
2.	Type your password.
3.	Press the Logon button
4.	Wait while WSFM verifies your credentials. If your log on is successful, WSFM will display the next page. If your log on is unsuccessful, WSFM will display an error message.

What to do if log on fails

Log on will fail if you make a mistake typing the user identification and/or the password. Check you have the correct user identification and re-type the password.

If you forget your user identification and/or password contact your administrator.

If you do not know your user identification and/or password contact your administrator.

Cancel WSFM without logging on

To cancel WSFM without logging on click the Cancel button and wait while WSFM closes the browser.

Content © LANSA Group
All Rights Reserved

Section 2 - Administration

This section provides conceptual information about WSFM that will help administrators manage WSFM effectively.

Architecture

Components and structure

Figure 5 (page 13) illustrates the architecture of WSFM and highlights the primary components.

WSFM is a Web application consisting of server components and a user interface presented in a browser. The user interface is a browser page consisting of HTML, CSS and JavaScript. No components of WSFM reside on the computer running the browser.

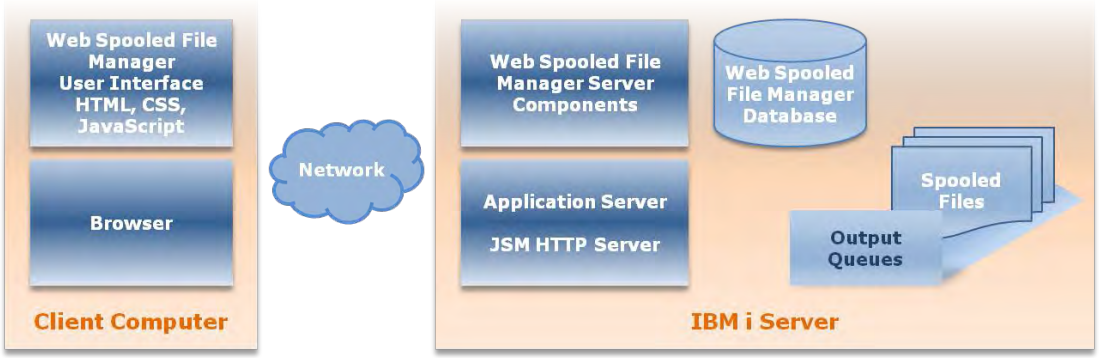

Figure 5: Web Spooled File Manager Architecture and Components

The server components are the application server (JSM HTTP Server) and WSFM itself running on the application server. WSFM operates a database for its data management.

Users connect to output queues and spooled files from their browser via WSFM. They search for output queues, search for spooled files and request spooled files to view. WSFM initiates the searches, marshals search results, retrieves spooled files and sends the data to the browser.

WSFM database

WSFM uses its database to store registered users, the folders they create and the filters or searches they build. The WSFM database comprises the tables listed in Table 1 (page 13).

Table 1: WSFM Database - SQL Tables

Names	Properties	Purpose
SFMUSER	*FILE PF-DTA	User tables contain details about registered users
SFMFOLDER	*FILE PF-DTA	Folder tables describe folders created by users
SFMFILTER	*FILE PF-DTA	Filter tables describe the filters (searches) created by users

WSFM creates and manages these files.

The configuration file defines the location (or library) where the files reside.

Content © LANSA Group
All Rights Reserved

Important reminders	Backup the WSFM database regularly. Backup the WSFM database before you uninstall and reinstall. Backup the WSFM database before you perform an upgrade.

Administrator responsibilities

Administrators are responsible for:

- Installing WSFM on the server
- Configuring WSFM server components
- Managing users
- Ensuring regular backups occur

Installation and configuration are once only or occasional tasks. Housekeeping is an ongoing task. Troubleshooting is an occasional task.

Managing users is an ongoing task. Administrators are responsible for notifying users of the WSFM log on page URL. In cases where users operate with a managed desktop, administrators will need to add a short cut to the desktop for users to start WSFM.

Before you start

This section describes issues you need to think through and decisions you must take before installing and configuring WSFM.

Prerequisites

The prerequisites for WSFM are:

- Installation media
- Licences

The prerequisite software from IBM is:

- iOS version 5, release 3 or later
- IBM Java JDK 1.4 (or greater)
- IBM host server daemons must be running to accept IBM Toolbox for Java connections
- IBM Toolbox for Java (the JAR file jt400.jar is shipped with WSFM)

Install the prerequisite software from IBM before installing WSFM.

Important reminder	WSFM will not operate successfully without the prerequisite software.

Decisions you need to make

Port number

Select the port or ports the JSM HTTP server will use for WSFM.

The default ports are 5563 or 5564 when using TLS/SSL.

Register users

Choose a method for registering users. The choice you make will determine the pre-installation work you will need to do. If you choose to load users as a batch task, you must assemble the user details and write SQL and/or programs to load the user details into the user table. If you choose automatic registration, the only work necessary is setting a parameter value in the configuration file.

Content © LANSA Group
All Rights Reserved

Read the section of this guide that describes user registration concepts ("Register users", page 16). The configuration section explains how to enable and disable automatic registration.

Installation and configuration process

The steps in the installation and configuration process are:

1.	Read the documentation. Read this guide and familiarise yourself with the WSFM User Guide.
2.	Install the prerequisite software on the server
3.	Install WSFM on the server
4.	Apply licences
5.	Configure the JSM HTTP server
6.	Configure WSFM
7.	Register users

You will reduce your workload if you are familiar with the options for configuration and registering users before you start.

Install server components

New installations

WSFM ships as part of aXes and installing aXes also installs WSFM. Refer to the aXes administration documentation to understand the installation procedures for WSFM.

During installation, WSFM copies the template configuration file named httpd-template.xml to an instance configuration named httpd.xml. This file contains default configuration settings. Once the installation is complete, WSFM requires no further installation or configuration tasks.

You can amend the instance configuration if necessary. Before amending the instance configuration, make a backup of the httpd.xml file.

Upgrades

During upgrades WSFM will add components, amend installed components and remove deprecated components. Upgrades will replace the existing copy of the configuration file named httpd-template.xml. Therefore, it is essential that you copy and backup configuration files before changing configuration items and before installing upgrades.

Upgrades will not replace the existing httpd.xml configuration file. However, upgrades may require changes to individual configuration items in the file.

Licences

Licence arrangements determine your use of WSFM.

To use WSFM your licence arrangements must include session and/or processor licences for WSFM.

Applying licences is part of the aXes installation process.

Content © LANSA Group
All Rights Reserved

Related products

Data Explorer (DE) may be installed beside Web Spooled File Manager (WSFM) and share its configuration with WSFM.

The section of this guide titled, "Running WSFM and DE side by side", (page 59) explains the options for configuring WSFM and DE together.

Register users

Why register users?

People using WSFM have access to corporate information in spooled files. Corporate best practice suggests that companies ought to know and control who accesses corporate data.

Ensure that only registered users can use WSFM to access output queues and spooled files. Each person who uses WSFM needs identifying credentials (unique user name and password). Shared or generic user identifications will compromise the ability to determine who accesses the information.

What is registration?

Users need an active IBM i user profile to register for WSFM.

WSFM includes a configuration parameter for user registration that determines how WSFM will behave when a user logs on. The parameter allows two behaviours:

- Register users manually
- Register users automatically

With WSFM configured for manual registration, everyone who logs on must already be known to WSFM. Manual registration means that an administrator must add each authorised user to the list of registered users before the person can use WSFM.

With WSFM configured to allow automatic registration, any person who logs on with an active IBM i user profile and is unknown to WSFM will be added as a registered user.

How to register users manually

To register a user to use WSFM you insert a record in the table SFMUSER.

There are several options for registering user manually:

- Use SQL to add a user
- Write a program to add a user
- Load multiple users as a batch job (using SQL and/or programs)

Using an appropriate CCSID is essential when registering users manually. WSFM's database is DBCS, uses uses a graphic field (CCSID 1200), and data in the tables includes square brackets [ ] and braces { }, also known as curly brackets. Use CCSID 37 as the job CCSID to ensure correct character conversions. This recommendation applies to all methods that register users manually, both interactive SQL and programmatic updates. Using other CCSIDs may produce incorrect conversions, two examples are CCSID 37 and CCSID 500:

CCSID 37 produces correct data: {"startupfilterid":0,"recent":[15],"showwelcome":true}

CCSID 500 produces incorrect data: {"startupfilterid":0,"recent":¢15!,"showwelcome":true}

The data created using CCSID 500 interprets the square brackets incorrectly, [becomes ¢ and] becomes !. CCSID 37 produces the correct result.

The command to set CCSID 37 for a job is: CHGJOB CCSID(37)

Use SQL to register users

You can add a registered user by running the following SQL:

```
INSERT INTO [Library]/SFMUSER (PROFILE,OPTIONS)
VALUES('USER','{"startupfilterid":0,"showwelcome":true}')
```

Where **[Library]** is the name of the library in which the table resides (typically, the library name is AXES).

Where **USER** is the user profile name in uppercase.

To use this SQL the CCSID for the job must not be 65535. Use the CHGJOB command to change the CCSID.

The user profile must be an active user profile for the IBM i server.

Before loading a new user, check SFMUSER to ensure that the user is not already loaded.

Write a program to register users

To automate user registration, write a program that accepts the user profile and inserts the user into the SFMUSER table. The program may use the SQL above to insert the user.

Register multiple users as a batch job

To load multiple users as a batch job, create a text file containing all users. Then load the users into the SFMUSER table using SQL or write a program to load the users into the table from the text file.

How to register users automatically

WSFM will register users when they log on, if configured to allow automatic registration.

Registering a large number of users will be a significant effort for administrators. One way to reduce this effort is to allow automatic registration for a short period after installation. As users log on WSFM will register their user identification. At the end of a short automatic registration period, change the registration parameter to manual. This approach will allow people to register automatically and reduce the administrative effort needed to register users.

