HP OpenView Select Federation

for the HP-UX, Linux, Solaris, and Windows operating systems

Software Version: 6.5

Release Notes

HP Select Federation 6.5 Enterprise Media: T3983BA

HP Select Federation 6.5 Premium Media: T3984BA

February 2006

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

- Trustgenix, IdentityBridge, and Trustgenix Federation Server are U.S. trademarks of Trustgenix, Inc.
- BEA and WebLogic are registered trademarks of BEA Systems, Inc.
- IBM, Tivoli, WebSphere are trademarks of International Business Machines in the United States, other countries or both.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- Sun, Sun Microsystems, Solaris, and Java™ are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
- All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies/owners.

Documentation Updates

This manual's title page contains the following identifying information:

- Software Version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This Web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

Release Notes

This document contains last-minute information about the product, such as known problems, documentation errata, etc.

Changes in this release

HP OpenView Select Federation 6.5 is a completely new major release. Please refer to the *HP OpenView Select Federation Configuration and Administration Guide* for more information.

Known issues

Error message occurs when Canceling the installation while Select Federation is installing

When using the Windows GUI installer, after all the configuration steps are completed and **Install** is clicked, clicking Cancel while viewing the progress bar produces the following error message:

```
"log4j:  WARN No appenders could be found for logger
com.trustgenix.tfs.MapConfig
log4j: WARN Please initialize the log4j system properly."
```

Installer does not support entering Non-UTF8 data

When the Select Federation Windows installer is used in a non-UTF8 locale (e.g. a Japanese locale) and non-UTF8 but non-ASCII characters are used in the provider name or the passwords for the keystore, they are saved in the `tfsconfig.properties` as question marks, as shown in the example below:

```
providerName=??????
```

Solution

Do not use non-UTF8 characters in the company/provider name or keystore password field. This will cause the keystore generation to fail. The provider name should follow the naming constraints specified by “keytool”.

Uniqueness constraint in Active Directory

The LDAP attribute `samAccountName` is required to be unique by Active Directory. When you are using Select Federation as a Service Provider (SP) with Active Directory and you are using `localNames` as the federation policy, make sure the `samAccountName` being used to create the directory entry is unique and does not conflict with either an existing `samAccountName` or a `samAccountName` of a user from another federation partner.

Solution

Use a different user attribute for storing the federated user name obtained from an IDP or always use the `Pseudonym` name federation policy.

Select Federation landing page not seen after installing on Linux, Solaris or HP-UX platforms

After Select Federation is installed, it launches the browser and points it to the Select Federation administration console landing page. When using the bundled application server mode on non-Windows platforms, in some cases, the landing page fails to launch. This is due to possible issues with permissions of the startup script.

Solution

To work around this issue, change the permissions of all files in the `$SF_HOME/bin` directory and manually run the script named `startup.sh`.

TLS client authentication needs configuring when SF deployed on the bundled application server

Additional steps are required to configure TLS client authentication with your federation partner Select Federation is deployed on the bundled application server. Use the following steps:

1 To configure an IDP to accept SSL/TLS Client Authentication to authenticate SOAP requests, there must be a SOAP endpoint configured for SSL/TLS with Client Authentication. Typically, this will be configured on a separate endpoint on the bundled application server. This is done so that non-SOAP interactions, such as user login pages, will not require TLS Client Authentication.

A configuration entry will be required corresponding to this new port that will be used for client authentication in the `server.xml` which is located under /conf in the installation directory. Your existing entry might look like the following:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

<Connector port="8443" maxHttpHeaderSize="8192"

      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

      enableLookups="false" disableUploadTimeout="true"

      acceptCount="100" scheme="https" secure="true"

      clientAuth="false" sslProtocol="TLS"

      keystoreFile="/opt/OV/SelectFederation/conf/
      sslkeystore.jks"

      keystorePass="password" />
```

To create your new TLS SOAP client authentication endpoint, add another entry (you can do this just by copying the text above). Change the port to be the one you would like for client authentication, and set `clientAuth` to “true”.

