Sun Java System Federation Manager 7.0 Release Notes

Sun microsystems

◆ ◆ ◆ **C H A P T E R 1**

1

Sun Java System Federation Manager 7.0 Release Notes

The *Sun Java™ System Federation Manager 7.0 Release Notes* contain important information about the release of Sun Java System Federation Manager, version 7.0. Features, known issues and limitations, and other information are addressed. Read this document before you install and use this release.

The *Federation Manager 7.0 Release Notes* contain the following sections:

Revision History

The following table shows the *Federation Manager 7.0 Release Notes* revision history.

TABLE 1–1 Revision History

Date	Description
October 2007	Added new issue
July 2006	Windows Release
June 2006	Linux Release
September 2005	2005Q4 publication

TABLE 1–1 Revision History   *(Continued)*

Date	Description
May 2005	Early Access publication

Related Third-Party Web Sites

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun Microsystems is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

About Sun Java System Federation Manager 7.0

Sun Java System Federation Manager 7.0 is the first product to focus on quickly establishing and extending services. Federation Manager 7.0 is a first-generation product that accelerates the introduction of new, revenue-generating services by organizing hub-and-spoke partner networks into secure and trusted domains. Federation Manager allows companies to act as *spokes* (or service providers) by providing extensible, easy-to-deploy federation solutions. Key features of Federation Manager include:

- Simplified deployment into existing internal technology infrastructures.
- Leveraging of the trusted domain's hub for authentication, authorization, and security policies.
- Support for all major federation protocols (Security Assertion Markup Language, Liberty Alliance Project).
- Repeatable integration for low-cost, rapid rollout to multiple partners.
- Extranet single sign-on.
- Automated identity federation.
- Single log-out.
- Centralized provider management.
- Trusted domain management.
- Liberty—based trusted authority and discovery/registry provider.
- Security Assertion Markup Language (SAML) assertion exchange.
- Web services development framework.

Hardware and Software Requirements

The following sections describe hardware and software requirements for this release of Federation Manager. If you have questions about support for other versions of these components, contact your Sun Microsystems technical representative.

Data Stores

Federation Manager configuration data, user authentication data and user federation data can be managed and retrieved from a database of the following type:

- Lightweight Directory Access Protocol (LDAP) version 3 compliant directories (for example, Sun Java System Directory Server or Microsoft™ Active Directory)
- Relational Database Management Systems (through customer plug-in implementations only)
- Flat files (default text file format for configuration data)

Note – Federation Manager does not come with a user administration system.

Platforms and Operating Systems

You can install Federation Manager on the following platforms running the applicable operating systems.

TABLE 1–2   Operating Systems

Platform	Operating System	Version
Sparc®	Solaris	8 / 9 / 10
x86	Solaris	9 / 10
x86	Linux	Red Hat™ Enterprise Linux 2.1, 3.0, and 4.0

TABLE 1–2 Operating Systems *(Continued)*

Platform	Operating System	Version
x86	Windows	▪ Windows 2000 Advanced Server SP4 or above
		▪ Windows 2000 Server SP4 or above
		▪ Windows 2000 Professional Edition SP4 or above
		▪ Windows XP Professional Edition SP2
		▪ Windows 2003 Enterprise Server
		Note – Federation Manager was only tested on Windows 2003 Enterprise Server.

Supported Web Containers

Federation Manager can be deployed in the following web containers. CPU and memory requirements are based on the needs of the web container.

TABLE 1–3 Supported Web Containers

Web Container	Minimum Version
Sun Java System Web Server	6.1sp4
Sun Java System Application Server	8.1
BEA WebLogic® Server	8.1
WebSphere® Application Server	5.1

Known Issues and Limitations

This section describes known issues and workarounds, if available, at the time of the release. Issues relevant to all supported operating systems and web containers are collected in this section.

- "Installation and Deployment" on page 7
- "Configuration" on page 11
- "Federation" on page 12

Installation and Deployment

The following issues are related to the installation of Federation Manager and its deployment on the supported web containers.