How to remove registered users

Remove a registered user by deleting the user from the WSFM database. That is, delete the user from the filter table (SFMFILTER), the folder table (SFMFOLDER) and finally the user table (SFMUSER). Deleting the user from the user table but not the other tables will leave folders and filters without a related user.

You can delete the rows manually, write SQL or write a program.

The steps in the removal process are:

1.	Determine the identification associated with the user. Run a SELECT query with a WHERE clause user profile is "user profile".
2.	Delete rows in the filter table using the identification.
3.	Delete rows in the folder table using the identification.
4.	Delete rows in the user table using the identification.

An automated removal process (using SQL or a program) will follow the same process.

User identifications beginning with the letter Q

WSFM prohibits users logging on with a user identification that begins with the letter Q.

If you wish to override this policy and allow the use of these user identifications, you must configure a parameter for each user identification you wish to allow.

Content © LANSA Group
All Rights Reserved

Fonts

Fonts control the rendering of spooled files when viewed in the available formats. Using fonts that are appropriate for your circumstances will ensure the optimum rendering of spooled files. WSFM provides three layers of font support:

- Internal fonts
- Optional IBM fonts
- Third part fonts

The internal fonts are the default choice for WSFM when displaying the content of spooled files. No other fonts are necessary provided that the internal fonts are adequate for your needs. However, if the internal fonts do not cater for your situation, install the optional IBM fonts and/or third party fonts.

Internal fonts

WSFM uses the internal fonts as the default and other fonts when they are available.

Table 2: Internal Fonts

Font Title	Description
COURIER	Cp1252, mono spaced
COURIER2	Cp1250, mono spaced
COURIER3	Cp1257, mono spaced
COURIER4	User defined true type font, mono spaced
MINCHO	Japanese HeiseiMin-W3
GOTHIC	Japanese HeiseiKakuGo-W5

WSFM includes these fonts at installation.

Constraints

Table 3 (page 18) presents constraints and dependencies related to fonts and languages. For example, WSFM uses internal or IBM fonts when displaying the content of a spooled file as a PDF, but WSFM depends on the browser when displaying the content of a spooled file as HTML and text.

Table 3: Font Constraints in WSFM

Context	Constraint Explanations
IBM iSeries Language CCSIDs	WSFM supports all.
View spooled files as PDF	WSFM depends on the installed IBM fonts.
View spooled files as PDF image	WSFM depends on the installed IBM fonts.
View spooled files as HTML	WSFM depends on font support in the browser to render Unicode HTML. WSFM does not use the installed IBM fonts.
View spooled files as text	WSFM depends on font support in the browser to render Unicode text. WSFM does not use the installed IBM fonts.

Content © LANSA Group
All Rights Reserved

Context	Constraint Explanations
IBM Host Print Transform (HPT)	WSFM depends on the capability of the IBM Java Toolbox and iSeries Host Print Transform services when you choose HPT as the encoding.
Traditional Chinese and Simplified Chinese on the same machine, displaying spooled files using IBM Host Print Transform (HPT) as the host encoding.	WSFM cannot use HPT encoding to display spooled files as HTML, PDF, PDF image or text when Traditional Chinese and Simplified Chinese are installed on the same machine. The IBM Host Print Transform imposes this limitation. To display Simplified Chinese the machine system value QCCSID must be 1388. To display Traditional Chinese the machine system value QCCSID must be 937.
Traditional Chinese and Simplified Chinese on the same machine, displaying spooled files using Copy Stream File (CSF) as the host encoding.	WSFM can display spooled files as HTML, PDF, PDF image or text when Traditional Chinese and Simplified Chinese are installed on the same machine by using the CSF as the host encoding
You need these fonts to view spooled files as a PDF image for DBCS code pages.	5769-FN1 Advanced Function Printing DBCS Fonts for AS/400: Option 1 - Japanese Option 2 - Korean Option 3 - Traditional Chinese Option 4 - Simplified Chinese Option 5 - Thai
You need these fonts to view spooled files as a PDF for SBCS and DBCS code pages.	5761SS1 i5/OS: Option 43 - Additional Fonts
You need these fonts to view spooled files as a PDF image for Latin code pages.	5761SS1 i5/OS: Option 8 - AFP Compatibility Fonts

Using HPT and CSF as the host encoding with Font Name as AUTO allows WSFM to determine the encoding and font automatically.

Optional IBM fonts

If you need additional fonts, obtain and install the optional IBM fonts.

Installing iSeries Licensed program, 5761SS1 i5/OS, Option 43 Additional Fonts, will load the font files into this directory in the IFS, /QIBM/ProdData/OS400/Fonts/TTFonts.

Table 4: Optional IBM font products

Licensed Program	Install Options
5761SS1 i5/OS	Option 8 - AFP Compatibility Fonts Option 43 - Additional Fonts

Content © LANSA Group
All Rights Reserved

Licensed Program	Install Options
5769-FN1 Advanced Function Printing DBCS Fonts for AS/400	Option 1 - Japanese Option 2 - Korean Option 3 - Traditional Chinese Option 4 - Simplified Chinese Option 5 - Thai

The fonts you need depend on language support requirements. For example if Japanese is the only language you need, it is unnecessary to install Korean, Chinese or Thai.

WSFM has built-in font support for Latin COURIER, Japanese MINCHO and GOTHIC.

Table 5: IBM iSeries Font Products

IBM iSeries Font Products
IBM Advanced Function Printing DBCS Fonts for AS/400 (Program 5769-FN1)
IBM Advanced Function Printing(TM) Fonts for AS/400(R) (Program 5769-FNT)
IBM AFP Font Collection for Workstations and OS/400(R) (Program 5648-B45)
IBM Infoprint Fonts for Multiplatforms (Program 5648-E77)

Third party fonts

If you prefer to use fonts supplied by a third party, you need to obtain and install the font files.

Table 6: Microsoft Fonts

Font		File Name
Simplified Chinese	SIMSUN	simsun.ttc
Traditional Chinese	DFKKAISB	kaiu.ttf
Traditional Chinese and HKSCS	MINGLIU	mingliu.ttc
Korean	BATANG	batang.ttc
European	COURIER NEW	cour.ttf

To use the Microsoft fonts, install the Microsoft/Ascender Fonts True Type Font files in the WSFM system folder (axes/jsm/instance/system/).

These fonts ship with Windows and reside in the \windows\fonts folder.

Use the DOS command mode to locate and copy these files to the c:\temp folder. Then use Windows Explorer to copy the files to the WSFM system folder in the IFS.

Fonts and server memory usage

When font files load they use server memory. A font file will load for every generation of a spooled file as PDF. If three users generate a spooled file as PDF concurrently, the font files will reside in memory three times. Eventually, you may run out of server memory.

Latin fonts use less memory than Asian fonts.

Content © LANSA Group
All Rights Reserved

Documentation

The documentation consists of a collection of documents formatted as PDF (Adobe Portable Document Format).

Administrator and user guides

Table 7 (page 21) lists the documentation available for WSFM and explains the purpose of each document.

Table 7: Documentation: Administrator and User Guides

Document	Purpose
Administrator Guide	The Administrator Guide explains how to configure WSFM and to manage access to services by people using WSFM. This guide is intended for use by administrators. The Administrator Guide is this document.
Pocket Guide	The Pocket Guide is a condensed version of the User Guide. This guide is a quick reference for WSFM users who run searches view spooled files more often than prepare spooled file filters or queue filters.
Questions and Answers	The Questions and Answers document the questions and answers sections from the User Guide. This guide is intended for use by any person who wants a quick answer to a question about WSFM.
User Guide	The User Guide provides conceptual information about WSFM and explains how to use WSFM to search for output queues, search for spooled files and view the content of spooled files. This guide is mandatory reading if you want to understand how to make the best use of WSFM. The guide is intended for use by people preparing and running searches with spooled file filters and queue filters. Administrators should familiarise themselves with this guide when they provide service desk assistance to WSFM users. This is the most extensive of the documents.

The User Guide is essential reading for users who want to create searches.

Administrators who provide advice to users need to be familiar with the content of all the documentation.

Portfolios

A portfolio is a collection of documents. The documentation is packaged in two portfolios. The portfolios are the administrator portfolio and the user portfolio.

Table 8 (page 21) shows the content of the administrator portfolio.

Table 8: Documentation: Administrator Portfolio

Documents
Administrator Guide
Pocket Guide
Questions and Answers

Content © LANSA Group
All Rights Reserved

Documents
User Guide

Table 9 (page 22) shows the content of the user portfolio.

Table 9: Documentation: User Portfolio

Documents
Pocket Guide
Questions and Answers
User Guide

The user portfolio is accessible from the Help button at the top of the WSFM page.

Content © LANSA Group
All Rights Reserved

Section 3 – Housekeeping and troubleshooting

This section describes how to perform housekeeping tasks, track down problems and contact support.

Logging

This section explains administrator tasks for managing access log files and error log files. These files accumulate with use and administrators should archive and/or clear the files periodically.

Log files: names and locations

In a typical installation log files reside in a logging folder.

Location	axes/jsm/instance/www/instance/logs/
Log File Names	error.log access.log

Examining the content of these files will reveal information about activity and errors.

Enable and disable logging

The errorlog and accesslog directives in the configuration file control logging activity.

To enable logging for both error and access logs, set the value of the enabled parameter as true:

```
<errorlog enabled="true" file="www/instance/logs/error.log"/>
<accesslog enabled="true" file="www/instance/logs/access.log"/>
```

To disable logging for both error and access logs, set the value of the enabled parameter as false:

```
<errorlog enabled="false" file="www/instance/logs/error.log"/>
<accesslog enabled="false" file="www/instance/logs/access.log"/>
```

Error and access logs operate independently. For example you can enable error logging and disable access logging.

Archive log files

Archive log files by copying them to another location.

WSFM provides no archiving tools.

Delete log files

Do not delete the active error.log and access.log files.

WSFM will archive the active log files periodically. Before deleting the archived log files, ensure you either have a backup or archive copy of the files.