```
<Connector port="TLSclientauthport" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="true" sslProtocol="TLS"
        keystoreFile="/opt/OV/SelectFederation/conf/
        sslkeystore.jks"
        keystorePass="password" />
```

2 Once you have configured the endpoint to use for SOAP w/ SSL/TLS Client Authentication, set the `providerBaseTLSClientAuthSOAPURL` parameter in `conf/tfsconfig.properties` at the IDP, e.g.

```
providerBaseTLSClientAuthSOAPURL=https://youridp.com:TLSclientauthpo
rt/tfs-soap
```

3 Once this configuration parameter is set, you will notice that you now have the option to download metadata for your site that advertises the TLS Client Auth SOAP Endpoint. Provide this metadata to any partners that you wish to use SSL/TLS Client Authentication to authenticate SOAP requests.

4 The Select Federation signing certificates are the ones used for TLS client authentication. You might be using either a self-signed certificate or one that might be issued by a 3rd party Certificate Authority. In either case, make sure to import the CA certificate chain into the trusted store of the JRE being used at both partners. In case of the built-in server, the CA certificate will have to be imported into `_jvm/lib/security/cacerts` at the IDP as well as the SP.

5 Finally, go into the Select Federation admin console. If your site is the IDP, go to Manage Partners. Click on the partner with which you want to setup TLS client auth. From the drop-down list above, select **Application Protocol Policy**. Click **Edit** and then select the **SSL/TLS client auth** from the **Authenticate SOAP Requests From SP Using** drop-down list. Save your changes. Similar configuration is required at the partner site (SP), i.e. Authority Protocol Policy needs to be set to **SSL/TLS client auth**.

Partners created containing i18n characters do not display correctly

In the admin console, after creating a partner with non-UTF8 characters (e.g. Japanese characters) in the name, the partner name is displayed incorrectly. This happens on Windows Servers (W2k, W2k3 etc.) in the non-UTF8 locale, running on WebSphere with MSSQL or Oracle as the DB. This problem does not occur on Solaris, the initial creation of the non-UTF8 partner happens correctly.

Workaround

After creating the partner, click the partner's name and click **Edit** to edit the partner. Replace the erroneous characters with the proper ones and save. The non-UTF8 characters are saved correctly and the partner name is displayed as it should be.

Environment variable update on HP-UX does not work when using the bundled application server

The environment variables `LANG`, `JAVA_OPTS`, and `CATALINA_OPTS` are not being updated correctly in `catalina.sh` found under `bin/` in the installation directory.

Workaround

Replace every occurrence of `UTF-8` in `catalina.sh` with `en_US.utf8`.

Add the following line to the `$SF_HOME/bin/catalina.sh` to ensure that international characters are handled properly:

lang= en_US.utf8

export lang

Artifact pickup over SSL/TLS with Client Authentication security on WebSphere 6.0.2 does not work when acting as an SP

When Select Federation is installed on IBM WebSphere 6.0.2 and is operating as a service provider (SP) and when using the "SSL with Client Authentication" security mode, the SP cannot perform an artifact pickup because it fails to present the client certificate.

Workaround

Configure the partner connection to be one of the other supported security modes, e.g. SSL/TLS with Basic Authentication or Digital Signatures

Errata

Missing / incorrect documentation for disabling privacy manager

Page 93 of the "Configuration and Administration Guide" under section "Configuring use of end user privacy policies" incorrectly states that the privacy manager is disabled by default and uncommenting the line:

```
userPolicy.services=profile
```

from the `tfsconfig.properties` will enable the privacy manager. The correct documentation should read:

The privacy manager is enabled by default. To disable the privacy manager, add the following line to the `tfsconfig.properties`:

```
userPolicy.services=
```

(i.e. empty value).