- "*Error 404-Not Found* When Deploying `federation.war` on WebLogic 8.1 Application Server Under Windows" on page 7
- "Federation Manager installation error on Linux if Application Server 8 is installed by JES4 (6434059)" on page 7
- "Escape special characters in silent install file and sample XML files (6431990)" on page 9
- "Update the Java Web Services Developer Pack packages before installing on Solaris 9/10. (6334913)" on page 9
- "`fmwar` does not prompt for a `JAVA_HOME` value. (6333234)" on page 9
- "`SUNWjhrt` is not installed when `JAVA_HOME` is not set. (6324701)" on page 10
- "Installation fails if space is used in `INST_ORGANIZATION` property value (6324192)" on page 10
- "Stock ticker sample does not work on WebSphere Application Server (6322964)" on page 10

Error 404-Not Found When Deploying `federation.war` on WebLogic 8.1 Application Server Under Windows

The root cause is that Federation Manager can not find the right authentication module XML file due to the use of an incorrect file separator. This problem happens with JDK 1.4.x only.

WORKAROUND: Run the following command to add the proper separator before the final start command in the `startWeblogic.bat` script:

```
# set JAVA_OPTIONS=%JAVA_OPTIONS% -Dfile.separator=/
# echo %JAVA_OPTIONS%
```

Federation Manager installation error on Linux if Application Server 8 is installed by JES4 (6434059)

Federation Manager is based on Access Manager 6.3. Thus, the shared components are conflict with those in JES4 (which includes Access Manager 7.0).

WORKAROUND: The following procedure will install Federation Manager correctly.

1. Install Java Enterprise System 4 with Application Server 8 selected.

   Note – This will install the shared components.

2. Install the Federation Manager Linux rpm only using the command: `fmsetup install -s` *silent_installation_file* `-p`

> **Note –** Ignore error messages complaining about an rpm file conflict or that the installed rpm is newer than that bundled with Federation Manager.

3. Force install imq using the following command: `rpm -i --force imq-3_5-03.i386.rpm`

4. Run `fmwar` to generate the WAR using the following command: `fmwar -n federation -d /var/opt/sun/identity/fm/war_staging -s` *silent_installation_file* `-g`

5. Deploy the generated WAR on Application Server.

6. Add the follow lines to `java.policy`:

```
// Federation Manager RELATED ADDITIONS
    grant {
        permission java.util.PropertyPermission "user.language", "write";
    };
    grant codeBase "file:${BASEDIR}/${PROD_DIR}/fm/web-src/WEB-INF/lib/am_sdk.jar" {
        permission java.net.SocketPermission "*", "connect,accept,resolve";
    };
    grant codeBase "file:${BASEDIR}/${PROD_DIR}/fm/web-src/WEB-INF/lib/am_services.jar" {
        permission java.net.SocketPermission "*", "connect,accept,resolve";
    };
    grant codeBase   "file:$AS81_VARDIR/domains/$AS81_DOMAIN/applications/j2ee-modules/${DEPLOY_WARPREFIX}/-" {
        permission java.net.SocketPermission "*", "connect,accept,resolve";
    };
    grant {
        permission java.lang.RuntimePermission "modifyThreadGroup";
        permission java.lang.RuntimePermission "setFactory";
        permission java.lang.RuntimePermission "accessClassInPackage.*";
        permission java.util.logging.LoggingPermission "control";
        permission java.lang.RuntimePermission "shutdownHooks";
        permission javax.security.auth.AuthPermission "insertProvider.Mozilla-JSS";
        permission java.security.SecurityPermission "putProviderProperty.Mozilla-JSS";
        permission javax.security.auth.AuthPermission "getLoginConfiguration";
        permission javax.security.auth.AuthPermission "setLoginConfiguration";
        permission javax.security.auth.AuthPermission "modifyPrincipals";
        permission javax.security.auth.AuthPermission "createLoginContext.*";
        permission java.security.SecurityPermission "insertProvider.Mozilla-JSS";
        permission javax.security.auth.AuthPermission "putProviderProperty.Mozilla-JSS";
        permission java.io.FilePermission "ALL FILES", "execute,delete";
        permission java.io.FilePermission "$VAR_SUBDIR/logs/*", "delete,write";
        permission java.util.PropertyPermission "java.util.logging.config.class", "write";
        permission java.security.SecurityPermission "removeProvider.SUN";
        permission java.security.SecurityPermission "insertProvider.SUN";
        permission java.security.SecurityPermission "removeProvider.Mozilla-JSS";
        permission javax.security.auth.AuthPermission "doAs";
        permission java.util.PropertyPermission "java.security.krb5.realm", "write";
```

```
    permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
    permission java.util.PropertyPermission "java.security.auth.login.config", "write";
    permission javax.security.auth.kerberos.ServicePermission "*", "accept";
    permission javax.net.ssl.SSLPermission "setHostnameVerifier";
};
```

Escape special characters in silent install file and sample XML files (6431990)

Special characters must be escaped (preceded with a back slash) in the silent installation file. Also, after installation, if you want to run the Liberty SSO or SPI samples, you need to edit the metadata XML files and escape the special characters before loading them using the amadmin command line tool.