Content © LANSA Group
All Rights Reserved

Tracing

This section explains the administrator tasks for collecting data to assist with tracking errors. Administrators need to enable and disable tracing services and clear trace files when they are no longer needed.

Tracing allows you to collect information about the activity of WSFM. When enabled, tracing directs STDOUT and STDERR to the trace files STDOUT.TXT and STDERR.TXT.

The Java Virtual Machine and instance information is logged to a MANAGER.TXT file.

Trace files: names and locations

In a typical installation trace files reside in two folders.

The first location provides high level trace information.

Location	axes/jsm/instance/trace/[job number]/
Log File Names	CLASSPATH.TXT MANAGER.TXT STDERR.TXT STDOUT.TXT
Sample	axes/jsm/instance/trace/189002/STDOUT.TXT

Where [job number] is the job number of the active job when tracing occurred.

The second location provides detailed trace information.

Location	axes/jsm/instance/trace/[job number]/[date]/
Log File Directory Names	HTTP00000000 HTTP00000001 HTTP00000002 HTTP00000003
Sample	axes/jsm/instance/trace/309001/2009-11-24/HTTP00000004

Enable and disable tracing

The trace and clienttrace directives in the configuration file control tracing activity. These directives are in the virtual host section of and are associated with services.

To enable tracing for a service, set the value of the trace and/or clienttrace parameter as true:

```
trace="true" clienttrace="true"
```

To disable tracing for a service, set the value of the trace and/or clienttrace parameter as false:

```
trace="false" clienttrace="false"
```

Tracing directives operate independently. For example you can enable tracing for one service or all services.

Content © LANSA Group
All Rights Reserved

Clear trace files

Use the command CLRJSM command to clear trace files and subdirectories. The command has the following parameters:

INSTANCE	The instance defaults to a value of *DEFAULT. This is the recommended value.
TRACEDIR	The option defaults to a value of *YES. Valid values are *YES, *NO. The value *YES removes files and sub-directories in the trace directory.
TEMPDIR	The option defaults to a value of *YES. Valid values are *YES, *NO. The value *YES removes all files and sub-directories in the TEMP directory. Do not clear the TEMP directory while JSM services are running, as this action will delete temporary files used by the services. Always use *NO when clearing trace files from a running JSM instance.
KEEP	Valid values are in the range 0 to 99 days. Zero means do not keep the files. Running the command will delete ALL files and sub-directories. Use 1 to keep only today's files. Use 2 to keep today's and yesterday's files.

Archive trace files

Archive trace files by copying them to another location, before clearing the files.

WSFM provides no archiving tools.

Certificate management

Use the Java keytool command to create a private key and certificate suitable for the TLS/SSL server credentials.

```
%JDKPATH%\bin\keytool  -genkey —alias sslkey —keyalg RSA —keysize 1024
                       -sigalg SHA1withRSA
                       -keypass password —keystore wwwssl.jks
                       -storepass password —validity 365
                       -dname "CN=Web Applications,OU=Web Services,O=My
                       Company,L=My Location,S=My State,C=US"
```

Substitute your equivalent values for My Company, My Location, My State and C (country).

Troubleshooting

The troubleshooting section suggests the parts of WSFM to check when it does not operate as expected.

Installation and configuration

JSM HTTP server does not start

1.	Check the manager.properties httpd directive: httpd=system/httpd.xml Ensure that the name specified for the httpd configuration file is the name of the actual httpd configuration file.
2.	Check the JSM trace file MANAGER.TXT for JSM HTTP server start up messages.
3.	Review the configuration directives in the instance tag.
4.	Confirm that the JSM HTTP server is started by using a browser to access the home index.html file.

Ensure that the configuration is complete before attempting the start the JSM HTTP server.

IBM Toolbox for Java not installed

1.	Ensure that the IBM Toolbox for Java is installed. Verify that the file, "jt400.jar", resides in the JSM jar directory.

Installing the IBM Toolbox for Java is an essential prerequisite for operating WSFM.

File ownership and permissions for files in the IFS

1.	The JSM HTTP server by default runs as the JSM job description user profile. Any files and directories created should be owned by that user profile.
2.	Verify the user profile, file and directory ownership.
3.	Change ownerships if necessary.

WSFM database not found

1.	WSFM uses tables to store its information. The tables must exist in the library specified in the database.library directive.
2.	Verify that the tables are in the library defined in the database.library directive. SFMUSER (PF-DTA) SFMUSER1 (LF) SFMUSER2 (LF) SFMFOLDER (PF-DTA) SFMFOLDER1 (LF) SFMFILTER (PF-DTA) SFMFILTER1 (LF) SFMFILTER2 (LF)
3.	Change the database.library directive to the library where the files reside. Or, move the files to the library defined in the database.library directive.

Content © LANSA Group
All Rights Reserved

Problems when running spool filters and queue filters

Users encounter errors when running a spooled file filter.

1.	Check the library and output queue names are correct.
2.	Check whether the use is authorised to use the output queue. Users must have read access to output queues to use them in searches.

Problems viewing the content of spooled files

Users cannot view the content of spooled files as PDF or PDF image.

1.	Ensure that the user has Adobe Acrobat Reader installed or has access to a network version of Adobe Acrobat Reader.
2.	If Adobe Acrobat Reader is not installed, the user needs to install the reader or be granted access to a network version of the reader.
3.	Ensure that Adobe Acrobat Reader is at version 5.0 or higher. The most recent version is the preferred version.

When spooled files do not display correctly when viewed as PDF in Chrome, install the Google Chrome PDF plugin.

When spooled files do not display correctly when viewed as PDF in Firefox, the Firefox configuration must be set to allow PDFs to open. You must configure Firefox so that the content type Adobe PDF Document has the action "Use Adobe Acrobat (in Firefox)".

1.	If the spooled file uses Advanced Function Printing (AFP), view it with the PDF image option. HTML, PDF and text options will not display spooled files that use AFP.
2.	If the spooled file contains graphics, view it with the PDF image option.

Browser response is slow or unresponsive

The spooled file display appears slow and unresponsive.

1.	Browsers expect fast responses from HTML pages and want to exit from long running requests. The reason for this behaviour is to minimise the wait time. When pages appear to wait for some time the browser will ask users if they wish to cancel the request. Each browser behaves differently.
2.	IE displays a blank page. IE displays a blank page (or white window) when it waits for long running requests. Wait until IE re-displays the page or close the browser.
3.	When JavaScript is doing a lot of processing, the browser may assume the page is in a loop and prompt the user to end the JavaScript execution. Users may continue JavaScript execution, end JavaScript execution or close the browser.
4.	Cancelling the request and/or closing the browser will end the WSFM session. Users will have to log on again. Cancelling a request or closing the browser has no effect on spooled files.

Content © LANSA Group
All Rights Reserved

Browsers allow you to configure the action to take for long running JavaScript. Firefox has a configuration item named "dom.max_script_run_time". Safari allows you to disable the Runaway JavaScript Timer.

The performance of IBM i servers influences long running requests. When a server is slow to respond, configuring the browser to ignore or wait for long running requests will have no effect.

Creating PDFs becomes slower and slower

Loading font files when generating a PDF requires server memory. The higher the number of users that initiate PDF generation concurrently, the more times the font files will load and as a consequence memory requirements will rise. PDF generation will become slower and slower as more and more memory is used.

Managing errors

SSL related errors

Error	javax.net.ssl.SSLException: The certificate container *SYSTEM could not be accessed.
Cause	WSFM does not have authority to access certificates.
Action	Change the object authority by issuing the following commands: CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(AXES) DTAAUT(*RX) CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(AXES) DTAAUT(*R) CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.RDB') USER(AXES) DTAAUT(*R)

Error	javax.net.ssl.SSLException: Validity time period of the certificate is expired.
Cause	The default container certificate is out-of-date.
Action	Obtain a new certificate.

Browser errors

Error	Firefox does not close automatically when you logoff and exit.
Cause	The configuration item, dom.allow_scripts_to_close_windows is set as false.
Action	Change the setting for dom.allow_scripts_to_close_windows to true. This change is not mandatory for WSFM. It is a user preference. The alternative action is to exit WSFM and then close Firefox manually.

Content © LANSA Group
All Rights Reserved

Before you contact aXes support

Table 10 (page 29) contains the information you need to send to support if you experience problems.

Table 10: Information to Send to Support

Context	Information
Contact and customer details	Your company name Your name Customer name
aXes version(s)	What version of aXes being is being reported? What aXes PTFs installed and applied to this version? Are other versions of aXes also installed on the same IBM i? Is Terminal Server (TS) installed? Is the Web Spooler (WS) installed? Is the Intersession Option installed as well? Has another version of aXes been successfully deployed on the same IBM i? (If so, please provide details). How is aXes licensed — processor or session based? If processor based, how many processors are licensed? If session based, how many sessions are licensed?
IBM hardware	Model number (QMODEL) Serial number (QSRLNBR) Processor Feature Number (QPRCFEAT) Processor Group (Tier) Is aXes running in an LPAR? If yes, how many processors are allocated to that LPAR?
IBM operating system software	What operating system version is running aXes? (Version, Release and Modification) What operating system version of the IBM i Licensed Internal Code (LIC) is installed? What IBM operating system PTFs have been installed? Are the latest PTFs applied?
Problem report	Provide a detailed description of the problem. Include a full history of events leading up to the occurrence of the problem. For example, did the problem occur after you installed new software, applied PTFs or upgraded the operating system? The more detailed the information, the easier it is for Support to understand your problem.

Content © LANSA Group
All Rights Reserved

Section 4 — Configuration

This section explains the tools and configuration options available to administrators who will manage WSFM.

The configuration process

The steps in the configuration process are:

1.	Copy and rename the configuration file, httpd-template.xml. The recommended name for the copied file is: system/httpd.xml You can use any valid name but you should choose a name that indicates the file content.
2.	Change the httpd property in the manager.properties file to the new name allocated when you copied the original httpd configuration file. For example, if you used the recommended name for the copied httpd configuration file, change the httpd property in manager.properties to: httpd=system/httpd.xml If not, use the name allocated to the copied file.
3.	Configure axinfo.json
4.	Configure the JSM HTTP server instance.
5.	Configure the services (for example database drivers).
6.	Configure the user registration properties.

The configuration process assumes you have completed the installation successfully.

Important reminders	Always make a copy of the httpd configuration file before you edit its contents. Keep a separate copy of the httpd configuration file that is active in your production environment.

Use a text editor or XML editor when changing configuration items and parameters in the httpd configuration file. Exercise care when editing and make sure you do not change tag names.

About the configuration files

The configuration details reside in three files: manager.properties, httpd.xml and axinfo.json. This section describes the content of the configuration files. Later sections describe how to change individual configuration items.

File locations

Table 11 (page 30) provides the folder locations of the configuration files.

Table 11: Configuration File Locations

Configuration Files	Locations
axinfo.json	myaxes/jsm/

Configuration Files	Locations
httpd.xml	myaxes/jsm/instance/system/
httpd-template.xml	myaxes/jsm/instance/system/
manager.properties	myaxes/jsm/instance/system/

The root folder (myaxes) in the location is the folder name chosen on installation.

Manager.properties file

The properties file, manager.properties, contains information about the installed instance of WSFM. Table 12 (page 31) explains the properties manager.properties.

Table 12: Explanation of manager.properties

Properties	Definitions
httpd=system/httpd.xml	Name of the httpd configuration file
httpd.axes.release=V2R1M0	Version of aXes installed (used for licence checking)
httpd.axes.instance=AXES	Name of the instance (used for licence checking)

After updating the httpd configuration file property in manager.properties, the configuration file will look like the following example (Table 13, page 31).

Table 13: Example of an Updated manager.properties File

Properties

# httpd=system/httpd-template.xml 	
httpd=system/httpd.xml
httpd.axes.release=V2R1M0
httpd.axes.instance=AXES
#
tcp.port=5560
console.tcp.port=5561
studio.client.address=*none
console.client.address=*none

The line beginning with a hash (#) is a comment line.

The name of the instance (httpd.axes.instance=AXES) in manager.properties does not need to be the same as the instance name in the httpd configuration file.

Httpd configuration file

The configuration file named httpd.xml contains the configuration items and parameters for WSFM.

Table 14: Structure of the httpd Configuration File

Structure of httpd Configuration File
<?xml version="1.0" encoding="UTF-8"?> <configuration>   <instance name="WebServer" active="true" root="www/instance/htdocs"

Structure of httpd Configuration File

```
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256"
            buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        +<virtual host="*" active="true">
    </instance>
</configuration>
```

Table 14 (page 31) shows the structure of the httpd configuration file.

The configuration contains an instance of the JSM HTTP server. The instance has a set of configuration parameters (instance, errorlog, accesslog and listen tags). The instance includes configuration items for access, MIME types (Internet Media Types) and virtual hosts.

Table 15 (page 32) provides a list of recommendations for changing configuration items and parameters in the httpd configuration file.

Table 15: Mandatory and Optional Changes to Configuration Items and Parameters

Configuration Items	Change Mandatory/Optional
JSMHTTPServiceFile (match URI, class)	Do not change these items
MIME types (server instance)	Optional, but not recommended
MIME types (virtual host)	Optional, but not recommended
Port	You must choose port numbers, if you do not wish to use the default port numbers
Realm (protect tag, virtual host)	Do not change any items in the protect tag
Virtual host name and active	Do not change these items unless you choose multiple instances and/or multiple virtual hosts

The default values of many configuration items and parameters in the httpd configuration will be appropriate for operating WSFM. Some values you must change and some are optional.

Important reminders	Copy the original httpd configuration file. Do not use the original httpd configuration file for your configuration settings. Version upgrades and fixes may alter the parameters in the httpd configuration file and will over-write your configuration settings when installed.

Axinfo configuration file

The axinfo configuration file defines whether WSFM is enabled, the ports and URI for the WSFM service.

Table 16: axinfo.json Configuration File for WSFM

axinfo.json Configuration Example

`{`
`  "sfm":`
`  {`
`  "enabled": true,`
`  "port": 5563,`
`  "sslport": 5564,`
`  "uri": "/axes/spooled-file-manager.html"`
`  }`
`}`

Table 17 (page 33) explains the items in axinfo.json.

Table 17: Configuration Items in axinfo.json

Configuration Items	Definitions
Enabled	"enabled":true indicates that WSFM is active "enabled":false indicates that WSFM is inactive (that is, the service is unavailable)
Ports	Port = the non SSL port (not encrypted) SSLPort = the SSL port (encrypted)

Configure ports

The axinfo and httpd configuration files contain items to define the ports WSFM will use. Table 18 (page 33) shows the default ports.

Table 18: Default Ports

Port Numbers	Definitions
5560	JSM Server TCP port is used internally and does not accept connections.
5561	JSM Console TCP port is used internally and does not accept connections.
5563	JSM HTTP Server (default port for WSFM without TLS/SSL)
5564	JSM HTTPS Server (default port for WSFM with TLS/SSL)

Content © LANSA Group
All Rights Reserved

To change ports follow these steps:

1.	Edit axinfo.json.
2.	Change the port parameter. Change the sslport parameter.
3.	Save axinfo.json
4.	Edit httpd.xml (or the equivalent file if you use a different name).
5.	Under the listen tag of the instance: Change the port parameter. Change the sslport parameter.
6.	Save httpd.xml

The configuration files shipped with WSFM are configured to use the default ports. You do not need to change the port configurations if the default ports are suitable for your installation.

Configure JSM HTTP server

This part of the administrator guide explains how to configure the sections of the httpd configuration file that apply to the JSM HTTP server. There are separate sections that explain how to configure individual services that the JSM HTTP server supports.

Server instance configuration

Table 19 (page 34) shows the set of configuration items and parameters that apply to the JSM HTTP server instance.

Table 19: Configure Server Instance

Configure Server Instance Example
<?xml version="1.0" encoding="UTF-8"?> <configuration>
<instance name="WebServer" active="true" root="www/instance/htdocs" **index="index.html">** **<errorlog enabled="true" file="www/instance/logs/error.log"/>** **<accesslog enabled="true" file="www/instance/logs/access.log"/>** **<listen secure="false" store="pki/wwwssl.jks" password="password"** **port="5563"** **sslport="5564"** **interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"** **nodelay="false" timeout="5"/>**
+<access> +<mimetype> +<virtual host="*" active="true">**</instance>** </configuration>

In this example, the instance of WSFM has error logging and access logging enabled (the value of the parameter is "true"). The server will place errors into error.log and access events into access.log. The instance will listen on port "5563".

Table 20: What to Configure for the Server Instance

To configure	Apply these settings	Change default
Access logging	Set accesslog enabled to true. Define the access log file name.	Optional
Active	Active must be true	Do not change
Backlog	Choose the depth of the TCP/IP queue.	Optional
Buffer receive	Set the size (bytes) of the receive buffer	Optional
Buffer send	Set the size (bytes) of the send buffer	Optional
Error logging	Set errorlog enabled to true. Define the error log file name.	Optional
Index	Define the index document	Optional
Instance name	Choose a name	Optional
Interface	Use *ALL for all addresses or choose the interface address. Default is all interfaces.	Optional
No delay	Set to True to enable TCP/IP no delay. False uses the operating system settings.	Optional
No TSL/SSL	Set listen secure to false. When listen secure is false, the JSM HTTP server ignores store and password values.	Optional
Port	Insert the port number you want to use.	Mandatory The server expects either port and/or sslport.
Root	Define the root directory (folder)	Optional
Secure connection with TSL/SSL	Set listen secure to true. Define the name of the store. Insert the password.	Optional
SSLport	Insert the port number you want to use.	Mandatory The server expects either port and/or sslport.
Timeout	Set the connection timeout in seconds.	Optional

Whether you need to change the optional items depends on the environment of your WSFM installation and your performance requirements.

Controlling access to the server instance

The access directive (at the instance level) specifies rules for accessing the instance of the JSM HTTP server. Using the access directive you can:

- Allow addresses
- Deny addresses

You use combinations of allow and deny directives to control access to the server instance. Addresses can be specific (10.2.45.1), masks (10.2) or generic (indicated by the asterisk (*)).

Do not use directives for user agents or content lengths in this section.

Table 21 (page 36) shows an example of allow and deny directives (at the instance level).

Table 21: Control Access to the Server Instance

Server Instance Access (Allow and Deny) Configuration Example
<?xml version="1.0" encoding="UTF-8"?> <configuration> <instance name="WebServer" active="true" root="www/instance/htdocs" index="index.html"> <errorlog enabled="true" file="www/instance/logs/error.log"/> <accesslog enabled="true" file="www/instance/logs/access.log"/> <listen secure="false" store="pki/wwwssl.jks" password="password" port="5563" sslport="5564" interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1" nodelay="false" timeout="5"/>
<access> <allow address="*"/> </access>
+<mimetype> +<virtual host="*" active="true"></instance> </configuration>

In this example <allow address= "*"/> allows access from any address. The other allow and deny directives are inside comments and ignored by the JSM HTTP server.

Table 22: What to Configure for Server Instance Access

To configure	Apply these settings	Change defaults
Allow any address	Use allow address=* <allow address="*"/>	Optional
Access for specific addresses	Add new a directive for each allowed address. <allow address="10.2.1.45"/>	Optional
Deny any address	Use deny address=* <deny address="*"/>	Optional

To configure	Apply these settings	Change defaults
Deny access for specific addresses	Add new a directive for each denied address. <deny address="10.2.1.45"/>	Optional

MIME types for the server instance

Table 23 (page 37) shows the configuration for MIME types. This part of the httpd configuration file defines MIME types applicable to the whole instance.