WORKAROUND: Replace **&** with **\&**, or a space with \ . For example, rather than defining the INST_ORGANIZATION parameter in the silent installation file as INST_ORGANIZATION=dc=a b & c, use INST_ORGANIZATION=dc=a\ b\ \&\ c.

Update the Java Web Services Developer Pack packages before installing on Solaris 9/10. (6334913)

A fresh installation of the Solaris Operating System v.9/10 contains older versions of the following packages:

- SUNWjaxb
- SUNWjax
- SUNWwscl
- SUNWxrpcrt
- SUNWxsrt

These older versions are numbered 7.x. The newer versions installed by the Federation Manager installer are numbered 1.2.x. Because of this numbering convention, the newer packages will not be installed. Thus, the Java Web Services Developer Pack (JWSDP) packages need to be manually updated prior to installing Federation Manager. If this is not done, the installation might be successful, but a user will not be able to login to the Console due to a java.lang.NoClassDefFoundError exception.

Note – The package timestamp can be used to verify which package is older.

WORKAROUND: Before installing Federation Manager, use pkginfo -l to check that the shared packages are the supported version as stated in the *Sun Java System Federation Manager 7.0 User's Guide*. If an older package is found, remove it manually using pkgrm. The installer will deploy the correct packages.

fmwar does not prompt for a JAVA_HOME value. (6333234)

fmwar checks for the java file in the /usr/bin/ directory. If that file is present, fmwar assumes all Java components are present which is not always the case.

WORKAROUND: Set the JAVA_HOME environment variable to the location of the latest installed release of Java.

SUNWjhrt **is not installed when** JAVA_HOME **is not set. (6324701)**

SUNWjhrt is a shared package that performs an internal check for one of the following versions of Java before the package can be installed:

- pkginfo -q *SUNWj2rt*
- pkginfo -q *SUNWj3rt*
- pkginfo -q *SUNWj5rt*

If none of these versions is found, the installation script will abort, causing Federation Manager installation to fail.

WORKAROUND: Install the SUNWj3rt package bundled with the Federation Manager binary. Change to the directory where the Federation Manager binary was unpacked and run the following command from within the common directory:

pkgadd -d . SUNWj3rt

Alternately, you can download the Java Development Kit (JDK) version 1.5 from the Sun Developer Network and install the SUNWj5rt package from that binary. After installing the correct package, rerun fmsetup to install Federation Manager.

Installation fails if space is used in INST_ORGANIZATION **property value (6324192)**

Installation will fail if a space is used between individual components of the root distinguished name (DN). For example, the DN dc=sun, dc=com would cause the installation to fail. dc=sun,dc=com is acceptable.

WORKAROUND: Remove any typed space(s) between individual components of the root DN.

Stock ticker sample does not work on WebSphere Application Server (6322964)

The web service sample does not work when Federation Manager is deployed on WebSphere Application Server. This sample simulates a stock ticker and is located in the */FederationManager-base*/SUNWam/fm/samples/liberty/webservices/stockticker directory.

WORKAROUND: Copy /usr/share/lib/jax-qname.jar to the classpath in *websphere_install_root*/WebSphere/AppServer/config/cells/*cell-name*/nodes/ *node-name*/servers/*server-instance*/server.xml. For example:

```
<jvmEntries xmi:id="JavaVirtualMachine_1" verboseModeClass="false"
verboseModeGarbageCollection="false" verboseModeJNI="false"
initialHeapSize="256" maximumHeapSize="256" runHProf="false"
hprofArguments="" debugMode="false" debugArgs="-Djava.compiler=NONE
```

```
-Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
genericJvmArguments="-Dcom.iplanet.am.serverMode=true">
<classpath>/usr/share/lib/jax-qname.jar</classpath>
```

Configuration

The following issues are related to configuring Federation Manager.

- "Exception thrown when transferring configuration data to Sun Java System Directory Server on Solaris 8 (6324142)" on page 11
- "Unable to use default `ldapmodify` in Solaris 8 against Microsoft Active Directory (6328437)" on page 11
- "`amadmin` throws exception when Federation Manager is deployed on BEA WebLogic Server (6320391)" on page 11

Exception thrown when transferring configuration data to Sun Java System Directory Server on Solaris 8 (6324142)

Service configuration data cannot be migrated from flat file to Directory Server when Directory Server is running on Solaris 8.