The MIME type directives allow the JSM HTTP server to correctly understand the nature of files. Administrators do not need to change these directives.

Table 23: MIME Types for the Server Instance

Server Instance MIME Types Configuration Example

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        <mimetype>
            <map extension="png" type="image/png"/>
            <map extension="gif" type="image/gif"/>
            <map extension="jpg" type="image/jpeg"/>
            <map extension="jpeg" type="image/jpeg"/>
            <map extension="tiff" type="image/tiff"/>
            <map extension="ico" type="image/x-icon"/>
            <map extension="pdf" type="application/pdf"/>
            <map extension="css" type="text/css; charset=utf-8"/>
            <map extension="xsl" type="text/xls; charset=utf-8"/>
            <map extension="xml" type="text/xml; charset=utf-8"/>
            <map extension="htm" type="text/html; charset=utf-8"/>
            <map extension="html" type="text/html; charset=utf-8"/>
            <map extension="js" type="application/x-javascript; charset=utf-8"/>
        </mimetype>
        +<virtual host="*" active="true">
    </instance>
</configuration>
```

MIME type directives in the virtual host section of the configuration file override MIME types specified in this section.

To determine allowed MIME types, the JSM HTTP server looks at MIME types in the virtual host section of the httpd configuration file and then at MIME types in the server instance. Place MIME types in the server instance that will apply all virtual hosts. Place MIME types that are unique to a virtual host in the MIME types section of the virtual host.

Table 24: What to Configure for the Server Instance MIME Types

To configure	Apply these settings	Change defaults
MIME types	Use the default list	Not recommended
Add MIME types	Add new a directive for each MIME type.	Optional

Virtual host configuration

The JSM HTTP server is capable of managing multiple virtual hosts. Table 25 (page 38) shows the virtual host configuration for WSFM.

Table 25: Virtual Host Configuration

Virtual Host Configuration Example

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        + <access>
        + <mimetype>
        <virtual host="*" active="true">
            + <access>
            + <protect>
            + <script>
            + <mimetype>
        </virtual>
    </instance>
</configuration>
```

The host is the name of the virtual host to match with the HTTP host property. In this case the asterisk ("*") indicates acceptance of requests from any host.

Table 26: What to Configure for One Virtual Host

To configure	Apply these settings	Change defaults
Virtual host	Use the default value asterisk (*)	Do not change
Active	Use the value true	Do not change

The active parameter has two values "true" and "false". The value of the active parameter must be "true" for WSFM to operate.

If you wish to use multiple instances and/or multiple virtual hosts in your configuration refer to the section titled, "Running WSFM and DE side by side" (page 59).

Access, protect, script and MIME type are sub sections of the virtual section in the httpd configuration file.

Virtual host access

The access directives in the virtual host section in the httpd configuration file control access to services provided by the JSM HTTP server. These directives override the access directives defined for the server instance. Using the virtual host access configuration you can:

- Allow addresses
- Deny addresses
- Allow user agents
- Deny user agents
- Allow content lengths
- Deny content lengths

Table 27 (page 39) shows an example of configuring virtual host access directives.

Table 27: Virtual Host Access Directives

Virtual Host Access Directives Configuration Example

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        <virtual host="*" active="true">
            <access>
                <allow address="*"/>
                <deny useragent="webos"/>
                <deny useragent="android"/>
                <deny useragent="ipad"/>
                <deny useragent="iphone"/>
                <allow useragent="*"/>
                <allow useragent="?"/>
                <deny contentlength="4096"/>
            </access>
            +<protect>
            +<script>
```

Virtual Host Access Directives Configuration Example
+<mimetype> </virtual> </instance> </configuration>

In this example, requests from any address are acceptable, deny access is explicit for several user agents, other user agents are acceptable and content length greater than 4096 is unacceptable.

Table 28: What to Configure for Virtual Host Access

To configure	Apply these settings	Change defaults
Allow any address	Use allow address=*	Optional
Access for specific addresses	Add a directive for each address.	Optional
Allow any user agent	Use allow useragent=*	Optional
Allow specific user agents	Add a directive for each user agent	Optional
Allow content lengths	Use allow contentlength= "value"	Optional
Deny any address	Use deny address=*	Optional
Deny access for specific addresses	Add a directive for each address.	Optional
Deny any user agent	Use deny useragent=*	Optional
Deny specific user agents	Add a directive for each user agent	Optional
Deny content lengths	Use deny contentlength= "value"	Optional

Access directives in the virtual host section of the configuration file override access directives specified in the access section of the server instance.

The default setting allows access for all addresses, useragents and content lengths.

Virtual host protect

Warning	You do not need to configure this section of the httpd configuration file to use WSFM.

The protection section of the httpd configuration file maps authentication methods to parts of the Web site or application. The realm describes the authentication method and the match URI associates the realm with the protected part of the Web site or application.

Table 29 (page 41) shows an example of the protect configuration.

Table 29: Virtual Host Protect Configuration

Virtual Host Protect Configuration Example

<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <instance name="WebServer" active="true" root="www/instance/htdocs"
  index="index.html">
  <errorlog enabled="true" file="www/instance/logs/error.log"/>
  <accesslog enabled="true" file="www/instance/logs/access.log"/>
  <listen secure="false" store="pki/wwwssl.jks" password="password"
  port="5563"
  sslport="5564"
  interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
  nodelay="false" timeout="5"/>
  +<access>
  +<mimetype>
  <virtual host="*" active="true">
  +<access>

<protect> <realm name="Area 51"> <user name="user" access="bb644a9819425bfd8586b408896a1031"/> </realm> <match uri="/restricted" realm="Area 51" authentication="basic,digest"/> </protect>
+<script> +<mimetype> </virtual> </instance> </configuration>

In this example the realm is "Area 51", the user name is "user", and access is a hash of the user, password and realm information. The configuration uses both basic and digest authentication methods. The match uri = "/restricted" associates the realm with URIs including the match URI.

Table 30: Configuring Virtual Host Protect

To configure	Apply these settings	Change defaults
Realm	Define the realm name.	Do not change the default values.
Realm / user	Add one or more user names with their access hash into the realm. You need to generate an access hash for each user in each realm and include them in the configuration. This applies even when the same user is in different realms. The tool to generate the access hash is not supplied with this version of WSFM.	Do not change the default values.

To configure	Apply these settings	Change defaults
Match URIs	Add one or more full or partial URIs with their associated realms.	Do not change the default values.

You do not need to configure this section of the httpd configuration file to use WSFM.

Virtual host script

The script section of the httpd configuration file contains configuration items associated with the available services. WSFM uses the following services:

- Spooled file service (HTTPServiceSpool)
- File access service (JSMHTTPServiceFile)

Each service has one or more parameters that control the way the service operates. Examples of parameters are:

- Autoregister
- Database.library

Table 31 (page 42) shows an example of a script configuration.

Table 31: Virtual Host Script Configuration

Virtual Host Script Configuration Example

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        <virtual host="*" active="true">
            +<access>
            +<protect>
            <script>
                <match uri="/axes/sfmservice.jsp"
                    class="com.lansa.jsm.service.HTTPServiceSpool"
                    trace="false" clienttrace="false">
                    <parameter name="autoregister" value="false"/>
                    <parameter name="database.host" value="LOCALHOST"/>
                    <parameter name="database.library" value="AXES"/>
                </match>
                <match uri="/" class="com.lansa.jsm.JSMHTTPServiceFile"
                    trace="false" clienttrace="false">
                    <parameter name="cache.maxage" value="28800"/>
                    <parameter name="cache.maxage.pdf" value="28800"/>
```

Virtual Host Script Configuration Example

```
                <parameter name="cache.maxage.image" value="28800"/>
            </match>
        </script>
        +<mimetype>
    </virtual>
  </instance>
</configuration>
```

WSFM requires configuration for the spooled file service (sfmservice) and the JSM HTTP file service to operate successfully.

This guide includes individual sections that describe how to configure each service. See the sections under "Configure services", (from page 44).

Virtual host MIME types

Table 32 (page 43) shows the configuration for MIME types applicable to the virtual host.

Table 32: Virtual Host MIME Type Configuration

Virtual Host MIME Type Configuration Example

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <instance name="WebServer" active="true" root="www/instance/htdocs"
        index="index.html">
    <errorlog enabled="true" file="www/instance/logs/error.log"/>
    <accesslog enabled="true" file="www/instance/logs/access.log"/>
    <listen secure="false" store="pki/wwwssl.jks" password="password"
      port="5563"
      sslport="5564"
      interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
      nodelay="false" timeout="5"/>
    +<access>
    +<mimetype>
    <virtual host="*" active="true">
      +<access>
      +<protect>
      +<script>
      <mimetype>
        <map extension="pdf" type="application/pdf"/>
      </mimetype>
    </virtual>
  </instance>
</configuration>
```

The MIME types defined in this section of the httpd configuration file override MIME types defined for the server instance.

Table 33: What to Configure for Virtual Host MIME Types

To configure	Apply these settings	Change defaults
MIME types	Use the default list	Do not change
Add MIME types	Add new a directive for each MIME type.	Optional

Configure services

The configure services section provides explanations for configuring each of the services that support WSFM. The configuration items and parameters reside in the script section of the httpd configuration file.

JSM HTTP file service configuration

The JSM HTTP server uses the service titled, com.lansa.jsm.JSMHTTPServiceFile, to retrieve files associated with the requested page.

Table 34 (page 44) shows the configuration for this service.

Table 34: Configure JSM HTTP File Service

Configure JSM HTTP File Service

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        <virtual host="*" active="true">
            +<access>
            +<protect>
            <script>
                +<match uri="/axes/sfmservice.jsp"
                <match uri="/" class="com.lansa.jsm.JSMHTTPServiceFile"
                    trace="false" clienttrace="false">
                    <parameter name="cache.maxage" value="28800"/>
                    <parameter name="cache.maxage.pdf" value="28800"/>
                    <parameter name="cache.maxage.image" value="28800"/>
                </match>
            </script>
            +<mimetype>
        </virtual>
```

Configure JSM HTTP File Service
 </instance> </configuration>

In this example the match URI is set to "/" to indicate the match applies to all URIs. The cache parameters set the maximum period for caching files and images. In this case the value used for both parameters is 28,800 seconds (or 8 hours).

Table 35: What to Configure for JSM HTTP File Service

To configure	Apply these settings	Change defaults
Match URI	Use the default "/"	Do not change
Class	Use com.lansa.jsm.JSMHTTPServiceFile	Do not change
Cache Maxage	The default maximum age for cached files is 28,800 seconds (8 hours). Do not remove this parameter.	Optional
Cache Maxage Image	The default maximum age for cached image files is 28,800 seconds (8 hours). Do not remove this parameter.	Optional

Do not remove this service from the httpd configuration file.

Allow and deny user access to services

The parameters, service.user.allow and service.user.deny, define identifications (or profiles) that are permitted (or allowed) to use WSFM or excluded from (or denied access to) WSFM services. The service.user.allow parameter defines acceptable users and the service.user.deny parameter defines users not permitted to use WSFM services. Table 36 (page 45) explains the syntax of these parameters. You may include multiple instances of the service.user.allow and service.user.deny parameters.

Table 36: User Identification/Profile service.user Allow and Deny Parameter Syntax

Parameter	Action by aXes-Cloud
<parameter name= "service.user.allow" value= "UserId"/>	The parameter value defines allowed (or acceptable) user identifications.
<parameter name= "service.user.allow" value= "UserId,UserId,UserId,UserId"/>	The parameter value is a list of user identifications separated by commas. The service.user.allow parameter allows (or accepts) user identifications in the list.
<parameter name= "service.user.deny" value= "UserId"/>	The parameter value denies (excludes) access to one user.
<parameter name= "service.user.deny" value= "UserId,UserId,UserId,UserId"/>	The parameter value is a list of user identifications separated by commas. The service.user.deny parameter denies (excludes) access to user identifications in the list.
<parameter name= "service.user.allow" value= "*USER"/>	The value *USER is a special case. It is a collective value that allows all user identifications.

Parameter	Action by aXes-Cloud
<parameter name= "service.user.deny" value= "*USER"/>	The value *USER is a special case. It is a collective value that denies all user identifications.

The user authentication process looks for instances of the service.user.deny parameter and then instances of the service.user.allow parameter.

By default, WSFM denies access to user identifications beginning with the letter Q. To enable access for these user identifications, each user identification must be configured explicitly using a service.user.allow parameter.

Table 37 (page 46) illustrates a configuration that includes the service.user.allow and service.user.deny parameters.

Table 37: Example Configuration for service.user Allow and Deny Parameters

Configuration for service.user.allow and service.user.deny Parameters

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="HTTP Instance" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        <virtual host="*" active="true">
            +<access>
            +<protect>
            <script>
                <match uri="/axes/sfmservice.jsp"
                    class="com.lansa.jsm.service.HTTPServiceSpool"
                    trace="false" clienttrace="false">
                    <parameter name="service.user.deny" value="JohnS,MaryB"/>
                    <parameter name="service.user.deny" value="GeorgeD,WendyF"/>
                    <parameter name="service.user.allow" value="*USER"/>
                    <parameter name="service.user.allow" value="QSYSOPR "/>
                    <parameter name="autoregister" value="false"/>
                    <parameter name="database.host" value="LOCALHOST"/>
                    <parameter name="database.library" value="AXES"/>
                </match>
                +<match uri="/" class="com.lansa.jsm.JSMHTTPServiceFile"
            </script>
            +<mimetype>
        </virtual>
```

Configuration for service.user.allow and service.user.deny Parameters
</instance> </configuration>

Table 38 (page 47) provides examples and explanations for configuring the service.user.allow and service.user.deny parameters.

Table 38: Controlling Access to Services – service.user Allow and Deny Examples

Parameter	Explanation
<parameter name= "service.user.allow" value= "*USER"/>	This value allows every user identification, except for those beginning with the letter Q.
<parameter name= "service.user.deny" value= "*USER"/>	This value denies access to every user identification, including those beginning with the letter Q. Using the *USER value on a service.user.deny parameter locks out every user. It overrides all values for the service.user.allow parameter.
<parameter name= "service.user.allow" value= "JohnS,MaryB,GeorgeD,WendyF"/>	This configuration allows all user identifications in the list.
<parameter name="service.user.deny" value= "JohnS,MaryB"/> <parameter name="service.user.allow" value= "*USER"/>	This configuration denies access to the users JohnS and MaryB, but allows all other users, except those beginning with the letter Q. This example illustrates the optimum method for allowing most users and denying a small number of users.
<parameter name="service.user.allow" value= "JohnS,MaryB"/>	This configuration allows only users JohnS and MaryB.
<parameter name="service.user.allow" value= "*USER,QSECOFR,QSYSOPR"/>	This service.user.allow value allows all users and both QSECOFR and QSYSOPR. It is unnecessary to include service.user.deny parameters for user identifications beginning with the letter Q; aXes denies access to these user identifications by default.

To use WSFM services, users must be authorised by an implicit or explicit service.user.allow parameter and also registered as a WSFM user.

User registration

User registration is one of the tasks managed by the service sfmservice.jsp. Table 39 (page 47) describes the values for the autoregister parameter associated with the service sfmservice.jsp.

Table 39: Autoregister Parameter for the Service sfmservice.jsp

Parameter	Action by WSFM
<parameter name= "autoregister" value= "true"/>	WSFM will register any person who logs on with an active profile on the server.

Parameter	Action by WSFM
<parameter name= "autoregister" value= "false"/>	Setting the value to false prevents WSFM registering users automatically. Administrators will register users manually.

For manual user registration change the value of the autoregister parameter to "false".

For automated user registration change the value of the autoregister parameter to "true".

Table 40 (page 48) shows an example of a configuration file using manual user registration.

Table 40: Autoregister Parameter for Automated or Manual User Registration

Configuration for the Auto Register Parameter

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <instance name="WebServer" active="true" root="www/instance/htdocs"
            index="index.html">
        <errorlog enabled="true" file="www/instance/logs/error.log"/>
        <accesslog enabled="true" file="www/instance/logs/access.log"/>
        <listen secure="false" store="pki/wwwssl.jks" password="password"
            port="5563"
            sslport="5564"
            interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
            nodelay="false" timeout="5"/>
        +<access>
        +<mimetype>
        <virtual host="*" active="true">
            +<access>
            +<protect>
            <script>
                <match uri="/axes/sfmservice.jsp"
                    class="com.lansa.jsm.service.HTTPServiceSpool"
                    trace="false" clienttrace="false">
                    <parameter name="autoregister" value="true"/>
                    <parameter name="database.host" value="LOCALHOST"/>
                    <parameter name="database.library" value="AXES"/>
                </match>
                +<match uri="/" class="com.lansa.jsm.JSMHTTPServiceFile"
            </script>
            +<mimetype>
        </virtual>
    </instance>
</configuration>
```

Table 40 (page 48) shows an example httpd configuration file <script> section and the configuration of the sfmservice. In this example the value of the autoregister parameter is "false", indicating manual user registration.

Users cannot set the value of the autoregister parameter from the WSFM user interface.

Reference guide: JSM HTTP server configuration

The reference guide provides explanations of the individual items in the httpd configuration files.

Configuration item reference

Table 41 (page 49) provides explanations of configuration items in the JSM HTTP server httpd configuration file. The items in the table are in name sequence. The configuration item name is the name and position of the parameters in the httpd configuration file. For example, the item named "listen port" is the port on the listen directive.

Table 41: Server Reference: Configuration Item Reference

Configuration Items	Definitions
Access allow	List of addresses, content lengths and/or user agents allowed access to the JSM HTTP server. Example: <allow address="10.2.1.45">
Access deny	List of addresses, content lengths and/or user agents denied access to the JSM HTTP server. Example: <deny address="10.2.1.45">
Access log enabled	WSFM logs all access events when access log enabled is "true". WSFM logs no access events when access log enabled is "false".
Access log file	Name and location of the access log file. Example: "www/instance/logs/access.log"
Cache maxage	Maximum age for cached files in seconds.
Cache maxage image	Maximum age for cached image files in seconds.
Cache maxage pdf	Maximum age for cached PDF files in seconds.
Error log enabled	WSFM logs all errors when error log enabled is "true". WSFM logs no errors when error log enabled is "false".
Error log file	Name and location of the error log file. Example: "www/instance/logs/error.log"
Instance active	To operate WSFM this parameter will always be "true". The JSM HTTP server supports multiple instances and needs this parameter to indicate which instances to activate at run time.
Instance index	Name of the index page. Example: "index.html"

Content © LANSA Group
All Rights Reserved

Configuration Items	Definitions
Instance name	Name allocated the JSM HTTP server. Example: "WebServer" or "My HTTP Instance" This name does not need to be the same as the instance name in the manager.properties file (httpd.axes.instance=AXES).
Instance root	Name of the directory from which the documents will be served by the JSM HTTP server. Also known as document root. Example: "www/instance/htdocs"
Listen backlog	The backlog defines the depth of the TCP/IP queue.
Listen buffer receive	TCP/IP receive buffer size in bytes. Special case value "-1" means use operating system default.
Listen buffer send	TCP/IP send buffer size in bytes. Special case value "-1" means use operating system default.
Listen interface	TCP/IP interface address that the JSM HTTP server will bind to and accept connections on. Default value is *ALL *ALL will bind to all interfaces on the server.
Listen no delay	True enables TCP/IP no delay option. False means use the operating system setting for this parameter.
Listen password	Password that will open the store file used for TLS/SSL configuration. Example: "password"
Listen port	TCP/IP port number the server will use to accept connections on.
Listen secure	When true, the JSM HTTP server uses TLS/SSL When false, the JSM HTTP server uses plain sockets.
Listen sslport	TCP/IP port number the server will use to accept connections when using TLS/SSL.
Listen store	Path for the store file that contains the private key and public certificates (used when TLS/SSL enabled). Fully qualified name and location of the store file. Example: "pki/wwwssl.jks"
Listen timeout	Time out count in seconds (integer).
Mimetype map extension	File extension used to identify the MIME type. Example: "png"