WORKAROUND: On Solaris 8, before running the `fmff2ds` migration script, install patch 110165-05.

Unable to use default `ldapmodify` in Solaris 8 against Microsoft Active Directory (6328437)

The default version of `ldapmodify` included with Solaris 8 (Sparc) will not run against Active Directory on a Windows 2000 Advanced Server.

WORKAROUND: Before running the `fmff2ds` script against Active Directory, upgrade your `ldapmodify` by downloading the Directory Server Resource Kit from http://www.sun.com/download/products.xml?id=3f74a0db.

`amadmin` throws exception when Federation Manager is deployed on BEA WebLogic Server (6320391)

After `amadmin` loads meta data, it uses Remote Procedure Calls (RPC) to send notifications to the server. With WebLogic Server, use `jaxrpc 1.0`.

WORKAROUND: Change the `Makefile` to bundle the `jaxrpc 1.0` jars. Take the following steps after installing with `fmsetup`:

1. Remove the default `jaxrpc` using the following command:

   # **rm** *war staging dir*/**web-src/WEB-INF/lib/jaxrpc***

2. Copy the `jaxrpc 1.0` to the war staging directory using the following command:

   # **cp /***FederationManager-base***/SUNWam/fm/jaxrpc_1.0/*** *war staging dir*/**web-src/WEB-INF/lib**

3. Change to the bin directory using the following command:

   # **cd /***FederationManager-base***/SUNWam/fm/bin**

4. Run fmwar to generate a new web archive (WAR):

   # **fmwar -n** *web-application-name* **-d** *war staging dir* **-s** *silent-install-file*

5. Redeploy the new WAR.

Federation

The following issues are related to the federation features of Federation Manager.

- "ambulkfed script refers to wrong paths on Linux (6435835)" on page 12
- "Single Sign-On Using Artifact Fails when Federation Manager is Deployed in WebSphere Application Server 5.1.1.3 (6431994)" on page 12
- "Web Browser Artifact Profile fails when Federation Manager is Deployed in WebSphere Application Server (6320498)" on page 13
- "Federation fails when Federation Manager is deployed in WebSphere Application Server and using Secure Sockets Layer (6322995)" on page 13
- "Federation fails when Federation Manager is deployed in BEA WebLogic Server and using Secure Sockets Layer (6324673)" on page 14

ambulkfed **script refers to wrong paths on Linux (6435835)**

The ambulkfed script federates LDAP users in bulk with remote providers.

WORKAROUND: Change the following lines in the ambulkfed script:

```
gettext=/usr/bin/gettext
ECHO=/usr/bin/echo
RM=/usr/bin/rm
```

to

```
gettext=/bin/gettext
ECHO=/bin/echo
RM=/bin/rm
```

Single Sign-On Using Artifact Fails when Federation Manager is Deployed in WebSphere Application Server 5.1.1.3 (6431994)

WebSphere Application Server 5.1.1.3 bundles an older version of javax.xml.namespace.QName which does not have the getPrefix method.

WORKAROUND: After installing Federation Manager, copy *fm_staging_dir*/web-src/WEB-INF/lib/jax-qname.jar to *websphere_install_root*/AppServer/lib/qname.jar

Web Browser Artifact Profile fails when Federation Manager is Deployed in WebSphere Application Server (6320498)

When Federation Manager is deployed in WebSphere Application Server, federation using the Web Browser Artifact Profile fails when the service provider attempts to send an artifact back to the identity provider.

WORKAROUND: You must override WebSphere's default SOAP factory by doing the following:

1. Edit WebSphere's `server.xml` file by replacing:

   ```
   <jvmEntries xmi:id="JavaVirtualMachine_1" classpath="" bootClasspath=""
   verboseModeClass="false" verboseModeGarbageCollection="false"
   verboseModeJNI="false" runHProf="false" hprofArguments=""
   debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug
   -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,
   address=7777" genericJvmArguments="">
   ```

   with

   ```
   <jvmEntries xmi:id="JavaVirtualMachine_1" verboseModeClass="false"
   verboseModeGarbageCollection="false" verboseModeJNI="false"
   initialHeapSize="256" maximumHeapSize="256" runHProf="false"
   hprofArguments="" debugMode="false" debugArgs="-Djava.compiler=NONE
   -Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
   genericJvmArguments="-Dcom.iplanet.am.serverMode=true">
   <classpath>/usr/share/lib/saaj-api.jar:/usr/share/lib/saaj-impl.jar</classpath>
   ```

   `server.xml` is located in *websphere-base*/WebSphere/AppServer/config/cells/*cell-name*/nodes/*node-name*/servers/*server-instance*/. The *cell-name*/*node-name*/*server-instance* variables identify the name of the cell/node/server in which Federation Manager is deployed. For example, /opt/WebSphere/AppServer/config/cells/moonriver/nodes/moonriver/servers/server1/server.xml

2. Restart the WebSphere instance.

Federation fails when Federation Manager is deployed in WebSphere Application Server and using Secure Sockets Layer (6322995)

User federation between an identity provider and a service provider fails when Federation Manager is deployed in WebSphere Application Server and using Secure Sockets Layer (SSL).

WORKAROUND: You must find the Java Development Kit (JDK) 1.4 or above and modify WebSphere's `server.xml` file as described below. `server.xml` is located in *websphere-base*/WebSphere/AppServer/config/cells/*cell-name*/nodes/*node-name*/servers/*server* The *cell-name*/*node-name*/*server-instance* variables identify the name of the cell/node/server in which Federation Manager

is deployed. For example,
`/opt/WebSphere/AppServer/config/cells/moonriver/nodes/moonriver/`
`servers/server1/server.xml`.

1. Add Sun Microsystems' library to the classpath by adding the following to the `jvmEntries` element:

    ```
    <classpath>JAVA_HOME/jre/lib/jsse.jar</classpath>
    ```

    Note – The `jsse.jar` used here must be from the same version of the JDK that WebSphere is using.

2. Add the protocol handler package to the `genericJvmArguments` property of `jvmEntries` element by adding the following:

    ```
    -Djava.protocol.handler.pkgs=com.sun.net.ssl.internal.www.protocol
    ```

    It will look like this:

    ```
    <jvmEntries xmi:id="JavaVirtualMachine_1" verboseModeClass="false"
    verboseModeGarbageCollection="false" verboseModeJNI="false"
    runHProf="false" hprofArguments="" debugMode="false"
    debugArgs="-Djava.compiler=NONE -Xdebug -Xnoagent
    -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
    genericJvmArguments="-Djava.protocol.handler.pkgs=
    com.sun.net.ssl.internal.www.protocol">
    <classpath>/usr/j2se/jre/lib/jsse.jar</classpath>
    </jvmEntries>
    ```

3. Copy the stronger `US_export_policy.jar` and `local_policy.jar` files to the `/jdk/jre/lib/security` directory if the SSL handshake requires.

4. Restart WebSphere.

Federation fails when Federation Manager is deployed in BEA WebLogic Server and using Secure Sockets Layer (6324673)

User federation between an identity provider and a service provider fails when using SSL and Federation Manager is deployed in WebLogic Server.

WORKAROUND: Modify the `startWebLogic.sh` script by adding the following:

```
-DUseSunHttpHandler=true
```

Redistributable Files

Sun Java System Federation Manager 7 does not contain any files that you can redistribute to non-licensed users of the product.

How to Report Problems and Provide Feedback

If you have problems with Federation Manager, contact Sun customer support using one of the following mechanisms:

- Sun Support Resources (SunSolve)

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract.

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs, and its impact on your operation.
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem.
- Detailed steps on the methods you have used to reproduce the problem.
- Any error logs or core dumps.

Sun Welcomes Your Feedback

Sun Microsystems is interested in improving its documentation and welcomes your comments and suggestions. To share your thoughts, go to `http://docs.sun.com` and click the Send Comments link at the top or bottom of the page. In the online form provided, include the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is *Sun Java System Federation Manager 7 Release Notes*, and the part number is 819–2400.

Additional Sun Resources

For product downloads, professional services, patches, support, and additional developer information, go to the following locations:

- Download Center (`http://wwws.sun.com/software/download/`)
- Technical Support (`http://www.sun.com/service/support/software/`)
- Sun Java Systems Services Suite
  (`http://www.sun.com/service/sunjavasystem/sjsservicessuite.html`)
- Sun Enterprise Services, Solaris Patches, and Support (`http://sunsolve.sun.com/`)
- Developer Information (`http://developers.sun.com/prodtech/index.html`)

If you have technical questions about any Sun products, contact Sun Support and Services (`http://www.sun.com/service/contacting`).