Content © LANSA Group
All Rights Reserved

Configuration Items	Definitions
Mimetype map type	The type describes the nature of the MIME type. Examples: "image/png"
Protect match authentication	Type of authentication, values are: "basic", "digest" or "basic,digest". Basic: Basic authentication is a concatenation of user name, a colon and the password encoded with the Base64 algorithm. Digest: Digest authentication is an application of MD5 cryptographic hashing of user credentials. It provides stronger encoding than basic authentication.
Protect match realm	Name of the realm used for authentication to parts of the Web site or application. The realm is associated with the matched URIs.
Protect match uri	URIs used to match against requests. When a match occurs the associated realm provides the authentication details.
Protect realm name	Name assigned to a realm.
Protect realm user access	Access is a digest of user information (including the password).
Protect realm user name	User name for authentication.
Script match	The match definitions describe services that the JSM HTTP server will use depending on the match criteria in the URI.
Script match class	Class is the name of a service.
Script match client trace	Use this parameter to trace activity associated with specific clients. Tracing will slow performance. When "true" tracing will occur from the client URI using the "?trace=true" query string parameter. The value "false" disables tracing.
Script match trace	Use this parameter to trace activity associated with all clients. Broader scope than client trace. The value "true" enables tracing for all services and user agents that match the match URI. The value "false" disables tracing.
Script match URI	The match URI is the match criteria the JSM HTTP server uses to determine the services to use.
Virtual access allow	List of addresses, content lengths and/or user agents allowed access to the JSM HTTP server. Example: <allow useragent="safari">

Content © LANSA Group
All Rights Reserved

Configuration Items	Definitions
Virtual access deny	List of addresses, content lengths and/or user agents denied access to the JSM HTTP server. Example: <deny useragent="safari">
Virtual active	When the value is "true" this virtual host is active. When the value is "false" the virtual host is inactive. To operate WSFM the value must be "true". Services configured in the virtual host are unavailable when the virtual host is inactive.
Virtual host	Name of the virtual host to match with the HTTP host property. This allows multi homing. HTTP requests can be directed to different virtual host sections of the configuration in the server instance. If a virtual host is not found then the connection request is rejected. The special case value "*" accepts requests from any HTTP host. Specific names take precedence.
Virtual mimetype map extension	File extension used to identify the MIME type. Example: "png"
Virtual mimetype map type	The type describes the nature of the MIME type. Examples: "image/png"

MIME types

MIME type describes the nature of content of file for the JSM HTTP server. Table 42 (page 52) provides examples of MIME types.

Table 42: JSM HTTP Server Reference: MIME type Examples

Extension	Type
css	text/css; charset=utf-8
gif	image/gif
htm	text/html; charset=utf-8
html	text/html; charset=utf-8
ico	image/x-icon
jpeg	image/jpeg
jpg	image/jpeg
js	application/x-javascript; charset=utf-8
pdf	application/pdf
png	image/png
tiff	image/tiff
xls	text/xls; charset=utf-8

Content © LANSA Group
All Rights Reserved

Extension	Type
xml	text/xml; charset=utf-8

Access allow and deny directives

Table 43 (page 53) shows examples of the access allow/deny directive for addresses.

Table 43: Server Reference: Access Allow and Deny Addresses

Allow / Deny	Syntax and Examples
Allow any address	<allow address="*">
Allow addresses in a range	<allow address="10.2.1">
Allow a specific address	<allow address="10.2.1.45">
Deny any address	<deny address="*">
Deny addresses in a range	<deny address="10.2.1">
Deny a specific address	<deny address="10.2.1.45">

Table 44 (page 53) shows examples of the access allow/deny directive for content length.

Table 44: Server Reference: Access Allow and Deny Content Length

Allow / Deny	Syntax and Examples
Allow access for content less than or equal to the specified length	<allow contentlength="4096">
Zero content length is a special case to allow access for no content connections from the browser	<allow contentlength="0">
Deny access for content greater than the specified length	<deny contentlength="4096">

User agents are applications or services that act on behalf of the user. When a user requests a web page (or URL), the browser acts as a user agent by sending the page request to the JSM HTTP server. Examples of user agents are browsers, web crawlers, link checkers, bots and email clients. Access allow and deny directives control which user agents the JSM HTTP server will allow or deny access.

Table 45 (page 53) shows examples of user agents and the syntax of the allow access and deny access directives.

Table 45: Server Reference: Access Allow and Deny User Agents

Allow / Deny	Syntax and Examples
Allow access for any user agent	<allow useragent="*"
Allow access if no user agent provided	<allow useragent="?"
Allow access to Chrome	<allow useragent="chrome"
Allow access to the Internet Explorer	<allow useragent="explorer"
Allow access to Firefox	<allow useragent="firefox"

Content © LANSA Group
All Rights Reserved

Allow / Deny	Syntax and Examples
Allow access to Safari	<allow useragent="safari"
Deny access for any user agent	<deny useragent="*"
Deny access if no user agent provided	<deny useragent="?"
Deny access to Chrome	<deny useragent="chrome"
Deny access to Internet Explorer	<deny useragent="explorer"
Deny access to Firefox	<deny useragent="firefox"
Deny access to Safari	<deny useragent="safari"

The evaluation of the directives starts with the first item in the list and continues until it finds a true condition. Any combinations of address, user agent and content length are acceptable. However, it is possible to negate the effect of a directive by its position in the list. For example, placing an allow any user agent (<allow useragent="*"/>) ahead of a deny for a specific user agent (<deny useragent="webos"/>) will cause the JSM HTTP server to ignore the deny directive.

Table 46 (page 54) presents lists of user agents.

Table 46: Server Reference: Sample List of User Agents

Browser User Agents	Bots and Device User Agents
android	googlebot
chrome	googletoolbar
explorer	ipad
firefox	iphone
opera	lansaua
safari	msnbot
webos	yahoobot

Sample configurations

Default configuration for WSFM

Table 47 (page 54) shows the default httpd configuration file including MIME types, allow and deny directives.

Table 47: Server Reference: Default httpd Configuration for WSFM

Default Configuration for WSFM
<?xml version="1.0" encoding="UTF-8"?> <configuration>   <instance name="WebServer" active="true" root="www/instance/htdocs"   index="index.html">   <errorlog enabled="true" file="www/instance/logs/error.log"/>   <accesslog enabled="true" file="www/instance/logs/access.log"/>   <listen secure="false" store="pki/wwwssl.jks" password="password"

Default Configuration for WSFM

```
        port="5563"
        sslport="5564"
        interface="*ALL" backlog="256" buffersend="-1" bufferreceive="-1"
        nodelay="false" timeout="5"/>
    <access>
        <allow address="*"/>
    </access>
    <mimetype>
        <map extension="png"  type="image/png"/>
        <map extension="gif"  type="image/gif"/>
        <map extension="jpg"  type="image/jpeg"/>
        <map extension="jpeg" type="image/jpeg"/>
        <map extension="tiff" type="image/tiff"/>
        <map extension="ico"  type="image/x-icon"/>
        <map extension="pdf"  type="application/pdf"/>
        <map extension="css"  type="text/css; charset=utf-8"/>
        <map extension="xsl"  type="text/xls; charset=utf-8"/>
        <map extension="xml"  type="text/xml; charset=utf-8"/>
        <map extension="htm"  type="text/html; charset=utf-8"/>
        <map extension="html" type="text/html; charset=utf-8"/>
        <map extension="js"   type="application/x-javascript; charset=utf-8"/>
    </mimetype>
    <virtual host="*" active="true">
        <access>
            <deny useragent="webos"/>
            <deny useragent="opera"/>
            <deny useragent="android"/>
            <deny useragent="ipod"/>
            <allow useragent="*"/>
            <allow useragent="?"/>
        </access>
        <protect>
            <realm name="Area 51">
                <user name="user" access="bb644a9819425bfd8586b408896a1031"/>
            </realm>
            <match uri="/restricted" realm="Area 51" authentication="basic,digest"/>
        </protect>
        <script>
            <match uri="/axes/sfmservice.jsp"
                class="com.lansa.jsm.service.HTTPServiceSpool"
                trace="false" clienttrace="false">
                <parameter name="autoregister" value="false"/>
                <parameter name="database.host" value="LOCALHOST"/>
                <parameter name="database.library" value="AXES"/>
            </match>
```

Default Configuration for WSFM

```
            <match uri="/" class="com.lansa.jsm.JSMHTTPServiceFile"
                trace="false" clienttrace="false">
                <parameter name="cache.maxage" value="28800"/>
                <parameter name="cache.maxage.pdf" value="28800"/>
                <parameter name="cache.maxage.image" value="28800"/>
            </match>
        </script>
        <mimetype>
            <map extension="pdf" type="application/pdf"/>
        </mimetype>
    </virtual>
  </instance>
</configuration>
```

Appendices

Glossary

Table 48 (page 57) presents definitions for abbreviations and terms used in this guide.

Table 48: Glossary of Abbreviations and Terms

Abbreviations and Terms	Definitions and Explanations
CCSID	Coded Character Set Identifier
DBCS	Double Byte Character Set
DE	Data Explorer (DE) is a product related to WSFM and may share the same httpd configuration file.
Directives	Configuration directives are the parameters and settings that control the behaviour of the JSM HTTP server.
Filter	WSFM uses the word "filter" to describe a collection of search criteria when searching for tables and selection criteria for queries.
IFS	The Integrated File System is a part of the IBM i operating system. It supports stream input/output and storage management capabilities like personal computer and UNIX operating systems.
Internet Media Type	Internet Media Type (IMT) is an identifier for file formats on the Internet. An example is the IMT for the Portable Document Format: application/pdf See also MIME type.
JSM	Java Services Manager
MIME	Multipurpose Internet Mail Extensions MIME is an Internet standard that describes content. An example is PNG for Portable Network Graphic files. See also Internet Media Type.
Output queue	An output queue is a place where spooled files are held until printed or deleted.
Queue filter	Queue filters describe the search or selection criteria to find output queues.
Realm	A realm is a database containing a list of valid users of a web application. The user information in the database is user name, password and a set of roles associated with the user.
SBCS	Single Byte Character Set
Spool filter	Spool filters describe the search or selection criteria to find spooled files in one or more output queues.

Content © LANSA Group
All Rights Reserved

Abbreviations and Terms	Definitions and Explanations
Spooled file	A spooled file is a report generated by a program. A spooled file can be as simple as a printed copy of a screen or as complex as a report consisting of many pages.
System directory	System directory is a synonym for system folder.
System folder	The location of the system folder is: axes/jsm/instance/system
Toolbox for Java JDBC driver	The Toolbox for Java JDBC driver provides access to the database.
WSFM	Web Spooled File Manager WSFM is a product related to DE and may share the same httpd configuration file.

Referenced documents and sources

Table 49 (page 58) defines documents and information sources referenced in this guide.

Table 49: Referenced Documents and Information Sources

References
IBM i and System i Information Center at http://publib.boulder.ibm.com/iseries/
IBM Toolbox for Java (IBM i software) at http://www-03.ibm.com/systems/i/software/toolbox/faqjdbc.html#faqA1

Assumed and prerequisite knowledge

Table 50 (page 58) defines the prerequisite knowledge needed to use the guide.

Table 50: Assumed and Prerequisite Knowledge

Subject Matter	Explanations
Libraries	The guide assumes that you understand the concepts behind libraries for IBM i servers.
Search concepts	The guide assumes that you understand the concepts behind searching for output queue and spooled files on IBM i servers.
Output queue	The guide assumes that you understand the relationship; between output queues and spooled files.
Spooled file	The guide assumes that you understand how to create spooled files.
Using the clipboard	You need to know how to use the clipboard for copying and pasting data between applications.
XML files	The directives for WSFM reside in the configuration file, formatted as XML. You need to be able to read and edit the XML.

Content © LANSA Group
All Rights Reserved

Browser behaviour differences

The browser you use and the browser settings and preferences will influence the way WSFM operates. Table 51 (page 59) identifies examples of differences in the way each browser behaves in specific circumstances.

Table 51: Browser Behaviour Differences

Actions	Chrome	Firefox	Internet Explorer	Safari
Pressing Cancel on the log on screen will close the browser	Yes	No ❶	Yes	Yes

Notes

❶ Firefox will close the WSFM page but not the browser.

Workstation requirements

This section describes prerequisites and system requirements for running WSFM on your computer or mobile device.

Hardware

Devices with faster processors and more memory will provide better performance.

WSFM requires no disk space other than the cache used by the browser.

Software

To use WSFM you need one of the supported browsers and apart from the operating system no other software is necessary.

Connectivity

To use WSFM you need a TCP/IP connection to an IBM i server from an internal network or the Internet.

Running WSFM and DE side by side

Data Explorer (DE) may be installed beside WSFM and share its configuration with WSFM.

Several configuration options are available when installing both WSFM and DE. The choice of which configuration to use depends on the user communities who will use each product. You need the least access separation when the same user communities will use both products. You need the most access separation when different user communities will use each product. For example, you may allow internal user communities to use DE but external user communities may use only WSFM. When all user communities are internal the need for separate access reduces.

Content © LANSA Group
All Rights Reserved

Configuration options

The simplest configuration is one instance and one virtual host for both WSFM and DE. When both products are configured in the same instance they share the same port.

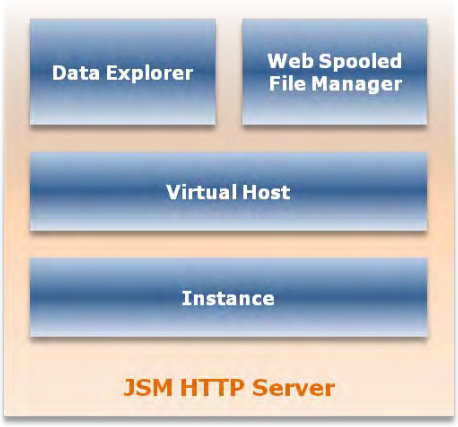

Figure 6: WSFM and DE on a single instance and virtual host

Characteristics of the configuration

Single instance (both WSFM and DE)

One virtual host (both WSFM and DE)

WSFM and DE share the same port

Simplest configuration

Fewest options for separating access to WSFM and DE

Suitable for deployment when the same user communities will operate both WSFM and DE.

You cannot have WSFM active and close down DE or keep DE active and close down WSFM with a configuration consisting of a single instance and one virtual host.

With both products installed, the virtual host script section of the httpd configuration file may include configuration items for both DE and WSFM. Alternatively, you could use two virtual hosts, one virtual host for DE and a second virtual host for WSFM.

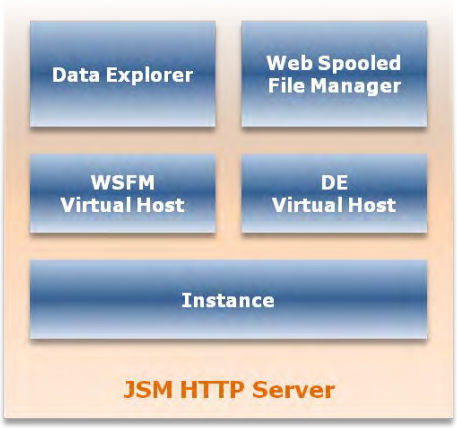

Figure 7: WSFM and DE on a single instance and two virtual hosts

Characteristics of the configuration

Single instance (both WSFM and DE)

Virtual host for WSFM

Virtual host for DE

WSFM and DE share the same port

More effort to configure than one instance and one virtual host

More options for separating access to WSFM and DE than one virtual host

Suitable for deployment when one port is adequate but you want flexibility in separating access to WSFM and DE

Separate virtual hosts for WSFM and DE provide more flexibility for deployment than a single virtual host as the products share fewer configuration items. The configuration allows you to close down DE and leave WSFM active or close down WSFM and leave DE active.

The best separation is to use one port for WSFM and a second port for DE. To use different ports the httpd configuration file must include two instances, one instance for DE and a second instance for WSFM.

Content © LANSA Group
All Rights Reserved

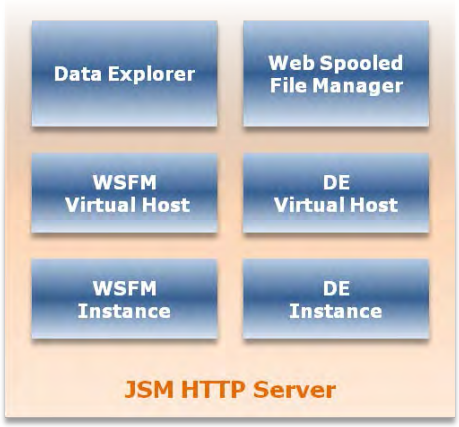

Figure 8: WSFM and DE on two instances and two virtual hosts

Characteristics of the configuration

An instance for WSFM

A virtual host for WSFM

An instance for DE

A virtual host for DE

WSFM has a port

DE has a port

Most complex configuration

Best separation of access to WSFM and DE

Suitable for deployment when different user communities will operate WSFM and DE

Deploying two instances provides separate virtual hosts as a virtual host will reside in each instance. This configuration allows you to close down the whole instance of DE and leave WSFM active or close down the whole instance of WSFM and leave DE active.

User registration when operating both WSFM and DE

The user registration for WSFM and DE are discrete processes. Any user who wishes to operate both WSFM and DE must register for each product.

The separated registration ensures that administrators do not provide access to corporate databases indiscriminately.

Configuration files

axinfo.json

Table 52: axinfo.json Configuration File for both DE and WS

axinfo.json Configuration Example both DE and WS

```
{
    "sfm":
        {
            "enabled":    true,
            "port":       5563,
            "sslport":    5564,
            "uri":        "/axes/spooled-file-manager.html"
        },
    "dbm":
        {
            "enabled":    true,
            "port":       5563,
            "sslport":    5564,
            "uri":        "/axes/database-manager.html"
        }
}
```

IBM i printing reference

Definitions

Host print transform

Host print transform (HPT) is an OS/400 function that converts an SNA character string (SCS) or advanced function print (AFP) data streams into an ASCII data stream. The conversion takes place on the IBM i server and thereby provides a consistent ASCII data stream to any devices or emulators.

WSFM supports host print transform.

Stream files and SCS

"A stream file is a randomly accessible sequence of bytes, with no further structure imposed by the system. The integrated file system provides support for storing and operating on information in the form of stream files. Documents that are stored in your server's folders are stream files. Other examples of stream files are PC files and the files in UNIX® systems. An integrated file system stream file is a system object that has an object type of *STMF." [2]

WSFM supports stream files for retrieving the content of spooled files from IBM i servers.

Host Print Transform: limitations and constraints

"Host Print Transform has an interesting algorithm for deciding the encoding of the spooled data. Sometimes HPT has to fall back to system value settings. On systems with mixed languages this can create problems.

"I've had cases where application developers had to give up on HPT and do the processing using CPYSPLF and CPYTOSTMF.

"In this way one can force the character encoding to be used in transferring of data and get it into the encoding desired on the receiving system."

Rodney A Johnson

Technical Team Lead for i5/OS (AS/400) Spool Dept GJC IBM Rochester, Minnesota

http://newsgroups.derkeiler.com/Archive/Comp/comp.sys.ibm.as400.misc/2007-12/msg00073.html

Content © LANSA Group
All Rights Reserved